**Case C-215/20**

**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:**

19 May 2020

**Referring court:**

Verwaltungsgericht Wiesbaden (Germany)

**Date of the decision to refer:**

13 May 2020

**Applicant:**

JV

**Defendant:**

Bundesrepublik Deutschland

---

**Subject matter of the main proceedings**

Permissibility of the transfer of passenger name record data

**Subject matter and legal basis of the request**

Interpretation of EU law, Article 267 TFEU

**Questions referred**

1. In the light of its objective and the need for clarity and proportionality, is Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the [use of passenger name record (PNR) data for the] prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132) ('the PNR Directive'), under which air carriers transfer comprehensive data on every single passenger to the passenger information units (PIUs) established by the Member States, where the data are used without justification for automated comparison against

databases and profiles, after which they are retained for a period of five years[,] compatible with the Charter of Fundamental Rights of the European Union, especially Articles 7, 8 and 52 thereof?

2. In particular:

(a) In the light of the need for sufficient clarity and proportionality and inasmuch as it defines the term 'serious crime' within the meaning of the PNR Directive as the offences listed in Annex II that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State, is point (9) of Article 3 of the PNR Directive, read in conjunction with Annex II to the PNR Directive, compatible with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union?

(b) Inasmuch as they require the transfer of the name (first sentence of Article 8(1) of the PNR Directive, read in conjunction with point (4) of Annex I to the Directive), frequent flyer information (first sentence of Article 8(1) of the PNR Directive, read in conjunction with point (8) of Annex I to the Directive) and general remarks in a 'free text' box (first sentence of Article 8(1) of the PNR Directive, read in conjunction with point (12) of Annex I to the Directive), are the passenger name record data ('PNR data') to be transferred defined with sufficient clarity to justify interference with the rights set out in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union?

(c) Is the fact that data are collected not only on passengers, but also on third parties, such as travel agency/travel agent (point (9) of Annex I to the PNR Directive), guardians of minors (point (12) of Annex I to the PNR Directive) and other travellers (point (17) of Annex I to the PNR Directive), compatible with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and the purpose of the PNR Directive?

(d) Inasmuch as the PNR data of minor passengers are transferred, processed and retained, is the PNR Directive compatible with Articles 7, 8 and 24 of the Charter of Fundamental Rights of the European Union?

(e) In the light of the principle of data minimisation and inasmuch as it allows air carriers to transfer API data to the PIUs of the Member States even where they are identical to PNR data, is Article 8(2) of the PNR Directive, read in conjunction with point (18) of Annex I to the Directive, compatible with Articles 8 and 52 of the Charter of Fundamental Rights of the European Union?

(f) As the legal basis for determining the criteria for data comparison ('profiles'), is Article 6(4) of the PNR Directive a sufficient legitimate basis laid down by law within the meaning of Article 8(2) and Article 52 of the

Charter of Fundamental Rights of the European Union and Article 16(2) TFEU?

(g) As the data transferred are retained by the PIUs of the Member States for a period of five years, does Article 12 of the PNR Directive limit interference with the rights enacted in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union to what is strictly necessary?

(h) Where depersonalisation in accordance with Article 12(2) of the PNR Directive is no more than pseudonymisation that can be reversed at any time, does it reduce the personal data to the minimum required under Articles 8 and 52 of the Charter of Fundamental Rights of the European Union?

(i) Are Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union to be interpreted as meaning that the passengers whose data are de-depersonalised during passenger data processing (Article 12(3) of the PNR Directive) must be notified accordingly and thus afforded the opportunity to seek a judicial review?

3. Inasmuch as it allows PNR data to be transferred to third countries which do not have an appropriate level of data protection, is Article 11 of the PNR Directive compatible with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union?

4. As the 'free text' box for 'general remarks' (point (12) of Annex I to the PNR Directive) can be used to transfer information such as choice of meal, from which particular categories of personal data can be inferred, does the fourth sentence of Article 6(4) of the PNR Directive afford adequate protection against the processing of those particular categories of personal data within the meaning of Article 9 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 (OJ 2016 L 119, p. 1) and Article 10 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89)?

5. Is the fact that air carriers simply refer passengers on their website to the national transposing legislation (in this case, the Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Law on the Processing of Passenger Name Record (PNR) Data for the purpose of transposing Directive (EU) 2016/681) of 6 June 2017

(*BGBl* (Federal Law Gazette) I, p. 1484) compatible with Article 13 of the General Data Protection Regulation?

