Reports of Cases

OPINION OF ADVOCATE GENERAL
PITRUZZELLA
delivered on 27 January 2022 [1]

Case C-817/19

Ligue des droits humains
v
Conseil des ministres

(Request for a preliminary ruling
from the Cour constitutionnelle (Constitutional Court, Belgium))

(Reference for a preliminary ruling – Protection of personal data – Processing of passenger name record (PNR) data – Regulation (EU) 2016/679 – Scope – Directive (EU) 2016/681 – Validity – Charter of Fundamental Rights of the European Union – Articles 7, 8 and Article 52(1))

Table of contents

[1] Original language: French.

I. Introduction

1. By this request for a preliminary ruling, the Cour constitutionnelle (Constitutional Court, Belgium) puts before the Court of Justice a series of 10 questions concerning the interpretation 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; 'the GDPR')[2] and concerning the validity and interpretation 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 ('the PNR Directive')[3] and of Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data ('the API Directive').[4] These questions have arisen in an action brought by the not-for-profit association Ligue des droits humains (LDH), seeking annulment in full or in part 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) ('the PNR Law'),[5] which transposes the PNR Directive and the API Directive into Belgian law.

2. The questions on which the Court is required to rule in this case embody one of the principal dilemmas of contemporary liberal democratic constitutionalism: what balance should be struck between the individual and society in this data age in which digital technologies enabled huge amounts of personal data to be collected, retained, processed and analysed for predictive purposes? The algorithms, big data analysis and artificial intelligence used by public authorities can serve to further and protect the fundamental interests of society to a hitherto unimaginable degree of effectiveness – from the protection of public health to environmental sustainability, from combating terrorism to preventing crime, and serious crime in particular. At the same time, the indiscriminate collection of personal data and the use of digital technologies by public authorities may give rise to a digital panopticon – where public authorities can be all-seeing without being seen – an omniscient power able to oversee and predict the behaviour of each and every person and take the necessary measures, to the point of the paradoxical outcome imagined by Steven Spielberg in the film *Minority Report*, where the perpetrator of a crime that has not yet been committed is deprived of his liberty. It is well known that in some countries society takes precedence over the individual and the use of personal data legitimately enables effective mass

2 OJ 2016 L 119, p. 1.

3 OJ 2016 L 119, p. 132.

4 OJ 2004 L 261, p. 24.

5 *Moniteur belge* of 25 January 2017, p. 12905.

surveillance aimed at protecting what are considered to be fundamental public interests. In contrast, European constitutionalism, whether national or supranational, in which the individual and the individual's liberties hold centre stage, imposes a significant obstacle to the advent of a mass surveillance society, especially now that the protection of privacy and personal data have been recognised as fundamental rights. To what extent, however, can that obstacle be set up without seriously undermining certain fundamental interests of society – such as those cited above – which may nevertheless be bound up with the constitution? This is at the heart of the relationship between the individual and society in the digital age. That relationship, on the one hand, calls for delicate balancing acts between the interests of society and the rights of individuals, premised on the paramount importance of the individual in the European constitutional tradition, and, on the other, makes it necessary to establish safeguards against abuse. Here, too, we have a contemporary twist on a classic theme of constitutionalism since, as *The Federalist* categorically asserted, men are not angels, which is why legal mechanisms are needed to constrain and monitor public authorities.

3. This Opinion addresses those broad questions, necessarily confined as it is to interpreting EU law in the light of the Court's earlier case-law, using well-established techniques including that of interpreting national law in conformity with EU law. I will resort frequently to that mechanism in this Opinion, where the law appears to allow it, as I seek to strike the balance necessary, in constitutional terms, between the public objectives that underpin the system for the transfer, collection and processing of passenger name record data ('PNR data') and the rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

II. Legal framework

A. European Union law

1. The Charter

4. Under Article 7 of the Charter 'everyone has the right to respect for his or her private and family life, home and communications'.

5. According to Article 8 of the Charter:

'1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority'.

6. Under Article 52(1) of the Charter 'any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made 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.'

2. The GDPR

7. According to Article 2(2)(d) of the GDPR, the regulation does not apply 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.'

8. Under Article 23(1)(d) of the GDPR:

'[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:

…

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

3. The PNR Directive

9. I will set out below only a brief sketch of how the system established by the PNR directive functions. During the legal analysis I will provide more details of the contents of the provisions of the PNR Directive relevant to the answers to be given to the questions referred.

10. According to Article 1, the PNR Directive, adopted under Article 82(1)(d) and Article 87(2)(a) TFEU, organises at EU level a system for the transfer by air carriers of PNR data relating to extra-EU flights [6] and for the collection, processing and retention of those data by the competent authorities of the Member States for the purposes of combating terrorism and serious crime.

11. Under Article 3(5) of that directive, 'passenger name record' or 'PNR' is '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'.

12. Annex I to the PNR Directive ('Annex I') lists the passenger name record data as far as collected by air carriers that are transferred within the meaning of and in accordance with the arrangements established in Article 8 of that directive.

13. Annex II to the PNR Directive ('Annex II') contains a list of the offences that constitute 'serious crime' within the meaning of Article 3(9) of that directive.

[6] Under Article 3(2) of the PNR Directive, an 'extra-EU flight' is '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'.

14. Article 2 of the PNR Directive provides that Member States may decide to apply the directive also to 'intra-EU flights' [7] or to selected such flights it considers 'necessary' to include in order to pursue the objectives of the directive.

15. Under Article 4(1) of the PNR Directive '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")'. According to Article 4(2)(a), the PIU is to be responsible inter alia for 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 of the PNR Directive. Under Article 7(2), those authorities are 'authorities competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime'. [8]

16. According to the second sentence of Article 6(1) of the PNR Directive, '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.' Article 6(2) is worded as follows:

'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.'

17. Article 12 of the PNR Directive contains the provisions relating to the retention of PNR data.

18. Article 5 of the PNR Directive provides that each PIU is to appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards. Furthermore, under Article 15 of that directive, each Member State must entrust the national supervisory authority referred to in Article 25 of Framework Decision 2008/977/JHA, [9] replaced by Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on

7 Under Article 3(3) of the PNR Directive, an 'intra-EU flight' is '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'.

8 Under Article 7(1) of the PNR Directive each Member State is to 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. The Commission published that list in 2018 (OJ 2018 C 194, p. 1; corrigendum OJ 2020 C 366, p. 55).

9 Council Framework Decision 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).

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 ('the Policing Directive'),[10] with monitoring the application within its territory of the provisions adopted pursuant to that directive. That authority, which conducts its activities with a view to protecting fundamental rights in relation to the processing of personal data,[11] is responsible, inter alia, for, first, dealing with complaints lodged by any data subject, investigating the matter and informing the data subjects of the progress and the outcome of their complaints within a reasonable time period; and, secondly, verifying the lawfulness of the data processing and conducting investigations, inspections and audits in accordance with national law, either on its own initiative or on the basis of a complaint.[12]

4. Other relevant EU legislation

19. The legal framework of the present case also includes the API Directive and the Policing Directive. For ease of reading, I will set out in this Opinion the contents of the relevant provisions of those acts where necessary to address the questions relating to those provisions or where required for the legal analysis in general.

B. Belgian law

20. According to Article 22 of the Belgian Constitution, 'everyone is entitled to respect for private and family life except in the cases and under the circumstances laid down by law'.

21. According to Article 2, the PNR Law transposes the API Directive and the PNR Directive and partially transposes Directive 2010/65/EU.[13]

22. According to Article 3(1) of the PNR Law, 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'. Under Article 4(1) and (2) of that law, 'carrier' means 'any legal or natural person that carries people by air, sea, rail or land on a professional basis' and 'tour operator' means 'any travel organiser or agent within the meaning of the Law of 16 February 1994 governing the travel-organisation contract and the travel-agency contract'.

23. Article 8 of the PNR Law provides:

'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) and (19) and Article 90*ter*(3) of the Code d'instruction criminelle [(Criminal Procedure Code)];

10 OJ 2016 L 119, p. 89. Article 41 of the Policing Directive has replaced Article 25 of Framework Decision 2008/977.

11 See Article 15(2) of the PNR Directive.

12 See Article 15(3)(a) and (b) of the PNR Directive.

13 Directive 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).

(2) detection and prosecution (including the execution of penalties or measures depriving the person concerned 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, Articles 198, 199, 199 *bis*, 207, 213, 375 and 505 of the Code pénal [(Criminal Code)];

(3) prevention of serious disturbances to public security in the context of violent radicalisation, through monitoring of developments and groupings in accordance with Article 44/5(1)(2) and (3) and 44/5(2) of the loi du 5 août 1992 sur la fonction de police [(Law of 5 August 1992 on the police service)];

(4) monitoring the activities referred to in Article 7(1) and (3/1), 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)];[14]

(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 December 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.'

24. Article 9 of the PNR Law contains a list of the data that may be transferred. Those data correspond to those listed in Annex I.

25. Under Article 18 of the PNR Law, 'passenger data shall be retained in the passenger database for a maximum period of five years from being entered. They shall be destroyed on expiry of that period'.

26. Article 19 of that law provides that 'on expiry of six months from the entry of passenger data in the passenger database, all passenger data shall be depersonalised by masking out the information'.

27. Article 24 of the PNR Law provides:

'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 context of their functions or with the lists of individuals drawn up by the competent services in the context of their functions.

[14] *Moniteur belge* of 18 December 1998, p. 40312.

(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) …'

28. Article 25 of the PNR Law reproduces the contents of Article 6(4) of the PNR Directive.

29. Chapter 11 of the PNR Law contains the provisions governing the processing of passenger data with a view to improving border controls and combating illegal immigration. Those provisions transpose the API Directive into Belgian law.

30. Article 44 of the PNR Law provides that the PIU is to appoint a data protection officer within the service public fédéral intérieur (Home Affairs Federal Public Service, Belgium). The Commission de la protection de la vie privée (Commission for the protection of privacy) is to supervise application of the provisions of the PNR Law.

31. Article 51 of the PNR Law amends the Organic law of 30 November 1998 on the intelligence and security services by inserting Article 16/3, worded as follows:

'1. The intelligence and security services may, for the better exercise of their functions, make a duly reasoned decision to access the passenger data referred to in Article 7 of the [PNR Law].

2. The decision referred to in Paragraph 1 shall be made by the head of department and notified in writing to the Passenger Information Unit referred to in Chapter 7 of the aforementioned law. The decision and the relevant statement of reasons shall be notified to the Comité permanent R [(Standing Intelligence Agencies Review Committee; "Standing Committee I")].

Standing Committee I shall prohibit the intelligence and security services from using data gathered in circumstances that do not comply with the statutory conditions.

The decision may cover a set of data relating to a specific intelligence investigation. In such a case, Standing Committee I shall be provided once a month with a list of the passenger data searches.'

C. The dispute in the main proceedings, the questions referred and the procedure before the Court of Justice

32. By an application made to the Cour constitutionnelle (Constitutional Court) on 24 July 2017, LDH brought an action seeking annulment in full or in part of the PNR Law. It relied on two pleas in law in support of its action.

33. By its first, and primary, plea, alleging infringement of Article 22 of the Belgian Constitution, read in conjunction with Article 23 of the GDPR, Articles 7, 8 and Article 52(1) of the Charter as well as Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950 ('the ECHR'), LDH asserts that the contested law infringes the principle of proportionality in respect of its scope and the categories of data to which it refers, the data processing operations it establishes, the purposes of those operations and the period for which data are retained. Specifically, it argues that the definition of PNR data is too broad and can result in the disclosure of sensitive data, and that the definition of 'passenger' in that law allows the systematic, non-targeted processing of the data of all the passengers

concerned. LDH is also of the view that the PNR Law does not define with sufficient clarity the nature and precise details for the pre-screening of the passenger databases or the criteria used as 'threat indicators'. Lastly, it contends that the PNR Law goes beyond what is strictly necessary because it provides for PNR data to be processed for purposes broader than those allowed by the PNR Directive and because the five-year retention period for PNR data is disproportionate. By its second plea, submitted in the alternative and alleging infringement of Article 22 of the Belgian Constitution, read in conjunction with Article 3(2) TEU and Article 45 of the Charter, LDH challenges the provisions of Chapter 11 of the PNR Law transposing the API Directive.

34. The Conseil des ministres (Council of Ministers) of the Kingdom of Belgium, as intervener before the Cour constitutionnelle (Constitutional Court), contests LDH's action, claiming that the two pleas advanced in its support are inadmissible and also ill-founded.

35. The Cour constitutionnelle (Constitutional Court), for its part, makes the following observations.

36. In respect of the first plea, it has doubts, first of all, as to whether the definition of PNR data in Annex I is sufficiently clear and precise. In its view, some of those data are described by way of example rather than exhaustively. The referring court then notes that the definition of 'passenger' in Article 3(4) of the PNR Directive involves the collection, transfer, processing and retention of PNR data in relation to any person carried or to be carried who is on the passengers list, regardless of whether there are substantial grounds to believe that the data subject has committed an offence, is on the point of committing an offence or has been found guilty of an offence. In respect of the processing of PNR data, it observes that those data systematically undergo advance assessment that involves cross-checking the PNR data of all passengers against databases or pre-determined criteria in order to find matches. The Cour constitutionnelle (Constitutional Court) states that, although the criteria must be specific, reliable and non-discriminatory, it believes it is nevertheless technically impossible to define any further the pre-determined criteria to be used to identify risk profiles. As regards the retention period for PNR data under Article 12(1) of the PNR Directive, according to which those data can be retained for five years, the referring court finds that PNR data are retained irrespective of whether or not the passengers in question were identified, in the advance assessment, as presenting a public security risk. Under those circumstances, the referring court is uncertain whether, in the light of the case-law established in, inter alia, the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*,[15] and Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017,[16] the system for collecting, transferring, processing and retaining PNR data established by the PNR Directive can be considered not to go beyond what is strictly necessary. Against that background, the referring court enquires, also, whether the PNR Directive precludes national rules, such as those resulting from Article 8(1)(4) of the PNR Law, under which PNR data may be processed for a purpose other than those established by that directive. Lastly, it asks whether the PIU can be regarded as 'another national authority' able, under Article 12(3)(b)(ii) of the PNR Directive, to authorise the disclosure of full PNR data after a period of six months. In relation to the second plea, the referring court observes that it is directed against Article 3(1), Article 8(2) and Articles 28 to 31 of the PNR Law, governing the collection and processing of passenger data for the purposes of combating illegal immigration and improving border controls. Recalling that, according to Article 3(1), that law covers flights to and from and transiting through national territory, the referring court notes that the national legislature had included intra-EU flights within the scope of the said law in order to obtain 'a fuller picture of the passengers who

15 C-203/15 and C-698/15, EU:C:2016:970 ('*Tele2 Sverige* judgment').

16 EU:C:2017:592 ('Opinion 1/15').

represent a potential threat to … security [within the European Union] and national security', relying on the option available under Article 2, read in conjunction with recital 10, of the PNR Directive.

37. In that context, the Cour constitutionnelle (Constitutional Court) decided to stay the 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 [PNR Law], which transposes [the PNR Directive] as well as [the API Directive] and Directive [2010/65]?

(2) Is Annex I … compatible with Articles 7, 8 and Article 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 [that Annex I], 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 … compatible with Articles 7, 8 and Article 52(1) of the [Charter], given that, having regard to the word "including", the data referred to in those paragraphs are 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 … compatible with Articles 7, 8 and Article 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 Article 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?

(6) Is Article 6 of [the PNR Directive] compatible with Articles 7, 8 and Article 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 [PNR Law], 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 Article 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 or 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 [PNR Law] 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 th[at] law?'

38. LDH, the Belgian, Czech, Danish, German and Estonian Governments, Ireland, the Spanish, French, Cypriot, Latvian, Netherlands, Austrian, Polish and Finnish Governments and the European Parliament, the Council of the European Union and the European Commission submitted written observations under Article 23 of the Statute of the Court of Justice of the European Union. In accordance with Article 24 of the Statute of the Court of Justice of the European Union, the Commission, the European Data Protection Supervisor (EDPS) and the European Union Agency for Fundamental Rights (FRA) were invited to reply in writing to questions put by the Court. A hearing took place on 13 July 2021.

III. Analysis

A. The first question referred

39. By its first question, the referring court asks the Court in essence whether Article 2(2)(d) of the GDPR must be interpreted as meaning that that regulation – especially Article 23(1), according to which EU or Member State law may, on grounds listed exhaustively in that article, restrict by way of a legislative measure the scope of the obligations and rights provided for – applies to data processing operations carried out under national legislation, such as the PNR Law, which transposes the PNR Directive, the API Directive and Directive 2010/65 into internal law.

40. Article 2(2) of the GDPR lays down exceptions to the scope of that regulation, which is defined, very broadly,[17] in Article 2(1).[18] As derogations from application of a regulation governing the processing of personal data and capable of encroaching upon fundamental freedoms, those exceptions must be interpreted strictly.[19]

41. Article 2(2)(d) of the GDPR contains, in particular, an exception according to which the regulation does not apply 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'. That exception is premised on a dual criterion which is both subjective and objective. Data processing operations are accordingly excluded from the scope of that regulation where they are carried out (i) by the 'competent authorities' and (ii) for the purposes listed in that article. It is therefore necessary to assess the various types of data processing covered by the PNR Law in the light of that dual criterion.

42. In the first place, the data processing operations carried out by carriers (whether air, rail, land or sea) to PIUs or by tour operators for service provision or commercial purposes, even though they are covered by that law, remain governed by the GDPR since neither the subjective component nor the objective component of the exception in Article 2(2)(d) of that regulation is satisfied.

43. In the second place, the transfer of PNR data to PIUs by the carriers or tour operators which is, in itself, 'processing' within the meaning of Article 4(2) of the GDPR,[20] is not so obviously included in the scope of that regulation.

44. First, the transfer is not by a 'competent authority' within the meaning of Article 3(7) of the Policing Directive, which can appropriately be referred to by analogy because the GDPR does not define that concept.[21] An economic operator, such as a transport undertaking or tour operator, which is subject only to a statutory obligation to transfer personal data and which has not been entrusted to exercise public powers,[22] cannot be regarded as a body or entity within the meaning of Article 3(7)(b).[23]

17 See, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2021:504, paragraph 61).

18 Under Article 2(1) of the GDPR, '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'.

19 See judgments of 16 July 2020, *Facebook Ireland and Schrems* (C-311/18, EU:C:2020:559, paragraph 84), and of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2021:504, paragraph 62).

20 See, to that effect, judgment of 6 October 2020, *Privacy International* (C-623/17, EU:C:2020:790, paragraph 41 and the case-law cited) ('*Privacy International* judgment'). Under Article 4(2) of the GDPR, 'processing' includes 'any operation … which is performed on personal data or on sets of personal data, … such as … disclosure by transmission …'.

21 See, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2021:504, paragraph 69). According to Article 3(7)(a) and (b) of the Policing Directive, '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 same purposes.

22 No suggestion to that effect is apparent from the order for reference.

23 Nor can such an operator be classified as a 'processor' within the meaning of Article 4(8) of the GDPR or Article 3(9) of the Policing Directive, since it is instead a 'controller' within the meaning of the second part of Article 4(7) of the GDPR. Under Article 4(8) of the GDPR and Article 3(9) of the Policing Directive, which are drafted identically, 'processor' means a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'. Under the first part of Article 4(7) of the GDPR, 'controller' means 'the natural or legal person, public authority, agency or other body which … determines the purposes and means of the processing …'. The second part of that article specifies that 'where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.

45. Secondly, transport undertakings and tour operators transfer PNR data in order to perform an obligation imposed by the law in order to achieve the aims listed in Article 2(2)(d) of the GDPR.

46. To my mind it is clearly apparent from the wording of that provision that only processing operations that satisfy both the subjective and the objective component of the exemption criterion set out in that article fall outside the scope of the GDPR. The transfer of PNR data to the PIU by transport undertakings and tour operators as required by the PNR Law is therefore covered by that regulation.

47. In respect of the provisions of the PNR Law that transpose the PNR Directive, that finding is corroborated by Article 21(2) of that directive, according to which the directive 'is without prejudice to the applicability of [Directive 95/46/EC] [24] to the processing of personal data by air carriers'. To my mind, the interpretation of that article suggested by the French Government, among others, to the effect that it merely provides that carriers remain subject to the obligations laid down by the GDPR in respect of data processing operations not referred to in the PNR Directive, must be rejected. Given its wording, the scope of that 'without prejudice' caveat is broad and defined only by reference to the person carrying out the processing, since it makes no mention of either the purpose of the processing or the context in which it takes place, whether it is carried out in the course of the commercial activity of an air carrier or in performance of a legal obligation. I also note that Article 13(3) of the PNR Directive contains a caveat to the same effect, referring specifically to air carriers' obligations under the GDPR 'to take appropriate technical and organisational measures to protect the security and confidentiality of personal data'. That provision is one of the provisions organising the protection of personal data processed under the PNR Directive and follows Article 13(1) of that directive according to which, in general terms, all data processing carried out under the PNR Directive is subject to the provisions of Framework Decision 2008/977 to which it refers. Contrary to the French Government's assertion, that approach means, first, that Article 13(3) can be read as bringing within the scope of the GDPR only the data processing under the PNR Directive that is not carried out by 'competent authorities' within the meaning of the Policing Directive and, secondly, that the reference to compliance with the data security and confidentiality obligations imposed by that regulation can be understood as a reminder of the safeguards which must in all cases be in place when carriers transfer PNR data to PIUs.

48. The conclusion set out in point 46 of this Opinion is not undermined by recital 19 of the GDPR or recital 11 of the Policing Directive, to which the German Government, Ireland and the French Government, among others, refer when they argue that the PNR Directive is *lex specialis*. For the personal data processing operations covered by it, that directive does admittedly establish a data protection framework independent of the GDPR. Nevertheless, that specific framework only applies to the processing of PNR data carried out by a 'competent authority' within the meaning of Article 3(7) of the Policing Directive – an expression that includes, inter alia, PIUs – whereas the transfer of PNR data to the PIU remains subject to the general framework laid down by the GDPR by virtue of, inter alia, the 'without prejudice' caveat in Article 21(2) of the PNR Directive.

49. In support of their line of argument to the effect that the GDPR does not apply to the transfer of PNR data to the PIUs by carriers and tour operators, the Belgian Government, Ireland, and the French and Cypriot Governments refer to the judgment of 30 May 2006, *Parliament* v *Council*

[24] Directive 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). That directive was repealed and replaced by the GDPR. See Article 94 of the GDPR.

and Commission,[25] in which the Court held that the transfer of PNR data by Community air carriers to the authorities of the United States of America, under an agreement negotiated between that country and the European Community, did constitute the processing of personal data in accordance with the first indent of Article 3(2) of Directive 95/46[26] and did not, in consequence, fall within the scope of that directive. In reaching that conclusion, the Court took account of the purpose behind the transfer and the fact that it '[fell] within a framework established by the public authorities', even though the data were collected and transferred by private operators.[27]

50. It is sufficient to note in that respect that, in its judgment of 6 October 2020, *La Quadrature du Net and Others*,[28] the Court held in essence that the *Parliament* v *Council* judgment could not be transposed to the context of the GDPR.[29]

51. Furthermore, in paragraph 102 of the *La Quadrature du Net* judgment,[30] applying by analogy the reasoning followed in the *Tele2 Sverige* judgment and the judgment of 2 October 2018, *Ministerio Fiscal*,[31] the Court stated that 'although [the GDPR] states, in Article 2(2)(d) thereof, that it does not apply to processing operations carried out "by competent authorities" for the purposes of, inter alia, the prevention and detection of criminal offences, including the safeguarding against and the prevention of threats to public security, it is apparent from Article 23(1)(d) and (h) of that regulation that the processing of personal data carried out by individuals for those same purposes falls within the scope of that regulation'.[32]

52. For the reasons set out above, I am persuaded that it is clearly apparent merely from the wording of Article 2(2)(d) of the GDPR that the transfer of PNR data by transport undertakings and tour operators to PIUs does fall under the GDPR, since that article refers only to processing operations carried out by 'competent authorities', and that it is not necessary to refer to the exception contained in Article 23(1) of that regulation.[33] The statement in paragraph 102 of the *La Quadrature du Net* judgment nevertheless constitutes a clear endorsement by the Court of that view.

25 C-317/04 and C-318/04, EU:C:2006:346 ('*Parliament* v *Council* judgment'). In the cases giving rise to that judgment, the Parliament was seeking, first, annulment of Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004 L 183, p. 83, and corrigendum, OJ 2005 L 255, p. 168) and, secondly, annulment of Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection (OJ 2004 L 235, p. 11).

26 Under the first indent of Article 3(2) of Directive 95/46, that directive did 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' (emphasis added).

27 On the 'teleological' and 'contextual' approach taken by the Court in the *Parliament* v *Council* judgment, see the Opinion of Advocate General Campos Sánchez-Bordona in Joined Cases *La Quadrature du Net and Others* (C-511/18 and C-512/18, EU:C:2020:6, points 47 and 62).

28 C-511/18, C-512/18 and C-520/18, EU:C:2020:791 ('*La Quadrature du Net* judgment').

29 See *La Quadrature du Net* judgment, paragraphs 100 to 102.

30 See, to the same effect, *Privacy International* judgment, paragraph 47.

31 C-207/16, EU:C:2018:788, paragraph 34 ('*Ministerio Fiscal* judgment').

32 See, by analogy, *Tele2 Sverige* judgment, paragraphs 72 to 74 and *Ministerio Fiscal* judgment, paragraph 34. Those judgments concerned interpretation of the first sentence of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), which establishes exceptions similar to those contained in Article 23(1)(a) to (d) of the GDPR.

