**Case C-817/19**

**Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice**

**Date lodged:**

31 October 2019

**Referring court:**

Cour constitutionnelle (Belgium)

**Date of the decision to refer:**

17 October 2019

**Applicant:**

ASBL 'Ligue des droits humains'

---

## I. The subject matter of the proceedings and the parties' positions

1 The Belgian legislature has enacted a Law of 25 December 2016 on processing of passenger data (Moniteur Belge of 25 January 2017; also referred to below as the 'PNR Law'), essentially to transpose:

– 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 (also referred to below as 'the PNR Directive').

– Council Directive 2004/82/EC of 29 April 2004 'on the obligation of carriers to communicate passenger data' (also referred to below as 'the API Directive').

2 The PNR Law requires international passenger transport carriers in various sectors (air, rail, international road and sea), as well as tour operators, to transfer data on their passengers to a database managed by the SPF Intérieur (Ministry of the Interior, Belgium).

3 To that end, the law creates a 'passenger information unit' within the SPF Intérieur (Articles 12 to 14), which is made up inter alia of seconded members of the police, State security, intelligence and security and customs services, and has

responsibility for collecting, retaining and processing the passenger data transmitted by the carriers and tour operators.

4 The 'passenger database' includes reservation ('API') data and check-in and boarding ('PNR') data (Article 9).

5 Those data are processed for purposes including detection, prosecution and execution of penalties in relation to criminal offences referred to in the law, as well as prevention of serious public security disturbances in the context of violent radicalisation and furthering the activities of the intelligence and security services, and are also processed with a view to improving border controls on individuals at external borders and combating illegal immigration (Article 8).

6 The data may be processed in the course of advance assessment of passengers (before their departure or arrival) (Articles 24 to 26) or in the course of ad hoc searches (Article 27).

7 The law provides for passenger data to be retained in the passenger database for a maximum period of five years from being entered (Articles 8 to 23).

8 The ASBL (not-for-profit association) 'Ligue des droits humains' (Human Rights League) has raised objections to the following seven aspects of the law:

– the provisions for implementation of the Law of 25 December 2016 (Article 3(2) and Article 7(3));

– the concepts of 'identity documents' and 'travel documents' (Article 7(1) and (2));

– the data to which it relates (Articles 4 9° and 9);

– the definition of 'passenger' (Article 4(10°));

– the purposes for which the PNR data are to be processed (Article 8);

– the management of the passenger database and the processing of data in the context of advance assessment of passengers and ad hoc searches (Articles 12 to 16, 24 to 27, and 50 and 51);

– the period of time for which PNR data is retained (Article 18).

9 It claims that there are irregularities in those aspects of the law and has brought an action for annulment before the Cour constitutionnelle (Constitutional Court, Belgium), in which it advances two pleas.

10 The first plea is essentially based on Article 23 of Regulation (EU) 2016/679, [1] Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 8 of the European Convention on Human Rights ('the ECHR').

11 The Ligue des droits humains essentially maintains that the interference with the right to private life and the right to protection of personal data is unlawful in that it does not meet the tests of legality, necessity or proportionality.

12 First, the PNR Law gives significant discretion to the executive, providing, contrary to the principle of legality, for it to define certain essential elements by way of Royal Decree. The principle of legality requires that such interference is provided for by law or, in the case of delegation to the King, that the essential elements are provided for by law in a sufficiently precise and detailed manner.

Furthermore, the contested law does not pursue a legitimate objective. It provides for an advance assessment or pre-screening process which consists of an evaluation of the risk presented by the passengers before arrival in, transit through or departure from Belgium.

13 The applicant goes on to dispute that the contested measures are necessary to achieve the objective of the law.

It maintains that data matching, which would involve significantly less intrusion into private life than the creation of a database, would be equally capable of achieving the objective pursued.

14 Finally, it argues that the contested law is disproportionate, in that the data is collected by the operators in an indiscriminate and generalised way, and transferred to the competent authorities to be stored for five years, without distinction, differentiation, limitation or exception by reference to the objective pursued.

15 More specifically, the law does not conform to the principle of proportionality having regard (a) to its scope and the categories of data to which it relates, (b) to the data processing for which it provides, (c) to its purposes and (d) to the length of time for which the data is stored.

16 First, the contested law defines the data to be collected in very broad terms, and those data clearly go beyond what is strictly necessary.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119, p. 1 (also referred to below as 'the GDPR').

17 The applicant observes that it seems — although the law is not clear — that the pre-screening is to be carried out within the central PIU database, using pre-defined criteria as threat indicators. However, the PNR Law does not state either the precise nature of the databases to be used in the process of comparison, or how that process is to be carried out. Equally, it does not provide that the comparison is limited to databases operated for the purposes of combating terrorism and serious crime.

18 The applicant also objects to the ad hoc searches for which the law provides without specifying what data is actually accessible.

19 It also challenges the purposes for which the data is to be processed, which are significantly broader than those provided for by the PNR Directive and include combating illegal immigration, activities capable of amounting to a threat to the fundamental interests of the State, and 'violent radicalisation', which is only defined in a circular.

20 Finally, the applicant objects to the period of five years for which the data is retained. The legislature has given no justification for opting for maximum period permitted by the PNR Directive, and the fact that it did so reveals the disproportionality of the measure.

21 The Council of Ministers (which defends the law) submits principally that the first plea is inadmissible, in that it is based on a breach of Article 23 of the GDPR, when it is clear both from recital 19 of the GDPR and from Article 1 of the PNR Directive that processing of PNR data is not subject to the GDPR, but is a matter of judicial and police cooperation between Member States falling within Directive (EU) 2016/680. [2]

22 It also submits that there is no infringement of the principle of legality, as the law does lay down the essential elements of the measures for which it provides, and the terms in which it confers power on the King are sufficiently precise. Furthermore, the requirement of legality is to be understood in a practical sense, according to the European Court of Human Rights, such that regulatory acts are within the meaning of 'law' in the European Convention on Human Rights.

The PNR Law is intended to ensure public security, not only by enabling terrorist offences and certain serious crimes to be prosecuted, but also, through advance analysis of the data collected, by preventing the commission of such offences. The Court of Justice has recognised that those are legitimate objectives for the purposes of Article 52(1) of the Charter of Fundamental Rights of the European Union, both in its judgment of 8 April 2014, *Digital Rights Ireland and*

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, p. 89) ('Directive 2016/680').

*Others*(C-293/12 and C-594/12, EU:C:2014:238) and in Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592.

23 The Council of Ministers submits that the contested measures are proportionate.

24 As regards the creation of a 'passenger' database, the Council of Ministers observes that the applicant has merely asserted, and not demonstrated, that the objective pursued could have been achieved by data matching, and that this would have been less intrusive in terms of the right to respect for private life. It adds that data matching would not be sufficient for the advance assessments to be carried out in order to identify security risks. The creation of a database is also a way of addressing recital 25 of the PNR Directive, which states that the data should be retained for as long as is necessary having regard to the objectives pursued.

25 As to the linking of the various databases, the Council of Ministers points out that Articles 24 and 25 of the PNR Law transpose Article 6 of the PNR Directive. Furthermore, it is apparent from the preparatory work that the legislature did not intend the 'passenger' database to be linked to all the other databases to which the competent authorities have access, but only to those corresponding to the objectives pursued by the contested law. Those measures are in conformity with Opinion 1/15 of the Court of Justice, given that Article 6(3) of the PNR Directive similarly does not specify which databases are to be available for the purposes of comparison. Nor is the existence of a discretion incompatible with the principle of legality, as interpreted by the European Court of Human Rights.

Moreover, the objective of the law could not be achieved if passengers knew, in advance, the criteria which would lead to a positive match, as they would then be able to adapt their behaviour accordingly. Article 16 of the contested law clearly states, furthermore, that the pre-screening is to be carried out within the 'passenger' database, which is thus in conformity with the principle of legality.

