Anonymised version

Case C-148/20

Request for a preliminary ruling

Date lodged:

16 March 2020

Referring court:

Amtsgericht Köln (Germany)

Date of the decision to refer:

20 January 2020

Applicant:

AC

Defendant:

Deutsche Lufthansa AG

[...] Promulgated on 20 January 2020
[...]

Amtsgericht Köln (Local Court, Cologne)

Order

In the legal proceedings

AC v Deutsche Lufthansa AG

the Local Court, Cologne,

ordered on 28 October 2019:

[...]

I. The proceedings are stayed.

II. The following question is referred to the Court of Justice of the European Union for a preliminary ruling:

Is the PNR Directive (Directive (EU) 2016/681 of 27 April 2016) compatible with Articles 7 and 8 of the Charter of Fundamental Rights (the Charter) in relation to the following points:

(1) Are the PNR data to be transferred under the directive sufficiently specified, having regard to Articles 7 and 8 of the Charter?

(2) In view of its scope and having regard to Articles 7 and 8 of the Charter, does the directive provide for sufficient objective differentiation when PNR data are collected and transferred, in relation to the type of flights **[Or. 2]** and the threat level in a particular country and in relation to the comparison against databases and patterns?

(3) Is the blanket, indiscriminating retention period for all PNR data compatible with Articles 7 and 8 of the Charter?

(4) Having regard to Articles 7 and 8 of the Charter, does the directive provide for adequate procedural protection of passengers in respect of the use of retained PNR data?

(5) Having regard to Articles 7 and 8 of the Charter, does the directive adequately safeguard the level of protection of European fundamental rights when PNR data are transferred to third country authorities by third countries?

Grounds

I.

The subject matter of the dispute is an action brought by the applicant against the defendant air carrier for an injunction to prevent the transfer of her PNR data under the Law on passenger data ('the FlugDaG') to the Federal Republic of Germany in respect of a flight initially booked for 5 March 2020 from Munich to Ankara with a return flight to Munich on 10 March 2020.

On 10 June 2017 the Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie EU 2016/681 (Law on the Processing of Passenger Data Implementing Directive (EU) 2016/681) – the FlugDaG – entered into force in Germany. European Union Directive 2016/681 ('the PNR Directive') of 4 May

2016 concerns the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. This directive governs the transfer of PNR data of airline passengers on flights from EU Member States to third countries and from third countries to Member States and the processing of the **[Or. 3]** data. Article 2 contains an enabling provision for national legislatures, under which intra-EU flights can also be covered. Article 4 of the directive requires Member States to establish passenger information units (PIUs) responsible for collecting PNR data from air carriers and for storing, processing and transmitting them to the competent authorities, as well as for exchanging PNR data and the results of processing. Furthermore, under Article 8 of the directive, Member States must require all air carriers to transmit, using the push method, PNR data as defined in Annex I to the directive to the passenger information units in whose territory the flights concerned arrive or from which they depart. Under Articles 9 and 11 of the directive, PNR data may be requested and transferred between passenger information units and, under certain conditions, PNR data may also be transferred to third countries. Article 12 provides that data are to be retained for five years and that the data must be depersonalised, in the sense that certain data elements, which could serve to identify passengers, must be masked out, after six months. Lastly, Article 6 of the directive governs the processing of PNR data by the passenger information units, and allows the data to be automatically compared against databases and 'patterns'. The FlugDaG transposes the provisions into national law. The Bundeskriminalamt (Federal Criminal Police Office) was designated as passenger information unit with the Bundesverwaltungsamt (Federal Administrative Office) acting as commissioned data processor of the passenger information unit. The defendant is required by law to transfer all PNR data of passengers on civil flights that take off in Germany and land in another country or that land in Germany having taken off from another country.

The applicant asked the defendant not to transmit to the Federal Criminal Police Office her data concerning the flights booked to Ankara and back. To date, the defendant has not complied with this request.

The applicant is of the opinion that the provisions of the FlugDaG infringe EU law and that the transmission of the data also infringes her general right of personality, in the form of her right of 'informational self-determination' (i.e. the right of individuals to determine themselves the privacy of their information). In the present case, the applicant seeks an injunction against the defendant. **[Or. 4]**

The defendant takes the view that the action for an injunction is inadmissible and that the applicant lacks a need for legal protection. Moreover, the defendant argues that the only legal test is the transmission of the data by it.

The Federal Republic of Germany, represented by the Federal Criminal Police Office, intervened in the case in support of the defendant.

II.

The outcome of the legal dispute hinges on whether the defendant's obligation under the FlugDaG to transfer the applicant's PNR data to the intervener in support of the defendant – the Federal Republic of Germany – is lawful; this is because, in the view of the court, the contract of carriage by air concluded between the parties and, in any event, the second sentence of Paragraph 1004(1) of the Bürgerliches Gesetzbuch (Civil Code, 'the BGB') and analogously Paragraph 823 BGB, give rise to an obligation on the part of the defendant to refrain from passing on personal data without a sufficient legal basis as this would constitute an infringement of the applicant's general right of personality in the form of the right to informational self-determination. Conversely, the applicant would have to tolerate this transfer if the FlugDaG constituted a sufficient statutory basis. This requires, however, that the basis of this law, Directive 2016/681, be in accordance with EU law, in particular with the Charter and in particular Articles 7 and 8 thereof. If the directive infringes EU law, this means that the transposition into national law by the FlugDaG is also unlawful and that law cannot justify, in the relationship between the parties, the transfer by the defendant of the applicant's PNR data to the intervener.