33 The reference to Article 15(1) of Directive 2002/58 was justified in the context of that directive, since the exception that it contains in Article 1(3) refers, in general terms, to the 'activities of the State in areas of criminal law'.

53. Since the transfer of PNR data by transport undertakings and tour operators does fall within the scope of the GDPR, national legislation, such as the PNR Law, under which those undertakings and operators are obliged to transfer those data, is a 'legislative measure' for the purposes of Article 23(1)(d) of the GDPR and must, therefore, meet the conditions laid down in that article. [34]

54. As regards, in the third place, PNR data processing operations carried out by the PIU and the competent national authorities, as is apparent from the foregoing considerations, whether or not the GDPR applies depends on the purposes of those operations.

55. First, the PNR data processing operations carried out by the PIU and by the competent national authorities for the purposes listed in Article 8(1)(1) to (3) and (5) of the PNR Law [35] are excluded from the scope of the GDPR where, as would appear to be the case, those purposes are among those covered by the exception in Article 2(2)(d) of the GDPR. The protection of the personal data to which those processing operations relate is a matter of national law, subject to application of the Policing Directive [36] and, in respect of matters within its scope, of the PNR Directive.

56. Secondly, the same is true of PNR data processing operations carried out by the PIU and by the security and intelligence services in the course of monitoring the activities referred to in the provisions of the Organic law on the intelligence and security services listed in Article 8(1)(4) of the PNR Law, where those processing operations pursue the purposes listed in Article 2(2)(d) of the GDPR, a matter which is for the referring court to determine.

57. The Belgian Government submits that the processing operations carried out under Article 8(1)(4) of the PNR Law are in any event covered by the exceptions established in Article 2(2)(a) of the GDPR and Article 2(3)(a) of the Policing Directive, because the activities of the security and intelligence services do not fall within the scope of EU law.

58. Whilst noting that no question has been referred to the Court seeking interpretation of those provisions, I observe, first of all, that the Court has already held that national legislation that imposes processing obligations on private operators falls under the provisions of EU data protection law, even where it concerns the protection of national security. [37] It follows that the transfer of PNR data imposed on carriers and tour operators by the PNR Law does in principle fall under the GDPR even where it is carried out under Article 8(1)(4) of that law.

59. Next, I note that, although recital 16 of the GDPR states that the regulation does not apply to 'activities concerning national security' and recital 14 of the Policing Directive states that 'activities concerning national security, activities of agencies or units dealing with national security … should not be considered to be activities falling within the scope of [that] Directive', the criteria according to which the processing of personal data carried out by a Member State public authority, unit or agency either falls within the scope of a particular act of EU law organising the protection of the data subjects in relation to such processing or falls outside the scope of EU law correspond to a logic based on both the functions attributed to that authority, unit or agency and the purposes of that processing. In that vein, the Court has held that Article 2(2)(a) of the GDPR, read in the light of recital 16 thereof, 'must be regarded as being designed solely to exclude from the scope of that regulation the processing of personal data

34 See, by analogy, *Privacy International* judgment, paragraphs 38 and 39.

35 This refers to the processing operations governed by Chapters 7 to 10 and 12 of the PNR Law.

36 See, to that effect, *La Quadrature du Net* judgment, paragraph 103, and *Privacy International* judgment, paragraph 48.

37 See among others, *La Quadrature du Net* judgment.

carried out by State authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category, with the result that the mere fact that an activity is an activity characteristic of the State or of a public authority is not sufficient ground for that exception to be automatically applicable to such an activity'.[38] The Court also stated that 'the activities having the aim of safeguarding national security that are envisaged in Article 2(2)(a) of the GDPR encompass, in particular, … those that are intended to protect essential State functions and the fundamental interests of society'.[39] This means that, where a Member State entrusts its security and intelligence services with tasks in the fields listed in Article 3(7)(a) of the Policing Directive, the data processing operations carried out by those services in order to perform those tasks would fall within the scope of the Policing Directive and, where applicable, the PNR Directive. More generally, I note that, when interpreting Article 4(2) TEU, which is relied upon by the Belgian Government, among others, the Court has repeatedly held that the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law,[40] thereby demonstrating a reluctance to exclude Member States' activities relating to the protection of national security automatically and en masse from the scope of EU law.

60. Thirdly, in accordance with the view of all the interested parties that have submitted observations, with the exception of the French Government, it should be found that the PNR data processing operations carried out by the competent Belgian authorities for the purposes set out in Article 8(2) of the PNR Law, that is to say, 'improving external border controls on individuals and with a view to combating illegal immigration',[41] are not covered by the exception under Article 2(2)(d) of the GDPR or by any other exception established in that article and, therefore, fall within the scope of that regulation. In contrast to the French Government's contention, they argue that those operations cannot be governed by the PNR Directive, whose Article 1(2) provides that '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' nor, in principle, by the Policing Directive, which provides in Article 1(1) thereof that it applies only 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'. As can be seen from the order for reference, Article 8(2) of the PNR Law and Chapter 11 of that law, which contains the provisions governing the processing of passenger data with a view to improving border controls and combating illegal immigration and to that end provides that those data are to be transferred by the PIU to, inter alia, the police services responsible for border control, are intended to transpose the API Directive and Directive 2010/65 into Belgian law. Both those directives require the competent authorities to comply with the provisions of Directive 95/46 in respect of the data processing operations they establish.[42] Contrary to the contention of the French Government, the reference to the data protection rules under that directive must be understood as encompassing any processing of personal data carried out under the API Directive and Directive 2010/65. The fact that the API Directive existed before Framework Decision 2008/977 came into force is irrelevant in that respect, because both that

38 See judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2021:504, paragraph 66).

39 See judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2021:504).

40 See *La Quadrature du Net* judgment, paragraph 99 and the case-law cited.

41 Chapter 11 of the PNR Law lays down the conditions under which those data are processed.

42 See recitals 8, 9 and 12 and Article 6 of the API Directive and Article 8(2) of Directive 2010/65.

framework decision and the Policing Directive which replaced it concern only the personal data processing operations referred to in Article 3(1) of the API Directive carried out by competent authorities for law enforcement purposes. [43]

61. On the basis of all the foregoing, I propose that the Court should answer the first question referred to the effect that Article 23, read in conjunction with Article 2(2)(d) of the GDPR, must be interpreted as meaning that:

– it applies to national legislation that transposes the PNR Directive to the extent that that legislation governs the processing of PNR data by carriers and other economic operators, including the transfer of PNR data to the PIUs under Article 8 of that directive;

– it does not apply to national legislation that transposes the PNR Directive to the extent that the PNR Directive governs data processing carried out for the purposes referred to in Article 1(2) of that directive by the competent national authorities, including the PIUs and, where applicable, the security and intelligence services of the Member State concerned;

– it applies to national legislation that transposes the API Directive and Directive 2010/65 with a view to improving external border controls on individuals and with a view to combating illegal immigration.

B. The second, third, fourth, sixth and eighth questions referred

62. By its second, third, fourth and sixth questions referred, the Cour constitutionnelle (Constitutional Court) asks the Court whether the PNR Directive is valid in the light of Articles 7, 8 and Article 52(1) of the Charter. The eighth question referred, although worded as a question of interpretation, likewise requests, in essence, the Court to rule on the validity of that directive.

63. Those questions concern the various components of the PNR data processing system established by the PNR directive, and in respect of each component ask the Court to determine whether it complies with the conditions for the limitations on the exercise of the fundamental rights set out in Articles 7 and 8 of the Charter to be lawful. The second and third questions referred relate to the list of PNR data in Annex I, the fourth concerns the definition of 'passenger' in Article 3(4) of the PNR Directive, the sixth relates to the use of PNR data for the advance assessment under Article 6 of that directive, and the eighth addresses the PNR data retention period under Article 12(1) of that directive.

1. The fundamental rights set out in Articles 7 and 8 of the Charter

64. Under Article 7 of the Charter everyone is guaranteed the right to respect for his or her private and family life, home and communications. In Article 8(1), the Charter explicitly recognises that everyone has the right to the protection of personal data concerning him or her. According to consistent case-law, those rights, which concern any information relating to an

[43] The use of advance passenger information ('API data') by the law enforcement services is expressly envisaged under the last subparagraph of Article 6(1) of the API Directive.

identified or identifiable individual, are closely linked, because access to a natural person's personal data with a view to their retention or use affects that person's right to respect for private life. [44]

65. The rights enshrined in Articles 7 and 8 of the Charter are nevertheless not absolute rights, but must be considered in relation to their function in society. [45] Under Article 8(2) of the Charter the processing of personal data is therefore authorised if certain conditions are satisfied. That article provides that personal data must be processed 'fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.

66. Any limitation on the right to the protection of personal data or on the right to private life must also comply with the requirements of Article 52(1) of the Charter. Any such limitation must therefore be provided for by law, respect the essence of those rights and, in accordance with the principle of proportionality, be necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

67. When evaluating a measure that limits those rights, account must also be taken of the importance of the rights enshrined in Articles 3, 4, 6 and 7 of the Charter and of the importance of the objectives of protecting national security and combating serious crime in contributing to the protection of the rights and freedoms of others. [46] In that regard, Article 6 of the Charter lays down the right of every individual not only to liberty but also to security. [47]

68. Furthermore, Article 52(3) of the Charter is intended to ensure that the rights listed in the Charter have the necessary consistency with the corresponding rights guaranteed in the ECHR, which must be taken into account as the minimum threshold of protection. [48] The right to respect for family and private life enshrined in Article 7 of the Charter corresponds to the right guaranteed under Article 8 ECHR, and must therefore be regarded as having the same meaning and the same scope. [49] It can be seen from the case-law of the European Court of Human Rights ('the ECtHR') that any interference with the rights guaranteed by Article 8 can only be justified under Article 8(2) if it is in accordance with the law, pursues one or more of the legitimate aims to which Article 8(2) refers and is necessary in a democratic society in order to achieve any such aim. [50] The measure must also be compatible with the rule of law, which is expressly mentioned in the preamble to the ECHR and inherent in the object and purpose of Article 8 thereof. [51]

44 See, to that effect, among others, judgment of 16 July 2020, *Facebook Ireland and Schrems* (C-311/18, EU:C:2020:559, paragraph 170 and the case-law cited).

45 See, among others, judgment of 16 July 2020, *Facebook Ireland and Schrems* (C-311/18, EU:C:2020:559, paragraph 172 and the case-law cited).

46 See, to that effect, *La Quadrature du Net* judgment, paragraph 122.

47 See *La Quadrature du Net* judgment, paragraph 123.

48 See *La Quadrature du Net* judgment, paragraph 124 and the case-law cited.

49 See judgment of 18 June 2020, *Commission* v *Hungary (Transparency of associations)* (C-78/18, EU:C:2020:476, paragraph 122 and the case-law cited).

50 See, inter alia, ECtHR, judgments of 18 May 2010, *Kennedy v. United Kingdom* (CE:ECHR:2010:0518JUD002683905, § 130); of 4 December 2015, *Roman Zakharov v. Russia* (CE:ECHR:2015:1204JUD004714306, § 227); and of 25 May 2021, *Centrum för Rättvisa v. Sweden* (CE:ECHR:2021:0525JUD003525208, § 246).

51 See ECtHR, judgments of 4 May 2000, *Rotaru v. Romania* (CE:ECHR:2000:0504JUD002834195, § 52); of 4 December 2008, *S. and Marper v. United Kingdom* (CE:ECHR:2008:1204JUD003056204, § 95); of 4 December 2015, *Roman Zakharov v. Russia*, (CE:ECHR:2015:1204JUD004714306, § 228); of 18 May 2021, *Kennedy v. United Kingdom* (CE:ECHR:2010:0518JUD002683905, § 151); and of 25 May 2021, *Centrüm för Rättvisa v. Sweden* (CE:ECHR:2021:0525JUD003525208, § 246).

69. The questions referred by the cour constitutionnelle (Constitutional Court) concerning validity must be examined in the light of those principles.

2. Interference with the fundamental rights set out in Articles 7 and 8 of the Charter

70. The Court has already held that provisions imposing or allowing the communication of the personal data of natural persons to a third party must be characterised, in the absence of the consent of those natural persons and irrespective of the subsequent use of the data at issue, as an interference in their private life and therefore as a limitation on the right guaranteed in Article 7 of the Charter, without prejudice to the potential justification of such provisions. [52] The same is true even in the absence of circumstances which would allow that interference to be defined as 'serious', without it being relevant that the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way. [53] Access by public authorities to that information is likewise an interference with the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because it constitutes the processing of personal data. [54] Similarly, the retention of data relating to an individual's private life for a certain period is an interference with rights enshrined in Articles 7 and 8 of the Charter. [55]

71. The Court has also held that PNR data, as listed in Annex I, include information on identified individuals, namely the air passengers concerned, and that, therefore, the various processing operations which those data may undergo affect the fundamental right to respect for private life guaranteed in Article 7 of the Charter. Those processing operations also fall within the scope of Article 8 of the Charter and, accordingly, must necessarily satisfy the data protection requirements laid down in the said article. [56]

72. In consequence, the PNR data processing operations permitted by the PNR Directive and in particular, in so far as concerns this case, the transfer of those data by air carriers to the PIUs, their use by those units, their subsequent transfer to competent national authorities within the meaning of Article 7 of that directive and their retention, are all interferences with the fundamental rights guaranteed by Articles 7 and 8 of the Charter.

73. As regards how serious that interference is, it should be noted, first, that the PNR Directive envisages the systematic and continuous transfer to the PIUs of PNR data relating to any air passenger, as defined in Article 3(4) of that directive, on an 'extra-EU flight' within the meaning of Article 3(2) thereof. Such a transfer involves general access by the PIUs to all the PNR data disclosed. [57] In contrast to the claims of a number of Member States in these proceedings, the foregoing finding is not undermined by the fact that, because those data undergo automated processing, the PIUs will in practice only have access to data where their analysis has produced a positive result. On the one hand, that fact has not, to date, prevented the Court from finding, in relation to similar systems for the automated processing of personal data collected or retained 'in

52 See, among others, judgment of 18 June 2020, *Commission* v *Hungary* (C-78/18, EU:C:2020:476, paragraphs 124 and 126, and the case-law cited); see also ECtHR, judgments of 26 March 1987, *Leander v. Sweden* (CE:ECHR:1987:0326JUD000924881, § 46); of 4 May 2000, *Rotaru v. Romania* (CE:ECHR:2000:0504JUD002834195, paragraph 48); and of 29 June 2006, *Weber and Saravia v. Germany* (CE:ECHR:2006:0629DEC005493400, § 79).

53 See, among others, *Ministerio Fiscal* judgment, paragraph 51 and the case-law cited.

54 See, among others, judgment of 18 June 2020, *Commission* v *Hungary* (C-78/18, EU:C:2020:476, paragraph 126), and *Ministerio Fiscal* judgment, paragraph 51 and the case-law cited.

55 See judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238, paragraph 34) ('*Digital Rights* judgment').

56 See Opinion 1/15, paragraphs 121 to 123.

57 See, by analogy, *Privacy International* judgment, paragraphs 79 and 80 and the case-law cited.

bulk' that the public authorities concerned have general access to those data. On the other hand, merely making personal data available to public authorities to be processed and retained by them involves those authorities having a priori general and full access to those data and an interference with the fundamental rights to respect for private life and the protection of personal data.

74. Secondly, under Article 2(1) of the PNR Directive, the Member States may decide to apply the directive to 'intra-EU' flights within the meaning of Article 3(3). I note in that respect that the PNR Directive does not merely establish an option for Member States to extend its application to intra-EU flights, but also lays down both the formal and substantive conditions governing exercise of that option [58] and states that where it is exercised only in respect of selected intra-EU flights, those flights must be selected on the basis of the objectives pursued by that directive. [59] Furthermore, the PNR Directive establishes the consequences of exercising that option by providing, in Article 2(2), that where a Member State decides to apply the directive to intra-EU flights, all the provisions of the 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.'

75. Under those circumstances, I believe, in contrast to the assertions of a number of governments that have submitted observations in these proceedings, that, even though application of the PNR Directive to intra-EU flights is a matter of choice for the Member States, where such a choice is made, the PNR Directive constitutes the legal basis of interferences with the rights to the respect for private life and the protection of personal data associated with the transfer, processing and retention of PNR data from those flights.

76. Apart from the Kingdom of Denmark, which is not subject to that directive, [60] almost all the Member States do in fact apply the regime it establishes to intra-EU flights. [61] That regime therefore applies to all flights entering and leaving the European Union and to virtually all flights within it.

77. Thirdly, Annex I lists the PNR data to be transferred under 19 headings, relating to biographical data, [62] particulars of the air travel [63] and other data collected in the context of the contract of transport by air such as telephone number, email addresses, payment information, travel agency or agent, baggage information and general remarks. [64] As the Court noted in paragraph 128 of Opinion 1/15, ruling on the headings in the Annex to the draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name

58 See Article 2(1) to (3) of the PNR Directive.

59 See Article 2(3) of the PNR Directive.

60 In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, since that Member State did not take part in the adoption of the PNR directive, it is neither bound by it nor subject to its application (see recital 40 of that directive). It nevertheless emerges from the written observations submitted by the Danish Government that in 2018 the Kingdom of Denmark adopted a law on the collection, use and retention of PNR data whose provisions broadly correspond to those of the PNR Directive. It can be seen from recital 39 of the PNR Directive that under Article 3 of the Protocol No 21 on the position of United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the TEU and the TFEU, Ireland notified its wish to take part in the adoption and application of that directive.

61 The Commission published an Updated list of Member States who have decided the application of the PNR Directive to intra-EU flights as referred to in Article 2 of [the PNR Directive] (OJ 2020 C 358, p. 7), with a corrigendum in September 2021 which added Slovenia and deleted reference to the United Kingdom (OJ 2021 C 360, p. 8). Ireland and Austria are not on that list. The Report from the Commission to the European Parliament and the Council on the review of [the PNR Directive] of 24 July 2020 (COM(2020) 305 final) ('the 2020 Commission report'), p. 11, mentions that all the Member States, with one exception, have extended the collection of PNR data to intra-EU flights.

62 See inter alia paragraphs 4 and 18 of Annex I concerning the passenger's names, gender, date of birth, nationality and identity documents.

63 See among others, paragraphs 2, 3, 7, 13 and 18 of Annex I to the PNR Directive which refer, inter alia, to the flight number, airports of departure and arrival and the times and dates of departure and arrival.

64 See paragraphs 5, 6, 9, 12 and 16 of Annex I.

Record data ('the draft Canada-EU PNR agreement'), which are in broadly similar terms to those in Annex I, 'even if some of the PNR data, taken in isolation, does not appear to be liable to reveal important 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 air passengers and the financial situation of air passengers, their dietary habits or state of health, and may even provide sensitive information about those passengers'.

78. Fourthly, according to Article 6 of the PNR Directive, the data transferred by air carriers are intended to be analysed by the PIUs by automated means and systematically, that is to say, regardless of whether there is the slightest indication that the data subjects might be involved in terrorist offences or serious crime. Specifically, in the context of the advance assessment of passengers under Article 6(2)(a) of that directive and in accordance with Article 6(3), those data may be verified by cross-checking against 'relevant' databases (Article 6(3)(a)) and processed against pre-determined criteria (Article 6(3)(b)). That first type of processing may provide additional information on the private lives of the data subjects [65] and, depending on the databases used for the cross-checking, may even allow an exact profile of those individuals to be mapped. Under those circumstances, the argument advanced by several governments, to the effect that the PNR Directive permits access to only a relatively limited set of personal data, does not properly reflect the potential extent of the interference with the fundamental rights protected by Articles 7 and 8 of the Charter entailed by the directive, in terms of the extent of the data to which it could allow access. In respect of the second type of data processing, under Article 6(3)(b) of the PNR Directive, in paragraphs 169 and 172 of Opinion 1/15 the Court emphasised that any kind of analysis based on pre-determined criteria will inherently involve some margin of error, including a number of false positives. According to the numerical data in the Commission Staff Working Document [66] ('2020 working document') annexed to the 2020 Commission report, the number of positive matches which prove to be incorrect following the individual review under Article 6(5) of the PNR Directive is fairly substantial, amounting in 2018 and 2019 to at least five out of six individuals identified. [67]

79. Fifthly, according to Article 12(1) of the PNR Directive, PNR data are retained in a database for five years from the time they are transferred to the PIU of the Member State on whose territory the flight arrival or departure point is situated. The PNR Directive therefore makes it possible for information on the private lives of air passengers to be available for a particularly long period of time. [68] Furthermore, since the transfer of PNR data concerns virtually all flights departing from and entering the European Union, and those within it, and since flying has become a habitual mode of transport, the personal data of a significant proportion of air passengers could be retained on a practically constant basis, simply because they travel by air at least twice every five years.

80. Lastly, in more general terms, the PNR Directive lays down measures which, considered globally, seek to set up a Union-wide surveillance system which is a 'non-targeted', that is to say, not triggered by a suspicion relating to one or more specific individuals; 'mass', in so far as it includes the personal data of a large number of individuals [69] covering one category of individuals

65 See, to that effect, Opinion 1/15, paragraph 131.

66 SWD(2020) 128 final.

67 The 2020 working document (p. 28 and footnote 55) refers to a rate of positive matches of 0.59% for 2019, of which only 0.11% were transmitted to the competent authorities. For 2018, the corresponding percentages were 0.25% and 0.04% respectively.

68 See Opinion 1/15, paragraph 132.

69 Before the health crisis, the system established by the PNR Directive could cover up to a billion passengers a year, data available at https://ec.europa.eu/eurostat/databrowser/view/ttr00012/default/table?lang=en

in its entirety;[70] and 'proactive' system, since it is intended not only to investigate known threats but also to find or identify hitherto unknown dangers.[71] Such measures inherently give rise to serious interference with the fundamental rights protected by Articles 7 and 8 of the Charter,[72] as a result in particular of their preventive and predictive purpose, which requires personal data to be assessed in relation to broad segments of the population, since the aim is to 'identify' individuals who, depending on the outcome of that assessment, should be subject to further examination by the competent authorities.[73] Furthermore, the increasingly widespread use, in order to prevent certain forms of serious crime, of the processing of large quantities of diverse personal data collected 'in bulk' as well as the identification of links between, and the combined processing of, those data has a 'cumulative effect' which amplifies the seriousness of the restrictions on the fundamental rights to respect for private life and the protection of personal data and risks favouring a gradual slide towards a 'surveillance society'.[74]

81. On the basis of all the foregoing, in my view the PNR Directive entails interference with the fundamental rights protected by Articles 7 and 8 of the Charter that must be described as at least 'serious'.

82. Admittedly, as the Commission in particular argues, the safeguards and guarantees established by the PNR Directive, in particular to prevent the misuse of PNR data, can, as a whole, reduce the degree or seriousness of that interference. The fact nevertheless remains that the seriousness of the impact on the protected fundamental rights of any regime under which public authorities can gain access to and process personal data is inherent in the objective characteristics of that regime. I believe it is necessary to determine how serious that impact is before ascertaining, as part of the evaluation of whether that interference is proportionate, whether the guarantees laid down by that regime are sufficient and adequate. That appears to have been the Court's approach up to now.

83. In order to be compatible with the Charter, the interference that the PNR Directive entails with the fundamental rights to respect for private life and the protection of personal data must satisfy the requirements set out in points 65 and 66 of this Opinion, which will be examined below, to the extent that this falls within the matters that the referring court has put before the Court

70 That is to say, any individual satisfying the definition of 'passenger' in Article 3(4) of the PNR Directive who takes an 'extra-EU flight' or, in practice, an 'intra-EU flight'.

71 In a study adopted by the European Commission for Democracy through Law ('the Venice Commission') in 2015, such measures are found to fall within the definition of 'strategic surveillance' and to follow an 'overarching trend' to use 'proactive surveillance' of the population. See *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on Democratic Oversight of Signals Intelligence Agencies*, adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20 and 21 March 2015), https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)006-e, paragraph 61.

72 On Article 8 ECHR, see ECtHR judgment of 25 May 2021, *Big Brother Watch and Others v. United Kingdom* (CE:ECHR:2021:0525JUD005817013, § 325) ('*Big Brother Watch* judgment'), on bulk interception measures, in which the ECtHR states that the degree to which those measures interfere with the right to respect for private life increases as the process progresses through the various stages, that is to say, the interception and initial retention of communications and related data, automated processing by applying selectors, examination by analysts and the subsequent retention of data and use of the 'final product'.

73 See, to that effect, recitals 6 and 7 of the PNR Directive. For a thorough analysis of the purpose and implications for the protection of private life and personal data, see the report entitled *Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards*, prepared by Korff, D., with the contribution of Georges, M., https://rm.coe.int/16806a601b ('the Korff report').

74 As the Korff report states, 'PNR is not an isolated issue, but a new symptom of a much wider disease'.

3. Justification for the interference resulting from the PNR Directive

84. Whereas the third question referred concerns compliance with the condition under the first sentence of Article 52(1) of the Charter, according to which any interference with a fundamental right must be 'provided for by law', the second, fourth, sixth and eighth questions seek guidance from the Court in particular on compliance with the principle of proportionality, referred to in the second sentence of that provision.