26 As regards the length of time for which the data is retained, the Council of Ministers considers that it is not unreasonable to provide for a retention period of five years, which, moreover, corresponds to the shortest limitation period applicable to public prosecutions for offences classified as being of intermediate seriousness, or treated as such despite a higher classification.

Thus the retention period, which is in conformity with the period provided for by the PNR Directive, is in no way disproportionate.

27 The second plea, which is advanced in the alternative, is based essentially on breach of Article 3(2) TFEU, read in conjunction with Article 45 of the Charter.

28 The applicant submits that Article 3(1), Article 8(2) and Chapter 11 (containing Articles 28 to 31) of the PNR Law are contrary to the free movement of persons, in that they relate not only to extra-EU transport, but also to intra-EU transport (including scheduled stops). In other words, the applicant argues that by extending

the PNR system to intra-EU flights, the contested provisions indirectly re-establish border controls which infringe the right of free movement of persons.

29 The Council of Ministers submits that the contested law does not re-establish any border controls and is not contrary to the free movement of persons in any way. The PNR Directive does not apply to illegal immigration and it is not only that directive, but also the API Directive, which is transposed by the contested law.

The plea, as formulated, relates only to Article 3 § 1, Article 8 § 2 and Chapter 11 of the contested law. However, it follows from the definition of 'external borders' that the PNR Law is directed only to extra-EU controls. Furthermore, the PNR Law transposes Directive 2004/82/EC, and thus cannot be regarded as re-establishing border controls within the Schengen area.

Lastly and very much in the alternative, recital 10 of the PNR Directive expressly provides for the use of PNR data to be extended to intra-EU flights, which shows that the measure does not inherently contravene either freedom of movement or Regulation (EC) No 562/2006.

## II. Legal background

### *The European Convention on Human Rights*

30 Article 8 provides:

'1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

### *European Union law*

*The Charter of Fundamental Rights of the European Union*

31 Article 7 of the Charter ('Respect for private and family life') provides:

'Everyone has the right to respect for his or her private and family life, home and communications.'

32 Article 8 of the Charter ('Protection of personal data') provides:

'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'.

33 Article 52(1) of the Charter provides:

'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.'

*The General Data Protection Regulation (GDPR)*

34 Article 2(2)(d) provides:

'2. This Regulation does not apply to the processing of personal data:

…

(d) 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.'

35 Article 23 provides:

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

(a) national security;

(b) defence;

(c) public security;

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

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

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

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

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

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

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

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

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

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

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

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

*The PNR Directive*

36 Article 3 reads as follows:

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

…

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

37 Article 4 provides:

'Passenger Information Unit

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

2. The PIU shall be responsible for:

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

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

…'.

38 Article 6 provides:

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

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

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

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

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

… .'

39 Article 12 provides:

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

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

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

(b) address and contact information;

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

(d) frequent flyer information;

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

(f) any API data that have been collected.

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

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

(b) approved by:

(i) a judicial authority; or

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

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

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

40 Annex I to the PNR Directive, headed 'Passenger name record data as far as collected by air carriers', refers amongst other things to:

'…

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

…

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

…'

*The API Directive*

41 Article 1 provides:

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

***Belgian law***

42 The relevant provisions of the PNR Law (as amended by the Laws of 15 and 30 July 2018, and by the Law of 2 May 2019) are as follows:

'CHAPTER 2 Scope

Art. 3 § 1 This law lays down the obligations of carriers and tour operators regarding the transfer of data relating to passengers travelling to or from Belgium, or transiting through Belgian territory.

§ 2 The King shall prescribe, by decree deliberated in the Council of Ministers, in respect of each sector of the transport industry and in respect of tour operators, the passenger data to be transferred and how they are to be transferred, after an opinion has been given by the competent authority for the supervision of processing of personal data. …

CHAPTER 3 Definitions

Art. 4 'For the purposes of this law and its implementing decrees, the following definitions shall apply:

…

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

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

…

CHAPTER 5 Purposes for which data may be processed

Art. 8 § 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 liberty) of offences referred to [in the] Criminal Procedure Code;

2° detection and prosecution (including the execution of penalties or measures depriving the person concerned of his liberty) of offences referred to [in the] 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 Article 44/5 § 2 of the Law of 5 August 1992 on the police service;

4° furthering the activities referred to in Article 7 1° and 3°/l, and Article 11, § 1 1° to 3° and 5°, of the Organic law of 30 November 1998 on the intelligence and security services;

5° detection and prosecution of the offences referred to [in various laws].

§ 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.

CHAPTER 6 — Passenger data

Art. 9 § 1 As regards booking information, passenger data may include but shall be limited to the following details:

1° PNR record locator;

2° date of reservation and issue of ticket;

3° dates of intended travel;

4° full name and date of birth;

5° address and contact information (telephone number, email address);

6° payment information, including billing address;

7° complete travel itinerary for the relevant passenger;

8° information on members of loyalty schemes (such as frequent flyer programmes);

9° travel agency or agent;

10° travel status of passenger, including confirmations, check-in status, no-show or go-show information;

11° split or divided PNR information;

12° general remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent);

13° ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields;

14° seat number and other seat information;

15° code share information;

16° all baggage information;

17° number and other names of travellers on the PNR;

18° any advance passenger information (API) data which has been collected, as itemised in § 2;

19° all historical changes to the PNR listed in 1° to 18°.

§ 2 As regards check-in and boarding information, the advance passenger information referred to in § 1, 18° comprises:

1° type of travel document;

2° document number;

3° nationality;

4° country of issue of document;

5° expiry date of document;

6° full name, gender and date of birth;

7° carrier/tour operator;

8° transport number;

9° date of departure and of arrival;

10° place of departure and of arrival;

11° time of departure and of arrival;

12° total number of passengers carried on that transport;

13° seat number;

14° PNR record locator;

15° number of items of baggage, together with their weights and identification codes;

16° the border crossing point of entry into Belgian territory.

…

CHAPTER 7 The Passenger Information Unit

Art. 12 A Passenger Information Unit is hereby created within the Service Public Fédéral Intérieur (Ministry of the Interior, Belgium).

Art. 13 § 1 The PIU shall be responsible for:

1° collecting passenger data from carrier and tour operators, retaining and processing those data, and managing the passenger database;

2° exchanging both passenger data and the result of processing such data with the PIUs of other Member States of the European Union, with Europol, and with third States, in accordance with Chapter 12.

§ 2 Without prejudice to other provisions of law, the PIU may not use the data retained pursuant to Chapter 9 for purposes other than those contemplated by Article 8.

Art. 14 § 1 The PIU shall be made up of:

1° an official … responsible for:

(a) the organisation and functioning of the PIU;

(b) monitoring compliance by carriers and tour operators with the obligations imposed on them by Chapter 4;

(c) the management and operation of the passenger database;

(d) processing of passenger data;

(e) ensuring that the processing referred to in Chapter 10 is carried out in a lawful and regular manner;

… .

2° members seconded from the following … services:

(a) the police services …;

(b) the national security service …;

(c) the general intelligence and security service …;

(d) the customs and excise administration …;

… .

CHAPTER 8 The passenger database

Art. 15 § 1 A passenger database under the management of the Ministry of the Interior shall be established, in which passenger data shall be stored.

… .

§ 4 Processing of passenger data carried out pursuant to this law is subject to the data protection law. The competent authority for processing of personal data shall exercise the powers provided for in the law on protection of private life. …

…

CHAPTER 9 Retention period

Art. 18 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.

…

CHAPTER 10 Processing of data

Section I. Processing of passenger data in connection with the advance assessment of passengers

Art. 24 § 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.