**Provisions of EU law cited**

Charter of Fundamental Rights of the European Union ('the Charter'), Articles 7, 8, 24, 47 and 52.

Article 16 TFEU

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132)

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

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

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)

**Provisions of national law cited**

Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Law on the Processing of Passenger Name Record (PNR) Data for the purpose of transposing Directive (EU) 2016/681) ('the FlugDaG')

**Brief summary of the facts and procedure**

1 The FlugDaG transposing Directive 2016/681 into German law entered into force on 10 June 2017. That directive regulates the transfer of PNR data of passengers flying from Member States of the European Union to third countries and from third countries to Member States of the European Union and the processing of those data.

2 According to Article 1(2) of Directive 2016/681, its purpose is to prevent, detect, investigate and prosecute terrorist offences and serious crime. Article 4 of the Directive requires the Member States to establish a passenger information unit (PIU) responsible for collecting PNR data from air carriers, for storing, processing and transferring those data to the competent authorities and for exchanging both PNR data and the result of processing such data. According to Article 8 of Directive 2016/681, read in conjunction with Annex I thereto, the Member States are required to oblige all air carriers to transfer predefined PNR data to the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart. Article 9 of Directive 2016/681 allows the Member States to request and transfer PNR data from and to one another. Data can also be transferred to third countries subject to the requirements of Article 11 of the Directive. Article 12(2) of Directive 2016/681 states that the PNR data stored, which must be retained for a period of five years, must be 'depersonalised' upon expiry of a period of six months by masking out the data elements which could serve to identify directly the passenger to whom the PNR data relate. However, those data elements can be de-depersonalised subject to the requirements of Article 12(3) of Directive 2016/681. Article 6 of the Directive regulates processing of the data, in particular by automated comparison of the data against databases and pre-determined criteria (referred to in the FlugDaG as 'profiles').

3 The applicant flew with the air carrier Lufthansa from Frankfurt am Main (Germany) to Bogota (Columbia) on 28 April 2019 and from Rio de Janeiro (Brazil) back to Frankfurt am Main on 7 May 2019. He has requested the defendant to erase his data in respect of those flights.

**Brief summary of the basis for the request**

4 The decision in the main proceedings depends on whether, as a whole or in part, Directive 2016/681 infringes the Charter. If it does, the transposition law (FlugDaG) would not be applicable, the contested data processing would consequently be unlawful and the applicant would be entitled to have the data erased.

***Question 1: Is Directive 2016/681 as a whole compatible with the Charter?***

5 The various ways in which PNR data may be processed under Directive 2016/681 and the FlugDaG interfere with the scope of the fundamental right to respect for private life guaranteed under Article 7 of the Charter, as that right concerns any information relating to an identified or identifiable individual (see judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 52), including therefore the information listed in Annex I to Directive 2016/681 on the data subject whose PNR data are processed. Furthermore, the processing of PNR data provided for in Directive 2016/681 also comes within the scope of Article 8 of the Charter, because it constitutes the processing of personal data within the meaning of that article and, accordingly,

must necessarily satisfy the data-protection requirements laid down in that article (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 123).

6 As the Court of Justice has held, the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental right enshrined in Article 7 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to the data with a view to its use by public authorities. In this connection, it does not matter whether the information communicated is to be regarded as being of a sensitive character or whether the persons concerned have been inconvenienced in any way (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 124). The same is true of Article 8 of the Charter where personal data are being processed (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 126).

7 Although the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, they must be considered in relation to their function in society (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 136). It is perfectly permissible to limit those rights in order to attain an objective of general interest, which would include combating terrorist offences and serious crime (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 149). However, interference with fundamental rights must be appropriate and necessary to attain the objectives and must not prove to be disproportionate in the narrow sense. Moreover, Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must 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 (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 138).

8 It is settled case-law of the Court of Justice that the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives (judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 46). So far as concerns the right to respect for private life, the Court's settled case-law requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52).

9 In order to meet that requirement, the legislation containing the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards. The persons whose data are transferred must have sufficient guarantees to protect effectively their personal data against the risk of abuse. The legislation must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing

of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are subjected to automated processing. This applies in particular where the protection of the particular category of personal data that is sensitive data is at stake (judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55).

10 Serious doubts exist as to whether Directive 2016/681 takes full account of those requirements.

11 Directive 2016/681 requires air carriers to transfer the PNR data of every single passenger on every single flight to the Member States' PIUs, where the data are subjected to automatic processing and continued storage. There is no need to establish a precise reason for this, such as specific evidence of a connection to international terrorism or organised crime. This means that hundreds of billions of data items are processed and stored within short periods of time. The 'retention of data' on passengers therefore manifestly affects the fundamental rights of a very large section of the overall population of Europe.