(a) Compliance with the requirement that any limitation on the exercise of a fundamental right laid down by the Charter must be provided for by law

85. According to well-established case-law of the Court,[75] based on the case-law of the ECtHR,[76] the requirement that any limitation on the exercise of a fundamental right must be 'provided for by law' not only refers to the fact that the interference must have a basis 'in law' – which is not at issue in the present case – but also implies that the legal basis permitting the interference with those rights must itself define clearly and precisely the scope of the limitation. Since it concerns the 'quality of the law' and, therefore, the fact that the measure at issue must be accessible and foreseeable,[77] that second limb contained within the expressions 'provided for by law' within the meaning of Article 52(1) of the Charter, 'laid down by law' within the meaning of Article 8(2) of the Charter and 'in accordance with the law' within the meaning of Article 8 ECHR is not only intended to secure compliance with the principle of lawfulness and adequate protection against arbitrary interference,[78] but reflects a need for legal certainty. That requirement is further confirmed in the Opinion of 19 August 2016 on the Data protection implications of the processing of Passenger Name Records ('the 19 August 2016 opinion')[79] of the Consultative Committee of Convention 108 Committee.[80]

86. By adopting the PNR Directive, the EU legislature itself restricted the rights enshrined in Articles 7 and 8 of the Charter. The interference with those rights permitted by that directive cannot therefore be regarded as resulting from the choice of the Member States,[81] notwithstanding any margin of discretion the latter may have had when transposing the directive into national law, but has its legal basis in the PNR Directive itself. Accordingly, in order to uphold

75 See, among others. judgments of 16 July 2020, *Facebook Ireland and Schrems* (C-311/18, EU:C:2020:559, paragraph 175); and of 8 September 2020, *Recorded Artists Actors Performers* (C-265/19, EU:C:2020:677, paragraph 86 and the case-law cited); and *Privacy International* judgment, paragraph 65.

76 See, among others, ECtHR judgments of 8 June 2006, *Lupsa v. Romania*, (CE:ECHR:2006:0608JUD001033704, §§ 32 and 33), and of 15 December 2020, *Pişkìn v. Turkey* (CE:ECHR:2020:1215JUD003339918, § 206); see also *Big Brother Watch* judgment, § 333. On the need to give the expression 'provided for by law' in Article 52(1) of the Charter the same interpretation as that given by the ECtHR, see Opinion of Advocate General Wathelet in *WebMindLicenses* (C-419/14, EU:C:2015:606, points 134 to 143).

77 See, lastly, *Big Brother Watch* judgment, § 333.

78 See judgment of 17 December 2015, *WebMindLicenses* (C-419/14, EU:C:2015:832, paragraph 81); see also ECtHR, judgment of 1 July 2008, *Liberty and Others v. United Kingdom* (CE:ECHR:2008:0701JUD005824300, § 69; and *Big Brother Watch* judgment, § 333.

79 https://rm.coe.int/16806b051e, pp. 3 and 5. The explanatory report accompanying the protocol amending Convention 108 ('the explanatory report to the modernised Convention 108') also emphasises the requirement that the measure that provides for interference with the rights to respect for private life and the protection of personal data must be 'accessible', 'predictable', 'sufficiently detailed' and 'clearly formulated'. See paragraph 91 of that explanatory report,

80 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, adopted in Strasbourg on 28 January 1981 and ratified by all the Member States, better known as 'Convention 108'. A modernising protocol amending that convention was drawn up in 2018. By Council Decision (EU) 2019/682 of 9 April 2019 (OJ 2019 L 115, p. 7), the Member States were authorised to ratify that protocol, in the interests of the European Union, in so far as its provisions fall within the exclusive competence of the European Union. In the rest of this Opinion, I will refer also to the text of the modernised Convention 108 which, although it has not yet been ratified by all the Member States and has not yet come into force, establishes safeguards based on the same principles as are set out in the GDPR and the Policing Directive, as can be seen from Decision 2019/682.

81 For an argument *a contrario*, see judgment of 3 December 2019, *Czech Republic* v *Parliament and Council* (C-482/17, EU:C:2019:1035, paragraph 135).

the case-law summarised in point 85 of this Opinion and the 'high standards' for the protection of the fundamental rights contained inter alia in the Charter and the ECHR and referred to in recital 15 of the PNR Directive, the EU legislature needed to lay down clear and precise rules defining both the scope of the measures providing for that interference and how they are to be applied.

87. While by its third question the referring court is specifically enquiring whether that obligation was complied with in respect of paragraphs 12 and 18 of Annex I, in order to examine the second, fourth and sixth questions referred, by which that court raises doubts as to whether the interference that the PNR Directive entails with the fundamental rights set out in Articles 7 and 8 of the Charter qualifies as necessary, the Court will also have to determine whether the provisions at issue of the PNR Directive are sufficiently clear and precise.

88. Even though, as I indicated in point 85 of this Opinion, that analysis concerns the legality of the interference, as referred to in the first sentence of Article 52(1) of the Charter, I will analyse that aspect as part of my examination of its proportionality, addressed in the second sentence of that paragraph, in line with the approach followed by both the Court and the ECtHR in the cases on measures relating to the processing of personal data. [82]

(b) Respect for the essence of the rights set out in Articles 7 and 8 of the Charter

89. According to the first sentence of Article 52(1) of the Charter, any limitation on the exercise of fundamental rights must not only have a sufficiently precise legal basis but must also respect the essence of those rights.

90. As I set out in point 66 of this Opinion, that requirement – which is to be found in the constitutions of various Member States [83] and, whilst not expressly laid down by the ECHR, is nevertheless well established in the case-law of the ECtHR [84] – is enshrined in Article 52(1) of the Charter. [85] Recognised by the Court a long time before it was codified, [86] that requirement has been consistently confirmed in the case-law of the EU Courts, even after entry into force of the Treaty of Lisbon.

91. It emerges from the judgment of 6 October 2015, *Schrems*, [87] among others, that where an EU act fails to respect the essence of a fundamental right it is *automatically* void or invalid, and there is no requirement to engage in a balancing exercise of competing interests. The Court has accordingly held that any fundamental right represents a 'hard nucleus' that guarantees to each and every individual a sphere of liberty that must always remain free from interference by the public authorities and may not be subject to limitations [88] without calling into question the democratic principle and the principles of the rule of law and respect for human dignity that

82 See among others, *La Quadrature du Net* judgment, paragraph 132 and the case-law cited; see also ECtHR, *Big Brother Watch* judgment, § 334.

83 See, in that respect, Tridimas, T., and Gentile, G., 'The essence of Rights: an unreliable Boundary?', *German Law Journal*, 2019, Vol. 20, p. 796; Lenaerts, K., 'Limits on limitations: The Essence of Fundamental Rights in the EU', *German Law Journal*, 2019, Vol. 20, p 779 et seq.

84 Starting with the judgment of the ECtHR of 24 October 1979, *Winterwerp v. Netherlands*, CE:ECHR:1979:1024JUD000630173, § 60.

85 See Explanations Relating to the Charter of Fundamental Rights (OJ 2007 C 303, p. 17, in particular 'Explanations on Article 52', p. 32) ('the Explanations relating to the Charter').

86 See, already to that effect, among others, judgments of 14 May 1974, *Nold* v *Commission* (4/73, EU:C:1974:51, paragraph 14), and of 13 December 1979, *Hauer* (44/79, EU:C:1979:290, paragraph 23).

87 C-362/14, EU:C:2015:650, paragraphs 94 to 98 ('*Schrems I* judgment').

88 See Lenaerts, K., op. cit., p. 781, Tridimas, T., and Gentile, G., op. cit., p. 803.

underpin the protection of fundamental rights. It is also apparent, both from the wording of Article 52(1) of the Charter and from the Court's case-law, in particular the *Schrems I* judgment, that the existence of interference with the essence of the fundamental right at issue must be determined before and independently of evaluation of whether the measure complained of is proportionate. That test, in other words, is autonomous.

92. That having been established, determining what constitutes the 'essence' and, therefore, the inalienable substance, of a fundamental right whose exercise may be limited is an extremely complex task. Although, so that it can perform its function, that concept should be capable of being defined in absolute terms in the light of the essential characteristics of the fundamental right at issue, the subjective and objective interests it is intended to protect and, more generally, its function in a democratic society based on respect for human dignity, [89] in practice it is almost impossible to do so, at least without taking into account criteria normally used when examining whether interference with the right at issue is proportionate, such as how serious that interference is or its extent or temporal dimension and, therefore, without taking into account the specific features of each particular case.

93. As regards the fundamental right to respect for private life in particular, account should be taken not only of the importance of having a private sphere in which to develop the inner personal core for the mental and physical health of all individuals, their well-being, autonomy, self-development and their ability to enter into and cultivate social relationships, but also of the role of that right in preserving other rights and freedoms such as freedom of thought, conscience, religion, expression and information, which can only be fully enjoyed if a private sphere is recognised. In more general terms, account should be taken of the function that respect for private life performs in a democratic society. [90] When determining whether the essence of that right has been infringed, the Court appears to consider both the *intensity* and the *extent* of the interference, suggesting that such infringement is defined quantitatively rather than qualitatively. Accordingly, on the one hand, in the *Digital Rights* judgment the Court found in essence that the retention of data required by Directive 2006/24/EC [91] was not so serious that it would affect the essence of the right to private life, because it did not permit 'the acquisition of knowledge of the content of the electronic communications as such'. [92] On the other hand, in Opinion 1/15 the Court found in essence that a limitation confined to only certain aspects of the private life of the individuals concerned could not give rise to interference with the essence of that fundamental right. [93]

94. As regards the fundamental right to the protection of personal data, the Court appears to find the essence of that right to be preserved when the measure providing for the interference limits the purposes of the processing and establishes rules ensuring that the data in question will be secure, in particular from accidental or unlawful destruction, or accidental loss or alteration. [94]

89 The Explanations relating to the Charter expressly acknowledge that 'the dignity of the human person is part of the substance of the rights laid down in [the] Charter' and that 'it must therefore be respected, even where a right is restricted'.

90 I refer in that respect to the considerations contained in the partly concurring opinion of Judges Lemmens, Vehabović and Bošnjak annexed to the *Big Brother Watch* judgment, §§ 3 to 10.

91 Directive of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

92 See *Digital Rights* judgment, paragraph 39; see also, as regards Directive 2002/58, *Tele2 Sverige* judgment paragraph 101.

93 See Opinion 1/15, paragraph 150.

94 See to that effect, among others, *Digital Rights* judgment, paragraph 40.

95. In the present case, although the referring court has not explicitly referred to the requirement to respect the essence of the rights set out in Articles 7 and 8 of the Charter, the matter of compliance with that requirement in my view lies behind the fourth and sixth questions. That is why I suggest that it should be addressed by the Court.

96. I would call to mind that, in paragraph 150 of Opinion 1/15, while acknowledging that PNR data 'may, in some circumstances, reveal very specific information concerning the private life of a person'[95] and may, directly or indirectly, reveal sensitive information about the person concerned,[96] the Court nevertheless found that the infringement of the fundamental right to respect for private life resulting from the draft Canada-EU PNR agreement was not liable adversely to affect the essence of that right, because 'the nature of that information [was] limited to certain aspects of that private life, in particular, relating to air travel between Canada and the European Union'.

97. Apart from the fact that the PNR data covered by the draft Canada-EU PNR agreement were to be transferred to a third country and subsequently processed by the authorities of that third country on its territory, the interference with the fundamental right to respect for private life resulting from that draft agreement and the interference contemplated by the PNR Directive are broadly the same in nature. That is true of the PNR data involved, of the fact that the transfer and processing of those data are systematic and generalised and that the processing is automated, and of the retention of those data, among other factors. What distinguishes the two cases, in contrast, is what could be termed the 'geographical coverage' of that interference. As I stated in point 77 of this Opinion, the data processing at issue in this case is not limited to air links with a single third country, as in Opinion 1/15, but concerns almost all flights within the European Union and those entering and leaving it. Compared with the draft Canada-EU PNR agreement, the PNR Directive therefore requires the systematic handling of an appreciably greater number of air passengers, travelling by air inside and outside the European Union. Furthermore, given the larger volume of data processed and the frequency with which they are collected, the processing of those data is likely to provide both more precise and more plentiful information on the private life of the persons concerned (for example, travel habits, personal relationships and financial situation).

98. Nevertheless, as occurred in Opinion 1/15, that information is limited to certain aspects of private life relating to air travel. Since the concept of the 'essence' of fundamental rights must be defined restrictively, so that it continues to perform its role as a bastion against attacks on the very substance of those rights, I believe that the finding made by the Court in paragraph 150 of Opinion 1/15 can be transposed to the present case.

99. In Opinion 1/15 the Court also found that the essence of the right to the protection of personal data was not adversely affected.[97] In my view, that finding can likewise be transposed to the circumstances of the present case. As was the case with the draft Canada-EU PNR agreement, the PNR Directive, in Article 1(2), delimits the purposes of the processing of PNR data. Moreover, that directive, in common with the other EU acts to which it refers, including the GDPR and the Policing Directive, contains specific provisions intended to ensure, in particular, the security, confidentiality and integrity of those data and to protect them from unlawful access and

[95] See, in the same vein, Opinion 1/15, paragraph 128.

[96] See Opinion 1/15, paragraphs 164 and 165.

[97] See Opinion 1/15, paragraph 150.

processing. Although it cannot be found that rules such as those established by the PNR Directive affect the essence of the fundamental rights protected by Articles 7 and 8 of the Charter, they must nevertheless be subject to a strict and rigorous review of proportionality.

(c) Compliance with the requirement that the interference must satisfy an objective of general interest

100. The PNR Directive seeks in particular to ensure the internal security of the European Union and to protect the life and safety of persons by transferring PNR data to the competent authorities of the Member States to be used in combating terrorism and serious crime. [98]

101. Specifically, it can be seen from Article 1(2) of that directive, read in conjunction with recitals 6 and 7, and from the Commission's proposal which led to the adoption of the PNR Directive ('the proposal for a PNR directive') [99] that, in the context of that objective, PNR data are used in various ways by the law enforcement authorities. [100] First, those data are used to identify individuals involved in or suspected of being involved in terrorist offences or serious crime that have already been committed, to gather evidence and, where relevant, to find associates of criminals and unravel criminal networks ('reactive' use). Secondly, PNR data can be assessed before passengers arrive or depart in order to prevent the commission of a crime and to identify persons who were previously unsuspected of involvement in terrorist offences or serious crime but who, on the basis of the outcome of that assessment, should be subject to further examination by the law enforcement authorities (use 'in real time'). Lastly, PNR data are used to define assessment criteria that can then be applied to assess the risk that passengers pose before they arrive and before they depart ('proactive' use). That proactive use of PNR data should enable the law enforcement services to address the threat of terrorist offences and serious crime from a different perspective than through the processing of other categories of personal data. [101]

102. It can be seen from the case-law of the Court that the objective of protecting public security, which covers in particular preventing, investigating, detecting and prosecuting terrorist offences and serious crime, constitutes an objective of general interest of the European Union within the meaning of Article 52(1) of the Charter that is capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter. [102]

103. The Court has also held that the objectives of safeguarding public security and combating serious crimes contribute to the protection of the rights and freedoms of others. [103] Accordingly, when striking a balance between those objectives and the fundamental rights enshrined in Articles 7 and 8 of the Charter, [104] it is also necessary to take into account the importance of the rights enshrined in Articles 3, 4, 6 and 7 of the Charter. Although, in the *La Quadrature du Net* judgment, the Court found that Article 6 of the Charter 'cannot be interpreted as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal

98 See in particular recitals 5, 6, 15 and 22 of the PNR Directive.

99 Commission Proposal of 2 February 2011 for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime ((COM(2011) 32 final), p. 4).

100 In the interests of simplification, in this Opinion I will use the expressions 'law enforcement services' and 'law enforcement authorities' to refer in general terms to any authority with powers in the fields of the detection, prevention, prosecution or investigation of terrorism or serious crime covered by the PNR Directive.

101 See recital 7 of the PNR Directive. See also, proposal for a PNR directive, p. 5.

102 See, to that effect, Opinion 1/15 and judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraph 33 and the case-law cited) ('*Prokuratuur* judgment').

103 See, to that effect, Opinion 1/15, paragraph 149 and the case-law cited, and the *La Quadrature du Net* judgment.

104 See below for analysis of the proportionality of the interference.

offences',[105] conversely, as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons, the Court emphasised that positive obligations on the public authorities may result both from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life, and from Articles 3 and 4, as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment.[106]

104. Lastly, the Court has found that the importance of the objective of safeguarding *national security* goes beyond the objectives of combating crime in general, even serious crime, and of safeguarding public security and is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives.[107] Since terrorist activities can constitute threats to the national security of the Member States, the system enacted by the PNR Directive, because it serves as an instrument for combating such activities, contributes to the objective of safeguarding the national security of the Member States.

(d) Compliance with the principle of proportionality

105. According to the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be placed on the exercise of a fundamental right recognised by that article 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.

106. In that regard, according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.[108]

107. According to the Court's consistent case-law, the protection of the fundamental right to privacy requires that derogations from and limitations on the protection of personal data must 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.[109] Specifically, whether or not a limitation on the rights enshrined in Articles 7 and 8 of the Charter is proportionate must be assessed by measuring the seriousness of the interference entailed by such a limitation and verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness.[110]

108. It emerges from the Court's case-law that, in order to satisfy the proportionality requirement, the PNR Directive, as the legal basis entailing the interferences described in points 70 to 83 of this Opinion with the fundamental rights enshrined in Articles 7 and 8 of the

105 See *La Quadrature du Net* judgment, paragraph 125.

106 See *La Quadrature du Net* judgment, paragraph 126 and the case-law cited.

107 See *La Quadrature du Net* judgment, paragraph 136.

108 See *Digital Rights* judgment, paragraph 46 and the case-law cited.

109 See Opinion 1/15, paragraph 140, and *La Quadrature du Net* judgment, paragraph 130 and the case-law cited. Article 5 of Convention 108 also sets out the requirement that the processing of personal data must reflect at all stages 'a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake'.

110 See, to that effect, judgment of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788, paragraph 55 and the case-law cited); *La Quadrature du Net* judgment, paragraph 131; and *Prokuratuur* judgment, paragraph 32.

Charter, must lay down clear and precise rules governing the scope and application of the measures containing the interferences in question and must impose minimum requirements to ensure that the persons whose data have been transferred have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access to and use of those data.[111] The need for such guarantees is all the greater where, as in the present case, the personal data undergo automated processing and where the protection of a particular category of personal data – sensitive data – is at stake.[112]

109. As regards the extent of judicial review of compliance with the requirements flowing from the principle of proportionality, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the interference with that right entailed by the PNR Directive, the EU legislature's discretion is reduced, with the result that review should be strict.[113]

(1) Appropriateness of the PNR data processing operations envisaged by the PNR Directive in the light of the objective pursued

110. In paragraph 153 of Opinion 1/15, the Court stated in relation to the draft Canada-EU PNR agreement that the transfer of PNR data to Canada and subsequent processing of those data could be regarded as being appropriate for the purpose of ensuring that the objective relating to the protection of public security and safety was achieved. It does not seem to me that this finding that those operations are appropriate, which has long been acknowledged both at EU level and globally,[114] can be called into question as regards the collection and subsequent processing of PNR data for either extra-EU flights or intra-EU flights.[115]

111. Nevertheless, the efficacy of the system for the processing of PNR data established by the directive can only be determined in concrete terms, by assessing the results of its application.[116] From that perspective, that efficacy must be assessed continuously using the most precise and reliable statistical data possible.[117] In that respect, the Commission should at regular intervals conduct a review similar to that already established in Article 19 of the PNR Directive.

111 See, to that effect, *Digital Rights* judgment, paragraph 54; *Schrems I* judgment, paragraph 91; and Opinion 1/15, paragraph 141.

112 See Opinion 1/15, paragraph 141 and the case-law cited.

113 See, to that effect, *Digital Rights* judgment, paragraph 48.

114 See, to that effect, points 201 to 203 of this Opinion.

115 I refer in that respect to the data in the 2020 working document.

116 See, to that effect, Opinion of 19 August 2016, p. 5.

117 On the importance of statistics for assessing the efficacy of the system established by the PNR Directive see, among others, Opinion 1/2011 of 14 June 2011 on the proposal for a PNR directive, https://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_EN.pdf, point 2.1.2.1 ('FRA Opinion 1/2011').

(2) Whether the interference is strictly necessary

112. Although the Cour constitutionnelle (Constitutional Court) has not explicitly expressed doubts as regards whether, in defining the purposes for which PNR data may be processed, the PNR Directive contains clear and precise rules limited to what is strictly necessary,[118] I believe that when analysing the proportionality of the system laid down by that directive, as the referring court has requested, the Court must address that matter.[119]

(i) Defining the purposes for which PNR data may be processed

113. It is an essential requirement of any data processing system, especially for law enforcement purposes, that the purposes for which the competent authorities are allowed access to personal data and can subsequently use those data must be clearly defined. That requirement must also be satisfied in order to enable the Court to assess whether the measures at issue are proportionate, using the test established in the case-law, which compares the seriousness of the interference with the importance of the objective pursued.[120]

114. The Court has underscored the importance of clearly defining the purposes of measures which involve limitations on the fundamental rights to respect for private life and the protection of personal data, in particular in the *Digital Rights* judgment, in which it held Directive 2006/24 to be invalid. In paragraph 60 of that judgment, the Court noted that Directive 2006/24 failed to lay down 'any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference' and, in contrast, confined itself to referring 'in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law'.

115. Article 1(2) of the PNR Directive sets out a general criterion for limiting the purposes of processing, according to which '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'. Nevertheless, in contrast to Directive 2006/24, the PNR Directive does not merely set out that criterion, but itself, in Article 3(8) and (9), defines both 'terrorist offences' and 'serious crime', the former by reference to Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ 2002 L 164, p. 3) (replaced by Directive (EU) 2017/541),[121] and the second, on the one hand, by listing in Annex II the categories of criminal offences corresponding to that expression and, on the other, by establishing a threshold of seriousness according to the maximum custodial sentence or detention order by which those offences can be punished.

118 The Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), in contrast, has clearly raised that issue in Case C-215/20, pending.

119 The Commission has been invited to submit its observations in that regard, in a question requiring a written answer. The other interested parties were able to express their views at the hearing.

120 See point 107 *in fine* of this Opinion.

121 Directive of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475 and amending Council Decision 2005/671/JHA (OJ 2017 L 88, p. 6).

116. While the reference to the relevant provisions of Directive 2017/541 does enable the acts that can be classified as terrorist offences under Article 3(8) of the PNR Directive to be characterised sufficiently clearly and precisely and to determine their seriousness in order to weigh the importance of the objective of protecting public security pursued by that directive against the seriousness of the interference it involves with the fundamental rights enshrined in Articles 7 and 8 of the Charter, that finding is not so evidently true in relation to all the offences listed in Annex II.

117. In paragraph 177 of Opinion 1/15, the Court held that the draft Canada-EU PNR agreement defined the degree of seriousness of the offences covered by the expression 'serious transnational crime' with clarity and precision by requiring that they be 'punishable by a maximum deprivation of liberty of at least four years or a more serious penalty', referring to 'offences defined by Canadian law' and setting out 'the different situations in which a crime is considered to be transnational in nature'.

118. Compared with the legislation that the Court examined in that opinion, the PNR Directive (i) does not take into account, when it defines the offences concerned, the fact that they are transnational; (ii) establishes an exhaustive list of offences which are considered, by their nature, to amount to serious crime, provided they are punishable by at least the maximum penalty laid down in Article 3(9) of that directive; (iii) in principle, lowers the seriousness threshold by adopting a criterion based on the level of the maximum penalty and by setting that threshold at three years.

119. As regards, first, the absence of any limiting criterion based on the fact that the offences are transnational, confining the matters covered by the PNR Directive solely to 'cross-border' serious crime would admittedly have made it possible to target offences that may, by nature, have an objective, even if only potential, link with air travel, and, therefore, with the categories of data collected and processed under the PNR Directive.[122] However, in principle I share the view expressed by the Commission to the effect that, unlike in the context of an international agreement, where the situation concerns a mechanism to combat crime whose objective is to protect the internal security of the European Union, the relevance of such a criterion and the need for it is less obvious. Furthermore, as the Commission also states, the absence of cross-border elements is not in itself a sufficient indication that an offence is not serious.

120. In respect, secondly, of the criterion fixing the threshold of seriousness for the offences concerned – which, so that the seriousness can be assessed in advance, must be interpreted as referring to the maximum duration of the custodial sentence or detention order established by the legislation rather than to the sentence or detention order that may actually be imposed in a particular case – although it is based on at least the maximum penalty rather than on at least the minimum penalty, is not inherently incapable of identifying a level of seriousness sufficient to justify the interference which the data processing under the PNR Directive entails with the fundamental rights enshrined in Articles 7 and 8 of the Charter. To my mind, however, it should be interpreted as a criterion identifying a 'minimum' level of seriousness. Such a criterion, although it prevents the Member States from treating offences referred to in Annex II as 'serious crime' where their national criminal law establishes for those offences a custodial sentence or

[122] I note in that respect that the expression 'transnational crime' as defined, for example, in the draft Canada-EU PNR agreement, was sufficiently broad to also include offences committed in one country where the offender 'is in or intends to travel to another country' (see Article 3(3)(e) of the draft Canada-EU PNR agreement, whose wording is reproduced in paragraph 30 of Opinion 1/15). I also note that in its Opinion 1/2011 (see Sections 2.2.3.1 and 3.7), the FRA suggested limiting the EU PNR system to serious transnational crime. In contrast, the proposal for a PNR directive envisaged different automated processing for transnational crime and for non-transnational crime (see Article 4(2)(a) of that proposal).

detention order with a maximum duration of less than three years, it does not, conversely, oblige them automatically to treat as serious crime all the offences capable of being included in that annex and punishable with a penalty of or above the threshold laid down in Article 3(9) of the PNR Directive where, having regard to the specific features of their penal system, treating them as such would result in the regime established by the PNR Directive being used to prevent, detect, investigate and prosecute ordinary crimes, contrary to the purposes pursued by the directive.