III. **[Or. 5]**

There are doubts as to the compatibility of the PNR Directive with Articles 7 and 8 of the Charter:

Article 7 of the Charter protects private life. Article 8 of the Charter protects a person's personal data. Personal data relating to private life are protected. The PNR Directive covers such data. It provides for the collection, storage and processing of personal data in a PNR data set. Articles 7 and 8 of the Charter are thus affected by the directive.

Article 8(2) of the Charter allows the processing of personal data for specified purposes and on the basis of the consent of the person concerned, as well as where there is some other legitimate basis laid down by law. One objective serving the common good is to ensure public safety. This objective justifies far-reaching interference with the protective scope of Articles 7 and 8 of the Charter. Such objectives are pursued by the PNR Directive. They are aimed at the prevention, detection, investigation and prosecution of terrorist offences and serious crime. However, any interference serving these objectives must be proportionate. Limitations of the protection of personal data must be restricted to what is strictly necessary. This requires that the directive contain clear and precise rules on the scope and application of the measures for which it provides.

This results in the following five questions:

1.

In the light of the requirements to be met by the PNR Directive as outlined above, the PNR data to be collected and transferred must be clearly and precisely defined, otherwise there is not sufficient precision. Under items 8 and 12 of Annex I to the PNR Directive, the relevant data include, inter alia, frequent flyer information and general remarks. It is not clear what is meant by frequent flyer information. This may refer simply to confirmation of whether the person is participating in **[Or. 6]** a frequent flyer rewards programme or to specific information about flights and bookings of the person participating in such a programme. A free text box must be filled in for the general remarks. It is not clear from the directive what exactly can or should be entered here. The nature and scope of the information to be entered here is not conclusively defined, and there is no limitation provided for. This gives rise to the question posed under point 1, as to whether the directive is sufficiently specific with regard to the PNR data to be transferred, taking into account Articles 7 and 8 of the Charter.

2.

Furthermore, the scope of the directive must be proportionate in accordance with the requirements outlined above. The directive does not differentiate between the types of flights for which PNR data are to be transferred. All international flights are covered, regardless of the country of origin or destination or a specific or increased threat level in a country. This scope can be extended to intra-EU flights by means of the enabling provision. Nor are any distinctions drawn with regard to the data in terms of the objectives of the directive – combating terrorism and serious crimes – for instance with regard to the danger posed by or the suspicious nature of the persons involved. There are doubts as to whether the directive meets the requirement that the retention of data must satisfy objective criteria that clarify the link between the personal data retained and the objectives pursued.

This question of proportionality is continued in the follow-up question as to whether there are sufficient procedural or substantive legal rules for the further use of PNR data. Article 6(3) of the directive allows a comparison of the PNR data transmitted against existing databases and patterns without any particular reason. The legal requirements under which this comparison must be carried out are not specified in more detail. When assessing proportionality, the relationship between the means and the end needs to be considered. The purpose is further clarified in Annex II to the directive. However, data are allowed to be processed in the same way for all specified purposes, without any distinction being made **[Or. 7]** as to the extent to which the comparison of data actually contributes to the detection or prevention of the individual offences listed.

This give rise to the question set out under point 2, as to whether, in view of its scope and having regard to Articles 7 and 8 of the Charter, the directive provides

for sufficient objective differentiation when PNR data are collected and transferred, in relation to the type of flights **[Or. 2]** and the threat level in a particular country and in relation to the comparison against databases and patterns.

3.

In accordance with the above, the interference must be limited to what is absolutely necessary. According to Article 12 of the PNR Directive, PNR data must be retained for 5 years from the date of transfer; the data must be depersonalised after 6 months, but this may be reversed provided additional conditions are met. There is no differentiation with regard to any specific indications as to whether or not a person poses a risk. In particular, PNR data of non-suspicious persons who have already left the country are also retained, without any apparent link to the objectives of the directive. The question therefore arises whether the retention period is limited to what is absolutely necessary. This leads to the question set out under point 3, as to whether the blanket, indiscriminating retention period for all PNR data is compatible with Articles 7 and 8 of the Charter.

4.

Interference with the protective scope of personal data must not only be justified, it must also be possible for its lawfulness to be legally reviewed. The question arises as to whether and, if so, to what extent the directive itself provides for such procedural protection through independent supervisory bodies. In Article 12(3), the directive provides that a removal of depersonalisation requires an authorisation from the judicial authority or another national authority. However, in the light of Articles 7 and 8 of the Charter, procedural protection against interference could require a more extensive review by administrative bodies or by courts, even before the data are transmitted, **[Or. 8]** stored or used. This leads to the question posed under point 4, as to whether, having regard to Articles 7 and 8 of the Charter, the directive provides for adequate procedural protection of passengers in respect of the use of retained PNR data.

5.

Finally, the requirement to limit the protection of personal data to what is strictly necessary concerns the relationship with third countries to which PNR data are transferred. In order to guarantee that the level of protection applicable within the EU is also observed in the case of such transfers, it may be necessary to take

measures to ensure observance. Such measures are not provided for in the relevant Article 11 of the directive. This leads to the fifth and final question, as to whether, having regard to Articles 7 and 8 of the Charter, the directive adequately safeguards the level of protection of European fundamental rights when PNR data are transferred to third country authorities by third countries.

[...]