[methods of advance assessment]

Art. 25 …

§ 2 Assessment of passengers prior to arrival, transit or departure against pre-determined criteria shall be carried out in a non-discriminatory manner. The pre-determined criteria may not concern the identification of an individual and must be targeted, proportionate and specific.

§ 3 They may not be based on data indicating a person’s race or ethnic origin, religion or philosophical beliefs, political opinions, trade union membership, health, sexual life or sexual orientation.

…

Section 2 — Processing of data in connection with ad hoc searches

Art. 27 Passenger data shall be used in carrying out ad hoc searches for the purposes contemplated by Article 8 § 1 1°, 2°, 4° and 5°, subject to the conditions laid down in Article 46 septies of the Criminal Procedure Code, Article 16/3 of the Organic law of 30 November 1998 on the intelligence and security services, and Article 281 § 4 of the General law on customs and excise duties, consolidated on 18 July 1977.

CHAPTER 11 Processing of passenger data with a view to improving border controls and combating illegal immigration

Art. 28 § 1 This Chapter applies to the processing of passenger data by the police services responsible for border control and by the foreign nationals bureau, carried out with a view to improving external border controls on individuals and combating illegal immigration.

…

Art. 29 § 1 …

§ 2 Only [API] data relating to the following categories of passenger shall be transferred:

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

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

3° passengers who intend to pass through, are located in, or have passed through an international transit area situated in Belgium.

§ 3 The passenger data referred to in § 2 shall be transferred to the police services referred to in Article 14, § 1 2° (a) immediately after they have been entered in the passenger database. The police services shall save those data in a temporary file and delete them within 24 hours of the transfer.

§ 4 … the passenger data referred to in § 2 shall be transferred to the foreign nationals bureau immediately after they have been entered in the passenger database. The foreign nationals bureau shall save those data in a temporary file and delete them within 24 hours of the transfer.

… .

Art. 31 Within 24 hours of completion of the transport, as referred to in Article 4 3° to 6°, the carriers and tour operators shall delete all the passenger data referred to in Article 9, § 1 18°, … .

…

CHAPTER 15 Amending provisions

Section I. Amendment of the Criminal Procedure Code

Art. 50 There shall be inserted, in the Criminal Procedure Code, an Article 46 septies which shall read as follows:

"Art 46 septies In detecting the offences referred to in Article 8 § 1 1°, 2° and 5° of the Law of 25 December 2016 on the processing of passenger data, the crown prosecutor may, by reasoned written decision, instruct the officer of judicial police to direct the PIU to transmit passenger data in accordance with Article 27 of the Law of 25 December 2016 on the processing of passenger data.

…

Section 2 Amendment of the Organic law of 30 November 1998 on the intelligence and security services

Art. 51 There shall be inserted, in Chapter III, Section I, Sub-section 2 of the Law of 30 November 1998 on the intelligence and security services, an Article 16/3 which shall read as follows:

"Art. 16/3 § 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 27 of the Law of 25 December 2016 on the processing of passenger data … ".

## III. The assessment of the Cour constitutionnelle (Constitutional Court)

43 The Cour constitutionnelle (Constitutional Court) begins by stating that, in considering the action, it has taken account of the amendments to the Law of 25 December 2016 which were made by the Laws of 15 and 30 July 2018 and the Law of 2 May 2019.

44 It also narrows the scope of the action for annulment by determining that the first plea is directed only against Article 3 § 2, Article 4 9° and 10°, Articles 7 to 9, Articles 12 to 16, Article 18, Articles 24 to 27 and Articles 50 and 51 of the law, and that the second plea is directed against Article 3 § 1, Article 8 § 2, and Articles 28 to 31 of the law.

### *1. Admissibility of the first plea: is Article 23 of the GDPR applicable to the PNR Law?*

45 The referring court observes that the protection conferred by the GDPR is based on Article 16(2) TFEU and that in principle, 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 is

governed not by the GDPR, but by Directive 2018/680. That directive lays down specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities.

46 The PNR Law makes provision as to the collection and transfer of PNR data, the creation of a passenger database, managed by the PIU, the purposes for which that database may be used, and access to it. Essentially it transposes the PNR Directive, but its content goes beyond transposition of that directive.

47 Making reference to Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592), the referring court observes that provisions governing the collection, transfer and processing of PNR data may fall within the ambit of both data protection (Article 16 TFEU), and police cooperation (Article 87 TFEU).

It also points out that recital 5 of the PNR Directive states that the objectives of that directive are '*inter alia, to ensure security, to protect the life and safety of persons, and to create a legal framework for the protection of PNR data with regard to their processing by competent authorities*'. Recital 38 of the PNR Directive nevertheless indicates that the objectives of the directive are '*the transfer of PNR data by air carriers and processing of those data for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime*', which may give those objectives precedence over that of data protection.

The referring court observes, furthermore, that national law does not exclude the PNR Law in its entirety from the scope of Article 23 of the GDPR.

48 On that basis, the Cour constitutionnelle (Constitutional Court) concludes that in order to determine whether the requirements of Article 23 of the GDPR apply to the PNR Law, which principally, though amongst other things, transposes the PNR Directive, it is necessary to refer a first question to the Court for a preliminary ruling.

### *2. Substance of the first plea*

The Cour constitutionnelle (Constitutional Court) goes on to examine the plea on its merits, as regards the seven matters set out in paragraph 8 of this summary. It holds that the first two objections, relating to the 'provisions for implementation' of the law and the concepts of 'identity documents' and 'travel documents', are without foundation. It proceeds to examine the other five objections and expresses doubt as to the interpretation to be given to certain provisions of the PNR Directive, and, having regard to the Charter, as to their validity.

*The data to which the PNR Law relates (Articles 4 9° and 9)*

49 The applicant submits that the very broad range of passenger data contemplated by Articles 4 9° and 9 of the PNR Law is manifestly disproportionate in the light of the objective pursued. It contends that the data in question may reveal sensitive information, such as membership of a trade union, personal affinities or personal or professional relationships.

50 The referring court observes that interference by the public authorities with enjoyment of the right to respect for private life must not only be based on a legislative provision which is sufficiently precise, but must also be justified in a democratic society by a pressing social need, and proportionate to the legitimate aim pursued. The legislature has a margin of appreciation in the matter but this has limits; in order for a legal standard to be compatible with the right to respect for private life, the legislature must have established a fair balance between all the relevant rights and interests.

In its Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592), the Court observed that interference with the right to protection of personal data must be limited to what is 'strictly necessary' (see paragraphs 140 and 141).

51 The Cour constitutionnelle (Constitutional Court) observes that the objective of the PNR Law is to ensure public security by making provision for the transfer of passenger data, and the use of such data, in the context of efforts to combat terrorist offences and serious cross-border crime. Those are objectives of general interest capable of justifying interference with the right to respect to private life and the right to protection of personal data (judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 42). The Court of Justice has, moreover, confirmed that those objectives of general interest are capable of justifying the transfer and processing of passenger data (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 148 and 149).

52 The referring court then considers whether the interference is sufficiently precise, proportionate, and limited to what is 'strictly necessary', having regard to the breadth of the data to which the PNR Law relates.

The collection of passenger data envisaged by the PNR Law is subject to safeguards relating to the content of that data. The data are exhaustively defined in Article 9 of the PNR Law. They comprise information relating directly to the journey involving the transport which falls within the scope of the PNR Law — information which, in principle, is already available to the carriers and tour operators. Furthermore, the data reflect Annex I of the International Civil Aviation Organization (ICAO) guidelines. They are therefore relevant to the objectives pursued by the PNR Law.