12 The data to be transferred, which are prescribed in the first sentence of Article 8(1) of Directive 2016/681, read in conjunction with Annex I thereto, are extremely comprehensive and include, in addition to the passenger's name, address and complete travel itinerary, information on his or her luggage, other travellers, all forms of payment information and unspecified 'general remarks'. Very accurate inferences concerning the private and professional life of the data subjects can be drawn from these overall data, such as who travelled where and when and with whom, what means of payment were used and what contact data were provided and whether the data subject travelled lightly or with heavy luggage. Additional data, the extent of which is entirely unclear (see below), can be provided in the 'free text' box for 'general remarks'.

13 In the opinion of the referring court, there is a similarity between PNR data processing and storage and the retention of data in the telecommunications sector, which the Court of Justice has held constitutes a wide-ranging and particularly serious interference with the rights laid down in Articles 7 and 8 of the Charter. This is because the unjustified large-scale retention of comprehensive data that allow inferences to be drawn concerning the private and professional life of the data subject is likely to generate a feeling of constant surveillance in the minds of the persons concerned (judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 37).

14 In its first judgment on the retention of data, the Court found that it was contrary to fundamental rights, not least because data are also retained on persons in respect of whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime (judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 58). This is also true for the processing and retention

of PNR data, which illustrates that the rules in Directive 2016/681 go beyond what is necessary to attain the objectives of the Directive and are therefore disproportionate within the meaning of the Court's case-law. Furthermore, unlike telecommunications traffic data, not only are PNR data retained without justification but they are also subjected to further processing in the form of automated comparison against databases and 'profiles'.

***Question 2(a): Definition of 'serious crime'***

15 The question also arises as to the precision and proportionality of PNR data collection and processing with regard to the crimes that this procedure is designed to combat. The stated objective of Directive 2016/681 is the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Point (9) of Article 3 of the Directive defines 'serious crime' as the offences listed in Annex II that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State. Annex II to Directive 2016/681 contains a list of 26 offences referred to in point (9) of Article 3. They include, for example, corruption (point (6)), fraud (point (7)), computer-related crime/cybercrime (point (9)) and environmental crime (point (10)).

16 The first question that arises is the precision of that legislation. For example, the crime of 'corruption' does not exist in German penal law, in which it is used as a generic heading for a number of offences. The same is true of the terms 'fraud', 'computer-related crime' and 'environmental crime'.

17 Due to this and the reference to the penalty imposed in the individual Member States in point (9) of Article 3 of Directive 2016/681, PNR data are not used uniformly in the different Member States. In fact, it is left to the individual Member States to include certain crimes by providing for their punishment under their national penal code as 'serious crime' within the meaning of the Directive, or to choose not to do so.

18 Moreover, the referring court has doubts as to whether the penalty of a maximum period of at least three years laid down in point (9) of Article 3 of Directive 2016/681 is an appropriate rule. It would appear to be highly questionable to classify the plethora of offences that this would include under German penal law as 'serious crime'. For example, the penalty for ordinary fraud under Paragraph 263 of the Strafgesetzbuch (German Criminal Code; 'the StGB') is a custodial sentence for a maximum period of five years. The same applies, for example, to receiving stolen goods (Paragraph 259 of the StGB), computer fraud (Paragraph 263a of the StGB) and breach of trust (Paragraph 266 of the StGB). All of these offences can be subsumed under offences listed in Annex II to Directive 2016/681 (especially 'fraud' as referred to in point (7)). However, these offences are 'day-to-day' crimes committed frequently and possibly also in minor cases, meaning that their inclusion within the scope of Directive 2016/681 has nothing to do with the prevention and prosecution of serious crime.

***Question 2(b): Precision of PNR data***

19 In the light of the fact that the Court requires the legislation to lay down clear and precise rules governing the scope and application of the measures in question (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 141), some of the PNR data which air carriers have to send to the Member States' PIUs are not defined with sufficient precision in Annex I to Directive 2016/681.

