Case C-222/20

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:

27 May 2020

Referring court:

Verwaltungsgericht Wiesbaden (Germany)

Date of the decision to refer:

15 May 2020

Applicant:

OC

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. Are Article 21 and Article 67(2) TFEU to be interpreted as meaning that they preclude national legislation (in this case, Paragraph 2(3) of the Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 of 6 June 2017 (Law on the Processing of Passenger Name Record (PNR) Data for the purpose of transposing Directive (EU) 2016/681, *BGBl* (Federal Law Gazette) I, p. 1484, as amended by Article 2 of the Law of 6 June 2017, *BGBl* I, p. 1484), ('the FlugDaG') that provides, in application of the flexibility clause in Article 2(1) of Directive (EU) 2016/681 of the

European Parliament and of the Council of 27 April 2016 on the [use of passenger name record (PNR) data for the] prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132; 'the PNR Directive'), for air carriers to transfer comprehensive data on every single passenger of also intra-EU flights to the passenger information units (PIUs) established by the Member States where, except for the flight booking, the data are retained without justification and used for automated comparison against databases and profiles, after which they must be retained?

2. Does it follow from Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union that the national legislation transposing point (9) of Article 3 of the PNR Directive, read in conjunction with Annex II to the Directive, (in this case: Paragraph 4(1) of the FlugDaG) has to enumerate each of the relevant provisions of national criminal law for each of the offences listed in the PNR Directive?

3. Are Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union to be interpreted as meaning that they preclude domestic legislation of a Member State (in this case, Paragraph 6(4) of the FlugDaG) that allows the authorities of that Member State, inasmuch as they perform prosecution-related tasks, to process the PNR data transferred for purposes other than the prevention, detection, investigation and prosecution of terrorist offences and serious crime where findings, including in the light of additional information, give cause to suspect another specific offence?

4. Is the flexibility clause in Article 2(1) of the PNR Directive permitting national legislation (in this case, Paragraph 2(3) of the FlugDaG) that allows the PNR Directive to be applied to intra-EU flights also, meaning that PNR data are collected twice within the European Union (country of departure and country of arrival collect PNR data)[,] compatible with Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union in the light of the principle of data minimisation?

5. If the PNR Directive does not infringe higher-ranking law (see order of the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) of 13 May 2020, reference 6 K 805/19.WI) and is therefore applicable:

   (a) Are Article 7(4) and (5) of the PNR Directive to be interpreted as meaning that they preclude domestic legislation of a Member State (in this case, Paragraph 6(4) of the FlugDaG) that allows the authorities of that Member State, inasmuch as they perform prosecution-related tasks, to process the PNR data transferred for purposes other than the prevention, detection, investigation and prosecution of terrorist offences and serious crime where findings, including in the light of further information, give cause to suspect another specific offence (so-called by-catch)?

(b) Is the practice of a Member State of including in the list of competent authorities under Article 7(1) of the PNR Directive an authority (in this case, the Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)) which, under national law (in this case, Paragraph 5(1), read in conjunction with Paragraph 3(1), of the Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und das Bundesamt für Verfassungsschutz (Law on Cooperation between the Federal Government and the Federal *Länder* in Matters of the Protection of the Constitution and the Federal Office for the Protection of the Constitution)), does not have police powers due to the separation of powers required under domestic law, compatible with Article 7(2) of the PNR Directive?

Provisions of EU law cited

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

Articles 21 and 67 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) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ 2016 L 77, p. 1)

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')

Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Law on Cooperation between the Federal Government and the Federal *Länder* in Matters

of the Protection of the Constitution and the Federal Office for the Protection of the Constitution) ('the BVerfSchG'), Paragraphs 3, 5 and 8

Brief summary of the facts and procedure

1 The FlugDaG, which transposed 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 Article 4 of Directive 2016/681 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 to the Directive, the Member States must 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 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 is an Italian national resident in Brussels (Belgium). On 2 November 2019, he flew from Brussels to Berlin (Germany) and, on 5 November 2019, he flew from Berlin back to Brussels. He is seeking judgment declaring processing of his PNR data relating to those flights to be unlawful and ordering the erasure of those data.