121. As regards, thirdly, the list in Annex II, it should be noted, first of all, that the fact that the PNR Directive lists exhaustively the offences covered by the definition of 'serious crime' is a fundamental formal and substantive safeguard intended to ensure that the system established by the PNR Directive is lawful and to ensure legal certainty for passengers. Nevertheless, that list includes not only offences that are inherently and indisputably extremely serious – such as human trafficking, the sexual exploitation of children and child pornography, illicit trafficking in weapons or nuclear or radioactive materials, unlawful seizure of aircraft/ships, serious crimes within the jurisdiction of the International Criminal Court, murder, rape and kidnapping, illegal restraint and hostage-taking [123] – but also offences which are not so obviously extremely serious, such as fraud, counterfeiting and piracy of products, forgery of administrative documents and trafficking therein and trafficking in stolen vehicles. [124] Furthermore, among the offences listed in Annex II, some are, by their very nature, more likely than others to be transnational and therefore to have a link with the carriage of passengers by air, such as human trafficking, illicit trafficking in narcotic drugs or weapons, the sexual exploitation of children, facilitation of unauthorised entry and residence and the unlawful seizure of aircraft.

[123] I note also that some of the offences referred to in Annex II fall within areas of crime classified as 'particularly serious' in the first subparagraph of Article 83(1) TFEU and listed in the second subparagraph of that article. These include trafficking in human beings, the sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime. In several of those areas the EU legislature has adopted directives under Article 83(1) TFEU laying down 'minimum rules concerning the definition of criminal offences and sanctions'. See in particular, Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA (OJ 2011 L 101, p. 1); Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1); Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ 2013 L 218, p. 8); Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (OJ 2019 L 123, p. 18); Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (OJ 2017 L 198, p. 29); and Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law (OJ 2018 L 284, p. 22).

[124] I would nevertheless point out that all the offences referred to in Annex I, with the exception of 'industrial espionage', are contained in Article 2(2) of Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedure between Member States (OJ 2002 L 190, p. 1). Although they are not expressly classified as serious, where they reach the threshold for a custodial sentence laid down in Article 3(9) of the PNR Directive they nevertheless result in surrender under a European arrest warrant, without verification of the double criminality of the act. Nearly all those offences, with the exception of 'sabotage', 'unlawful seizure of aircraft' and 'industrial espionage', are also included in Annex I to Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (OJ 2018 L 295, p. 138), which lists the 'forms of serious crime' with which Eurojust is competent to deal.

122. The level of clarity and precision of the headings in Annex II is, likewise, very variable. Although the list in that annex must be regarded as exhaustive, several of its headings are 'open-ended' [125] and others refer to generic concepts capable of including a very large number of offences of varying degrees of seriousness, albeit always within the maximum threshold under Article 3(9) of the PNR Directive. [126]

123. In that respect, I note, first, that the harmonising directives adopted in the areas referred to in Article 83(1) TFEU and mentioned in footnote 123 to this Opinion provide information relevant to identifying at least some of the serious criminal offences capable of falling under the corresponding headings of Annex II. For example, Directive 2013/40, in Articles 3 to 8, defines various offences covered by the concept of 'computer-related crime/cybercrime' referred to in paragraph 9 of that Annex II and takes care in each case to include only acts constituting 'cases which are not minor'. [127] Similarly, Directive 2019/713 defines a number of categories of offences of fraud, and Directive 2017/1371 defines the elements constituting 'fraud to the [EU]'s financial interests'. It is also appropriate to mention in that context Directive 2008/99/EC, adopted under Article 175(1) EC on the protection of the environment through criminal law, [128] which, in Article 3, defines a series of serious environmental offences capable of falling under heading 10 of Annex II, including acts qualifying as 'illicit trafficking in endangered animal species and in endangered plant species and varieties', excluding all conduct that has a negligible impact on the protected good. I would call to mind, lastly, Directive 2002/90/EC, [129] which defines the facilitation of unauthorised entry, transit and residence; Framework Decision 2002/946/JHA, [130] intended to strengthen the penal framework to prevent those offences; Framework Decision 2003/568/JHA, [131] which defines the criminal offences classified as 'active and passive corruption in the private sector'; and Framework Decision 2008/841/JHA, [132] which defines the offences relating to participation in organised crime.

124. Secondly, I note, as the Commission correctly observed, that since substantive criminal law has not been completely harmonised, the EU legislature cannot be criticised for not further particularising the offences referred to in Annex II. Accordingly, in contrast to what will be seen below in this Opinion in relation to the list of PNR data contained in Annex I, the transposition into internal law of the list of offences in Annex II necessarily requires the Member States to define the offences capable of being on that list, according to the specific features of their national penal systems. In doing so, they must nevertheless fully satisfy the test that any interference with the fundamental rights set out in Articles 7 and 8 of the Charter must be limited to what is strictly necessary. For example, I believe there is nothing to prevent the Member States from stipulating that the use of PNR data must be limited, for certain offences, such as, for example, those referred to in paragraphs 7, 16, 17, 18 and 25 of Annex II, to situations where those offences are cross-border offences, are committed in the context of organised crime or involve certain aggravating circumstances. It will be for the Member State

125 These include paragraphs 7, 8, 10 and 16.

126 This applies, for example, to 'fraud' (paragraph 7), 'corruption' (paragraph 6), 'computer-related crime/cybercrime' (paragraph 9) and 'environmental crime' (paragraph 10). In Case C-215/20, pending, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) is enquiring of the Court in particular in relation to offences of fraud.

127 In its Article 9, that directive also establishes the minimum duration of the maximum prison sentence by which those offences must be punishable, which only in certain circumstances is three years or more.

128 Directive of the European Parliament and of the Council of 19 November 2008 (OJ 2008 L 328, p. 28).

129 Council Directive of 28 November 2002 defining the facilitation of unauthorised entry, transit and residence (OJ 2002 L 328, p. 17).

130 Council Framework Decision of 28 November 2002 on the strengthening of the penal framework to prevent the facilitation of unauthorised entry, transit and residence (OJ 2002 L 328, p. 1).

131 Council Framework Decision of 22 July 2003 on combating corruption in the private sector (OJ 2003 L 192, p. 54).

132 Council Framework Decision of 24 October 2008 on the fight against organised crime (OJ 2008 L 300, p. 42).

courts, subject to review by the Court, to interpret the national provisions transposing that list into internal law in conformity with both the PNR Directive and the Charter, in order to ensure, for each heading, that the processing of PNR data is limited to offences of the high level of seriousness required by that directive and to the offences for which such processing is relevant. [133]

125. Subject to the clarifications in points 120 and 124 of this Opinion, I believe that Article 3(9) of the PNR Directive and the list of offences in Annex II to that directive do satisfy the requirements as to clarity and precision and do not go beyond what is strictly necessary.

126. It must nevertheless be acknowledged that the solution illustrated in point 124 of this Opinion is not completely satisfactory. First, it leaves a significant margin of discretion to the Member States, with the effect that the matters in respect of which PNR data are processed can vary appreciably between Member States, thereby jeopardising the objective of harmonisation pursued by the EU legislature. [134] Secondly, it means that the proportionality of the limits imposed on the purposes of that processing, which constitute a fundamental component of the system, is reviewed *ex post* as part of the national transposing measures rather than *ex ante* as part of the PNR Directive itself. In the event that the Court finds, as I suggest it should, that Article 3(9) of the PNR Directive and the list of offences in Annex II are in conformity with Articles 7, 8 and Article 52(1) of the Charter, I therefore recommend that it should draw the attention of the EU legislature to the fact that that assessment is only provisional and requires the legislature to verify whether it is necessary, in the light of the transposition of that provision and that list by the Member States and on the basis of the statistical data referred to in Article 20 of the PNR Directive (i) to further specify the categories of offences in that list by confining their scope; (ii) to remove from that list any offences for which the processing of PNR data proves disproportionate, irrelevant or ineffective; and (iii) to increase the threshold of seriousness of the offences referred to in Article 3(9) of the PNR Directive. [135] I note in that regard that although Article 19(2)(b) of the PNR Directive requires the Commission to conduct a review of all the components of that directive, paying particular attention to 'the necessity and proportionality of collecting and processing PNR data for each of the purposes set out' in it, neither the 2020 Commission report nor its accompanying 2020 working document in my view contains a satisfactory examination in that respect.

(ii) The categories of PNR data covered by the PNR Directive (second and third questions referred)

127. The PNR Directive provides for the transfer to the PIUs of 19 categories of PNR data collected by air carriers for the purpose of flight booking. Those categories, which are listed in Annex I, correspond to the categories in the booking systems of the airlines and those listed in Annex I to the Guidelines on Passenger Name Record Data adopted by the International Civil Aviation Organisation (ICAO) in 2010 [136] ('the ICAO guidelines').

133 See in particular recitals 7 and 22 of the PNR Directive.

134 See recital 35 of the PNR Directive.

135 See, by analogy, judgments of 16 December 2008, *Arcelor Atlantique et Lorraine and Others* (C-127/07, EU:C:2008:728, paragraphs 61 and 62), and of 17 October 2013, *Schaible* (C-101/12, EU:C:2013:661, paragraphs 91 and 94).

136 See document 9944, approved by the Secretary General of ICAO and published under his authority. The English-language version of that document is available on the site https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf. According to Section 9.22 of Annex 9 (Facilitation) to the Convention on International Civil Aviation, signed in Chicago on 7 December 1944 ('the Chicago Convention'), the Contracting States of that convention that require PNR data must align their requirements for data and data processing with, inter alia, those guidelines.

128. By its second question, the referring court asks whether Annex I is valid in the light of Articles 7, 8 and Article 52(1) of the Charter in view of, first, the breadth of the personal data listed in that annex – in particular the API data referred to in paragraph 18, in so far as they go beyond the data listed in Article 3(2) of the API Directive – and, secondly, the fact that those data, taken as a whole, may reveal sensitive data and therefore go beyond the limits of what is 'strictly necessary'. By its third question – which, as I have already had the opportunity to note, concerns compliance with the first of the three conditions under Article 52(1) of the Charter, according to which any interference with a fundamental right must be 'provided for by law' – the Cour constitutionnelle (Constitutional Court), in contrast, enquires of the Court as to the validity of paragraphs 12 and 18 of Annex I, in particular having regard to the fact that they are 'open-ended'.

129. Since the examination to be carried out under the second question referred presupposes that the Court has examined whether the categories of personal data referred to in Annex I are sufficiently clear and precise, I will address the third question first.

– Whether paragraphs 12 and 18 of Annex I are sufficiently clear and precise (third question referred)

130. It should be noted, as a preliminary matter, that the extent and seriousness of the interference with the fundamental rights set out in Articles 7 and 8 of the Charter entailed by a measure that imposes limitations on the exercise of those rights depends, primarily, on the extent and nature of the personal data being processed. It is therefore essential to identify those data and any legal basis establishing such a measure must in all cases do so as clearly and precisely as possible.

131. That requirement was acknowledged by Opinion 1/15 in relation to the processing of PNR data. Ruling on the headings in the annex to the draft Canada-EU PNR agreement, which contains a list of the PNR data covered by the envisaged agreement, the Court held in particular, in that opinion, that the use of general categories of information that insufficiently determined the scope of the data to be transferred, and the use of illustrative lists of data that did not in any way limit the nature and scope of the information that could be included under the heading concerned, did not satisfy the requirements as to clarity and precision.

132. The third question referred must be examined in the light of those principles.

133. Paragraph 12 of Annex I is worded as follows:

'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).'

134. Since it refers to 'general remarks', that paragraph, like heading 17 of the annex to the draft Canada-EU PNR agreement, constitutes a 'free text' heading intended to include all the information collected by air carriers in the course of providing their services over and above that expressly listed in other paragraphs of Annex I. As the Court found in paragraph 160 of Opinion 1/15, such a heading 'provides no indication as to the nature and scope of the information to be communicated, and it may even encompass information entirely unrelated to the purpose of the transfer of PNR data'. Furthermore, since the clarification in parentheses contained in

paragraph 12 of Annex I, concerning information about unaccompanied minors, is provided only by way of example, as the use of the word 'including' attests, that paragraph does not in any way limit the nature and scope of the information it can cover. [137]

135. In those circumstances, paragraph 12 of Annex I cannot be regarded as being defined with sufficient clarity and precision.

136. Although the Commission and the Parliament appear to agree with that finding, the Member States that have submitted observations on the third question, and the Council, demur, on the basis of broadly overlapping lines of argument.

137. In the first place, a first series of arguments seeks in general terms to dispute that the findings made by the Court in Opinion 1/15 can be transposed to this case.

138. In that respect, while I am aware of the different contexts of the two cases, here I will merely observe that the conclusion reached by the Court in paragraph 160 of Opinion 1/15 concerning heading 17 of the annex to the draft Canada-EU PNR agreement was based on an exclusively semantic and structural interpretation of that heading. That interpretation is fully transposable to paragraph 12 of Annex I which, apart from the example, is worded identically to that heading and has a similar structure. Furthermore, as will be seen in greater detail below, both the rules at issue have the same multilateral regulatory context comprising in particular the ICAO guidelines, to which the Court furthermore referred expressly in paragraph 156 of Opinion 1/15. That being so, not only does nothing preclude following the same interpretation in respect of paragraph 12 of Annex I as that adopted by the Court in paragraph 160 of Opinion 1/15 for heading 17 of the annex to the draft Canada-EU PNR agreement, but in fact nothing justifies departing from that interpretation.

139. In the second place, many Member States assert that the various paragraphs of Annex I, including paragraph 12, correspond to the headings of Appendix 1 to the ICAO guidelines, with which the air carriers are very familiar and to which they are fully capable of attributing precise contents. That paragraph 12 to my mind corresponds in particular to the last two headings of that annex, headed 'General remarks' and 'Free text/code fields in OSI [Other Supplementary Information], SSR [Special Service Request], SSI [Special Service Information], remarks/history' respectively and referring to 'supplemental' or 'requested service' information. [138]

140. I note first of all in that respect that the correspondence between the headings in Annex I to the draft Canada-EU PNR agreement, on the one hand, and the headings in Appendix 1 to the ICAO guidelines, on the other, did not prevent the Court from finding in Opinion 1/15 that some of the headings in Annex I to the said draft agreement did not satisfy the requirements as to clarity and precision that must be met by a measure that limits the exercise of fundamental rights. Thereafter, contrary to the view that certain Member States seem to take, I would note that a reference to the ICAO guidelines, which is moreover not explicit, [139] does not further clarify the nature and scope of the information capable of falling under paragraph 12 of Annex I. On the

[137] To the same effect, see Opinion 1/15, paragraph 160.

[138] See paragraphs 2.1.2 and 2.1.5 of the ICAO guidelines.

[139] The only reference to the ICAO guidelines in the PNR Directive is in recital 17 and concerns only the 'supported data formats for transfers of PNR data by air carriers to Member States'.

contrary, a reading of those guidelines reinforces the conclusion that a 'free text' heading, such as paragraph 12, includes an undefined number of diverse items of information in addition to those automatically contained in the PNR. [140]

141. In the third place, some governments argue that it is for the Member States, by means of internal legislative measures and subject to the limits imposed by Articles 7, 8 and Article 52(1) of the Charter, to specify the information that can appear in paragraph 12 of Annex I. In their view, it is in the very nature of a directive that it leaves a margin of discretion to the Member States as regards the means necessary to implement the provisions it lays down.

142. As I have already stated in point 86 of this Opinion, my view is that when measures that entail interference with the fundamental rights established by the Charter originate in an EU legislative act, it is for the EU legislature, complying both with the abovementioned criteria of clarity and precision and the principle of proportionality, to determine the exact scope of that interference. It follows that, where the instrument chosen by the EU legislature is a directive, that legislature cannot, to my mind, delegate to the Member States, when they transpose the directive into their national law, the task of determining essential components that define the scope of the interference such as, in relation to limitations on the fundamental rights set out in Articles 7 and 8 of the Charter, the nature and scope of the personal data to be processed.

143. In the fourth place, a number of Member States observe that paragraph 12 of Annex I must be understood as referring solely to information relating to the provision of transport services. Interpreted in that way, that paragraph would be compatible with Articles 7, 8 and Article 52(1) of the Charter.

144. I find that argument also to be unconvincing. First of all, the information that can be included under a 'general remarks' heading and under the OSI, SSI, and SSR codes is very diverse (medical care, special dietary requirements or preferences, any request for assistance, information about unaccompanied minors, and so on) [141] and is all related to provision of transport services since it is intended, inter alia, to enable the air carrier to adapt the service to the requirements of each passenger. An interpretative criterion based on the relevance of the information to the provision of transport services does not in my view enable the scope of that paragraph 12 to be specified more precisely. Thereafter, I would note that, although in paragraph 159 of Opinion 1/15 the Court used that criterion to interpret a different heading of the annex to the draft Canada-EU PNR agreement in conformity with the requirements of clarity and precision, it nevertheless held that it could not do so in relation to heading 17 of that annex, which corresponds to paragraph 12 of Annex I.

145. In the fifth place, a number of Member States have drawn attention to the fact that the information intended to be covered by paragraph 12 of Annex I is provided to the air carriers voluntarily by passengers themselves, who are duly informed that those data will subsequently be transferred to the public authorities. The notion underlying that argument seems to be that the passenger concerned gives a form of implied consent to the data provided to the airlines then being transferred to the public authorities.

[140] Paragraph 2.1.5 of those guidelines refers to 'supplemental' or 'requested service information', which may relate to 'special dietary and medical requirements, "unaccompanied minor" information, requests for assistance, and so on.'. Paragraph 2.1.6, for its part, clarifies that the '"general remarks" field' may also contain 'some information, such as the internal dialogue or communication between airline staff and reservation agents'.

[141] See paragraphs 2.1.5 and 2.1.6 of the ICAO guidelines.

146. The Court has already had an opportunity to clarify that there can be no question of 'consent' where the data subjects are not free to object to the processing of their personal data.[142] In respect of much of the information that can fall under paragraph 12 of Annex I, the passenger concerned cannot genuinely choose, but is obliged to provide those data in order to have access to the transport service. That is true, for example, of persons with a disability or reduced mobility, those needing medical care or unaccompanied minors. I also note that in paragraphs 142 and 143 of Opinion 1/15 the Court clearly stated that since the processing of PNR data by public authorities pursues a different objective from that for which those data are collected by air carriers, it cannot be regarded as being based on any form of consent that passengers have given to that collection.

147. Lastly, the majority of the Member States assert that the data processing operations envisaged by the PNR Directive are surrounded by numerous safeguards including, as regards the transfer of data to PIUs, an obligation on those units to delete data not appearing in Annex I and data capable of revealing a person's racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

148. In that respect I will say at the outset that, in my view, to the extent to which rules defining the scope and nature of the data that can be transferred to the public authorities are intended to ensure that a measure that entails interference with the fundamental rights set out in Articles 7 and 8 of the Charter complies with the principles of legality and legal certainty, the sufficient clarity and precision of those rules must be assessed without having regard to the safeguards surrounding the processing operations to which those authorities will subject the data, since those safeguards only come into play in examination of the proportionality of the measure at issue. That is moreover how the Court assessed the headings in the draft Canada-EU PNR agreement in paragraphs 155 to 163 of Opinion 1/15. I would add, in more general terms, that particular attention should be paid to the need to maintain a clear distinction between the various phases of examination of a measure entailing interference with fundamental rights, and that where those various phases are amalgamated it is always, in my view, to the detriment of the effective protection of those rights.

149. In addition, I will merely note here, first, that the obligation on PIUs under Article 6(1) of the PNR Directive to delete data other than those listed in Annex I is irrelevant unless that annex contains a clear, closed list of the data to be transferred. The same is true of the obligation on PIUs under Article 13(4) of the PNR Directive to delete 'sensitive' data.[143] Indeed, a definition of the information to be transferred which is too vague, imprecise or open-ended increases both the probability that those data will be transferred indirectly and the risk that they will not be immediately identified and deleted. In other words, the safeguards referred to above can only meaningfully perform their function if the rules defining the nature and scope of the PNR data that air carriers are required to transfer to the PIUs are sufficiently clear and precise and if the list of those data is closed and exhaustive.

[142] See judgment of 17 October 2013, *Schwarz* (C-291/12, EU:C:2013:670, paragraph 32), concerning passport applicants who are required to have their fingerprints taken in order to obtain a document allowing them to travel to non-member countries.

[143] I will return to that category of data later in this Opinion.

150. On the basis of all the foregoing, as I have already indicated in point 135 of this Opinion, my view is that paragraph 12 of Annex I, in so far as it includes 'general remarks' among the data that air carriers are required to transfer to the PIUs under the PNR Directive, does not meet the requirements of clarity and precision laid down by Article 52(1) of the Charter as interpreted by the Court [144] and should therefore, to that extent, be found to be invalid.

151. In their written observations, the Commission and the Parliament have suggested that the Court should instead interpret paragraph 12 of Annex I 'in conformity with EU law', construing it as referring only to the information on minors explicitly mentioned in parentheses. I confess to having some difficulty in finding that reading not to go beyond what is merely an interpretation in conformity with EU law. It is admittedly true that, in accordance with a general principle of interpretation, an EU measure 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. [145] It is equally true that the fact that many of the recitals of the PNR Directive, in particular, emphasise the need fully to respect fundamental rights, the right to respect for private life and the principle of proportionality seems to suggest that such an interpretation of the directive is possible. [146] Nevertheless, consistent case-law has also established that an interpretation in conformity with EU law is only permissible where the wording of secondary EU law is open to more than one interpretation and it is therefore possible to give preference to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with that law. [147]

152. However, paragraph 12 of Annex I cannot, to my mind, be interpreted as the Commission and the Parliament suggest, unless it is construed *contra legem*. As indicated above, that paragraph covers a broad category of data of varying kinds, which cannot be identified in advance, of which data about minors is merely one subcategory. To read that paragraph as referring to that subcategory alone would not only amount to disregarding part of its wording but would also undermine the logical sequence of the statement it contains. Such an exercise, which consists in essence of removing the part of the wording of paragraph 12 of Annex I which is considered not to comply with the requirements as to clarity and precision, can in my view only be performed by partially annulling that paragraph.

153. The remainder of paragraph 12 of Annex I, which lists a series of data items concerning unaccompanied minors, does in my view satisfy the requirements as to clarity and precision provided it is interpreted as meaning that it encompasses only information concerning unaccompanied minors that is directly related to the flight and is expressly referred to in that paragraph.

144 The FRA expressed the same view in its Opinion 1/2011, p. 13. In its Opinion of 25 March 2011 on the proposal for a PNR directive (https://edps.europa.eu/sites/edp/files/publication/11-03-25_pnr_en.pdf), paragraph 47 ('EDPS opinion of 25 March 2011'), the EDPS proposed that the 'general remarks' heading should be excluded from the list in Annex I.

145 See, among others, judgments of 19 November 2009, *Sturgeon and Others* (C-402/07 and C-432/07, EU:C:2009:716, paragraph 47 and the case-law cited); of 19 September 2013, Review of *Commission* v *Strack* (C-579/12 RX-II, EU:C:2013:570, paragraph 40); and of 14 May 2019, *M and Others (Revocation of refugee status)* (C-391/16, C-77/17 and C-78/17, EU:C:2019:403, paragraph 77 and the case-law cited).

146 See in particular recitals 5, 7, 11, 15, 16, 20, 22, 23, 25, 27, 28, 31, 36 and 37 of the PNR Directive.

147 See judgments of 26 June 2007, *Ordre des barreaux francophones et germanophone and Others* (C-305/05, EU:C:2007:383, paragraph 28), and of 14 May 2019, *M and Others (Revocation of refugee status)* (C-391/16, C-77/17 and C-78/17, EU:C:2019:403, paragraph 77).

154. Paragraph 18 of Annex I is worded as follows:

'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).'

155. The structure of this paragraph is similar to that of paragraph 12 of Annex I. It also mentions a general category of data, that is to say, advance passenger information (API), followed, in parentheses, by a list of data considered to be included in that general category, which is given purely by way of example, as the use of the expression 'including' attests.

156. However, in contrast to paragraph 12 of Annex I, paragraph 18 refers to a category of data whose nature and scope are more easily identified. It is clear from recital 4 of the PNR Directive that where the directive refers to that category of data it is alluding to information which, under the API Directive, to which that recital makes direct reference, is transferred by air carriers to the competent national authorities for the purpose of improving border controls and combating illegal immigration. Those data are listed in Article 3(2) of the API Directive.

157. It is also apparent from recital 9 [148] of the PNR Directive and from Article 3(2) of the API Directive and the illustrative list contained in paragraph 18 of Annex I, that the API data to which that paragraph refers are, first, biographical data making it possible to verify the identity of the air passenger and, secondly, data about the flight booked. In respect specifically of the first category, biographical data, the information listed in Article 3(2) of the API Directive and paragraph 18 of Annex I encompasses data generated on check-in that can be taken from the machine-readable part of a passport (or other travel document). [149]

158. Paragraph 18 of Annex I, interpreted in the light of recitals 4 and 9 of the PNR Directive, does therefore in principle identify with sufficient clarity and precision at least the nature of the data it covers.