20 It is not clear what is meant by the 'name(s)' to be transferred (point (4) of Annex I to Directive 2016/681). This is illustrated in the German transposition by points (1) and (9) of Paragraph 2 of the FlugDaG, which states that the family name, name at birth, given names and any doctoral degree should be transferred, together with other nominal information. In common parlance, a person asked for his name will not generally also give his name at birth. Thus, it is unclear whether this comes under the 'name(s)' referred to in point (4) of Annex I to Directive 2016/681. The question also arises as to whether a name within the meaning of the Directive includes an academic title.

21 The legislation is also imprecise with regard to the transfer and processing of frequent flyer information (point (8) of Annex I to Directive 2016/681). In particular, it is unclear whether this simply refers to membership of a frequent flyer rewards scheme or to specific information about the flights and bookings of the members of such a scheme.

22 Point (12) of Annex I to Directive 2016/681 ('general remarks (including …')) is very broadly worded and imprecise. As the word 'including' suggests, the matters mentioned are examples, not an exhaustive list. Furthermore, information might be included in this 'free text' box that is entirely unrelated to the purpose of the collection of PNR data (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 160). In particular, the wording might also allow information to be transferred that is not required under Directive 2016/681, namely data of a sensitive character which, as is apparent from recital 15 of Directive 2016/681, should not be collected (see also Question 4 in this regard).

***Question 2(c): Third parties***

23 Article 1(1) of Directive 2016/681 provides for the transfer by air carriers of passenger name record (PNR) data of passengers of extra-EU flights and the processing of those data by the Member States. According to point (4) of Article 3 of the Directive, '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. However, Annex I to Directive 2016/681 refers to several items of data that do not relate to the passengers as defined above. In that regard, the rules laid down in the Directive are contradictory.

24 For example, that fact that point (9) of Annex I to the Directive provides for information to be collected on the travel agency and travel agent contradicts point (4) of Article 3 of Directive 2016/681. According to point (12) of Annex I to the Directive, the 'free text' box for 'general remarks' should be used in particular for information on the guardians of minors on departure and on arrival and on the agent.

25 Clearly, none of these data concerns the groups of passengers defined in point (4) of Article 3 of Directive 2016/681. Nevertheless, they are to be transferred by air carriers and retained by the Member States' PIUs. In that regard, the referring court assumes that the overall legislation is not limited to what is strictly necessary within the meaning of the Court's case-law (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 141). With regard to all third parties, the question also arises as to how they are to be informed in accordance with Article 14 of the GDPR about the processing of their personal data.

26 According to point (17) of Annex I to Directive 2016/681, the PNR data of other travellers should also be transferred and processed. As they are already subjected to PNR data processing as passengers, this means that the data are collected twice. This is a serious infringement of the data minimisation requirement (see Article 5(1)(c) of the GDPR).

***Question 2(d): Minors***

27 Directive 2016/681 requires air carriers to transfer the PNR data of every single passenger to the PIUs of the respective Member States, meaning that minors are also affected.

28 Data relating to minors may be processed for the purpose of preventive and/or punitive measures against minors (suspected of being) involved in terrorism or serious crime, on the one hand, or for the protection of minors, for example to detect or prosecute child trafficking, on the other. These two different objectives require differentiated legislation. This is illustrated by Article 6 of Directive 2016/680, which states that, as far as possible, a clear distinction must be made between personal data of different categories of data subjects. These different categories include in particular persons in regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence (Article 6(a) of Directive 2016/680) and victims of a criminal offence or persons in regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence (Article 6(c) of Directive 2016/680).

29 However, where data are collected and processed for the purpose of punitive or preventive measures against minors, care must be taken to ensure that prosecution based on findings from PNR data processing is possible only for adolescents who have reached the age of criminal responsibility. In that regard, Directive 2016/681

goes beyond what is strictly necessary, as it does not exclude the data of minors under the age of criminal responsibility.

30 With regard to the collection and processing of PNR data for the purpose of protecting minors, it has to be noted that children and adolescents are particularly vulnerable persons. This is highlighted in Article 24 of the Charter, which grants them fundamental EU rights of their own for their particular protection. This particular vulnerability also applies with regard to the processing of their personal data. Inasmuch as PNR data on minor passengers are collected and processed for the purpose of preventing or prosecuting crimes against children, Directive 2016/681 does not appear to contain appropriate rules. PNR data are processed for the purpose of detecting or identifying suspects. This is done by automated comparison of the PNR data against databases and profiles in order to identify suspects (see Article 6(2) of Directive 2016/681). However, in the context of the protection of minors from child trafficking, data on minors are data on vulnerable persons, not data on suspects. Therefore, they must also be handled differently. There is no need to compare them with profiles. In that regard, Directive 2016/681 is clearly lacking sufficiently differentiated rules for the handling of PNR data relating to minor passengers.