Furthermore, Articles 10 and 11 of the PNR Law, which are not challenged, provide that passenger data may not relate to a person's racial or ethnic origin, religious or philosophical convictions, political opinions, trade union membership, or data concerning his state of health, sexual life or sexual orientation. Where passenger data transferred by carriers and tour operators include data other than those enumerated in Article 9, or include data enumerated in Article 10, the PIU deletes those additional data permanently, upon receipt. These provisions ensure that sensitive data cannot, in principle, be collected or retained as 'passenger data'.

53 In Opinion 1/15 of the Court of Justice, of 26 July 2017, the Court also held, in relation to sensitive data, that '*Articles 7, 8 and 21 and Article 52(1) of the Charter preclude both the transfer of sensitive data to Canada and the framework negotiated by the European Union with that non-member State of the conditions concerning the use and retention of such data by the authorities of that non-member State*' (paragraph 167).

That observation can be transposed to the present case. While there are safeguards attaching to the passenger data covered by the PNR Law, the question must nevertheless be asked as to whether those safeguards are sufficient, having regard to the breadth of the data in question. The data referred to in Article 9(1) of the PNR Law, which reproduces the list of data in Annex I of the PNR Directive, do cover a very broad range, over and above check-in and boarding data. In particular, they include the passenger's complete itinerary, the travel agent, seat number, all baggage information, information relating to means of payment, including the billing address, and general remarks 'including all available information on unaccompanied minors under 18 years'.

In Opinion 1/15 of 26 July 2017, the Court also observed that, '*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, as defined in Article 2(e) of the envisaged agreement*' (paragraph 128).

In its Opinion of 19 August 2016 on the Data protection implications of the processing of Passenger Name Records ('Opinion of 19 August 2016'), the Consultative Committee of Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data ('the Consultative Committee of Convention 108') observed, equally, that '*PNRs contain information that is needed to facilitate a passenger's travel, and may include a number of sensitive data which could serve to indicate racial origin, political opinions or religious or other beliefs or data relating to a person's health or sexual orientation, not only under certain 'coded' data but also under the open field containing general remarks (such as dietary or medical*

*requirements, or the fact that a political or religious association benefited from reduced fares for the travel of its members) which could lead to direct discrimination*' (Council of Europe, Opinion of 19 August 2016, T-PD(2016)18rev, p. 7).

The European Union Agency for Fundamental Rights has also remarked that PNR data '*might include sensitive or special data under the heading "general remarks"*' (Opinion 1/2011 of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final), 14 June 2011, p. 8; see also ibid., p. 13).

54 In the light of their very wide scope, the data referred to in Article 9 of the PNR Law, while they may not literally contain sensitive data, may nevertheless indirectly reveal sensitive information which falls within the ambit of protection of personal data and respect for private life. Having regard to Opinion 1/15 of the Court of Justice, the Cour constitutionnelle (Constitutional Court) wonders whether those data, which include the data listed in Annex I of the PNR Directive, go beyond what is 'strictly necessary' to achieve the objectives pursued by that directive. It accordingly decides to refer a second question to the Court for a preliminary ruling.

55 In Opinion 1/15 of 26 July 2017, the Court also made the following observations, concerning the requirement for a clear and precise definition of the data contemplated by the draft agreement between Canada and the European Union on the transfer and processing of passenger data:

'*156. In this connection, although the 19 PNR data headings set out in the Annex to the envisaged agreement correspond, according to the observations of the Commission, to Appendix 1 to the Guidelines of the International Civil Aviation Organisation (ICAO) on PNR data, it should nonetheless be stated, as the Advocate General has observed in point 217 of his Opinion, that heading 5, which refers to "available frequent flyer and benefit information (free tickets, upgrades, etc.)", and heading 7, which covers "all available contact information (including originator information)", do not define in a sufficiently clear and precise manner the PNR data to be transferred.*

*157. Thus, as regards heading 5, the use of the term "etc." does not specify to the requisite standard the scope of the data to be transferred. Furthermore, it is not clear from the terms of that heading whether it covers information concerning merely the status of air passengers in customer loyalty programmes or whether, on the contrary, it covers all information relating to air travel and transactions carried out in the context of such programmes.*

*158. Similarly, the use of the terms "all available contact information" in heading 7 does not specify sufficiently the scope of the data to be transferred. In particular, it does not specify what type of contact information is covered, nor*

*does it specify whether that contact information also covers, as may be inferred from the Commission's written answer to the questions posed by the Court, the contact information of 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.*

*159. As regards heading 8, that heading relates to "all available payment / billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)". It is true that that heading may appear to be particularly broad inasmuch as it employs the expression "all available information". Nevertheless, as is clear from the Commission's answer to the questions posed by the Court, that heading must be regarded 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. Construed in that way, heading 8 may therefore be regarded as meeting the requirements as to clarity and precision.*

*160. As regards heading 17, that heading refers to "general remarks including Other Supplementary Information (OSI), Special Service Information (SSI) and Special Service Request (SSR) information". According to the explanations provided, inter alia, by the Commission, that heading constitutes a "free text" heading, intended to include "all supplementary information", in addition to that listed elsewhere in the Annex to the envisaged agreement. Consequently, 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 information referred to in that heading is listed only by way of example, as is shown by the use of the term "including", heading 17 does not set any limitation on the nature and scope of the information that could be set out thereunder. In those circumstances, heading 17 cannot be regarded as being delimited with sufficient clarity and precision.*

*161. Lastly, as regards heading 18, that heading relates to "any Advance Passenger Information (API) data collected for reservation purposes". According to the clarifications provided by the Council and the Commission, that information corresponds to the information referred to in Article 3(2) of Directive 2004/82, namely 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, and the initial point of embarkation. That heading, in so far as it is construed as covering only the information expressly referred to in that provision, may be regarded as meeting the requirements as to clarity and precision.*

*162. The provisions of Article 4(3) of the envisaged agreement, which require Canada to delete any PNR data transferred to it if it is not listed in the Annex to that agreement, do not serve to offset the lack of precision of headings 5, 7 and 17*

*of that annex. Since that list does not itself delimit with sufficient clarity and precision the PNR data to be transferred, those provisions are incapable of resolving the uncertainties as to the PNR data to be transferred.*

*163. In those circumstances, as regards the PNR data to be transferred to Canada, headings 5, 7 and 17 of the Annex to the envisaged agreement do not delimit in a sufficiently clear and precise manner the scope of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter*'.

56 As some of those observations may be transposable to the present case, in relation to the fact that Annex I of the PNR Directive, which is transposed by Article 9 of the PNR Law, refers to some of the data it covers by way of example, and not exhaustively, the referring court decides to refer a third question to the Court for a preliminary ruling.

*The definition of 'passenger' (Article 4 10° of the PNR Law)*

57 The applicant objects to the breadth of the definition of 'passenger', which leads to systematic, non-targeted automated processing of the data of all passengers.

58 The effect of the definition of 'passenger' (Article 4 10° of the PNR Law) is that the obligations to collect, transfer and process PNR data relating to 'passengers' are general and undifferentiated in nature, applying to every person carried or to be carried who appears on the list of passengers. The obligations imposed by the PNR Law thus apply regardless of whether there are substantial grounds to believe that that the persons concerned have committed an offence, are on the point of committing an offence, or have been found guilty of an offence.

59 In its Opinion of 19 August 2016, the Consultative Committee of Convention 108 observed in this regard that '*the processing of PNR data — providing the unique benefit of enabling the identification of individuals of interest — is the general and indiscriminate screening of all passengers, including individuals who are not suspected of any crime, by different competent authorities and concerns data initially collected for commercial purposes by private entities. In light of the degree of interference with the rights to private life and data protection that would arise from such processing, the fact that this processing is a necessary measure in a democratic society for a legitimate aim has to be clearly evidenced and the appropriate safeguards must be put in place. A specific demonstration of the necessity is needed for the collection and further use of PNR data*' (Opinion of 19 August 2016, T-PD(2016)18rev, p. 5).