[148] In so far as relevant here, recital 9 provides that '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'.

[149] To that effect, see also the proposal for a PNR directive, p. 7, paragraph 1. The same data are contained in the Guidelines on advance passenger information (API) drawn up by the World Customs Organization (WCO), the International Air Transport Association (IATA) and the ICAO, http://www.wcoomd.org/~/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/api-guidelines-and-pnr-doc/apiguidelines_eng.pdf?db=web ('API guidelines'), paragraph 8.1.5(a) as 'Core Data Elements as may be found in the Machine Readable Zone of the Official Travel Document'.

159. As regards the scope of those data, first, the wording of Article 3(2) of the API Directive is likewise 'open-ended', since the list of data it contains is preceded by the expression 'the information referred to above shall comprise',[150] and, secondly, the category of API data as defined in the relevant multilateral harmonising instruments also includes data other than those referred to both by the API Directive and by paragraph 18 of Annex I.[151]

160. Under those circumstances, if paragraph 18 of Annex I is to meet the requirements as to clarity and precision to be met by legal bases that entail interference with Articles 7 and 8 of the Charter it must be interpreted as covering only the API data expressly listed in that paragraph and in Article 3(2) of the API Directive that have been collected by air carriers in the normal course of their business.[152]

161. At this stage it is worth briefly examining the other paragraphs of Annex I which, in view of their wording, are also 'open-ended' or are not sufficiently precise, even though the referring court has not expressly enquired of the Court in relation to those paragraphs.[153]

162. First, although paragraph 5 of Annex I, which refers to 'address and contact information (telephone number, email address)', must be regarded as referring only to the contact information expressly mentioned in parentheses and is therefore exhaustive, nevertheless, in common with the corresponding heading of the draft Canada-EU PNR agreement,[154] it does not specify whether that contact information refers to the passenger alone or to 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.[155] Since to interpret paragraph 5 of Annex I as also covering the categories of third party mentioned above would extend the interference entailed by the PNR Directive to persons other than air passengers within the meaning of Article 3(4) of the PNR Directive, in the absence of precise data on the basis of which it can be found that the systematic and generalised acquisition of the contact information of those third parties is strictly necessary to the efficacy of the system for the processing of PNR data established by that directive, I suggest that the Court should interpret that paragraph as referring only to the contact information expressly referred to in it relating to the air passenger on behalf of whom the reservation is made. Admittedly, the PNR Directive does not preclude the personal data of individuals other than air passengers being transferred to the PIUs.[156] It is nevertheless essential that the situations in which that is possible are indicated clearly and explicitly, as they are for travel agents, mentioned in paragraph 9 of Annex I, or the guardians of unaccompanied minors, referred to in paragraph 12 of that annex. Only if that condition is satisfied can it be found that the decision to include those data in those that must be

150 Article 3(2) of the API Directive reads as follows: '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.' I would point out that in its work programme 2022 (COM(2021) 645 final), p. 9, the Commission envisaged updating the API Directive. In September 2020 it published an evaluation of that directive (SWD(2020) 174 final), which constitutes the basis for its future revision ('2020 working document on the API directive'). In that document, the Commission highlights in particular the fact that the list of data in Article 3(2) of the API Directive is not coherent with the international standards on API data, in particular to the extent that it does not include all the data contained in the machine-readable zone of identity documents (see in particular p. 48).

151 See API guidelines, paragraph 8.1.5(b) and (c).

152 Paragraph 161 of Opinion 1/15 contains a similar interpretation of the corresponding heading of the draft Canada-EU PNR agreement.

153 I note that the Court is currently examining a series of questions referred for a preliminary ruling concerning specifically whether several paragraphs of Annex I are sufficiently precise, in particular paragraphs 4, 8, 12 and 18 (see Case C-215/20, pending).

154 See Opinion 1/15, paragraph 158.

155 I would note that information about the travel agency or agent is already covered by paragraph 5 of Annex I.

156 See the definition of PNR data in Article 3(5) of the PNR Directive.

transferred to the PIUs has weighed up the various interests at stake for the purposes of recital 15 of the PNR Directive, and the third parties concerned can be adequately informed that their personal data will be processed.

163. In so far as concerns, next, paragraph 6 of Annex I, relating to 'all forms of payment information, including billing address', in accordance with the Court's finding in paragraph 159 of Opinion 1/15 concerning the corresponding heading of the annex to the draft Canada-EU PNR agreement, in order to meet the requirements as to clarity and precision, that paragraph must be interpreted as 'covering information relating solely to the payment methods for, and billing of, the air ticket, to the exclusion of any other information not directly relating to the flight'. That information cannot, therefore, include information relating to the payment methods for other services not directly connected with the flight, such as vehicle rental on arrival. [157]

164. As regards paragraph 8, concerning 'frequent-flier information', that information is defined in the ICAO guidelines as relating to the frequent flyer account number and elite level status. [158] Interpreted in that way, that paragraph does satisfy the requirements as to clarity and precision.

165. Paragraph 10 of Annex I, concerning the 'travel status of passenger, including confirmations, check-in status, no-show or go-show information' and paragraph 13, concerning 'ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields', despite their open-ended wording, relate only to very precise and clearly identifiable information directly related to the flight. The same is true of paragraph 14 of Annex I, on the 'seat number and other seat information' and paragraph 16, on 'all baggage information'.

– *The scope of the data listed in Annex I (second question referred)*

166. The factors that the Court takes into account in assessing the proportionality of a measure that entails interference with the rights enshrined in Articles 7 and 8 of the Charter include whether the personal data processed are adequate, relevant and not excessive ('data minimisation'). [159] The same test has been established in the case-law of the ECtHR [160] and laid down in Convention 108. [161]

167. It can be seen from recital 15 of the PNR Directive that the list of the PNR data to be obtained by a PIU was drawn up with the objective of both reflecting the legitimate requirements of public authorities in relation to combating terrorism and serious crime and of protecting the fundamental rights to respect for private life and the protection of personal data by applying 'high standards' in accordance with the Charter, Convention 108 and the ECHR. The same recital states that, among other requirements, the PNR data should only contain details of passengers' reservations and travel itineraries that enable the competent authorities to identify air passengers who represent a threat to internal security.

157 See also, to that effect, Opinion of Advocate General Mengozzi in Opinion 1/15 (EU-Canada PNR Agreement) (EU:C:2016:656, point 218).

158 See the corresponding heading of Appendix 1 to the ICAO guidelines.

159 See to that effect, among others, *Digital Rights* judgment, paragraph 57. On the requirement that the categories of data covered by a measure allowing access must be limited to what is strictly necessary for the purpose concerned, see, lastly, *Prokuratuur* judgment, paragraph 38. The principle of data minimisation is established, inter alia, in Article 5(1)(c) of the GDPR and in Article 4(1)(c) of the Policing Directive.

160 See, among others, ECtHR judgment of 18 April 2013, *M.K. v. France* (CE:ECHR:2013:0418JUD001952209, § 35).

161 See 1981 explanatory report on Convention 108 (https://rm.coe.int/09000016800ca434), Article 5, paragraph 40, and the explanatory report on the modernised Convention 108, Article 5, paragraph 51.

168. As regards, first, whether the PNR data in Annex I are adequate and relevant, the various paragraphs of that annex, including paragraphs 5, 6, 8 and 18, as I propose they should be interpreted, [162] and paragraph 12, with the exception of the part that I propose should be found to be invalid, [163] concern only data providing information directly related to the flights covered by the PNR Directive. Those data also have an objective connection with the purposes pursued by that directive. Specifically, API data can be used 'reactively' to identify individuals already known to the law enforcement services, for example because they are suspected of being involved in terrorist offences or serious crimes that have already been committed or of being about to commit such an offence, whereas PNR data are more likely to be used 'in real time' or 'proactively' to identify threats from individuals not yet known to the law enforcement services.

169. Secondly, the PNR data listed in Annex I, including those in paragraphs 5, 6, 8 12 and 18 of that annex, interpreted as I propose in points 134 to 164 of this Opinion, do not appear to be excessive in scope, bearing in mind, on the one hand, the importance of the public security objective pursued by the PNR Directive and, on the other, the fact that the regime established by that directive is appropriate in the pursuit of that objective.

170. The API data in particular, about which the referring court has specific doubts, are biographical data relating to the journey undertaken and as a general rule allow only limited information to be taken about the private life of the passengers concerned. Furthermore, while paragraph 18 of Annex I does indeed cover information not included in that expressly mentioned in Article 3(2) of the API Directive, that information, on the identity of the air passengers (gender), the travel document used (country of issuance and expiry date of any identity document) and the flight (airline, flight number, date and port of departure and of arrival), partly overlaps with or can be extracted from the PNR data contained in other paragraphs of Annex I, for example paragraphs 3, 7 and 13. In addition, to the extent that it relates to biographical data or the travel documents used, that information can assist the law enforcement services in verifying the identity of an individual and, thereby, as recital 9 of the PNR Directive notes, reduce the risk that innocent people will undergo unjustified checks and investigations. Lastly, it should be noted that merely because paragraph 18 of Annex I includes data supplementary to those in Article 3(2) of the API Directive does not automatically mean that those data are excessive, since the API Directive and the PNR Directive pursue different objectives.

171. The data concerning unaccompanied minors, listed in paragraph 12 of Annex I, covers a category of vulnerable persons who enjoy particular protection, including as regards respect for their private life and the protection of their personal data. [164] It may nevertheless prove necessary to limit those rights, in particular to protect children from serious crime of which they may be victims, such as the trafficking and sexual exploitation of children or child abduction. Paragraph 12 of Annex I, in so far as it requires the transfer of a larger amount of personal data in relation to unaccompanied minors, cannot therefore, a priori, be regarded as going beyond what is strictly necessary.

172. Although the personal data that air carriers are required to transfer to the PIUs in accordance with the PNR Directive do to my mind meet the requirements that they must be adequate and relevant, and although their scope does not go beyond what is strictly necessary to the functioning of the regime established by that directive, that transfer nevertheless concerns a

[162] See points 154 to 158 and 162 to 164 of this Opinion.

[163] See points 133 to 153 of this Opinion.

[164] Children's right to respect for private life is enshrined in particular in Article 16 of the New York Convention on the Rights of the Child, adopted on 20 November 1989, which came into force on 2 September 1990.

significant quantity of wide-ranging personal data for each passenger concerned and an extremely large quantity of personal data in absolute terms. Accordingly, it is of paramount importance that such a transfer is accompanied by sufficient safeguards in order, first, to ensure that only the data expressly provided for are transferred and, secondly, to ensure the security and confidentiality of the data transferred.

173. It should be noted in that respect, on the one hand, that the EU legislature, first of all, established a series of safeguards in order to limit the categories of PNR data made accessible to the law enforcement services and to ensure that such access is confined to the data whose processing is considered to be necessary for the objectives pursued by the PNR Directive. Accordingly, first, subject to the observations made in the context of the reply to the third question referred, that directive lists exhaustively and precisely the data that can be transferred to the PIUs. Secondly, the PNR Directive states explicitly that only the data on that list, which is the outcome of weighing up the various interests and requirements referred to in recital 15 of that directive, may be transferred to the PIUs (Article 6(1) of the PNR Directive). Thirdly, that directive stipulates that where the PNR data transferred include data other than those listed in Annex I, the PIUs are to delete such data 'immediately and permanently upon receipt' (Article 6(1) of the PNR Directive). Fourthly, that directive provides that the PNR data referred to in Annex I may only be transferred to the extent that they have already been collected by the air carriers in the normal course of their activities (Article 8(1) and recital 8 of the PNR Directive), which means that not all the data included in Annex I are systematically accessible to the PIUs, but rather only those included in the reservation system of the operator concerned. Fifthly, Article 8(1) of the PNR Directive requires air carriers to use the 'push' method to transfer PNR data to the PIUs. That method, which is recommended in the ICAO guidelines,[165] involves the air carriers themselves transferring the PNR data into the PIUs' databases. Compared with the 'pull' method, in which the competent authorities have access to the operators' systems and can take a copy of the data required from their databases, the 'push' method offers more safeguards because it gives the air carrier concerned a role as guardian and supervisor of the PNR data. Lastly, following the ICAO guidelines and the 'single window' principle,[166] the PNR Directive provides that PNR data will be transferred via a single body, the PIU, acting under the supervision of the data protection officer referred to in Article 5 of that directive and, in particular, under the supervision of the national supervisory authority referred to in Article 15.

174. On the other hand, the PNR Directive establishes a number of safeguards intended to preserve the *security* of PNR data. I refer in that respect to Article 13(2) of that directive, according to which Articles 28 and 29 of the Policing Directive, on the confidentiality of processing and data security, apply to all the personal data processing operations performed under that directive, and to Article 13(3) which recalls, in relation to the processing of PNR data by air carriers, the obligations on those carriers under the GDPR, in particular in relation to the appropriate technical and organisational measures to be taken to protect the security and confidentiality of those data.[167]

165 See paragraph 2.7.3 of the ICAO guidelines.

166 See paragraph 2.7.4 of the ICAO guidelines.

167 The requirement to ensure that data are transferred to the PIUs securely and reliably is also recalled in Article 16(1) of the PNR Directive on the electronic means used for that transfer and was one of the criteria followed by the Commission when adopting the common protocols and data formats to be used by air carriers for those transfers, as required in Article 16(3). See Commission Implementing Decision (EU) 2017/759 of 28 April 2017 on the common protocols and data formats to be used by air carriers when transferring PNR data to Passenger Information Units (OJ 2017 L 113, p. 48).

175. Lastly, it should be emphasised that in recitals 29 and 37 the PNR Directive recognises that passengers are entitled to be provided with 'accurate information that is easily accessible and easy to understand' about, inter alia, the collection of PNR data, and exhorts the Member States to ensure that this right is upheld. Although acknowledgement of that right is not translated into a binding provision in the text of the PNR Directive, I would note, as I did when examining the first question referred, that the provisions of the GDPR apply to the transfer of PNR data to the PIUs. Air carriers must therefore, when transferring those data, comply in particular with Articles 13 and 14 of the GDPR, according to which data subjects whose personal data are processed are entitled to be provided with information. Whereas it is desirable that Member States, when transposing the PNR Directive, expressly establish the right of air passengers to be provided with information, as recognised in recitals 29 and 37 of that directive, they are in any event precluded from restricting the scope of Articles 13 and 14 of the GDPR by virtue of Article 23(1) of that regulation, since to do so would contravene the spirit of the PNR Directive. To be effective, that right must also attach to the categories of PNR data being transferred.

176. In the light of all the foregoing, my view is that, subject to the limitations suggested and the clarifications made under the third question referred, the PNR data whose processing is provided for by the PNR Directive are relevant, adequate and not excessive in the light of the purposes pursued by that directive and that their scope does not go beyond what is strictly necessary to achieve those purposes.

– *Sensitive data*

177. The PNR Directive contains a general prohibition on the processing of 'sensitive data'. [168]

178. Although that directive does not define 'sensitive data', it is apparent from Article 13(4) of that directive that they include, at least, 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.' [169] In paragraph 165 of Opinion 1/15, the Court clarified that any measure based on the premiss that one or more of those characteristics 'may be relevant, in itself or in themselves and regardless of the individual conduct of the traveller concerned, having regard to the purpose for which PNR data is to be processed, would infringe the rights guaranteed in Articles 7 and 8 of the Charter, read in conjunction with Article 21 thereof'. By prohibiting any processing of the data referred to in Article 13(4), the PNR Directive therefore adheres to the limits that the Court has imposed on the use of those categories of data in the context of a system for the processing of PNR data, whether it is established by national law, EU law or an international agreement entered into by the European Union.

179. The general prohibition on the processing of sensitive data established by the PNR Directive also includes the *collection* of those data. As recital 15 of that directive expressly states, the 19 headings in Annex I are not based on the PNR data referred to in Article 13(4).

180. Although none of those headings refers explicitly to such data, those data may nevertheless be covered in particular by the 'general remarks' heading, referred to in paragraph 12 of Annex I, which is an 'open-ended field' and may include, as I have already had occasion to observe when examining the third question referred, an undefined number of diverse items of information.

168 See recital 37 of the PNR Directive.

169 The categories of personal data listed in Article 13(4) of the PNR Directive are all included among the categories defined as 'special categories of personal data' for the purposes of Article 9(1) of the GDPR.

Indeed, there is an actual risk, as the Court moreover noted in paragraph 164 of Opinion 1/15, that information falling under that heading and relating, for example, to dietary preferences, requests for assistance or price packages given to certain categories of persons or associations, may indirectly reveal sensitive data as referred to in Article 13(4) of the PNR Directive, concerning in particular the religious beliefs of the passengers concerned, their health or membership of a trade union or political party.

181. Since the processing of those data is in any event prohibited by the PNR Directive, their transfer by air carriers not only manifestly goes beyond what is strictly necessary but is also completely pointless. It is important to note in that respect that the fact that the PIUs must in any case, under the second sentence of Article 13(4) of the PNR Directive, immediately delete PNR data that reveals any of the information listed in the first sentence of that paragraph does not authorise or justify a transfer of those data,[170] since the prohibition on processing those data established by that directive must apply from the first stage of the processing of PNR data. The obligation to delete sensitive data is therefore merely a supplementary safeguard laid down by the directive in case, exceptionally, such data are transferred to the PIUs by mistake.

182. I also note, as Advocate General Mengozzi remarked in point 222 of his Opinion in Opinion 1/15,[171] that since the information under the 'free text' headings, such as the 'general remarks' heading in paragraph 12 of Annex I, that may contain sensitive data under Article 13(4) of the PNR Directive are communicated by passengers only on an optional basis, it is improbable that individuals involved in terrorist offences or serious crime will spontaneously communicate that information, with the effect that the systematic transfer of those data is in the majority likely to concern only individuals who have requested an additional service and are not in reality of any interest to the law enforcement services.[172]

183. In my examination of the third question referred, I have reached the conclusion that paragraph 12 of Annex I, to the extent that it relates to the 'general remarks' heading, does not satisfy the requirements as to clarity and precision laid down by the first sentence of Article 52(1) of the Charter. For the reasons set out above, I believe that including that heading in the categories of data that can be transferred systematically to the PIUs, without specifying which information may fall under it, likewise does not satisfy the necessity criterion established in the second sentence of Article 52(1) of the Charter, as interpreted by the Court.[173]

184. Nevertheless, excluding the 'free text' headings from the list of PNR data to be transferred to State authorities under the system for the processing of PNR data is not sufficient to eliminate the risk that sensitive data may nevertheless be made available to those authorities. Such data may in fact be both directly inferred from information under those headings and indirectly revealed or presumed on the basis of information contained in 'coded' headings. For example, an air passenger's name may provide indications or, at the very least, allow assumptions to be made, about the ethnic origin or religious affiliation of the passenger concerned. The same is true of nationality. Those data are not, in principle, easy to exclude from the list of PNR data to be transferred, or easily deleted by the authorities entitled to receive them. Accordingly, to avoid the

170 The claims advanced by several Member States who submitted observations on the second question referred, that there are technical means by which sensitive data transmitted by air carriers can easily be deleted, are to my mind irrelevant.

171 Opinion of Advocate General Mengozzi, Opinion 1/15 *(EU-Canada PNR Agreement)* (EU:C:2016:656).

172 I note that even the ICAO guidelines, while not denying that sensitive data that may be taken from the 'free text' headings may be relevant in determining the risk that a passenger might represent, nevertheless recommend that the Contracting States ensure that they are taken into consideration only if concrete indications exist which require the use of such data for the purposes pursued by their PNR schemes.

173 I call to mind that the EDPS had already suggested that that heading be excluded, in its opinion of 25 March 2011, paragraph 47.

risk that a large number of individuals who are nevertheless not suspected of any offence will be stigmatised on the basis of protected characteristics, a system for the processing of PNR data must establish sufficient safeguards to ensure, at each stage, that the processing of the data collected cannot directly or indirectly take those characteristics into account, for example by applying selectors based on them in the automated analysis. I will return to this issue later in my examination.

185. On the basis of all the foregoing, subject to the conclusion I reached in point 183 above, my view is that the PNR Directive does establish sufficient guarantees to protect sensitive data, at the stage at which PNR data are transferred to the PIUs.

(iii) The definition of a 'passenger' (fourth question referred)

186. By its fourth question, the referring court asks the Court in essence whether the system established by the PNR Directive is compatible with Articles 7, 8 and Article 52(1) of the Charter, to the extent that it permits the generalised transfer and processing of the PNR data of any person covered by the definition of 'passenger' within the meaning of Article 3(4) of that directive, regardless of whether there is any objective ground for considering that the data subject may present a risk to public security. It enquires in particular whether the Court's case-law on the retention of and access to data in the electronic communications sector can be transposed to the system for the processing of personal data established by the PNR Directive.

187. In that case-law, in so far as concerns these proceedings, the Court has held that legislation which, in order to combat serious crime, provides for the generalised and indiscriminate preventive *retention* of traffic data relating to electronic communications and location data,[174] so that the law enforcement authorities can have access to those data, without any differentiation, limitation or exception being made in the light of the objective pursued, cannot, in principle, be justified in a democratic society.[175] The Court made the same finding in respect of national legislation which, in order to combat terrorism, provided for the *automated analysis of all those data* by means of screening carried out by providers of electronic communications services at the request of the competent national authorities and applying the parameters set by those authorities.[176] According to the Court, such measures can only be justified in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable and where the decision imposing such measures is subject to effective review, either by a court or by an independent administrative body.[177] The use of those measures in such situations must, furthermore, according to the Court, be limited in time to what is strictly necessary and cannot in any event be systematic in nature.[178]

174 This refers to data that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses.

175 See, to that effect, *La Quadrature du Net* judgment, paragraphs 141 to 145, and *Tele2 Sverige* judgment, paragraphs 105 and 106, concerning the interpretation of Article 15(1) of Directive 2002/58, read in conjunction with Articles 7, 8 and 11 and Article 52(1) of the Charter, and *Digital Rights* judgment, paragraphs 57 and 58, in which the Court declared Directive 2006/24 invalid.

176 See *La Quadrature du Net* judgment, paragraph 177.

177 See *La Quadrature du Net* judgment, paragraphs 134 to 139 and 177. According to the Court, the Member States' responsibility in respect of national security 'corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities'. See *La Quadrature du Net* judgment, paragraph 135, and *Privacy International* judgment, paragraph 74.

178 See *La Quadrature du Net* judgment, paragraphs 138 and 178.

188. I note, furthermore, that although the Court did not go so far in that case-law as expressly to confirm that the essence of the right to respect for private life was compromised, as it did in the *Schrems I* judgment, it nevertheless found that the measures in question involved interference of a level of seriousness such that, with the exception of the limited instance of specific threats to the national security of a Member State, it was quite simply impossible to regard them as limited to what was strictly necessary and therefore in accordance with the Charter,[179] irrespective of any safeguards that may have been established against the risk of abuse and unlawful access to the data concerned.[180]

189. I have already had occasion to emphasise that rules such as those laid down by the PNR Directive and measures of the kind examined by the Court in the case-law summarised in the preceding points of this Opinion have a number of elements in common which make them particularly intrusive. That directive establishes a system for the generalised and indiscriminate collection and automated analysis of the personal data of a significant portion of the population, and applies comprehensively to everyone covered by the definition of 'passenger' in Article 3(4) of that directive and, in consequence, also to people for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with terrorist activities or serious crime. It is against that background that the referring court enquires whether that case-law can be transposed to a PNR data processing system such as that established by the PNR Directive.

190. I note in that respect that when the Court examined the scope *ratione personae* of the draft Canada-EU PNR agreement, in paragraphs 186 to 189 of Opinion 1/15, it avoided drawing any parallel between measures for the generalised and indiscriminate retention and access to the contents of electronic communications, traffic data and location data, on the one hand, and the transfer and automated processing of PNR data as part of the advance assessment of passengers under that agreement, on the other. At the time that opinion was delivered, there was nevertheless already well-established case-law – which had been confirmed only a few months previously by the *Tele2 Sverige* judgment, to which the referring court alludes – in which, save in specific individual situations,[181] those measures were found to be incompatible with the Charter.[182] The Court's more recent judgments in that field, in particular the *La Quadrature du Net* judgment, are directly in line with that case-law which they clarify and, in some respects, qualify.

191. In those paragraphs of Opinion 1/15, the Court explicitly found that the Canada-EU PNR Agreement did not appear to go beyond what was strictly necessary in so far as it allowed the *transfer* and the *automated processing* of PNR data of all passengers flying into Canada, for the purpose of their advance assessment, even though that transfer and that processing were assumed to take place 'regardless of whether there is any objective evidence permitting the inference that the passengers are liable to present a risk to public security in Canada'.[183] In paragraph 187 of that opinion, the Court even stated that 'the exclusion of certain categories of persons, or of certain areas of origin, would be liable to prevent the achievement of the objective

179 See, inter alia, *La Quadrature du Net* judgment, paragraphs 141 to 145.

180 See *La Quadrature du Net* judgment, paragraphs 115 and 116; see also Opinion of Advocate General Campos Sanchéz-Bordona in Joined Cases *SpaceNet and Telekom Deutschland* (C-793/19 and C-794/19, EU:C:2021:939, points 74 and 75).