***Question 2(e): API data***

31 Article 8(2) of Directive 2016/681 requires Member States to adopt the necessary measures to ensure that API data within the meaning of point (18) of Annex I to the Directive, 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, are transferred to the PIUs. In that regard, there are numerous overlaps between the API data and the PNR data, which are transferred anyway, such as the dates of intended travel (point (3) of Annex I to Directive 2016/681), names (point (4) of Annex I to Directive 2016/681) or complete travel itinerary (point (7) of Annex I to Directive 2016/681).

32 This duplicated processing of passenger data conflicts with the principle of data minimisation enshrined in Directive 2016/680 and elsewhere. That principle follows primarily from Article 4(1)(c) of Directive 2016/680, which states that personal data must not be excessive in relation to the purposes for which they are processed. Article 20(1) of Directive 2016/680 specifies this principle by requiring the Member States to provide for the controller to introduce measures designed to implement data-protection principles, such as data minimisation, in an effective manner. Furthermore, Article 20(2) of that directive states that only personal data which are necessary for each specific purpose of the processing should be processed.

***Question 2(f): Legal basis for profiles***

33 Article 6(3)(b) of Directive 2016/681 states that the data transferred to the Member States' PIUs by air carriers may be processed against pre-determined criteria ('profiles'). The second and fourth sentences of Article 6(4) of Directive 2016/681 specify that the pre-determined criteria must be targeted, proportionate and specific and must not be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. According to the third sentence of Article 6(4) of Directive 2016/681, it is for the Member States' respective PIUs to establish the profiles.

34 Thus, the executive of each Member State alone decides on the overall substantive configuration of profile comparison. This necessarily means that EU Member States use different profiles and passengers are subject, depending on their destination, to different profiles that may give completely different results.

35 It is questionable whether this is compatible with Article 8(2) and Article 52 of the Charter and with Article 16(2) TFEU. Article 8(2) of the Charter provides that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Under the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law. According to Article 16(2) TFEU, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, are to lay down the rules relating to the protection of individuals with regard to the processing of personal data by EU institutions, bodies, offices and agencies and by the Member States when carrying out activities which come within the scope of EU law.

36 Not only must some statutory rule exist, but it must also be sufficiently precise in order to justify interference with fundamental EU rights (see judgment of 21 December 2016, *AGET Iraklis*, C-201/15, EU:C:2016:972, paragraph 99). Persons subject to the law must be able to foresee the consequences of the law and a general rule must be accepted if a more precise rule is not possible for the subject matter of the legislation (judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 77).

37 Article 6(4) of Directive 2016/681 does not fulfil those requirements. The second sentence of Article 6(4) of the Directive is a string of imprecise and empty words that specify the criteria in appearance only. The third sentence of Article 6(4) of the Directive leaves the essential and fundamentally important decision as to what data should be used to establish criteria or profiles for automated comparison entirely up to the individual Member States. However, that is not strictly necessary given the subject matter of the legislation. The EU legislature could very easily have listed precise data or criteria that should or should not be used to

establish profiles. In that regard, neither the crime or terrorism being committed in the individual Member States nor the criteria used to identify suspects differ from one Member State to another.

38 The only mechanism by which the proportionality of the profiles developed by the Member States is controlled is the access to them granted to the data protection officer of the PIU under Article 6(7), read in conjunction with Article 5, of Directive 2016/681. However, according to Article 5(1) of the Directive, the data protection officer is appointed by the PIU itself and, as a rule, is employed by it; thus, there is from the outset no guarantee of independence (see, with regard to the independence of the data protection authority, judgments of 9 March 2010, *Commission* v *Germany*, C-518/07, EU:C:2010:125, and of 16 October 2012, *Commission* v *Austria*, C-614/10, EU:C:2012:631).

***Question 2(g): Period of retention***

39 According to Article 12(1) of Directive 2016/681, PNR data are retained for a period of five years. According to the second sentence of recital 25 of the Directive, because of the nature of the data and their uses, it is necessary that the PNR data be retained for a sufficiently long period. However, the reasons why a five-year retention period is necessary are not explained.