60 In the field of electronic communications, the Court has ruled on national legislation which provided for the general and indiscriminate retention of all traffic and location data relating to all subscribers and registered users, and to all methods of electronic communication, and imposed an obligation on providers of electronic communications services to retain such data systematically and

continuously, with no exceptions (judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970).

It held that '*while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight*' (paragraph 103).

The Court held, first, that the effect of such legislation was that the retention of traffic and location data was the rule, whereas the system put in place by Directive 2002/58 required the retention of data to be the exception, and secondly, that '*national legislation ... which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 57 and 58).*

*106. Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 59).*

*107. National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.*

*108. However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.*

*109. In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 54 and the case-law cited).*

*110. Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.*

*111. As regards the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.*

*112. Having regard to all of the foregoing, the answer to the first question referred in Case C-203/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication*'.

In answer to the second question in Case C-203/15 and the first question in Case C-698/15, the Court ruled that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted '*as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is*

*not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union*' (paragraph 125).

61 For its part, the European Court of Human Rights has since held Swedish legislation on bulk interception of electronic communications to be in conformity with Article 8 of the European Convention on Human Rights, in its judgment in *Centrum för Rättvisa v. Sweden*, of 19 June 2018. It stated, in particular, as follows:

'*The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security ... .In* Weber and Saravia *and* Liberty and Others *the Court accepted that bulk interception regimes did not per se fall outside this margin. Given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation*' (ECtHR, 19 June 2018, *Centrum för Rättvisa v. Sweden*, § 112).

The same court held, on the other hand, that United Kingdom law on the interception of communications infringed Article 8 ECHR, because it did not meet the criteria set out in its case-law. It also held that '*the operation of a bulk interception regime in principle falls within a State's margin of appreciation. Bulk interception is by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible*' (ECtHR, 13 September 2018, *Big Brother Watch v. the United Kingdom* § 317).

62 The question arises of how far the case-law referred to above, relating to generalised and indiscriminate retention of data in the area of electronic communications, can be transposed to generalised and indiscriminate collection, transfer and processing of passenger data, as provided for by the Law of 25 December 2016.

63 In Opinion 1/15 of 26 July 2015, the Court of Justice was considering a PNR scheme which was analogous but more limited in scope, as the draft agreement between Canada and the European Union on the transfer and processing of passenger data provided for '*the systematic and continuous transfer of PNR data of all air passengers flying between the European Union and Canada*' (paragraph 127). It held that '*the transfer of PNR data to Canada and subsequent processing of that data may be regarded as being appropriate for the purpose of*

*ensuring that the objective relating to the protection of public security and safety pursued by the envisaged agreement is achieved*' (paragraph 153).

As regards the passengers concerned, the Court held:

'*186.The envisaged agreement covers the PNR data of all air passengers flying between the European Union and Canada. The transfer of that data to Canada is 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.*

*187. In this connection, it should be pointed out that, as recalled in paragraphs 152 and 169 of this Opinion, the PNR data is intended, inter alia, to be subject to automated processing. As several of the interveners have stated, that processing is intended to identify the risk to public security that persons, who are not, at that stage, known to the competent services, may potentially present, and who may, on account of that risk, be subject to further examination. In that respect, the automated processing of that data, before the arrival of the passengers in Canada, facilitates and expedites security checks, in particular at borders. Furthermore, the exclusion of certain categories of persons, or of certain areas of origin, would be liable to prevent the achievement of the objective of automated processing of PNR data, namely identifying, through verification of that data, persons liable to present a risk to public security from amongst all air passengers, and make it possible for that verification to be circumvented.*

*188. Moreover, in accordance with Article 13 of the Chicago Convention, to which, in particular, the Council and the Commission have referred in their answers to the questions posed by the Court, all air passengers must, upon entrance into, departure from, or while within the territory of a contracting State, comply with the laws and regulations of that State as to air passengers' admission to or departure from its territory. All air passengers who wish to enter or depart from Canada are, therefore, on the basis of that article, subject to border control and are required to comply with the conditions on entry and departure laid down by the Canadian law in force. Furthermore, as is clear from paragraphs 152 and 187 of this Opinion, the identification, by means of PNR data, of passengers liable to present a risk to public security forms part of border control. Consequently, since they are subject to that control, air passengers who wish to enter and spend time in Canada are, on account of the very nature of that measure, subject to verification of their PNR data.*

*189. In those circumstances, the envisaged agreement does not exceed the limits of what is strictly necessary in so far as it permits the transfer of the PNR data of all air passengers to Canada*'.

64 The Cour constitutionnelle (Constitutional Court) raises the question of whether those considerations are applicable to the PNR Directive and to national legislation, such as the PNR Law, which transposes that directive and provides for

generalised and indiscriminate collection, transfer and use of PNR data relating to all passengers travelling by air, rail or bus, regardless of whether they cross an external border of the European Union. This system applies to individuals in relation to whom there is nothing giving reason to believe that their conduct may be linked — even indirectly or remotely — with serious crime, and is broader in scope than the system envisaged by the EU-Canada PNR agreement. Given the breadth of the data to which it relates, the question arises of whether the measure is confined to what is 'strictly necessary'. Before giving a substantive ruling, the Cour constitutionnelle (Constitutional Court) therefore decides to refer a fourth question to the Court for a preliminary ruling.

*The purposes for which PNR data are processed (Article 8 of the PNR Law)*

65 The applicant objects to the terms in which the purposes for which PNR data are processed are set out in Article 8 of the PNR Law, submitting that these are much broader than the 'specific purposes', limited to terrorist offences and serious crime referred to in the PNR Directive. It contends that those purposes go beyond what is 'strictly necessary'.

The purposes for which PNR data is to be processed, as laid down in Articles 1(2) and 6(2) of the PNR Directive, are limited to preventing, detecting, investigating and prosecuting terrorist offences and serious crime (see also recital 7 of the PNR Directive).

Some of the processing purposes contemplated by Article 8 of the PNR Law correspond to offences listed in Annex II of the PNR Directive, reflecting the objectives of preventing, detecting, investigating and prosecuting terrorist offences and serious crime pursued by that directive. However, some of the purposes for which PNR data is processed are additional to those provided for by the directive. Among these is 'furthering the activities referred to in Article 7 1° and 3°/l, and Article 11, § 1 1° to 3° and 5°, of the Organic law of 30 November 1998 on the intelligence and security services' (Article 8 § 1 4°).

The referring court considers whether those additional purposes are expressed in clear, precise rules which go no further than is strictly necessary, and expresses doubt as to whether that is so in relation to the purpose set out in Article 8 § 1 4° of the PNR Law.

The explanatory memorandum to the PNR Law states that this 'purpose relates to the functions of the intelligence services, namely State Security and the General Intelligence and Security Service (SGRS). In order to perform their functions of investigation, analysis and processing of information concerning activities representing a potential threat to the fundamental interests of the State, those services must be in a position to analyse passenger data in order to detect concrete threats as soon as possible, to monitor the movements of specific individuals, and to carry out analyses of broader developments or trends. This purpose encompasses functions relating to the investigation, analysis and processing of

information relating to the activities of foreign intelligence services on Belgian soil'. (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, p. 19-20).

While, generally speaking, the functions of the intelligence and security services do contribute to national and international security, the processing of PNR data in connection with the purpose referred to in Article 8 § 1 4° of the PNR Law seems very vague and general.

Furthermore, in relation to advance assessment of passengers, this purpose is treated in the same way as those referred to in Article 8 § 1 1°, 2° and 5° of the PNR Law (Articles 24 § 2 and 26 § 2).