181 See *Tele2 Sverige* judgment, paragraph 119.

182 See, to that effect, *Tele2 Sverige* judgment, paragraphs 103 to 107 and 119 and the case-law cited.

183 See Opinion 1/15, paragraphs 186 and 187.

of automated processing of PNR data, namely identifying, through verification of those 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'. [184]

192. Accordingly, at least in respect of the generalised and indiscriminate transfer of PNR data, the Court has distanced itself from the more rigorous approach taken in relation to the retention of and access to metadata.

193. Although, as can be seen in particular from paragraphs 152 and 188 of Opinion 1/15, the Court undeniably took into account in its reasoning, first, the finding that the automated processing of PNR data facilitates security checks, in particular at borders, and, secondly, the fact that, under the Chicago Convention, air passengers wishing to enter the territory of a the State Party to that convention must undergo the checks and comply with the conditions on entry and departure laid down by that State, including the verification of their PNR data, I believe there are other reasons militating in favour of that different approach, including, primarily, the nature of the data being processed.

194. The Court has repeatedly emphasised that not only the contents of electronic communications but also metadata may reveal information on 'a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health'; that those data, taken as a whole, 'may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them'; and that those data provide, in particular, the means of establishing 'a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications'. [185] I note furthermore that the rules examined by the Court to date, including those in Directive 2006/24, did not establish any exceptions and also applied to communications to or from social or religious services or professionals subject to a duty of professional secrecy. Accordingly, although it did not find that the essence of the right to respect for private life had been infringed, the Court nevertheless stated that 'in view of the sensitive nature of the information that traffic and location data may provide, the confidentiality of that data is essential for the right to respect for private life'. [186]

195. In contrast, although, as I noted in points 77 and 98 of this Opinion, in Opinion 1/15 the Court did indeed acknowledge that PNR data may in some circumstances reveal very precise information concerning a person's private life, [187] it nevertheless stated that the nature of that information is limited to certain aspects of that private life, [188] with the effect that access to those data is less intrusive than access to the contents of electronic communications or to traffic and location data.

184 In both the *Digital Rights* and *Tele2 Sverige* judgments (paragraphs 59 and 111 respectively) and in subsequent case-law (see, among others, *La Quadrature du Net* judgment, paragraphs 143 to 150), it is precisely the fact that the legislation concerned was not based on 'objective evidence' of the kind mentioned by the Court in paragraph 187 of Opinion 1/15 which makes it possible to target a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, that made that legislation disproportionate.

185 See *La Quadrature du Net* judgment, paragraph 117 and the case-law cited; see also *Prokuratuur* judgment, paragraph 36.

186 *La Quadrature du Net* judgment, paragraph 142.

187 See Opinion 1/15, paragraphs 128 and 150.

188 See Opinion 1/15, paragraph 150.

196. Secondly, not only do PNR data differ in nature from traffic and location data, but the amount and variety of the information that those various categories of data can reveal varies, since the information contained in PNR data is both quantitatively and qualitatively more limited. That fact is dictated both by the fact that systems for the generalised and indiscriminate processing of electronic communications data may affect nearly the whole of the target population, whereas systems for the processing of PNR data apply to a smaller, albeit numerically significant, group of individuals, and by the frequency with which means of electronic communication are used and the large number of those means. In addition, the PNR Directive provides for the collection and processing of a limited number of exhaustively defined items of PNR data, and excludes data falling within the categories listed in Article 13(4) of that directive, with the effect that at the very least the sensitivity, if not the quantity, of the information concerning the private life of the data subjects that may result from those data can, in part, be assessed in advance.[189] In the case of traffic and location data, it is only possible in part to limit the typology of the data concerned, and thereby to exclude much of the data that may contain sensitive information, given the number of users and means of communication involved.[190]

197. Thirdly, any processing of electronic communications metadata is not only capable of affecting the private sphere of almost the entire population, but also encroaches upon the exercise of other freedoms through which each individual participates in the social and democratic life of a country,[191] and, in particular, is liable to have a deterrent effect on the freedom of expression of users of means of electronic communication,[192] which constitutes 'one of the essential foundations of a pluralist, democratic society' and is one of the values on which the European Union is founded.[193] That aspect is inherent in the measures relating to those categories of personal data and in principle does not concern PNR data processing systems.

198. Fourthly, as a result primarily of the quantity and variety of sensitive information that can be extracted from the contents of electronic communications and from traffic and location data, the likelihood of arbitrariness is significantly higher in relation to the processing of those data than in respect of the systems for processing PNR data.

199. For all the reasons set out above, I submit that the stricter approach that the Court has followed in relation to electronic communications cannot be transposed as such to the systems for processing PNR data. The Court has already expressed that view, at least by implication, in Opinion 1/15, in relation to an international agreement establishing a system intended to protect the security of a third country. To my mind, the same position is even more justified in relation to the PNR Directive, whose objective is to protect the internal security of the European Union.

200. Moreover, it should be noted, in common with Advocate General Mengozzi in point 216 of his Opinion in Opinion 1/15,[194] that the raison d'être of systems for the processing of PNR data, whether they are adopted unilaterally or form the subject matter of an international agreement, is specifically to guarantee the bulk transfer of data that will allow the competent authorities to identify, with the assistance of automated processing tools and pre-determined scenarios or assessment criteria, individuals not known to the law enforcement services who may nonetheless

189 On the difficulty of such an assessment in relation to metadata, see *Prokuratuur* judgment, paragraph 40.

190 The German legislature attempted to do so in the legislation at issue in Joined Cases C-793/19 and C-794/19, *SpaceNet and Telekom Deutschland*, in which Advocate General Campos Sánchez-Bordona delivered his Opinion (EU:C:2021:939, points 60 and 61).

191 I refer in that respect to point 93 of this Opinion.

192 See *La Quadrature du Net* judgment, paragraph 118 and the case-law cited.

193 See *Tele2 Sverige* judgment, paragraph 93.

194 Opinion of Advocate General Mengozzi in Opinion 1/15 *(EU-Canada PNR Agreement)*, EU:C:2016:656.

present an 'interest' or a risk to public security and who are therefore liable to be subjected subsequently to more thorough individual checks. The requirement of a 'reasonable suspicion', found in the ECtHR case-law on targeted interception in criminal investigations [195] and in the Court's case-law on the retention of metadata [196] is, therefore, less relevant in the context of the transfer and processing just described. [197] The preventive objective of those schemes likewise cannot be achieved if their application is limited to a specific category of individuals, as the Court moreover confirmed in the points of Opinion 1/15 summarised in point 191 of this Opinion, and the scope of the PNR Directive therefore seems to ensure the effective attainment of that objective. [198]

201. The Commission has several times highlighted the strategic importance of the processing of PNR data as a vital tool in the EU common response to terrorism and serious crime and as a significant component of the Security Union. [199] As part of a 'global approach' to combating terrorism, the role of systems for the processing of PNR data has also been acknowledged by the United Nations Security Council which, in resolution 2396 (2017), [200] required its Member States to 'develop the capability to collect, process and analyse, in furtherance of ICAO standards and recommended practices, [PNR] data and to ensure PNR data is used by and shared with all their competent national authorities, with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offenses and related travel'. [201] That obligation was reaffirmed in resolution 2482 (2019) on terrorism and serious transnational crime. [202]

202. In that context, the adoption at EU level of a harmonised system for the processing of PNR data, both in relation to extra-EU flights and, for countries that have availed themselves of Article 2 of the PNR Directive, intra-EU flights, ensures that those data are processed in accordance with the high level of protection of the rights enshrined in Articles 7 and 8 of the Charter set by that directive and provides a benchmark legal system for negotiating international agreements on the processing and transfer of PNR data. [203]

203. Furthermore, whilst admittedly the system established by the PNR Directive concerns all air passengers indiscriminately, as the Parliament among others quite correctly noted in its written observations, and as the United Nations Security Council likewise highlighted in resolution 2396 (2017), which refers to the specific risk of civil aviation being used for terrorist purposes both as a

195 See among others, ECtHR, judgment of 4 December 2015, *Roman Zakharov v. Russia* (CE:ECHR:2015:1204JUD004714306, § 260).

196 See *La Quadrature du Net* judgment, paragraphs 146 to 151, and the *Tele2 Sverige* judgment, paragraph 119.

197 In relation to bulk interception measures, see *Big Brother Watch* judgment, § 348.

198 See, by analogy, judgment of 3 October 2019, *A and Others* (C-70/18, EU:C:2019:823, paragraph 61).

199 See, recently, Commission Communication on the EU Security Union Strategy, ((COM(2020) 605 final), p. 28) and Commission Communication: A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond (COM(2020) 795 final. p. 15 et seq.).

200 Resolution 21 December 2017 ('resolution 2396 (2017)'), https://undocs.org/en/S/RES/2396(2017).

201 See resolution 2396 (2017), paragraph 12. In the same paragraph, the United Nations Security Council 'urges ICAO to work with its Member States to establish a standard for the collection, use, processing and protection of PNR data'. Following that invitation, on 23 June 2020, the ICAO adopted Amendment 28 to Annex 9 to the Chicago Convention which, as already indicated, lays down international standards on facilitation and Chapter 9, Section D of which relates specifically to PNR. On 12 January 2021, the Commission adopted a proposal for a Council decision on the position to be taken on behalf of the European Union in the ICAO as regards that amendment (COM(2021) 16 final).

202 Resolution of 19 July 2019, paragraph 15(c) https://undocs.org/en/S/RES/2482(2019).

203 The European Union has currently concluded two international agreements, with Australia (Agreement between the European Union and Australia on the processing and transfer of [PNR data] by air carriers to the Australian Customs and Border Protection Service (OJ 2012 L 186, p. 4)) and the United States of America (Agreement between the United States of America and the European Union on the use and transfer of [PNR data] to the United States Department of Homeland Security (OJ 2012 L 215, p. 5)), respectively. A joint evaluation of both those agreements is in progress, with a view to concluding new agreements. On 18 February 2020, the Council also authorised the Commission to begin negotiations with Japan.

means of transportation and as a target,[204] there is an objective link between air transport and threats to public security in the service of, in particular, terrorism and, at the very least, certain forms of serious crime such as drug trafficking and people trafficking which, moreover, have a significant cross-border dimension.

204. Lastly, it should be noted, together with the Parliament, the Council and several Member States which have submitted written observations, that air passengers entering or leaving the European Union are obliged to undergo security checks.[205] As the Court also noted in Opinion 1/15, the transfer and processing of PNR data before arrival or before departure facilitates and speeds up those checks, by allowing the law enforcement services to concentrate on passengers for whom they have a fact-based reason to believe that they might pose an actual risk to security.[206]

205. Lastly, although it cannot be determined a priori that the extension of the system under the PNR Directive to intra-EU flights will not have any impact on the freedom of movement of Union citizens, enshrined in particular in Article 45 of the Charter, I do not believe that the interference with private life that the PNR Directive entails, although serious, is in itself such as to have a deterrent effect on the exercise of that freedom, and the public may even perceive the processing of PNR data to be a necessary measure in order to ensure that air travel is secure.[207] The possibility of such a deterrent effect must nevertheless be continuously assessed and monitored.

206. However, if it is to comply with the case-law summarised in points 107 and 108 of this Opinion, the PNR Directive cannot be limited to requiring that access to and the automated processing of the data of all air passengers be consistent with the objective pursued; it must also lay down clearly and precisely the substantive and procedural conditions governing that access and processing and the subsequent use of those data[208] and must establish appropriate safeguards at each stage of that process. In my examination of the second question referred, I have already alluded to the safeguards surrounding the transfer of PNR data to the PIUs. When examining the sixth question, I will review the safeguards that more specifically accompany the automated processing of those data and, as part of my examination of the eighth question, those relating to the retention of those data.

207. Before embarking on that examination, I would draw attention to the crucial importance, in the context of the system of safeguards put in place by the PNR Directive, of supervision by the independent authority referred to in Article 15 of that directive. According to that article, any data processing established by that directive is subject to supervision by an independent supervisory authority which has power to verify the lawfulness of that processing, conduct investigations, inspections and audits and deal with complaints lodged by any data subject. That supervision, carried out by an external agency responsible for protecting interests that potentially conflict with those of parties that process PNR data, which is entrusted with the role of ensuring compliance with all the limitations and guarantees that circumscribe that processing, is an essential safeguard, explicitly set out in Article 8(3) of the Charter, which protects the fundamental rights concerned even more effectively than the system of remedies provided for individuals. I therefore believe it is fundamental that the Court should interpret the scope of the

[204] See resolution 2396 (2017), p. 4.

[205] Including individuals with a right to move freely under EU law, see Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders (OJ 2017 L 74, p. 7).

[206] See also, to that effect, Opinion 1/15, paragraph 187. See also Commission Communication on the global approach to transfers of [PNR] data to third countries (COM(2010) 492 final, p. 6, paragraph 2.2).

[207] That is, after a fashion, what the Commission is implying in its proposal for a PNR directive, p. 3.

[208] See, to that effect, *Prokuratuur* judgment, paragraph 49 and the case-law cited.

supervisory powers laid down in Article 15 of the PNR Directive broadly and that, when transposing that directive into internal law, the Member States should grant the national supervisory authority those powers to their full extent by providing it with the material and human resources necessary to perform its functions.

208. On the basis of all the foregoing, my view is that the PNR Directive does not go beyond what is strictly necessary by allowing the transfer and automated processing of the data of any person meeting the definition of 'passenger' within the meaning of Article 3(4) of that directive.

(iv) Whether the advance passenger assessment is sufficiently clear, precise and limited to what is strictly necessary (sixth question referred)

209. By its sixth question, the referring court asks the Court in essence whether the advance assessment referred to in Article 6 of the PNR Directive is compatible with Articles 7, 8 and Article 52(1) of the Charter. Although the wording of that question focuses on the fact that the advance assessment entails automated processing of the PNR data of all passengers which is systematic and generalised, it emerges from the grounds of the order for reference that the Cour constitutionnelle (Constitutional Court) is seeking from the Court a more comprehensive assessment of whether the requirements of legality and proportionality are complied with in the context of that processing. I will now conduct that assessment, although referring to the analysis carried out in examination of the fourth question referred as regards the fact that the automated processing in question is non-targeted.

210. Under Article 6(2)(a) of the PNR Directive, the PIUs must carry out an advance assessment of air passengers prior to their scheduled arrival in or departure from the Member State. That assessment is intended to identify persons who require further examination by the competent authorities 'in view of the fact that such persons may be involved in a terrorist offence or serious crime'. Under Article 6(6) of the PNR Directive, the PIU of a Member State is to transmit the PNR data of persons identified in that assessment or the result of processing those data to the competent authorities referred to in Article 7 of the said directive, of the same Member State, for 'further examination'.

211. According to Article 6(3) of the PNR Directive, the advance assessment under Article 6(2)(a) is carried out by cross-checking the PNR data against 'relevant' databases (Article 6(3)(a)) or by processing them against pre-determined criteria (Article 6(3)(b)).

212. Before beginning to examine each of those two types of data processing, I would note that it is not clear from the wording of Article 6(3) whether the Member States are required to stipulate that the advance assessment of passengers must be carried out by systematically and in all circumstances conducting both types of automated analysis or whether, as appears to be corroborated by the use of the verb 'may' and the disjunctive conjunction 'or', they have power to organise their systems so that, for example, the examination under Article 6(3)(b) is reserved for specific situations. I would clarify in that respect that the proposal for a PNR directive provided that the advance assessment was to be carried out only in the context of combating serious transnational crime. [209]

[209] See Article 4(2)(a) of the proposal for a PNR directive.

213. Like the Commission, I believe it is apparent in particular from the scheme of the PNR Directive that the Member States are obliged to provide for both types of automated processing, for reasons also connected with the need to ensure that the EU system for the processing of PNR data is applied as uniformly as possible. However, that does not mean that the Member States are not permitted – and even required, in order to ensure that the data processing involved in the advance assessment conducted under Article 6(2)(a) of the PNR Directive is limited to what is strictly necessary – to circumscribe the analysis under Article 6(3)(b) of the PNR Directive according to how effective it is as regards each of the offences covered by the directive and, where applicable, to reserve it for only some of those offences. Recital 7 of the PNR Directive militates in favour of that interpretation, providing as it does that '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'.

– *Comparison of data against databases within the meaning of Article 6(3)(a) of the PNR Directive*

214. According to Article 6(3)(a), the first limb of the advance assessment carried out by the PIUs under Article 6(2)(a) of the PNR Directive involves comparing the PNR data against databases ('data matching') to find any hits. Those hits are then verified by the PIUs, in accordance with Article 6(5) of the PNR Directive and, where appropriate, converted to 'matches' before being reported to the competent authorities.

215. As the Court acknowledged in paragraph 172 of Opinion 1/15, the extent to which automated analyses of that kind interfere with the rights enshrined in Articles 7 and 8 of the Charter depends essentially on the databases on which those analyses are based. It is therefore essential that the provisions establishing that data processing identify sufficiently clearly and precisely the databases with which cross-checking of the data to be processed is permitted.

216. Under Article 6(3)(a) of the PNR Directive, the PIUs are to compare the PNR data against databases that are 'relevant'[210] to the objectives pursued by the directive. That provision also refers to a specific category of database, that is to say, databases of 'persons or objects sought or under alert', which the EU legislature therefore intended explicitly to classify as 'relevant' within the meaning of that provision.

217. Apart from that specification, the concept of 'relevant' databases is not further explained. In particular, the directive does not indicate whether, in order to be regarded as 'relevant', the databases used to cross-check PNR data must be managed by law enforcement authorities or by any public authority in general, or merely need to be directly or indirectly accessible to those authorities. Nor does it further specify the nature of the data that those databases may contain or their relationship to the objectives pursued by the PNR Directive.[211] It is also apparent from the

[210] Although in the French-language version Article 6(3)(a) refers to 'useful databases' ('bases de données utiles'), in the majority of the other language versions, that provision refers instead to 'relevant databases': see, in particular, the versions in Spanish ('pertinentes'), German ('massgeblich'), English ('relevant'), Italian ('pertinenti'), Dutch ('relevant') and Portuguese ('relevantes').

[211] As it is drafted, Article 6(3)(a) of the PNR Directive seems to permit analyses that take the form of data mining by cross-checking against very varied data, provided that data mining is aimed at furthering the objectives of that directive. On the risks associated with data mining in relation to PNR data, see Korff report, p. 77. In its opinion of 25 March 2011, paragraph 18, the EDPS stressed the lack of clarity and predictability in identifying the databases against which PNR data can be compared.

wording of Article 6(3)(a) of the PNR Directive that national, EU and international databases can all be classified as 'relevant' databases, which further expands the list of databases potentially covered and renders the concept even more open-ended. [212]

218. Under those circumstances, applying the general principle of interpretation recalled in point 151 of this Opinion, it is for the Court, in so far as possible, to interpret Article 6(3)(a) of the PNR Directive, and the concept of 'relevant' databases in particular, in accordance with the Charter requirements as to clarity and precision. Furthermore, since that provision envisages interference with the fundamental rights set out in Articles 7 and 8 of the Charter, it must be interpreted restrictively, taking into consideration the requirement to ensure a high level of protection of those fundamental rights, as stated in particular in recital 15 of the PNR Directive. It must also be interpreted in the light of the principle, set out in Article 1(2) of the PNR Directive, that PNR data may only be processed for limited purposes.

219. In the light of those criteria, the concept of 'relevant' databases should in my view be interpreted as covering only the national databases managed by the competent authorities under Article 7(1) of the PNR Directive and EU and international databases used directly by those authorities in the course of their work. Those databases must in addition relate directly and closely to the purposes of combating terrorism and serious crime pursued by the PNR Directive, thereby implying that they must have been developed for those purposes. Interpreted in that way, the concept covers, fundamentally if not exclusively, the databases on persons or objects sought or under alert explicitly referred to in Article 6(3)(a) of the PNR Directive.

220. Databases managed or used by the Member States' intelligence services in general fall outside the concept of 'relevant' databases, unless they comply strictly with the requirement that they must relate closely to the objectives pursued by the PNR Directive and the Member State in question confers specific law enforcement powers on its intelligence services. [213]

221. The interpretation proposed above complies with the recommendations made by the Court in paragraph 172 of Opinion 1/15.

222. Nevertheless, even interpreted in that way, Article 6(3)(a) of the PNR Directive does not enable the databases that will be used by the Member States when cross-checking PNR data to be identified with sufficient precision, and cannot be found to satisfy the requirements under Article 52(1) of the Charter, as interpreted by the Court. That provision must therefore be construed as meaning that it obliges the Member States to publish a list of those databases when they transpose the PNR Directive into national law, and to keep it up to date. In my view, a list should also be drawn up at EU level of the 'relevant' databases within the meaning of Article 6(3)(a) of the PNR Directive that are managed by the European Union in collaboration with the Member States, and of the international databases, so that practice in that respect is uniform in the Member States.

[212] The vague and open-ended wording of Article 6(3)(a) of the PNR Directive is reflected in its very varied transposition into national law, ranging from a strict interpretation of 'relevant' databases which limits the analysis provided for to comparison against the databases explicitly mentioned in that provision (this is the case in the Federal Republic of Germany, as can be seen from its government's observations submitted to the Court) to a broader interpretation encompassing any database available or accessible to the competent authorities in the course of their work (Article 24(1)(1) of the PNR Law in particular is worded in that way).

[213] In my view, a Member State must under no circumstances regard itself as obliged, on the basis of Article 6(3)(a) of the PNR Directive, to authorise its PIU to compare PNR data systematically against 'relevant' databases within the meaning of that provision, managed by its intelligence services.

– *The processing of PNR data on the basis of pre-determined criteria*

223. The second limb of the advance assessment under Article 6(2)(a) of the PNR Directive comprises an automated analysis against pre-determined criteria. In that analysis, PNR data are processed, in essence for predictive purposes, by applying algorithms that it is believed can 'identify' passengers who may be involved in terrorist offences or serious crime. In that context, the PIU is in essence conducting a profiling exercise.[214] Since processing of that nature can have significant consequences for the individuals identified by the algorithm,[215] both the procedures used and the safeguards that accompany it must be precisely circumscribed. As the Court noted in paragraph 172 of Opinion 1/15, the extent to which analyses of that kind interfere with the rights enshrined in Articles 7 and 8 of the Charter essentially depends on the models and pre-determined criteria on which those analyses are based.

224. In that regard, I note, first, that the second sentence of Article 6(4) of the PNR Directive stipulates that the pre-determined criteria on which the advance assessment under Article 6(3)(b) of that directive is based must be 'targeted, proportionate and specific'. The first of those requirements concerns the objective of the advance assessment under Article 6(2)(a), that is to say, identifying persons requiring further examination by the competent authorities, and therefore reflects the need for the criteria used to achieve results 'targeting' individuals who might be under a 'reasonable suspicion' of participation in terrorist offences or serious transnational crime, as the Court highlighted in Opinion 1/15.[216] 'Targeting' of that nature involves applying abstract assessment criteria or, to use an expression that occurs in the 2021 profiling recommendation,[217] using 'profiles' as a means of 'filtering' PNR data in order to detect passengers who match those profiles and who may, therefore, require further checks. The PNR Directive, in contrast, does not authorise the individual profiling of all air passengers whose data are analysed, for example by assigning each passenger to a risk category on a pre-determined scale, and to do so would infringe both Article 6(4) of that directive and the limits on the automated processing of PNR data imposed by the Court in Opinion 1/15.

225. According to the second sentence of Article 6(4), the pre-determined criteria under Article 6(3)(b) of the PNR Directive must, furthermore, be 'specific',[218] that is to say, appropriate to the purpose pursued by and relevant to it, and 'proportionate',[219] that is to say, not going beyond that purpose. In order to satisfy those requirements and, in particular, 'to ensure that the

214 Article 3(4) of the Policing Directive defines 'profiling' as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'. The same definition occurs in Article 4(4) of the GDPR and in Section 1.1(c) of the Appendix to Recommendation CM/Rec(2021)8 of 3 November 2021 of the Committee of Ministers of the Council of Europe on the protection of individuals with regard to automatic processing of personal data in the context of profiling, https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a46147 ('the 2021 profiling recommendation').

215 Section 1.1(j)(i) of the 2021 profiling recommendation defines 'high-risk profiling' as 'profiling operations that entail legal effects or have a significant impact on the data subject or on the group of persons identified by the said profiling'.

216 See Opinion 1/15, paragraph 272.

217 According to Section 1.1.(d) of the Appendix to the 2021 profiling recommendation, 'profile' refers to 'a set of data attributed to an individual, characterising a category of individuals or intended to be applied to an individual'. As explained in the Report on developments after the adoption of Recommendation (2010)13 on profiling (https://rm.coe.int/0900001680a0925c, p. 24), which preceded adoption of the 2021 profiling recommendation, the term 'profile' remains fully meaningful in systems which, like the PNR Directive, distinguish operations creating profiles (see, in particular, Article 6(2)(b) of that directive) from those that apply them, and allows 'transparency of the criteria to be applied in a second phase by the profiling operation'.

218 See Article 6(4) of the PNR Directive and Opinion 1/15, paragraph 172.

219 See Article 6(4) of the PNR Directive.

processing of PNR data remains limited to what is necessary', recital 7 of the PNR Directive, as I have already noted, 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'.