40 The referring court is not clear as to why such a long period of retention is necessary. Once passengers have been checked prior to their intended entry to a Member State or prior to their departure from a Member State in accordance with the first sentence of Article 6(4) of Directive 2016/681 and no irregularities have been identified, there is no objective evidence capable of suggesting that they might have a link, even an indirect one, with terrorist offences or serious crime. Thus, a sufficient connection between the retention of data and the objectives pursued by Directive 2016/681 does not exist. Continued storage would appear to be appropriate only in cases in which there is specific evidence that certain passengers present a risk (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 204 et seq.). However, the mere theoretical possibility that the data might be required for security reasons at a later date should not suffice to justify the wide-ranging interference with fundamental rights that the long-term retention of personal data represents.

41 The Court of Justice has already found in connection with the retention of data, which is another form of unjustified large-scale storage of personal data, that a directive providing for a retention period of up to 24 months does not limit the interference to what is strictly necessary (judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:2014:238, paragraph 63). If 24 months is too long for the retention of data, then five years, as in this case, is far too long.

***Question 2(h): Depersonalisation***

42 According to recital 25 of Directive 2016/681, depersonalisation is intended to guarantee a high level of data protection. That appears to be highly unlikely. The fact that Article 12(2) of the Directive requires data to be depersonalised after six months does not make the retention period any less disproportionate.

43 First, it has to be noted that the term 'depersonalisation' is alien to the system and misleading. It simply means pseudonymisation of the data within the meaning of point (5) of Article 3 of Directive 2016/680. This differs from anonymisation. Whereas, with anonymisation, it is made permanently and definitively impossible for the data to be ascribed to a particular person, depersonalisation can be reversed and a direct link to the person can easily be re-established (see Article 12(3) of Directive 2016/681). It is therefore unclear why the term pseudonymisation has not been used, as in Directive 2016/680. However, because it can be reversed, pseudonymisation reduces the intensity of the interference with fundamental rights far less than genuine anonymisation.

44 Account should also be taken of Article 4(1)(e) of Directive 2016/680, which states that personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed. With (so-called) depersonalisation in accordance with Article 12(2) of Directive 2016/681, identification of data subjects is possible throughout the five-year retention period; this is corroborated by Article 12(3) of Directive 2016/681 regulating (repeat) disclosure after expiry of the period of six months. However, it is not clear why this is necessary for the purposes of Directive 2016/681, nor is it explained by the EU legislature.

***Question 2(i): Notification following de-depersonalisation***

45 There is no rule in Directive 2016/681 providing for data subjects to be advised if their data retained by the Member States' PIUs are to be de-depersonalised in accordance with Article 12(3) of the Directive. The Directive merely stipulates that de-depersonalisation must be approved by a 'judicial authority' or by another national authority (Article 12(3)(b) of Directive 2016/681).

46 The Court of Justice has already held in its Opinion on the agreement between the European Union and Canada that, although, under the envisaged agreement, passengers were to be provided with general information about the processing of their data for the purposes of security and border control checks via a website, that general information would not afford them the possibility of knowing whether their data were being used by the competent authorities for more than those checks (Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 223). The Opinion of the Court also states: '…, in the situations … in which there is objective evidence justifying such use and necessitating the prior authorisation of a judicial authority or an independent administrative body, it is necessary to notify air passengers individually. The same is true in the cases in which air passengers'

PNR data is disclosed to other government authorities or to individuals' (Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 223).

47 The referring court holds that this assessment by the Court of Justice can be applied to Directive 2016/681 and therefore believes that data subjects must be informed individually of the de-depersonalisation of their data. Should the Court of Justice hold that immediately informing data subjects of the de-depersonalisation of their data might seriously undermine the objective pursued of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, the referring court would suggest that data subjects should be informed by no later than the point at which there is no longer any cause to fear that the purpose of de-depersonalisation will be jeopardised, for example because the investigation has been closed.

48 Data subjects also have a right under Article 47 of the Charter to review before an independent and impartial tribunal previously established by law rather than by a 'judicial authority'. However, any form of legal remedy is excluded in the present case.

***Question 3: Transfer to third countries***

49 According to Article 11(1) of Directive 2016/681, PNR data and the result of processing such data may be transferred to a third country on a case-by-case basis, provided that the conditions laid down in Article 13 of Framework Decision 2008/977/JHA are met, the transfer is necessary for the purposes of the Directive, the third country agrees to transfer the data to another third country only where it is strictly necessary for the purposes of the Directive and only with the express authorisation of the respective Member State, and the conditions of Article 9(2) of Directive 2016/681 are met.