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 FEU Treaty or the Charter. If it does, the transposition law (FlugDaG) would not be applicable, the contested data processing would accordingly be unlawful and the applicant would be entitled to have those data erased.

Question 1: Freedom of movement under Article 21 TFEU

5 According to Article 1(1) of Directive 2016/681, air carriers must transfer the PNR data of every single passenger on every extra-EU flight to the PIUs of the Member States, where those data are subjected to automated processing and retained for five years. Article 2(1) of the Directive contains a flexibility clause permitting the Member States to apply the Directive to intra-EU flights as well, in

which case, according to Article 2(2) of the Directive, all provisions of the Directive apply to intra-EU flights as if they were extra-EU flights.

6 Germany exercised that option in Paragraph 2(3)of the FlugDaG, which states that the PNR data of passengers of all non-military scheduled, charter and private flights departing from the Federal Republic of Germany and arriving in another State or departing from another State and arriving or stopping over in the Federal Republic of Germany must be transferred. Thus, under German law, the same legislation applies to all intra-EU flights from and to Germany as to extra-EU flights.

7 There is no need to establish a precise reason for processing the data, 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.

8 The data to be transferred, which are prescribed in Paragraph 2(2) of the FlugDaG, 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, can be provided in the 'free text' box for 'general remarks'.

9 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).

10 In the first proceedings on the retention of data, the referring court (High Court, Ireland) raised the question as to whether Directive 2006/24/EC is compatible with the right of citizens to move and reside freely within the territory of the Member States laid down in Article 21 TFEU (judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 18). As the Court had already found the Directive to be invalid on the ground of infringement of Articles 7 and 8 of the Charter, it held that there was no need to answer the question referred by the High Court concerning Article 21

TFEU (judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 72).

11 The fact that comprehensive PNR data processing is likely to generate a feeling of constant surveillance in the minds of the persons concerned suggests that it interferes with the right enshrined in Article 21 TFEU. Although PNR data processing does not prohibit or directly restrict the right to reside or move in the territory of the Member States, the Court has held that even indirect restrictions of Article 21 TFEU must be justified (see judgments of 13 June 2019, *Topfit and Biffi*, C-22/18, EU:C:2019:497, paragraph 47, and of 2 June 2016, *Bogendorff von Wolfersdorff*, C-438/14, EU:C:2016:401, paragraph 37). It has to be assumed that, if they have a feeling of being under constant surveillance by the State, many citizens will not exercise their rights under EU law, such as the right to move and reside freely, or will make only limited use of such rights. This constitutes indirect interference with the right enshrined in Article 21 TFEU.

12 The referring court has serious doubts as to whether that interference is justified. Although the Court has held that the objective of Directive 2016/681, namely to combat terrorism and serious crime, is an objective of general interest and thus a legitimate objective of the European Union (see Opinion 1/15 of 26 July 2017, EU:C:2017:592, point 139), measures which restrict a fundamental freedom, such as that provided for in Article 21 TFEU, may, however, be justified by objective considerations only if they are necessary for the protection of the interests which they are intended to secure and only in so far as those objectives cannot be attained by less restrictive measures (judgment of 6 September 2016, *Petruhhin*, C-182/15, EU:C:2016:630, paragraph 38).

13 In terms of necessity, there is serious cause to question whether the interference inherent in PNR data processing could not be attained by less restrictive measures. The referring court is of the opinion that the collection of very comprehensive data on every single passenger, the automated comparison of those PNR data against databases and pre-determined criteria (‘profiles’) and the retention of those data for five years are disproportionate to the objective pursued.