Against that background, the Cour constitutionnelle (Constitutional Court) decides to refer a fifth question to the Court, with a view to establishing whether this purpose is sufficiently clear and precise, and whether it is limited to what is strictly necessary.

*Management of the passenger database and processing of data in the context of advance assessment of passengers and ad hoc searches (Articles 16, 24 to 27, and 50 and 51 of the PNR Law)*

66 The applicant contends that the various ways in which personal data is processed and transferred are manifestly disproportionate.

67 Article 16 of the PNR Law provides that, as regards the purposes contemplated by Article 8 § 1, passenger data is to be subject to the processing contemplated by Articles 24 to 27.

– *Advance assessment of passengers (Articles 24 to 26)*

68 Passenger data is processed with a view to carrying out an assessment of passengers (pre-screening) prior to their scheduled arrival in, departure from, or transit through Belgian territory, in order to identify persons who require further examination. 'This is a matter of assessing the potential threat and determining which passengers are of interest from the point of view of the performance of their functions or, for example, necessitate the taking of a particular step (such as the execution of an arrest warrant, or a search)'. (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, p. 28).

There are two aspects to advance assessment: comparison of the passenger data against databases, and comparison of the data against pre-determined criteria.

69 As regards comparison against databases, the preparatory documents relating to the PNR Law state that 'the first aspect is a search for positive matches which is made by comparing the passenger data against processed data held in the databases managed by the competent services. This enables, for example, an assessment to be made as to whether an individual is particularly dangerous, on

the basis that he appears in a police database in connection with a terrorist matter, and it is apparent on analysis of his passenger data that he regularly travels to countries that harbour terrorist training camps, or countries of transit to such places. Equally, information available from the intelligence services might indicate that the individual in question is planning a hostage operation, and the transport data may show that he is travelling to a country in which, as its intelligence services know from information received, he would be able to recruit with a view to executing his plan. Furthermore, the greater the number of positive matches identified in relation to one and the same individual, by multiple services, the greater the probability that the threat is real.

The positive match may equally call for a step to be taken under a judicial order, such as the execution of an arrest warrant in respect of an individual preparing to leave Belgium.

A positive match may also be identified on comparison of the passenger data against international databases such as SIS II or Interpol (SLTD).

Naturally, the objective is not to link all the services' databases to the passenger database, but to implement technical restrictions on database comparisons relating directly to the purposes laid down by the law.

…

The comparison can also be made using the lists of persons specifically produced for this purpose by the competent services. Under the Law on the protection of private life, and more specifically Article 4 § 1 4° of that law, those lists must be updated regularly' (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, p. 28-29).

70 As regards comparison against pre-determined criteria, the preparatory documents relating to the PNR law state:

'The second aspect is a search for positive matches using one or more criteria which have been predetermined by the PIU and are applied to the passenger data. The criteria are made up of one or more objective indicators on the basis of which it can be inferred that the conduct of the corresponding persons carries a specific risk, capable of constituting a threat in relation to the purposes set out in Article 8 § 1 1°, 4° and 5° of the law.

The criteria may, for example, relate to certain specific behaviours concerning reservations or travel.

Their use is beneficial in that it may bring to light profiles of high-risk passengers who are not necessarily known to or mentioned in the services' databases.

The criteria may relate, for example, to a country of destination or departure, combined with certain information on the journey such as the means of payment

and reservation date'. (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, p. 29-30).

'The advance assessment carried out in relation to the purpose concerning phenomena of administrative policing and groupings linked with violent radicalisation is subject to conditions much more restrictive that those relating to the other purposes …

As regards the advance assessment carried out in relation to the other purposes, access is permitted to all the passenger data set out in Article 9' (ibid. p. 31).

'All positive matches must be validated by the PIU. In order to ensure that the right to protection of personal data … is fully respected, no decision which has legal consequences for an individual, or is capable of causing him serious prejudice, can be taken solely on the basis of automated processing of the data in the file containing information on his journey. For that reason, an assessment will always be made by a human being before a decision is taken which is binding on the person concerned.

Such validation must take place within 24 hours in order for a right of access to the passenger database to arise.

After validation of the positive match, the services which originally identified the match are responsible for pursuing the matter efficaciously and within an appropriate timescale. Pursuing the matter efficaciously may mean taking active steps (for example, carrying out a search or arrest), but equally, it may mean refraining from taking active steps for the time being. This operational assessment is entirely a matter for the competent services' (ibid. p. 30-31).

71 As to the assessment criteria which are predetermined by the PIU, these may not be based on data indicating a person's race or ethnic origin, religion or philosophical beliefs, political opinions, trade union membership, health, sexual life or sexual orientation. The assessment of passengers prior to arrival, transit or departure against pre-determined criteria must be carried out in a non-discriminatory manner. The pre-determined criteria may not relate to the identification of an individual and must be targeted, proportionate and specific.

72 In its Opinion of 19 August 2016 the Consultative Committee of Convention 108 stated as follows:

'*The processing of personal data may concern all passengers and not only the targeted individuals suspected of involvement in a criminal offence or posing an immediate threat to national security or public order.*

…

*This assessment of passengers by data mining may raise the question of predictability, in particular when operated on the basis of predictive algorithms*

*using dynamic criteria which may constantly evolve in light of self-learning capacities.*

*The development of data mining algorithms should be based on the results of regular assessments of the likely impact of the data processing on the rights and fundamental freedoms of data subjects.*

*The basic structure of the analyses should be based on predefined risk indicators which have been clearly identified in advance.*

*The relevance of individual results of such automatic assessments should be carefully examined on a case-by-case basis, by a person in a non-automated manner*' (Opinion of 19 August 2016, T-PD(2016)18rev, p. 8).

73 In the present case, the databases referred to in Article 24 are defined with precision and relate directly to the purposes contemplated by Article 8 of the PNR Law. They are the databases of the 'competent services', which means the police, State Security, General Intelligence and Security and Customs services.

Furthermore, Article 24 § 4 and § 5 of the PNR Law ensures, as required by Article 6(5) of the PNR Directive, that any positive match resulting from automated systematic processing is individually reviewed by non-automated means, to verify whether the competent authority needs to take action under national law.

74 In Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592), the Court of Justice also insisted on the need for individual re-examination by non-automated means before an individual measure is adopted (paragraph 173).

The requirement for human intervention, after a positive match has been identified, constitutes a safeguard serving to ensure that advance assessment is not solely based on automated methods, and thus contributes to the effectiveness of the system.

Accordingly, a systematic advance assessment of passengers is, in principle, a relevant measure with respect to the objective of identifying and preventing threats to public security.

As the Court of Justice nevertheless observed in Opinion 1/15 of 26 July 2017, the processing carried out in the course of advance assessment '*may provide additional information on the private lives of air passengers*' (paragraph 131); furthermore, '*the analyses are carried out without there being reasons based on individual circumstances that would permit the inference that the persons concerned may present a risk to public security*' (ibid., paragraph 132).

Noting that the automatic processing of PNR data, based on pre-established models and criteria, presented a significant margin of error (ibid., paragraphs 169-170), the Court nevertheless held that '*the pre-established models and criteria*

*should be specific and reliable, making it possible … to arrive at results targeting individuals who might be under a "reasonable suspicion" of participation in terrorist offences or serious transnational crime and should be non-discriminatory*', and that '*the databases with which the PNR data is cross-checked must be reliable, up to date and limited to databases used by Canada in relation to the fight against terrorism and serious transnational crime*' (ibid., paragraph 172). Lastly, in order to ensure that the assessment is not discriminatory and is limited to that which is strictly necessary, the Court held that '*the reliability and topicality of those pre-established models and criteria and databases used should, taking account of statistical data and results of international research, be covered by the joint review of the implementation of the envisaged agreement*', a year after its entry into force, and then at regular intervals (ibid., paragraph 174).