50 Article 11(2) of Directive 2016/681 enacts an exemption to that requirement by stipulating that, notwithstanding Article 13(2) of Framework Decision 2008/977/JHA (now Article 38 of Directive 2016/680), transfers of PNR data to third countries without prior consent of the Member State from which the data were obtained is permitted only in exceptional circumstances and only if such transfers to the third country are essential to respond to a specific and actual threat related to terrorist offences or serious crime in a Member State or a third country and prior consent cannot be obtained in good time.

51 As transfer to a third country gives its authorities access to the PNR data, all of the principles governing the use of data that safeguard the proportionality of the associated interference with fundamental rights and an appropriate level of data protection must also apply to the third country. In that regard, the Court of Justice clarified in its Opinion on the agreement between the European Union and Canada that a transfer of personal data from the European Union to a third country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European

Union. This should prevent the level of protection provided for in that agreement from being circumvented by transfers of personal data to third countries and ensure the continuity of the level of protection afforded by EU law (Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 214). The Court concluded from this that the transfer of personal data to a third country requires the existence of either an agreement between the European Union and the third country concerned equivalent to the agreement between the European Union and Canada, or a decision of the Commission, under Article 25(6) of Directive 95/46/EC (now Article 45(3) of the GDPR), finding that the third country ensures an adequate level of protection within the meaning of EU law and covering the authorities to which it is intended that PNR data be transferred (Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 214).

52 Article 11 of Directive 2016/681 does not fulfil those requirements. Article 11(1)(a) of the Directive refers to Article 13 of Framework Decision 2008/977/JHA. That framework decision was repealed by Directive 2016/680. References to the Framework Decision are now understood as references to Directive 2016/680 (see Article 59 of that directive). Articles 35 to 38 of Directive 2016/680 correspond in essence to Article 13 of repealed Framework Decision 2008/977/JHA.

53 Article 35(1)(d) of Directive 2016/680 states that transfer of data to a third country is permissible only where the Commission has adopted an adequacy decision pursuant to Article 36 of that directive, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 37, or, in the absence thereof, derogations for specific situations apply pursuant to Article 38. In that regard, the reference in Article 11(1)(a) of Directive 2016/681 to Article 13 of Framework Decision 2008/977/JHA, and thus to Article 35 of Directive 2016/680, does not ensure an appropriate level of data protection in the third country inasmuch as, in referring to Article 38 of Directive 2016/680, it allows PNR data to be transferred to third countries in the absence of an adequacy decision or appropriate safeguards, especially as the derogations within the meaning of Article 38 of Directive 2016/680 are regulated very broadly. In fact, that provision allows PNR data to be transferred to third countries without an appropriate level of data protection where necessary in individual cases for the purposes of Article 1(1) of Directive 2016/680 (the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security) or for the establishment, exercise or defence of legal claims (see Article 38(1)(d) and (e) of Directive 2016/680).

***Question 4: Choice of meal in 'free text' box***

54 The fourth sentence of Article 6(4) of Directive 2016/681 specifies that the criteria by which PNR data are subjected to automated comparison by the Member States' PIUs must in no circumstances be based on a person's race or ethnic origin,

political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

55 However, that provision is simply a declaration of intent, which is contradicted in particular by point (12) of Annex I to Directive 2016/681. That is because a plethora of information, especially particularly sensitive data, can be transferred to and used by the PIUs, via the 'free text' box for 'general remarks', which must be sent to the PIUs in every single case. For example, that 'free text' box could be used to transfer the information that a passenger requested a kosher or halal meal, from which, however, it is possible to infer the data subject's religious belief, which would be a particularly sensitive item of data in the above sense.

***Question 5: Information provided by air carriers***

56 Article 13(3) of Directive 2016/681 states that the Directive is without prejudice to the applicability of Directive 95/46/EC to the processing of personal data by air carriers, in particular their obligations to take appropriate technical and organisational measures to protect the security and confidentiality of personal data. Article 21(2) of Directive 2016/681 also clarifies that the Directive is without prejudice to the applicability of Directive 95/46/EC to the processing of personal data by air carriers.

57 Directive 95/46/EC was replaced by the GDPR (see Article 94(2) of the GDPR, which states that references to Directive 95/46/EC are to be construed as references to the GDPR).

58 Article 13 of the GDPR states that, where personal data are collected, the data subject are to be provided with the information listed therein. The term 'personal data' is defined in Article 4(1) of the GDPR. The collection of PNR data on passengers and third parties by air carriers qualifies as the collection of personal data in that sense, with the result that Article 13 of the GDPR applies to the air carriers in this case.