14 This is implied by the simple fact that, according to the defendant’s submissions, PNR data processing is borderline effective. The defendant submitted that, between activation of the system and 19 August 2019, it processed a total of 31 617 068 sets of PNR data, based on which 514 search operations were successfully carried out (57 arrests, 10 open checks, 66 discreet checks and 381 whereabouts investigations). However, checks and whereabouts investigations are quite simply preliminary measures that do not serve directly to avert danger or to prosecute the offences listed in Directive 2016/681. The referring court is of the opinion that such preliminary measures are disproportionate to the interference with fundamental rights inherent in PNR data processing. Moreover, the fact that there were ultimately only 57 cases of actual intervention raises doubts as to the general appropriateness of PNR data processing in terms of attaining the objectives of Directive 2016/681.

15 Furthermore, it is doubtful whether PNR data processing is compatible with Article 67(2) TFEU, which states that the European Union must ensure the absence of internal border controls for persons. The EU legislature implemented that principle by adopting Regulation (EC) No 562/2006 (judgment of 22 June 2010, *Melki and Abdeli*, C-188/10 and C-189/10, EU:C:2010:363, paragraph 66). That regulation was repealed by Regulation (EU) 2016/399, Article 22 of which states that internal borders may be crossed at any point without a border check on persons, irrespective of their nationality, being carried out. According to Article 23 of Regulation 2016/399, the absence of border controls must not affect the exercise of police powers by the competent authorities of the Member States under national law, in so far as the exercise of those powers does not have an effect equivalent to border checks. According to point (11) of Article 2 of Regulation 2016/399, 'border checks' means the checks carried out at border crossing points, to ensure that persons, including their means of transport and the objects in their possession, may be authorised to enter the territory of the Member States or authorised to leave it.

16 However, it is the opinion of the referring court that, as the PNR data of every passenger and third party are subjected to automatic comparison against databases and pre-determined criteria, PNR data processing has an effect equivalent to border checks. Thus, everyone entering an EU Member State is subject to automated checking, even in the absence of specific grounds for suspicion and regardless of the circumstances of the particular case. On the basis of those checks, persons on a wanted list, for example, may be denied entry to the EU Member State concerned.

17 Note also has to be taken of the case-law of the Court of Justice on the second sentence of Article 21(a) of the old Regulation (No 562/2006), which is now reproduced in the second sentence of Article 23(a) of Regulation 2016/399. The Court held that the indicia listed therein are indicators of the existence of an effect equivalent to border checks (judgment of 13 December 2018, *Touring Tours und Travel and Sociedad de transportes*, C-412/17 and C-474/17, EU:C:2018:1005, paragraph 54). These indicia or indicators exist in the present case at least inasmuch as PNR data processing is to be carried out in general for all passengers, rather than simply on a random basis. For that reason, processing, at least as regards the comparison of PNR data against databases, is not based on general police information and experience in connection with potential threats to public security, as it is performed irrespective of any suspicions.

Question 2: List of offences

18 According to Paragraph 4(1) of the FlugDaG, the German PIU processes the PNR data transferred by air carriers and compares them against databases and profiles to identify persons in regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence enumerated in a closed list.

19 For those affected, this processing of PNR data constitutes interference with the rights laid down in Articles 7 and 8 of the Charter. The fundamental right to respect for private life recognised by Article 7 of the Charter concerns any information relating to an identified or identifiable individual (see judgment of 9 November 2010, *Volker and Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 52). Furthermore, the processing of PNR data provided for in the FlugDaG 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).

20 As the Court 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).

21 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. Combating terrorist offences and serious crime, which are the stated objectives of the Directive transposed by the FlugDaG, are such objectives of general interest. 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).

22 It is settled case-law of the Court 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).

23 In order to meet that requirement, the legislation entailing the interference must lay down clear and precise rules governing the scope and application of the measure in question. It must also impose minimum safeguards so that the persons whose data are transferred 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).

24 The list of offences in Paragraph 4(1) of the FlugDaG includes offences that correspond to an offence listed in Annex II to Directive 2016/681 and are punishable by a custodial sentence for a maximum period of at least three years (point (6) of Paragraph 4(1) of the FlugDaG).