75 In addition, it appears to be technically impossible to define the pre-determined criteria which are to be used to identify high-risk profiles any further. As has been stated above, such criteria must be specific, reliable and non-discriminatory.

76 Although neither the PNR Directive nor the PNR Law indicates how the advance assessment criteria are to be pre-determined by the PIU, the safeguards surrounding the establishment of those criteria appear to be sufficient for the contested measure not to be regarded as disproportionate. It is nevertheless appropriate, in order to determine whether such advance systematic assessment is sufficiently clear, to refer a sixth question to the Court for a preliminary ruling.

– *Ad hoc searches (Articles 27, 50 and 51)*

77 Article 27 of the PNR Law authorises the processing of passenger data with a view to carrying out ad hoc searches for the purposes contemplated by Article 8 § 1 1°, 2°, 4° and 5°, subject to the conditions set out in Article 46 septies of the Criminal Procedure Code or Article 16/3 of the Law of 30 November 1998, which were inserted, respectively, by Articles 50 and 51 of the PNR Law. Under Article 20 of the PNR Law, the applicability conditions of Article 27 also govern requests for access made after the six-month period referred to in Article 19 has expired.

78 Article 46 septies of the Criminal Procedure Code concerns ad hoc searches relating to the purposes contemplated by Article 8 § 1 1°, 2° and 5° of the PNR Law. This measure is subject to a number of safeguards, including prior authorisation from the crown prosecutor.

79 As to Article 16/3 of the Law of 30 November 1998, this concerns ad hoc searches relating to the purpose contemplated by Article 8 § 1 4° of the PNR Law. This measure is subject to a number of safeguards, including a requirement to inform Permanent Committee R, which then performs a monitoring function.

80 The applicant submits that the personnel seconded from the police services to the PIU are not sufficiently independent to deal with requests for access in the context of such ad hoc searches.

81 The composition of the PIU is laid down by Article 14 § 1 of the PNR Law. The preparatory work indicates, in this regard, that '*the Belgian model is based on the concept of a multidisciplinary unit made up of a civil servant director responsible for its leadership, administrative staff, and personnel seconded from the competent services.*

*The PIU will be made up of:*

– *a civil servant director, assisted by a support department, who is responsible within the Ministry of the Interior for, amongst other things, management of the database, compliance by carriers and tour operators with their obligations, reporting, concluding protocols with the competent services, and compliance with the processing conditions. The support department will include analysts, lawyers, IT experts and the data protection officer, who will have the necessary security clearance.*

– *of personnel seconded from the competent services referred to (exhaustively) in § 1 2°, namely the police services, the intelligence services and Customs. The precisely defined purposes are, in themselves, the first restriction. For example, at combined police service level, it is clear that a neighbourhood officer in a local force could never become aware of passenger data inasmuch as the purposes do not form part of his functions.*

*The secondment of personnel from the competent services is intended to guarantee a certain level of expertise but in no way does it prevent those services from entering into secondment pooling agreements*.' (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, p. 22).

The Minister for Security and the Interior added that '*a data protection officer will also be designated, with responsibility for reporting to the Commission for the Protection of Private Life*' (Doc. Parl, Chamber, 2015-2016, DOC 54-2069/003, p. 24).

The Royal Decree of 21 December 2017 relating to the execution of the PNR Law makes detailed provision as regards the composition and organisation of the PIU. The report to the King which preceded that Royal Decree states that '*the database can only ... be consulted within the PIU, and only by members of the PIU, in the course of performing their functions, and the data protection officer*'. [3]

Procedural arrangements for secondment are laid down in Articles 12 to 21 of that Royal Decree. The participation of personnel seconded from the competent

[3] Moniteur Belge, 29 December 2017, second edition, p. 116833.

services in the operation of the PIU is intended to guarantee that it is made up of personnel with a certain expertise, in order to strengthen its effectiveness. The possibility of secondment is, moreover, expressly provided for in Article 4(3) of the PNR Directive.

There is nothing to justify the view that such persons do not act independently in performing their functions within the PIU, even if they retain their status in the service from which they have been seconded. Furthermore, members of the PIU may be subject to criminal law penalties if they do not respect professional secrecy, or if they consciously and deliberately retain information or data which obstructs the purposes contemplated by Article 8 (Articles 48 and 49).

82 As regards access to PNR data in the context of ad hoc searches after a period of six months has passed, the Court held, in Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592), that the use of PNR data so stored should '*be based on objective criteria in order to define the circumstances and conditions under which the Canadian authorities referred to in the envisaged agreement may have access to that data in order to use it*' and that '*that use should, 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; the decision of that court or body authorising the use being made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime*' (paragraph 208).

83 In order to establish whether the PIU should be regarded as 'another national authority competent under national law' within the meaning of Article 12(3) of the PNR Directive, it is appropriate, before ruling on the matter, to refer a seventh question to the Court of Justice for a preliminary ruling.

*The period during which PNR data are retained (Article 18 of the PNR Law)*

84 The applicant submits that the retention period of five years which applies to PNR data is disproportionate.

85 Recital 25 of the PNR Directive states:

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

86 Under the case-law of the Court of Justice, the period during which data are retained must '*continue to satisfy objective criteria that establish a connection between the data to be retained and the objective pursued*' (judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 93; Order of 16 March 2017, *Tele2 Sverige and Watson and Others*, C-203/15 REC and C-698/15 REC, EU:C:2017:222, paragraph 110; Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 191).

87 In relation more specifically to PNR data, the Court of Justice held, in Opinion 1/15 of 26 July 2017, that the five-year retention period '*does not exceed the limits of what is strictly necessary for the purposes of combating terrorism and serious transnational crime*' (paragraph 209) with the caveat that '*as regards air passengers in respect of whom no such risk has been identified on their arrival in Canada and up to their departure from that non-member country, there would not appear to be, once they have left, a connection — even a merely indirect connection — between their PNR data and the objective pursued by the envisaged agreement which would justify … the continued storage of the PNR data of all air passengers after their departure from Canada for the purposes of possibly accessing that data, regardless of whether there is any link with combating terrorism and serious transnational crime (see, by analogy, judgment of 21 December 2016,* Tele2 Sverige and Watson and Others, *C-203/15 and C-698/15, EU:C:2016:970, paragraph 119)*' (paragraph 205).

88 Article 18 of the PNR Law provides for passenger data to be retained in the passenger database for no more than five years from initial storage, and deleted on the expiry of that period. Under Article 21 § 1 of that law, the PIU is to ensure that passenger data are permanently erased from its database on expiry of the period mentioned in Article 18.

The period of five years must nevertheless be read in combination with Articles 19 et seq. of the PNR Law, which also make provision as regards the retention of data. Article 19 of the law must itself be read in conjunction with Article 4 14°, which defines 'depersonalisation through masking out of data elements' as 'making data elements capable of directly identifying the person concerned invisible to users, as provided for by Article 19'.

Article 20 of the PNR Law provides that on expiry of the six-month period referred to in Article 19, the passenger data can be transferred in its entirety only for the purposes of the data processing provided for by Article 27, and only on the conditions referred to in that article.

Furthermore, the result of the processing contemplated by Article 24 is only retained by the PIU for as long as is necessary to inform the competent authorities, and the PIUs of other Member States, that a positive match has been found (Article 21 § 3, first subparagraph).

Article 22 of the PNR Law ensures that it is only in the course of performing their functions that the official who heads the PIU and the data protection officer have access to all relevant data.

Finally, the processing of data is required to be logged and to relate directly to the purposes contemplated by Article 8 (Article 23 § 1). The PIU is responsible logging and is required to retain, for a period of five years, a documented history of all the systems and processing procedures within its remit (Article 23 § 2, first subparagraph).