59 In the light of the extent, already shown, to which PNR data processing interferes with fundamental rights, the referring court holds that the information requirements must be subject to strict standards.

60 In the opinion of the referring court, it is for the air carriers to provide data subjects with information in accordance with Articles 13 and 14 of the GDPR, as otherwise there would be a gap which would be incompatible with Articles 7 and 8 of the Charter. Therefore, air carriers should have to notify passengers explicitly of all the PNR data which they collect, of the fact that they intend to transfer those data to the Member States' PIUs, where the data will be further processed and retained for a period of five years, and of their specific rights as data subjects, as, without that information, the passengers concerned will scarcely be in a position to exercise their rights as data subjects. However, Directive 2016/681 contains no rules to that effect.

61 The Court of Justice has already held in its Opinion on the agreement between the European Union and Canada that, in order to guarantee those rights, air passengers must be notified of the transfer of their PNR data to Canada and of the use of those data as soon as that information is no longer liable to jeopardise the investigations being carried out by the authorities referred to in the envisaged agreement. That information is, in fact, necessary to enable the passengers to exercise their rights to request access to PNR data concerning them and, if appropriate, rectification of those data, and, in accordance with the first paragraph of Article 47 of the Charter, to an effective remedy before a tribunal (Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 220).

62 One example of inadequate information for passengers from air carriers is the information provided by the air carrier used by the applicant. Lufthansa AG provides the following information on its website (https://www.lufthansa.com/xx/de/informationen-zum-datenschutz, last retrieved on 11 May 2020):

> ***'Who is the controller?***
>
> *Deutsche Lufthansa ... wishes to inform you below of how your personal data are processed ...*
>
> ...
>
> ***Whom can I contact?***
>
> *If you have any ... queries regarding data protection ..., please contact our data protection officer:*
>
> ...
>
> ***On the basis of which … obligations do we process your data?***
>
> *We process passenger data on the basis of the legal obligations pursuant to Art. 6(1), subparagraph 1(c), of the GDPR:*
>
> *If obliged to do so by law, we process personal data in order to meet ... legal security requirements ...*
>
> *Data transmission to* ***immigration authorities****:*
>
> - *On the basis of the airline passenger data agreements between the European Union and the USA and between the European Union and Canada*
> - *On the basis of the German Airline Passenger Data Law*

- *API* (Advance Passenger Information) — we transmit data to the extent to which we are obliged to participate in international travel control activities*

**Data stored in the machine-readable zone in passports or identity documents*

*Further information can be obtained from the relevant authorities.*

…

***Who receives your data?***

*… your data may be passed on to the following categories of recipients:*

…

*state agencies and bodies, e.g. based on entry requirements or police activities and investigations.*

*In the process, personal data may be transmitted to third countries or international organisations. For your protection and the protection of your personal data, appropriate safeguards are provided for such data transmissions as per and in accordance with legal requirements.*

*If these transmissions do not have a legal basis or are carried out to a country for which the EU Commission has not issued an adequacy decision, we use EU standard contractual clauses.*

***What are your data-protection rights?***

*Lufthansa is committed to ensuring fair and transparent processing. That is why it is important to us that persons concerned can not only exercise their right to object but also exercise the following rights where the respective legal requirements are satisfied:*

*Right to information, Art. 15 of the GDPR*

*Right to rectification, Art. 16 of the GDPR*

*Right to erasure ("right to be forgotten"), Art. 17 of the GDPR*

*Right to restrict processing, Art. 18 of the GDPR*

*Right to data portability, Art. 20 of the GDPR*

*Right to object, Art. 21 of the GDPR*

*…'*

63 This information may be inadequate and misleading. For example, the information that API relates only to the data stored in the machine-readable zone in passports or identity documents is manifestly incomplete as, according to point (18) of Annex I to Directive 2016/681, any API collected must be transferred, including the airline, flight number and the departure and arrival dates, times and ports, which clearly goes beyond the data stored in the machine-readable zone of an identity document. Moreover, there is no reference whatsoever to Directive 2016/681, the only reference being to the FlugDaG. Furthermore, there is no information whatsoever on the contents of Directive 2016/681 or of the FlugDaG. Thus, which authority acts as the respective Member State's PIU and how it can be contacted, precisely how it processes PNR data and how long it may retain their data are not transparent to data subjects preparing to book a flight. In that regard, the information provided by Lufthansa AG to passengers, not to mention the other persons who must also be reported, does not appear to meet the requirements of Article 13 of the GDPR.