25 Thus, point (6) of Paragraph 4(1) of the FlugDaG does not refer to offences under the Strafgesetzbuch (German Criminal Code, 'the StGB); it simply refers to offences that have no precise equivalent under German criminal law. For example, Annex II to Directive 2016/681 lists corruption (point (6)), computer-related crime/cybercrime (point (9)) and environmental crime (point (10)). These do not qualify as crimes under the StGB. For example, the StGB does not recognise the crime of 'corruption', which it uses as a generic heading for a number of conceivable offences. Thus, for German authorities and, more importantly, for the persons concerned, there is no unequivocal definition of the crimes that this rule is intended to cover. The same is true of the terms 'computer-related crime' and 'environmental crime'. In that sense, the mere reference to Annex II to Directive 2016/681 in point (6) of Paragraph 4(1) of the FlugDaG renders the FlugDaG very imprecise.

26 Therefore, Paragraph 4(1) of the FlugDaG does not fulfil the requirement of 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). In the opinion of the referring court, what is needed here is an independent closed list of offences which enumerates each of the relevant provisions of national criminal law for each offence, in order to guarantee clarity as to the scope of the FlugDaG both for the persons (potentially) concerned and for the domestic authorities.

Question 3: Use for other purposes in the light of the Charter

27 Paragraph 6(4) of the FlugDaG allows the domestic authorities named in Paragraph 6(1) thereof to process the PNR data transferred to them for purposes

other than the purpose of the tasks referred to in Paragraph 4(1) of the FlugDaG (the prevention and prosecution of terrorism and serious crime), inasmuch as they perform prosecution-related tasks, including in the light of further information that gives cause to suspect another specific offence ('by-catch'). Thus, Paragraph 6(4) of the FlugDaG grants an exception to the rule laid down in Paragraph 6(3) thereof that the data transferred may be used only for the purposes for which they were transferred and allows for any number of other purposes.

28 The conformity of that rule with EU fundamental rights is questionable. The criterion for 'serious crime' in point (9) of Article 3 of Directive 2016/681 (offences 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) already sets the bar very low.

29 The rule laid down in Paragraph 6(4) of the FlugDaG, however, eliminates this, already low, standard altogether. It states that PNR data may be processed where there is good cause to suspect 'another specific offence', but does not impose any further preconditions with regard to that other offence. On the basis of the wording of Paragraph 6(4) of the FlugDaG, PNR data may be processed or the resultant findings used for the purpose of prosecuting even petty offences.

30 For that reason, the referring court considers that rule to be disproportionate. There is nothing here to suggest that the interference with fundamental rights has been limited to what is strictly necessary, as required by the case-law of the Court of Justice. Quasi-unlimited use of PNR data under Paragraph 6(4) of the FlugDaG has nothing to do with combating terrorism and serious crime. The rule in Paragraph 6(4) of the FlugDaG thus departs from, and goes clearly beyond, the objectives pursued by Directive 2016/681.

Question 4: Double collection

31 As numerous Member States have made use of the flexibility clause in Article 2(1) of Directive 2016/681 (including the Kingdom of Belgium, as the country of departure and arrival in this case), the PNR data of passengers on intra-EU flights must be transferred both to the country of departure and to the country of arrival, as well as to any stop-over country. For intra-EU flights, this means that the PNR data of every passenger or third party are processed and retained at least twice, as happened with the applicant in this case. Even where flights depart from or arrive in a third country but stop over in an EU Member State, the PNR data of the passengers concerned are collected several times as a result of this rule.

32 In the light of the principle of data minimisation, this is incompatible with Articles 7 and 8 of the Charter, in that the interference with those fundamental EU rights inherent in PNR data processing is not limited to what is strictly necessary.

33 The principle of data minimisation is enacted in Directive 2016/680. That directive was adopted together with and supplements Directive 2016/681. First, it

follows from Article 4(1)(c) of Directive 2016/680 that personal data should not be 'excessive' in relation to the purposes for which they are processed. Article 20(1) of that directive explains that principle by stipulating that the Member States must 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 Directive 2016/680 states that only personal data which are necessary for each specific purpose of the processing may be processed.