89 The period of retention of passenger data must be determined in the light of the purposes for which such data is processed, relating directly to the objectives of prevention, detection and prosecution of terrorist offences and serious crime.

90 The Commission for the Protection of Private Life had nevertheless observed that, where data is retained for a long period and is stored en masse, '*the risk of the persons concerned being profiled rises, as does the risk of function creep, or in other words the potential for illegitimate use of the data in relation to offences for which there was, initially, no (political) data transfer agreement*' (Commission for the Protection of Private Life, Opinion No 01/2010 of 13 January 2010, produced on the Commission's own initiative, on the Draft law ratifying the Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), done at Brussels on 23 July 2007 and at Washington on 26 July 2007, paragraph 3.3, p. 17-18).

In Opinion No 55/2015 of 16 December 2015 on the draft bill which became the PNR Law, the Commission for the Protection of Private Life also stated, in relation to the need to retain the data for five years, that a more precise and better supported justification was required.

In its Opinion of 19 August 2016, the Consultative Committee of Convention 108 had also observed that 'masked out data still enables individuals to be identified and continues as such to constitute personal data, and that its conservation should also be limited in time in order to avoid permanent and general surveillance' (Opinion of 19 August 2016, T-PD(2016)18rev, p. 9).

91 The Cour constitutionnelle (Constitutional Court) considers that in order to establish whether the retention period of five years, authorised by the PNR Directive, is, in the light of the foregoing and of the various safeguards referred to in paragraph 88 above, compatible with the observations of the Court of Justice referred to in paragraph 87 above, given that it makes no distinction on the basis of whether the passengers in question were identified, in the advance assessment, as presenting a public security risk, it is necessary to refer an eighth question to the Court for a preliminary ruling.

### *3. The second plea in law*

92 The applicant argues that by extending the PNR system to intra-EU flights, the contested provisions indirectly re-establish border controls which are contrary to the free movement of persons.

93 As regards the scope of the PNR Law, the preparatory work indicates that:

'The inclusion of intra-EU travel in the data collection will provide a fuller picture of passenger movements representing a potential threat to intra-Community and national security. Experience shows that certain 'returnees' (or 'foreign fighters' returning to Europe) board various different flights before taking travelling to their final destination.

The EU PNR Directive expressly permits Member States to process EU passenger data in relation to international transport within the European Union. Furthermore, on 21 April 2016, at the Council of Ministers for Justice and Home Affairs, all the Member States approved a declaration to the effect that the transposition of the EU PNR Directive into their national law would extend to intra-EU transport' (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, p. 7).

94 The Cour constitutionnelle (Constitutional Court) notes that the passengers referred to in Chapter 11 of the PNR Law are defined in limited terms, as are the data in question and the retention period.

The preparatory work indicates that '… the only passengers affected are those wishing to enter or leave Belgium via an external border, or already having done so, regardless of the mode of transport (sea, rail, land or air). Hence it is only the data of those passengers which will be processed by the police services responsible for border control and the foreign nationals bureau.

Passengers intending to transit through the international transit zone, for example, of an airport located in Belgium, are also affected inasmuch as the rules concerning access to the territory, residence, establishment and removal of foreign nationals also apply to them. Such persons must therefore hold the necessary travel documents. Certain persons are required to hold airport transit visas; controls are permitted in these zones and may, in certain circumstances, lead to refoulement.

… only the so-called API passenger data will be transferred to the police services and the foreign nationals bureau under this chapter. Those data are enumerated in Article 9(2) of the draft bill.

They essentially correspond to the data which air carriers are already required to transfer under the Royal Decree of 11 December 2006.

…

The use of the data is also restricted to 24 hours. Once 24 hours have passed, if the foreign nationals bureau requires access to passenger data for the purposes of performing the functions assigned to it by law, it must send a reasoned request to the PIU' (ibid. p. 34-35).

95 As has been noted above, recital 10 of the PNR Directive permits the PNR system to be extended to intra-EU flights. Article 2 of the PNR Directive makes provision as to the procedure for extending the scope.

The purpose of combating illegal immigration and improving border control relates only to the categories of passengers enumerated in Article 29 § 2 of the PNR Law, and is limited to the API data referred to in Article 9 § 1 18°, of that law. The processing carried out for that purpose is also limited. The contested provisions relate to the transposition of the API directive, which also pursues the objectives of combating illegal immigration and improving border control.

96 In Opinion No 55/2015 of 16 December 2015 on the draft bill which became the Law of 25 December 2016, the Commission for the Protection of Private Life nevertheless raised the issue of whether the PNR system it establishes, which relates 'both to journeys to and from the Schengen area (extra-Schengen), and to journeys entering and leaving the Schengen area (intra-Schengen)', and might thus lead 'indirectly to a re-establishment of internal border controls', is compatible with the free movement of persons (paragraphs 21 to 25).

97 The Cour constitutionnelle (Constitutional Court), being uncertain as to the interpretation and validity of the API Directive (Directive 2005/82) in the light of the Charter and of the TEU, decides to refer a ninth question to the Court for a preliminary ruling.

98 The Cour constitutionnelle (Constitutional Court) also refers a final question in relation to the possibility of making specific provision as to the temporal effects of its judgment.

## IV. Questions referred for a preliminary ruling

The Cour constitutionnelle (Constitutional Court) accordingly refers the following questions for a preliminary ruling:

1. Is 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' (the General Data Protection Regulation — GDPR), read in conjunction with Article 2(2)(d) of that regulation, to be interpreted as applying to national legislation such as the Law of 25 December 2016 'on the processing of passenger data', which 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', as well as 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'?

2. Is Annex I of Directive (EU) 2016/681 compatible with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union, given that the data it refers to are very wide in scope — particularly the data referred to in paragraph 18 of Annex I to Directive (EU) 2016/681, which go beyond the data referred to in Article 3(2) of Directive 2004/82/EC — and also given that, taken together, they may reveal sensitive information, and thus go beyond what is 'strictly necessary'?

3. Are paragraphs 12 and 18 of Annex I to Directive (EU) 2016/681 compatible with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union, given that, having regard to the word 'including', the data referred to in those paragraphs is given by way of example and not exhaustively, such that the requirement for precision and clarity in rules which interfere with the right to respect for private life and the right to protection of personal data is not satisfied?

4. Are Article 3(4) of Directive (EU) 2016/681 and Annex I of the that directive compatible with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union, 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 Directive (EU) 2016/681, read in conjunction with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union, to be interpreted as precluding national legislation such as the contested law, which includes, among the purposes for which PNR data is processed, furthering 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 Directive (EU) 2016/681 compatible with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union, given that the advance assessment for which it provides, which is made by comparing passenger data against databases and predetermined 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 Directive (EU) 2016/681 be interpreted as including the PIU created by the Law of 25 December 2016, which would then have power to authorise access to PNR data after six months had passed, for the purposes of ad hoc searches?

8. Is Article 12 of Directive (EU) 2016/681, read in conjunction with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union, 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 Directive 2004/82/EC compatible with Article 3(2) of the Treaty on European Union and Article 45 of the Charter of Fundamental Rights of the European Union, given that the obligations for which it provides apply to flights within the European Union?

(b) Is Directive 2004/82/EC, read in conjunction with Article 3(2) of the Treaty on European Union and Article 45 of the Charter of Fundamental Rights of the European Union, 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 Belgium, 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, Directive (EU) 2016/681, fails to fulfil one or more of the obligations arising under the provisions referred to in those questions, would it be open to it to maintain the effects of the Law of 25 December 2016 ‘on the processing of passenger data’, on a temporary basis, in order to avoid legal uncertainty and enable the data hitherto collected and retained to continue to be used for the purposes envisaged by the law?