226. Lastly, it is apparent from both the preamble and provisions of the PNR Directive and the requirements set out by the Court in Opinion 1/15 that the pre-determined criteria referred to in Article 6(3)(b) of the PNR Directive must also be 'reliable',[220] which means, first, that they must be designed to minimise the risk of error[221] and, secondly, that they must be 'topical'.[222] The third sentence of Article 6(4) of the PNR Directive requires the Member States to ensure that those criteria are 'set and regularly reviewed by the PIU in cooperation with the competent authorities referred to in Article 7'.[223] To ensure that those criteria are reliable and to minimise false positives so far as possible, as the Commission acknowledged in answer to a written question put by the Court, the criteria must also be designed so that they take into account both incriminating and exonerating circumstances.

227. Secondly, the PNR Directive expressly prohibits discriminatory profiling. The first sentence of Article 6(4) of that directive provides that the advance assessment against pre-determined criteria under Article 6(3)(b) 'shall be carried out in a non-discriminatory manner'. It should be clarified in that respect that, although the fourth sentence of Article 6(4) states that those 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', the general prohibition on discriminatory profiling must be understood as including all the grounds of discrimination referred to in Article 21 of the Charter, even where they are not referred to expressly.[224]

228. Thirdly, it emerges both from the wording of Article 6(3)(b) of the PNR Directive and from the system of safeguards surrounding the automated processing of PNR data under the PNR Directive that the algorithms used for the analysis provided for in that provision must function transparently, and that the result of their application must be traceable. That requirement of transparency clearly does not mean that the 'profiles' used must be made public. It does in contrast require the algorithmic decision-making to be identifiable. On the one hand, the requirement that the criteria on the basis of which that analysis is carried out must be 'pre-determined' means that they must not be modifiable without human intervention and, therefore, precludes the use of 'machine learning' artificial intelligence technology,[225] which, whilst it may be more precise, is difficult to interpret, even for the operators who carried out the automated processing.[226] On the other hand, if it is to be effective, the safeguard set out in Article 6(5) and (6) of the PNR Directive, according to which any positive match resulting from the automated processing of PNR data under Article 6(2)(a) must be individually reviewed by non-automated means, requires – in relation to the analysis under Article 6(3)(b) of the PNR

220 See Opinion 1/15, paragraph 172.

221 See recital 7 of the PNR Directive.

222 See Opinion 1/15, paragraph 174.

223 The same requirement is contained in paragraph 174 of Opinion 1/15.

224 I would point out that all the grounds of discrimination contained in Article 21 of the Charter are reproduced in recital 20 of the PNR Directive. In its Opinion 1/2011, p. 8, the FRA had suggested that the proposal for a directive be aligned with the list of prohibited grounds of discrimination in Article 21.

225 According to Section 1.1(g) of the Appendix to the 2021 profiling recommendation, 'machine learning processing' refers to 'processing using particular methods of AI based on statistical approaches to give computers the ability to "learn" from data, that is, to improve their performance in solving tasks without being explicitly programmed for each of them'.

226 On the effects of the opacity of algorithmic systems on the feasibility of human control to prevent the detrimental effects of those systems and their negative human rights impacts, see Recommendation CM/Rec(2020)1 of the Committee of Ministers of the Council of Europe to member States on the human rights impacts of algorithmic systems.

Directive – that it must be possible to understand why the program arrived at that match, which cannot be guaranteed when, for example, self-learning systems are used. The same is true as regards monitoring the lawfulness of the analysis – including in relation to the fact that the results obtained must be non-discriminatory, which is the responsibility of the data protection officer and the national supervisory authority, under Article 6(7) and Article 15(3)(b) of the PNR Directive respectively. Transparency in the functioning of the algorithms used is also a necessary precondition for the data subjects to be able to exercise their rights to complain and their right to an effective judicial remedy.

– *The safeguards surrounding the automated processing of PNR data*

229. I have already had occasion to mention some of the safeguards that accompany the automated processing of PNR data as part of the advance assessment under Article 6(2)(a) of the PNR Directive, which correspond to the requirements set out by the Court in Opinion 1/15, that is to say, the prohibition on processing based on discriminatory pre-determined criteria (first and fourth sentences of Article 6(4) of the PNR Directive; Opinion 1/15, paragraph 172); the regular updating of the pre-determined criteria on the basis of which the advance assessment under Article 6(3)(b) of that directive must be conducted (third sentence of Article 6(4) of the PNR Directive; Opinion 1/15, paragraph 174); the review by non-automated means of any positive match resulting from the automated processing of PNR data (Article 6(5) and (6) of the PNR Directive; Opinion 1/15, paragraph 173); and monitoring of the lawfulness of that processing by the data protection officer and the national supervisory authority (Article 6(7) and Article 15(3)(b) of the PNR Directive). In that context it is of paramount importance that the supervision by an independent authority, such as the authority referred to in Article 15 of the PNR Directive, first, is able to cover all aspects inherent in the automated processing of PNR data, including identifying the databases used to compare data within the meaning of Article 6(3)(a) of that directive and to draw up the pre-determined criteria used for the analysis under Article 6(3)(b) and, secondly, can take place both *ex ante* and *ex post*.

230. It needs to be emphasised that the foregoing safeguards must be regarded as applying across the board to both types of analysis referred to in Article 6(3) of the PNR Directive, notwithstanding how each is worded. Although the first sentence of Article 6(4) of that directive recalls the requirement to respect the principle of non-discrimination solely in relation to the advance assessment carried out on the basis of pre-determined criteria, that requirement applies at all stages of the PNR data processing process and therefore also when those data are compared against relevant databases in the context of the advance assessment referred to in Article 6(3)(a) of the directive. The same is true of the requirement that the pre-determined criteria used for the analysis under Article 6(3)(b) of the PNR Directive must be reliable and topical, which must be understood as applying also to the data in the databases used for the comparison under Article 6(3)(a) of that directive. In more general terms, I note that all the safeguards applicable to the automated processing of personal data provided for by the Policing Directive also apply in the context of the PNR Directive, and the automated analyses carried out under the PNR Directive must be regarded as falling within the scope of the Policing Directive.

231. Added to the safeguards set out in point 229 above is the safeguard established in Article 7(6) of the PNR Directive which has the effect of supplementing, first, the prohibition on basing any decision-making process exclusively on the results of the automated processing of PNR data and, secondly, the prohibition on discrimination in the processing and use of those data. Article 7(6) provides that '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' and that 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'. As I stated in point 227 of this Opinion in relation to the fourth sentence of Article 6(4) of the PNR Directive, that list of grounds of discrimination should be supplemented by adding those contained in Article 21 of the Charter not expressly mentioned.

232. In relation to the security of PNR data, Article 6(8) of the PNR Directive provides that the storage, processing and analysis of PNR data by the PIUs is to be carried out exclusively within a secure location or locations within the territory of the Member States.

– *Conclusion on the sixth question referred*

233. Having regard to all the foregoing and subject to the interpretations proposed in points 213, 219, 220, 222, 227, 228, 230 and 231 of this Opinion in particular, I am of the view that the automated processing of PNR data in the context of the advance assessment under Article 6(2)(a) of the PNR Directive does satisfy the requirements in terms of clarity and precision and is limited to what is strictly necessary.

(v) Retention of PNR data (eighth question referred)

234. By its eighth question, the referring court enquires of the Court whether Article 12 of the PNR Directive, read in conjunction with Articles 7, 8 and Article 52(1) of the Charter, must be interpreted as meaning that it precludes national legislation which provides for a general retention period of five years for PNR data, without making any distinction in terms of whether the advance assessment indicates that the passengers might present a risk to public security.

235. Article 12(1) of the PNR Directive provides that PNR data are retained in a database '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'. According to Article 12(2), on expiry of an 'initial retention period' [227] of six months, PNR data are to be depersonalised by masking out certain data elements which could be used to identify the data subject directly. Under Article 12(3), on expiry of that six-month period, disclosure of the full PNR data, including the masked out elements, is to be permitted only where it is 'reasonably believed' that it is necessary for the purposes referred to in point (b) of Article 6(2) and the disclosure is approved by a judicial authority or another national authority competent under national law to verify whether the conditions for disclosure are met. Lastly, Article 12(4) provides that the PNR data are to be deleted permanently on expiry of the five-year period referred to in paragraph 1.

236. It can be seen from the foregoing that the PNR Directive itself establishes the provisions governing the retention of PNR data, including the retention period, which it sets at five years, [228] with the effect that the Member States in principle have no discretion whatsoever in that respect, as the Commission has moreover confirmed. That being so, as I have already had occasion to note, although the eighth question referred is worded as a question of interpretation, it in fact invites the Court to rule on whether those provisions are compatible with the Charter.

[227] That definition is contained in recital 25 of the PNR Directive.

[228] To my mind, the statement in recital 37 of the PNR Directive that the directive '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' (emphasis added) does not cast doubt on the clear wording of Article 12(1) of that directive.

237. It is a general principle of data protection that personal data must not be kept in a form which permits data subjects to be identified, directly or indirectly, for longer than is necessary for the purposes for which the personal data are processed. [229] Furthermore, according to consistent case-law, legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the personal data to be retained and the objective pursued. [230]

238. In Opinion 1/15 the Court held, in relation to the data collected on entry into Canada, that the necessary connection between the PNR data and the objective pursued by the draft Canada-EU PNR agreement was established for all air passengers for as long as they were in that third country. [231] Conversely, as regards air passengers who had left Canada and in respect of whom no risk relating to terrorism or serious transnational crime was identified on their arrival in that third country or up to their departure from it, the Court found that there did not appear to be any connection of that nature, albeit indirect, which would justify their PNR data being retained. [232] It nevertheless held that it could be permissible to store those data 'in so far as, in specific cases, objective evidence is identified from which it may be inferred that certain air passengers may present a risk in terms of the fight against terrorism and serious transnational crime even after their departure from Canada'. [233]

239. Transposed to the context of the PNR Directive, the principles that the Court laid down in Opinion 1/15 would mean that the PNR data for extra-EU flights collected on entry into the European Union and the PNR data for intra-EU flights collected on entry into the Member State concerned, once they have undergone the advance assessment under Article 6(2)(a) of the PNR Directive, can only be retained for so long as the passengers concerned remain in the territory of the European Union or that of that Member State. The PNR data for extra-EU flights collected on departure from the European Union and the PNR data for intra-EU flights collected on departure from the Member State concerned could, in principle, only be retained, after that advance assessment, in relation to passengers in respect of whom there was objective evidence showing a risk in terms of combating terrorism and serious crime. [234]

240. In general, the governments and institutions that have submitted observations to the Court oppose transposing the principles relating to the retention of PNR data laid down in Opinion 1/15 to the present case. It is indeed conceivable that the Court's use of a criterion linked to the data subject's stay in the territory of Canada was influenced by the fact that it was dealing with the retention of personal data on the territory of a third country. It is equally possible that using such a criterion in the context of the PNR Directive may in fact have the effect of potentially causing more significant interference with the right to respect for private life and the protection of personal data in the case of certain categories of individuals, in particular those whose permanent residence is in the European Union and who travel within it or who are returning after a stay abroad. Lastly, as certain Member States and the Council have highlighted, that criterion may indeed be difficult to implement in practice, at least in relation to intra-EU flights.

229 In relation to the processing of personal data for the purposes of detecting, preventing, prosecuting and investigating criminal offences, see the Policing Directive, Article 4(e) and recital 26. See, more generally, Article 5(1)(e) of the GDPR and Article 5(4)(e) of the modernised Convention 108.

230 See, *Schrems I* judgment, paragraph 93; *Tele2 Sverige* judgment, paragraph 110; Opinion 1/15, paragraph 191; and *La Quadrature du Net* judgment, paragraph 133.

231 See Opinion 1/15, paragraph 197.

232 See Opinion 1/15, paragraph 205.

233 See Opinion 1/15, paragraph 207.

234 Paragraph 187 et seq. of Opinion 1/15 would be applied here by analogy, because that opinion envisaged only the situation of PNR data collected on entry into Canadian territory.

241. Nevertheless, even if the criterion used by the Court in Opinion 1/15 is rejected, the retention of all the PNR data of all air passengers, irrespective of the results of the advance assessment under Article 6(2)(a) of the PNR Directive and without making any distinction according to any risk of terrorism or serious crime based on objective and verifiable criteria, conflicts with the Court's consistent case-law summarised in point 237 of this Opinion, which the Court intended to apply in Opinion 1/15. Accordingly, while the considerations set out in points 201 to 203 of this Opinion under my examination of the fourth question referred do to my mind justify the generalised indiscriminate transfer of PNR data and their automated processing in the context of the advance assessment under Article 6(2)(a) of the PNR Directive, they do not, in my view, of themselves justify the generalised and indiscriminate retention of those data after that assessment.

242. I note furthermore that the same five-year retention period is applied both for the fight against terrorism and the fight against serious crime and, as regards the latter purpose, for all the offences referred to in Annex II without exception. As can be seen from the discussion in point 121 of this Opinion, that list is particularly extensive and covers offences of different types and varying severity. It is important to note in that respect that the justification offered by practically all the Member States and institutions that submitted observations in these proceedings, relating to the duration and complexity of investigations, is in actual fact only invoked for terrorist offences, certain eminently transnational offences such as people trafficking and drug trafficking and, in general, for certain forms of organised crime. I note moreover that in Opinion 1/15 the Court accepted a similar justification only in relation to the retention of the PNR data of air passengers in respect of whom there is an objective risk in terms of combating terrorism or serious transnational crime, for which a five-year data retention period was considered not to go beyond the limits of what is strictly necessary.[235] In contrast, that justification was found to be not such as to permit 'the continued storage of the PNR data of all air passengers … for the purposes of possibly accessing those data, regardless of whether there is any link with combating terrorism and serious transnational crime'.[236]

243. As emphasised by the Council, the Parliament, the Commission and all the governments that have submitted observations on the eighth question referred, the PNR Directive does indeed provide for specific safeguards both as regards the retention of PNR data, which are in part masked out after an initial period of six months, and as regards the use of those data during the retention period, which is subject to strict conditions. However, first, I note, on the one hand, that the draft Canada-EU PNR agreement likewise established a system for depersonalising PNR data by masking out information[237] and, on the other, as emphasised in particular by the Consultative Committee of Convention 108,[238] that although that depersonalisation may mitigate the risks entailed by a long period of data retention, such as abusive access, masked out data nevertheless still allow individuals to be identified and therefore still constitute personal data, whose retention must also be limited in time in order to prevent permanent and general surveillance. I would note in that respect that a five-year retention period means that a significant number of passengers, in particular those who travel within the European Union, could find themselves on file virtually all the time. Secondly, as regards the restrictions on the use of data, I observe that the retention of personal data and access to those data are distinct

235 See Opinion 1/15, paragraph 209.

236 See Opinion 1/15, paragraph 205.

237 The draft Canada-EU PNR agreement established that the names of all passengers would be masked out 30 days after they were received by Canada and that other information expressly listed would be masked out two years after it was received; see Article 16(3) of the draft Canada-EU PNR agreement examined by the Court and Opinion 1/15, paragraph 30.

238 See Opinion of 19 August 2016, p. 9.

interferences with the fundamental rights to respect for private life and the protection of personal data, and need to be justified separately. Although the impact of a surveillance measure on those fundamental rights can be comprehensively assessed thanks to strict safeguards relating to access to retained data, the fact remains that those safeguards do not eliminate the interference associated with prolonged general retention.

244. As regards the Commission's argument that it is necessary to retain the PNR data of all air passengers so that the PIUs can perform the task, referred to in Article 6(2)(c) of the PNR Directive, of updating or creating new criteria to be used in the assessments carried out under Article 6(3)(b), whilst I concede that, as the Commission states, the accuracy of those criteria depends in part on their being compared against 'normal' behaviour, they must nevertheless be drawn up on the basis of 'criminal' behaviour. That argument – which, moreover, is advanced by only a small number of Member States – does not to my mind have the decisive importance that the Commission appears to attribute to it and cannot, in itself, justify the general retention of the non-anonymised PNR data of all air passengers.

245. In the light of the foregoing, in order to ensure that Article 12(1) of the PNR Directive is interpreted in accordance with Articles 7, 8 and Article 52(1) of the Charter, I believe that it should be interpreted as meaning that the retention in a database of PNR data provided by air carriers to a PIU for five years from the time those data are transferred to the PIU of the Member State on whose territory the flight arrival or departure point is situated is permitted, after the advance assessment under Article 6(2)(a) has taken place, only where, on the basis of objective criteria, a connection is established between those data and the combating of terrorism or serious crime. By analogy with the Court's findings in the same case-law, the generalised and indiscriminate retention of non-anonymised PNR data can only be justified in the face of a serious threat to the security of the Member States that is shown to be genuine and present or foreseeable, concerning, for example, terrorist activities, and only on condition that the retention is limited to the period strictly necessary.

246. The limits to which a data retention measure under Article 12(1) of the PNR Directive must be subject may be based, for example, on a risk assessment or on the experience of the competent national authorities, enabling the targeting of certain air links, particular travel patterns or agencies through which bookings are made or given categories of individuals or geographical areas identified on the basis of objective and non-discriminatory evidence, as the Court has held in its case-law on the retention of metadata from electronic communications.[239] Furthermore, by analogy with Opinion 1/15, the requisite connection between the PNR data and the objective pursued by the PNR Directive must be found to exist for so long as the air passengers are in or are due to leave the European Union (or the Member State concerned). The same applies to the data of passengers in respect of whom there is a verified positive match.

247. Finally on the eighth question referred, I would like to say something about the rules governing access to PNR data and the use of those data once the advance assessment under Article 6(2)(a) of the PNR Directive has been carried out but before they are depersonalised on expiry of the initial six-month retention period laid down by Article 12(2) of the PNR Directive.

248. It emerges from reading Article 6(2)(b) in conjunction with Article 12(3) of the PNR Directive that, during that initial period, the non-depersonalised PNR data or the result of the processing may be provided to the competent authorities under Article 6(2)(b) without

[239] See, among others, *La Quadrature du Net* judgment, paragraphs 148 and 149.

complying with the requirements laid down in Article 12(3)(a) and (b).[240] Article 6(2)(b) of the PNR Directive in fact merely provides that requests from the competent authorities to process and provide those data must be 'duly reasoned' and 'based on sufficient grounds'.

249. According to consistent case-law, recalled by the Court in Opinion 1/15, EU legislation cannot merely require that access by an authority to legitimately retained personal data should be for one of the objectives pursued by that legislation; it must also lay down the substantive and procedural conditions governing that use,[241] in order, inter alia, to protect those data against the risk of abuse.[242] In that opinion, the Court held that the use of PNR data following verification of those data when air passengers arrived in Canada and during their stay in that country had to be based on new circumstances justifying that use,[243] and clarified that 'where there is objective evidence from which it may be inferred that the PNR data of one or more air passengers might make an effective contribution to combating terrorist offences and serious transnational crime, the use of that data does not exceed the limits of what is strictly necessary'.[244] Referring by analogy to paragraph 120 of the *Tele2 Sverige* judgment, the Court held that, in order to ensure that those conditions are fully respected in practice, 'it is essential that the use of retained PNR data, during the air passengers' stay in Canada, should, as a general rule, except in cases of validly established urgency, 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 the competent authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime'.[245] The Court therefore laid down a twofold condition for the use of retained PNR data after they have been verified at the time of the flight, which is both substantive – that is to say, there must be objective grounds justifying that use – and procedural – that is to say, it requires a review by a court or independent administrative authority. The Court's interpretation, far from being 'context based', is in fact the application to PNR data of the case-law laid down in particular in the *Digital Rights* and *Tele2 Sverige* judgments.

250. Accordingly, the system that the PNR Directive establishes for the first six months during which PNR data are retained, according to which, after the advance assessment under Article 6(2)(a) of that directive, PNR data may be disclosed and processed – potentially repeatedly – without appropriate procedural safeguards or sufficiently clear and precise substantive rules defining the subject matter of and arrangements for those various interferences, does not satisfy the requirements set out by the Court in Opinion 1/15. Nor does it appear to meet the requirement that use of PNR data must be limited to what is strictly necessary.

251. I therefore propose that the Court should interpret Article 6(2)(b) of the PNR Directive in such a way that data processing operations under that provision which take place during the initial six-month period laid down by Article 12(2) of that directive comply with the requirements laid down by the Court in Opinion 1/15.

240 The same is true of requests to provide PNR data made by the PIUs of other Member States under Article 9(2) of the PNR Directive.

241 See Opinion 1/15, paragraph 192 and the case-law cited. More recently, see *Privacy International* judgment, paragraph 77 and, by analogy, *Prokuratuur* judgment, paragraph 49 and the case-law cited.

242 See Opinion 1/15, paragraph 200.

243 See Opinion 1/15, paragraph 200.

244 See Opinion 1/15, paragraph 201.

245 See Opinion 1/15, paragraph 202.

252. As regards the first, substantive, condition laid down by the Court for the subsequent use of PNR data, I am of the view that the expressions 'reasonably believed', within the meaning of Article 12(3)(a) of the PNR Directive, and 'sufficient grounds', within the meaning of Article 6(2)(b), may without difficulty be interpreted as meaning that the requests from competent authorities to which those provisions refer must provide 'objective evidence from which it may be inferred that the PNR data of one or more air passengers might make an effective contribution to combating terrorist offences and serious … crime'. [246]

253. As regards the second, procedural, condition, Article 6(2)(b) of the PNR Directive, read in conjunction with Article 12(3) and in the light of Articles 7, 8 and Article 52(1) of the Charter, should to my mind be interpreted as meaning that the requirement under Article 12(3)(b) of that directive for prior approval by a judicial authority or an independent administrative authority applies to any processing of PNR data carried out under Article 6(2)(b).

4. Conclusions on the second, third, fourth, sixth and eighth questions referred

254. On the basis of all the foregoing, I suggest that the Court should declare paragraph 12 of Annex I to be invalid in so far as it includes 'general remarks' as one of the categories of PNR data that air carriers are required to transmit to the PIUs under Article 8 of the PNR Directive, and should find that examination of the second, third, fourth, sixth and eighth questions referred has not revealed any other factors capable of undermining the validity of that directive, subject to the interpretation of the provisions of that directive proposed in points 153, 160, 161 to 164, 219, 228, 239 and 251 of this Opinion.

255. In the light of the answer that I suggest be given to the questions referred concerning the validity of the PNR Directive, the request made by the Council in particular, that the effects of the PNR Directive be maintained in the event that the Court decided to declare the PNR Directive as a whole invalid in full or in part, cannot, leaving aside all other considerations, be granted.

C. The fifth question referred

256. By its fifth question, the referring court enquires of the Court in essence whether Article 6 of the PNR Directive, read in conjunction with Articles 7, 8 and Article 52(1) of the Charter, must be interpreted as meaning that it precludes national legislation according to which the monitoring of certain activities of the intelligence and security services is an acceptable purpose for the processing of PNR data. It can be seen from the order for reference that those activities are those carried on by State Security and the General Intelligence and Security Service in the context of their functions concerning the protection of national security.

257. As I indicated in points 113 and 114 of this Opinion, limitation of the purposes for which personal data may be processed is an essential safeguard that must be observed so that any interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter does not go beyond what is necessary within the meaning of the Court's case-law. I also made clear that in relation to the interference with those fundamental rights envisaged by the PNR Directive, the

[246] See, to that effect, Opinion 1/15, paragraph 201.

EU legislature had a duty, in order to uphold the principles of legality and proportionality enshrined in particular in Article 52(1) of the Charter, to establish clear and precise rules governing the scope and application of the measures entailing such interference.

258. Article 1(2) of the PNR Directive stipulates that the PNR data collected under that directive 'may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as provided for in paragraphs (a), (b) and (c) of Article 6(2)'. According to that article, the PIUs are only to process PNR data in order to carry out an advance assessment of air passengers (Article 6(2)(a)), to respond to individual requests from the competent authorities (Article 6(2)(b)) and to update or define new criteria to be used for the assessments carried out under Article 6(3)(b) (Article 6(2)(a)). In all three cases, the text refers expressly to the objectives indicated in Article 1(2) of the PNR Directive of combating terrorism and serious crime.

259. Furthermore, Article 7(4) of that directive states that both the processing of PNR data under Article 6 and the further processing of those data and of the results of that processing by the competent authorities of the Member States must be limited to 'the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime'.

260. The fact that the PNR Directive exhaustively defines the objectives it pursues is clear from the wording of Article 1(2) and is corroborated not only by Article 6(2) and Article 7(4), referred to above, but also by several articles and recitals of that directive which systematically associate each stage of the process of accessing, processing, retaining and sharing PNR data with those specific objects alone. [247]

261. It is apparent both from the wording of Article 1(2) of the PNR Directive and from interpretation of that article in the light of the principles of legality and proportionality, according to which the purposes of measures that entail interference with the fundamental rights to respect for private life and the protection of personal data must be exhaustively circumscribed, that any extension of the purposes of the processing of PNR data beyond the security objectives to which that provision refers expressly is contrary to the PNR Directive.

262. In my view, that prohibition on widening the objectives pursued by the directive applies especially in relation to the activities of Member States' security and intelligence services, inter alia because their modus operandi is typically non-transparent. In that respect I agree with the Commission that as a general rule those services should not have direct access to PNR data. In that context, the fact that the members of national PIUs may include officials seconded from the security services, as occurs with the Belgian PIUs, is to my mind in itself deserving of criticism. [248]

263. On the basis of the foregoing, the fifth question should to my mind be answered to the effect that the PNR Directive, and in particular Article 1(2) and Article 6, must be interpreted as precluding national legislation according to which the monitoring of certain activities of the intelligence and security services is an acceptable purpose for the processing of PNR data, since

[247] See in particular Article 4 and Article 7(1) and (2), Article 9(2), Article 10(2) and Article 12(4) of the PNR Directive; see, among others, recitals 6, 9, 10, 11, 15, 23, 25, 35 and 38 of that directive. I also note that the proposal for a PNR directive stated, in recital 28, that 'this Directive does not affect the possibility for Member States to provide, under their domestic law, for a system of collection and handling of PNR data for purposes other than those specified in this Directive'. However, that clarification was not reproduced in the final text of the PNR Directive.