34 Multiple processing of identical data by several agencies flouts the principle of data minimisation: even if it concerns the same PNR data, it deepens the interference with fundamental rights inherent in PNR data processing simply by reason of the fact that data are collected more than once and every Member State is responsible for setting its own criteria for automated comparison against pre-determined criteria (see the third sentence of Article 6(4) of Directive 2016/681).

Question 5(a): Use for other purposes in the light of Directive 2016/681

35 Article 7(4) of Directive 2016/681 states that PNR data and the result of processing those data may be further processed by the competent authorities of the Member States only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime. Article 7(5) of Directive 2016/681 states that Article 7(4) thereof is to be without prejudice to national law enforcement or judicial powers where other offences, or indications thereof, are detected in the course of enforcement action further to such processing.

36 Paragraph 6(4) of the FlugDaG allows the domestic authorities named in Paragraph 6(1) thereof to process the PNR data transferred to them for purposes other than the purpose of the tasks referred to in Paragraph 4(1) of the FlugDaG (the prevention and prosecution of terrorism and serious crime), inasmuch as they perform prosecution-related tasks, including in the light of further information that gives cause to suspect another specific offence.

37 If the Court of Justice should find that Paragraph 6(4) of the FlugDaG is compatible with Articles 7 and 8 of the Charter (see Question 3), the question then arises as to whether that provision is compatible with Article 7(4) and (5) of Directive 2016/681. In the view of the referring court, it is not.

38 The rule in Paragraph 6(4) of the FlugDaG goes beyond Article 7(5) of Directive 2016/681, as it does not include the requirement laid down by that provision that other offences (that is to say, offences which are not motivated by terrorism and are not serious crimes within the meaning of Directive 2016/681) must have been detected in the course of enforcement action further to PNR data processing. On the contrary, because of the way in which it is worded, it directly allows PNR data to be processed for purposes other than the prosecution of or fight against terrorism and serious crime, both where the findings come from processing PNR

data to combat terrorism or serious crime and where they originate from other sources. Thus, Paragraph 6(4) of the FlugDaG also allows PNR data to be used for other purposes even where PNR data processing itself does not detect offences already committed or about to be committed. This substantially deepens the interference with fundamental rights inherent in data processing, for which there is no basis in Directive 2016/681.

Question 5(b): Federal Office for the Protection of the Constitution

39 Article 7(1) of Directive 2016/681 requires each Member State to adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIUs in order to examine that information further or to take appropriate action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime. According to Article 7(2) of Directive 2016/681, the authorities referred to in paragraph 1 must be authorities competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime.

40 The list of competent authorities within the meaning of Article 7(1) of Directive 2016/681 compiled by Germany includes 22 authorities, one of which is the Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution) (see OJ 2018 C 194, p. 1). According to Paragraph 5(1), read in conjunction with Paragraph 3(1), of the BVerfSchG, the Federal Office for the Protection of the Constitution is tasked with collecting and evaluating information, especially on efforts to frustrate the free democratic rule of law, anti-security or intelligence activities and efforts to undermine the foreign interests of the Federal Republic of Germany or directed against the concept of international understanding.

41 According to Paragraph 8(3) of the BVerfSchG, the Federal Office for the Protection of the Constitution does not have police powers. This clarifies that the Federal Office for the Protection of the Constitution is simply an intelligence service, the purpose of which is not to avert dangers itself, but to report to the government and the public and to assist in the collection of information so that other agencies, in particular the police, can intervene where necessary. In that sense, Paragraph 8(3) of the BVerfSchG is an expression of the separation of powers required between the police and intelligence services. This does not exist in other Member States (such as France), where the constitutional authorities have policing powers.

42 Thus, there is very good cause to question whether the Federal Office for the Protection of the Constitution is an authority within the meaning of Article 7(2) of Directive 2016/681 which is competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime. In the opinion of the referring court, such an authority is not covered by Article 7(2) of Directive 2016/681. This is true in particular in the light of the fact that the German police authorities are already included in the list of authorities entitled to intervene under Article 7(1) of

Directive 2016/681; consequently, there is no need for the Federal Office for the Protection of the Constitution to have additional powers of intervention.