[248] That situation is nevertheless permitted by virtue of Article 4(3) of the PNR Directive, according to which 'staff members of a PIU may be seconded from competent authorities', at least where the intelligence and security services of the Member State concerned can be classified as 'competent authorities' for the purpose of Article 7(2) of that directive.

in the context of that purpose the national PIU would have reason to process those data and/or transmit them or the results of their processing to those services for purposes other than those exhaustively set out in Article 1(2) of that directive, which is a matter for the national court to determine.

D. The seventh question referred

264. By its seventh question, the referring court enquires of the Court, in essence, whether Article 12(3)(b) of the PNR Directive must be interpreted as meaning that the PIU is a 'national authority competent [under national law]' within the meaning of that article, capable of authorising the disclosure of full PNR data on expiry of the initial six-month period following the transfer of those data.

265. It will be recalled that according to Article 12(2) of the PNR Directive, on expiry of a period of six months PNR data are to be depersonalised by masking out certain data elements which could be used to identify directly the passenger to which they relate. After that period, those data may only be disclosed in their entirety in the circumstances laid down in Article 12(3), including where that disclosure has been approved in advance by a 'judicial authority' (Article 12(3)(b)(i)) or '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' (Article 12(3)(b)(ii)).

266. Most of the governments that have submitted written observations in these proceedings did not express a view on the seventh question. The Czech Government, together with the Commission, is of the view that Article 12(3) of the PNR Directive cannot be interpreted as meaning that the PIU can constitute a 'national authority competent [under national law]'. The Belgian Government,[249] Ireland and the Spanish, French and Cypriot Governments, in contrast, disagree with that interpretation. They contend, in essence, that there is no provision of the PNR Directive or of EU law that precludes a PIU from being designated as one of the competent national authorities for the purposes of Article 12(3)(b)(ii) of that directive and that a PIU is by nature a sufficiently independent authority to authorise the processing of PNR data.

267. For my part, I note, first, that it is clear from the wording of Article 12(3)(b) of the PNR Directive and, in particular, use of the conjunction 'or' between the two scenarios in points (i) and (ii) of that provision, that the EU legislature intended to place the supervision by the national authority referred to in point (ii) on the same footing as the supervision by the judicial authority referred to in point (i). It follows that the national authority in question must be independent and impartial to such an extent that supervision by it can be regarded as an alternative comparable to the review carried out by a judicial authority.[250]

[249] In respect of the doubts of the Belgian Government regarding the Court's jurisdiction to answer the seventh question, according to the wording of that question, the referring court is asking the Court for guidance on the interpretation of Article 12(3) of the PNR Directive, rather than whether the national legislation is compatible with that provision. In any event, according to consistent case-law, the Court may provide the national courts with indications enabling them to determine that compatibility (see among others judgment of 7 September 2016, *ANODE*, C-121/15, EU:C:2016:637, paragraph 54 and the case-law cited).

[250] See, in that respect, judgment of 5 November 2019, *Commission* v *Poland (Independence of common law courts)* (C-192/18, ECLI:EU:C:2019:924, paragraphs 108 to 110).

268. Secondly, it emerges from the preparatory work of the PNR Directive that the EU legislature, on the one hand, did not take up the Commission's proposal to entrust the head of the PIU with the task of authorising the disclosure of PNR data in their entirety, [251] and, on the other, extended the initial period for which those data could be retained, proposed by the Commission as 30 days, increasing it to 6 months. It is against that background of attempting to strike a balance between the length of the retention period before PNR data are depersonalised and the conditions subject to which they can be unmasked on expiry of that period that the EU legislature decided to impose stricter procedural requirements for full access to PNR data than those initially envisaged by the Commission and to entrust an independent authority with the task of verifying that those requirements for disclosure are satisfied.

269. Thirdly, as the Commission has correctly observed, it can be seen from the scheme of the PNR Directive that the raison d'être of the approval procedure established by Article 12(3) of the PNR Directive lies in the fact that an impartial third party is given the task, in each individual case, of striking a balance between the rights of the data subjects and the law enforcement purpose pursued by the directive.

270. Fourthly, it follows from the Court's case-law that a body entrusted with carrying out the prior review required in order to authorise access by the competent national authorities to legitimately retained personal data must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. The Court has also specified that the body in question must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence. [252] Specifically, in view of the requirement of independence that has to be satisfied, in particular in the criminal field, the authority entrusted with carrying out the prior review must be a third party in relation to the authority which requests access to the data and therefore must not be involved in the conduct of a criminal investigation and must have a neutral stance vis-à-vis the parties to the criminal proceedings. [253]

271. PIUs do not offer all the safeguards of independence and impartiality required of the authority responsible for the prior review under Article 12(3) of the PNR Directive. PIUs are in fact directly linked to the authorities competent in relation to the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Under Article 4(1) of the PNR Directive, the PIU is itself that authority or a branch of it. Moreover, according to Article 4(3), staff members of a PIU may be seconded from competent authorities. That occurs in particular in the Belgian PIU which, according to Article 14 of the PNR Law, is made up inter alia of seconded members of the police, State Security, General Intelligence and Security Service and customs and excise services.

272. Admittedly, as a general rule the members of a PIU must provide full safeguards of their integrity, competence, transparency and independence and it is for the Member States to ensure, where appropriate, that those safeguards can be observed in practice, having regard to the links between those members and the agencies to which they belong, in particular to prevent the competent authorities of which those members originally formed part from having direct access to the PNR database, rather than only to the results from data entered by the PIUs. The fact remains, however, that the members of the PIU seconded from the competent authorities

[251] The fourth sentence of Article 9(2) of the proposal for a PNR directive provided that 'access to the full PNR data shall be permitted only by the Head of the Passenger Information Unit'.

[252] *Prokuratuur* judgment, paragraphs 52 and 53.

[253] *Prokuratuur* judgment, paragraphs 53 and 54. To the same effect, see *Big Brother Watch* judgment, §§ 349 to 352.

referred to in Article 7(2) of the PNR Directive inevitably retain a connection with their original service while they are on secondment, and keep their status even if they are placed under the functional and hierarchical authority of the official in charge of the PIU.

273. The conclusion that the PIU is not a national authority within the meaning of Article 12(3)(b)(ii) of the PNR Directive is furthermore corroborated by the fact that, under that article, the data protection officer of the PIU concerned must be 'inform[ed]' of the request for disclosure and must carry out an '*ex post* review'. In reality, if a PIU was authorised under Article 12(3) of the PNR Directive, as 'another national authority', to approve a request for disclosure, the data protection officer, who is, under Article 5(1) of that directive, responsible, inter alia, for implementing the relevant safeguards surrounding the processing of PNR data, would be informed of the request for access at the time it was made and would necessarily carry out the relevant review *ex ante*.[254]

274. In the light of the foregoing, I suggest that the Court should reply to the seventh question that Article 12(3)(b) of the PNR Directive must be interpreted as meaning that the PIU is not 'another national authority competent [under national law]' within the meaning of that article.

E. The ninth question referred

275. By its ninth question, the referring court asks the Court in essence, first, whether the API Directive is compatible with Article 3(2) TEU and Article 45 of the Charter given that it applies to flights within the European Union, and, secondly, whether that directive, in conjunction with Article 3(2) TEU and Article 45 of the Charter, must be interpreted as meaning that it precludes national legislation which, for the purposes of combating illegal immigration and improving border controls, authorises a system of collection and processing of passenger data which may indirectly involve a re-establishment of internal border controls.

276. It can be seen from the order for reference that this question forms part of examination of LDH's second plea, advanced in the alternative. That plea, alleging infringement of Article 22 of the Belgian Constitution in conjunction with Article 3(2) TEU and Article 45 of the Charter, contests Article 3(1) and Article 8(2) and Chapter 11, in particular Articles 28 to 31, of the PNR Law. While Article 3(1) of the PNR Law sets out the subject matter of the law in general terms, stating that it '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', Article 8(2) of that law provides that 'subject to the conditions in Chapter 11 [thereof], passenger data shall also be processed with a view to improving external border controls on individuals, and with a view to combating illegal immigration'. In the context of that purpose, under Article 29(1) of the PNR Law, only the 'passenger data' covered by Article 9(1)(18) of that law (that is to say, the API data referred to in paragraph 18 of Annex I to the PNR Directive), in respect of three categories of passenger, are transferred to the police services responsible for border control and to the Office des Étrangers (Foreign Nationals Bureau, Belgium). Those are: passengers who intend to enter or have entered Belgian territory at an external border', 'passengers who intend to leave or have left Belgian territory at an external border' and 'passengers who intend to pass through, are located in, or have passed through an international transit area situated on Belgian territory'.[255] It can be seen from Article 29(3) of the PNR Law that those data are to be

[254] The fourth sentence of Article 9(2) of the proposal for a PNR directive provided that 'access to the full PNR data shall be permitted only by the Head of the Passenger Information Unit'.

[255] PNR Law, Article 29(1) and (2).

transferred by the PIU to the police services responsible for border control and to the Foreign Nationals Bureau 'immediately after they have been entered in the passenger database', and that they are to be destroyed within 24 hours of the transfer. Under that article, on expiry of that period, the Foreign Nationals Bureau may also send the PIU a reasoned request for access to those data where necessary in the context of its statutory functions. In view of the purpose of the data processing under Articles 28 and 29 of the PNR Law, the ninth question therefore steps outside the legislative framework of the PNR Directive into that of the API Directive. It is also apparent from the case file before the Court that LDH's second plea is based on an interpretation of the provisions of Chapter 11 of the PNR Law according to which those provisions also apply to crossings of Belgium's internal borders.

277. The first part of the ninth question is based on an incorrect assumption and to my mind does not require a response from the Court. It is unambiguously clear from Article 3(1), in conjunction with Article 2(b) and (d), of the API Directive that the API Directive lays down an obligation on carriers to transfer API data to the authorities responsible for carrying out checks on persons at external borders only in respect of flights taking passengers to a crossing point authorised for crossing the external borders of the Member States with third countries. Article 6(1) of that directive likewise provides for the processing of API data only in relation to those flights. Furthermore, while the PNR Directive does admittedly provide that Member States can extend the obligation to transfer the API data collected to include air carriers providing intra-EU flights, any such extension must be without prejudice to the API Directive.[256] Under the PNR Directive, the API data transferred will only be processed in relation to the law enforcement purposes envisaged by that directive. Conversely, recital 34 of the PNR Directive states that the directive is without prejudice to the current EU rules on the way border controls are carried out or to EU rules regulating entry in and exit from the territory of the European Union, and the second sentence of Article 6(9) of that directive stipulates that where assessments are carried out under Article 6(2) in relation to intra-EU flights between Member States to which the Schengen Borders Code applies,[257] the consequences of such assessments must comply with that regulation.

278. To reformulate that part of the ninth question referred, as the Commission suggests in the alternative, so that it enquires whether the PNR Directive, and in particular Article 2 of that directive, instead of the API Directive, is compatible with the Treaty and the Charter provisions, would mean not only changing the instrument of whose validity the referring court is seeking an assessment, but would also mean stepping outside the legal framework of that question. As I explained above, the provisions of Chapter 11 of the PNR Directive, to which the second plea relates, transpose the API Directive rather than the PNR Directive.

279. In case the Court does reformulate the question in that way, I present the following few considerations relating in particular to whether the advance assessment that the Member States are authorised to conduct on the PNR data of passengers on intra-EU flights, in accordance with the option available to them under Article 2 of the PNR Directive, can be considered equivalent to the exercise of 'border checks' within the meaning of Article 23(a) of the Schengen Borders Code.[258] First, although the advance assessment of PNR data takes place not 'at the border

256 See recital 10 of the PNR Directive.

257 Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ 2016 L 77, p. 1) ('the Schengen Borders Code').

258 Article 23(a) of the Schengen Borders Code states that the exercise of police powers may not be considered equivalent to the exercise of border checks when the police measures: '(i) do not have border control as an objective; (ii) are based on general police information and experience regarding possible threats to public security and aim, in particular, to combat cross-border crime; (iii) are devised and executed in a manner clearly distinct from systematic checks on persons at the external borders; (iv) are carried out on the basis of spot-checks'.

crossing' or 'at the time of the border crossing' but at an earlier time, it is nevertheless carried out 'in connection' with an imminent border crossing. Secondly, under Article 2 of the PNR Directive, the Member States may extend the prior assessment of PNR data under Article 6(2)(a) of the PNR Directive to passengers on all intra-EU flights, regardless of the behaviour of the data subjects or any circumstances establishing a risk to public security. That advance assessment is, furthermore, systematic. However, none of those factors appears to be one of the indicative circumstances referred to in the second sentence of Article 23(a), points (ii), (iii) and (iv), of the Schengen Borders Code.[259] Thirdly, in relation to the indicative circumstances referred to in the second sentence of Article 23(a), points (i) and (iii), I wonder whether the advance assessment under Article 6(2)(a) of the PNR Directive, at least in part, corresponds in purpose to the border checks conducted under Article 8(2)(b) and 8(3)(a)(vi) and (g)(iii) of the Schengen Borders Code, as amended by Regulation 2017/458, and above all whether the detailed rules governing that assessment clearly distinguish it from those systematic checks.[260] I note in that respect that Article 8(2e) and (3)(ia) of that code specify that those checks 'may be carried out in advance on the basis of passenger data received in accordance with [the API Directive] or in accordance with other [EU] or national law'. Nevertheless, it holds true that the purpose of the PNR Directive is not 'to ensure that persons *may be authorised* to enter the territory of the Member State or to leave it' or 'to prevent persons from circumventing border checks', which the Court has held to be the objectives of 'border control' for the purposes of the Schengen Borders Code,[261] since the purpose of that directive is exclusively law enforcement. Furthermore, point (ii) of the second sentence of Article 23(a) of that code explicitly states that the exercise of police powers may not be considered equivalent to the exercise of border checks where the controls are intended, inter alia, to combat cross-border crime.[262] Lastly, in its assessment the Court must also have regard to the fact, highlighted in particular by the Commission, that Article 2 of the PNR Directive authorises the Member States only to require air carriers to transfer PNR data that they have collected in the normal course of their business and therefore does not lay down an obligation similar to that established by the API Directive for external border crossings.

280. As regards the second part of the ninth question referred, in common with the Commission, I believe it must be understood as referring to internal border crossings and as seeking clarification from the Court to enable the referring court to determine whether the provisions of Chapter 11 of the PNR Law are compatible with the abolition of checks at the internal borders of the Member States in the Schengen area.

281. Since the Court has little information available to it, I will merely note that the provisions of Chapter 11 of the PNR Law can only be compatible with EU law, and Article 67(2) TFEU in particular, if they are interpreted as relating only to the transfer and processing of the API data of passengers crossing Belgium's external borders with third countries.

282. In case the Court decides to reformulate the second part of the ninth question so that it concerns interpretation of the PNR Directive in relation to the provisions of Chapter 11 of the PNR Law, I merely note that the processing of API data under Articles 28 and 29 of that law is grafted onto the system put in place by the Belgian legislature to transpose the PNR Directive.

259 See, by analogy, judgment of 13 December 2018, *Touring Tours und Travel and Sociedad de transportes* (C-412/17 and C-474/17, EU:C:2018:1005, paragraph 61 and the case-law cited), and order of 4 June 2020, *FU* (C-554/19, not published, EU:C:2020:439, paragraphs 49 to 56).

260 I note in that respect that in paragraph 188 of Opinion 1/15, the Court stated that 'the identification, by means of PNR data, of passengers liable to present a risk to public security forms part of border control'.

261 See judgment of 13 December 2018, *Touring Tours und Travel and Sociedad de transportes* (C-412/17 and C-474/17, EU:C:2018:1005, paragraph 55 and the case-law cited) (emphasis added).

262 See, to that effect, among others, order of 4 June 2020, *FU* (C-554/19, not published, EU:C:2020:439, paragraph 46).

Accordingly, first, the API data processed are those listed in paragraph 12 of Annex I to that directive, not only the data on the list in Article 3(2) of the API Directive. Secondly, under Article 29(1) of the PNR Law, those data are transferred to the police services responsible for border control and to the Foreign Nationals Bureau by the PIU – which is entrusted with collecting and processing PNR data only for the purposes pursued by the PNR Directive – instead of directly by the air carriers as established by the API Directive. Furthermore, that transfer also includes the data of passengers intending to leave or who have left Belgium, and the recipients of those data are not only the border control authorities but also the Foreign Nationals Bureau, which is responsible for managing the immigrant population and combating illegal immigration. Thirdly, under the second subparagraph of Article 29(4) of the PNR Law, the Foreign Nationals Bureau appears to be authorised to send requests for access to API data to the PIU even after those data were processed at the time the passengers concerned crossed the borders. The Foreign Nationals Bureau is therefore treated de facto as a competent authority under Article 7 of the PNR Directive, even though it is not by nature a competent authority and is not included on the list of competent authorities that Belgium notified to the Commission. To amalgamate the systems established by the API Directive and by the PNR Directive in that way cannot, to my mind, be permitted because it infringes the principle that the purposes set out in Article 1(2) of the PNR Directive must be limited. [263]

283. On the basis of all the foregoing, I propose that the Court should reply to the ninth question referred to the effect that Article 3(1) of the API Directive, under which the Member States are to take the necessary steps to establish an obligation on 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 referred to in Article 3(2), read in conjunction with Article 2(b) and (d) of that directive, concerns only passengers carried to a crossing point authorised for crossing the external borders of the Member States with third countries. National legislation which, solely in order to improve border controls and combat illegal immigration, extends that obligation to the data of persons crossing the internal borders of the Member State concerned by air or by other means of transport would be contrary to Article 67(2) TFEU and Article 22 of the Schengen Borders Code.

F. The tenth question referred

284. By its tenth question, the referring court enquires of the Court in essence whether, were it to conclude that the PNR Law infringes Articles 7, 8 and Article 52(1) of the Charter, it would be open to it to maintain the effects of that law on a temporary basis, in order to avoid legal uncertainty and enable the data previously collected and retained to continue to be used for the purposes envisaged by the PNR Law.

285. The Court responded to a question to the same effect in the *La Quadrature du Net* judgment which concerned the storage of metadata from electronic communications, handed down after this request for a preliminary ruling was made. In that judgment, the Court first of all recalled its case-law according to which 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. It then noted that, in its judgment of 29 July 2019, *Inter-Environnement Wallonie and Bond Beter Leefmilieu*

[263] In its 2020 working document on the API directive (p. 20), the Commission too noted that the overlap between the systems for the processing of PNR and API data at national level was problematic.

Vlaanderen,[264] concerning the lawfulness of measures adopted in breach of the obligation under EU law to conduct a prior assessment of the impact of a project on the environment and on a protected site, it held that if domestic law allows it, a national court may, by way of exception, maintain the effects of such measures where such maintenance is justified by overriding considerations relating to the need to nullify a genuine and serious threat of interruption in the electricity supply in the Member State concerned for as long as is strictly necessary to remedy the breach. It nevertheless found that unlike a breach of a procedural obligation such as the prior assessment of the impact of a project in the specific field of environmental protection, a failure to comply with fundamental rights guaranteed in Articles 7 and 8 of the Charter cannot be remedied by a procedure comparable to the procedure referred to in the judgment referred to above.[265] I believe that the same answer must be given to the tenth question referred in these proceedings.

286. Since the referring court, the Belgian Government, the Commission and the Council all enquire whether EU law precludes information or evidence obtained using PNR data collected, processed and/or retained in a manner incompatible with EU law from being used in criminal proceedings, I note that, in paragraph 222 of the *La Quadrature du Net* judgment, the Court stated that, subject to compliance with the principles of equivalence and effectiveness, as EU law currently stands it is, in principle, for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed serious criminal offences, of information and evidence obtained by such retention of data contrary to EU law. The Court held that the principle of effectiveness requires national criminal courts to disregard information and evidence obtained by means of the generalised and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact. Those principles can also be transposed *mutatis mutandis* to the circumstances of the main proceedings.

IV. Conclusion

287. On the basis of all the foregoing, I suggest that the Court should reply as follows to the questions referred by the Cour constitutionnelle (Constitutional Court, Belgium):

(1) 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), read in conjunction with Article 2(2)(d) of that regulation, must be interpreted as meaning that:

– it applies to national legislation that transposes 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 to the extent that that legislation governs the processing of PNR data by air carriers and other economic operators, including the transfer, under Article 8 of that directive, of PNR data to the passenger information units (PIUs) referred to in Article 4 of that directive;

[264] C-411/17, EU:C:2019:622, paragraphs 175, 176, 179 and 181.

[265] See *La Quadrature du Net* judgment, paragraphs 217 to 219.

– it does not apply to national legislation that transposes Directive 2016/681 to the extent that that legislation governs data processing carried out for the purposes referred to in Article 1(2) of that directive by the competent national authorities, including the PIUs and, where applicable, the security and intelligence services of the Member State concerned;

– it applies to national legislation that transposes Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data and 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, with a view to improving external border controls on individuals and with a view to combating illegal immigration.

(2) Paragraph 12 of Annex I to Directive 2016/681 is invalid in so far as it includes 'general remarks' among the data that air carriers are required to transmit to the PIUs under Article 8 of that directive.

(3) Examination of the second, third, fourth, sixth and eighth questions has not revealed any other factors capable of undermining the validity of Directive 2016/681.

(4) Paragraph 12 of Annex I to Directive 2016/681, in so far as concerns the part that has not been declared invalid, must be interpreted as encompassing only information concerning minors that is expressly referred to in that paragraph and directly related to the flight.

(5) Paragraph 18 of Annex I to Directive 2016/681 must be interpreted as covering only the advance passenger information expressly listed in that paragraph and in Article 3(2) of Directive 2004/82 that have been collected by air carriers in the normal course of their business.

(6) The concept of 'relevant' databases referred to in Article 6(3)(a) of Directive 2016/681 must be interpreted as covering only the national databases managed by the competent authorities under Article 7(1) of that directive, and EU and international databases used directly by those authorities in the course of their work. Those databases must relate directly and closely to the purposes of combating terrorism and serious crime pursued by that directive, thereby implying that they must have been developed for those purposes. When they transpose Directive 2016/681 into their national law, the Member States must publish a list of those databases and they must keep it up to date.

(7) Article 6(3)(b) of Directive 2016/681 must be interpreted as meaning that, in the context of the automated processing under that provision, it precludes the use of algorithmic systems in which pre-determined criteria on the basis of which that processing is carried out may be modified without human intervention and which do not enable the reasons for a positive match resulting from that processing to be identified clearly and transparently.

(8) Article 12(1) of Directive 2016/681, construed in conformity with Articles 7, 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that the retention in a database of PNR data provided by air carriers to a PIU for five years from the time they are transferred to the PIU of the Member State on whose territory the flight arrival or departure point is situated is permitted, after the advance assessment under Article 6(2)(a) of that directive has taken place, only where, on the basis of

objective criteria, a connection is established between those data and the combating of terrorism or serious crime. The generalised and indiscriminate retention of those non-anonymised PNR data can only be justified in the face of a serious threat to the security of the Member States that is shown to be genuine and present or foreseeable, concerning, for example, terrorist activities, and only on condition that the retention is limited to the period strictly necessary.

(9) Article 6(2)(b) of Directive 2016/681 must be interpreted as meaning that the disclosure of PNR data or the results of the processing of those data under that provision which takes place during the initial six-month period laid down by Article 12(2) of that directive must comply with the requirements laid down in Article 12(3)(b) of that directive.

(10) Directive 2016/681, and in particular Article 1(2) and Article 6, must be interpreted as precluding national legislation according to which the monitoring of certain activities of the intelligence and security services is an acceptable purpose for the processing of PNR data, since in the context of that purpose the national PIU would have reason to process those data and/or transmit them or the results of their processing to those services for purposes other than those exhaustively set out in Article 1(2) of that directive, which is a matter for the national court to determine.

(11) Article 12(3)(b) of Directive 2016/681 must be interpreted as meaning that the PIU is not 'another national authority competent [under national law]' within the meaning of that article.

(12) Article 3(1) of Directive 2004/82, under which the Member States are to take the necessary steps to establish an obligation on 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 referred to in Article 3(2), read in conjunction with Article 2(b) and (d) of that directive, concerns only passengers carried to a crossing point authorised for crossing the external borders of the Member States with third countries. National legislation which, solely in order to improve border controls and combat illegal immigration, extends that obligation to the data of persons crossing the internal borders of the Member State concerned by air or by other means of transport would be contrary to Article 67(2) TFEU and Article 22 of Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).

(13) A national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality, which it is bound to make under that law, in respect of national legislation which, in order to combat terrorism and serious crime, requires air, land and maritime carriers and tour operators to transfer PNR data, and provides for generalised and indiscriminate processing and retention of those data incompatible with Articles 7, 8 and Article 52(1) of the Charter of Fundamental Rights. In accordance with the principle of effectiveness, a national criminal court must disregard information and evidence obtained under such legislation which is incompatible with EU law, in the context of criminal proceedings against persons suspected of acts of terrorism or serious crime, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.