GEULEN & KLINGER
Rechtsanwälte

Dr. Reiner Geulen
Prof. Dr. Remo Klinger
10719 Berlin, Schaperstraße 15
Telefon +49 / 30 / 88 47 28-0
Telefax +49 / 30 / 88 47 28-10
e-mail: klinger@geulen.com
geulen@geulen.com
www.geulenklinger.com

Wiesbaden Administrative Court
Mainzer Straße 124

65189 Wiesbaden, Germany

13 May 2019

COMPLAINT

and

APPLICATION FOR A TEMPORARY INJUNCTION

from Mr **Emilio De Capitani**
..., Belgium,

– Plaintiff and Claimant –

Authorised representative:
Attorneys at law Dr. Reiner Geulen & Prof. Dr. Remo Klinger,
Schaperstraße 15, 10719 Berlin,

versus

The Federal Republic of Germany,
represented by the Federal Criminal Police Office,
65173 Wiesbaden, Germany,

– Defendant and Respondent –

in relation to: the storage, processing and transfer of passenger data pursuant to the Passenger Name Record Act (FlugDaG)

Provisional value of the claim: EUR 5,000.00

Provisional value of the requested ruling: EUR 2,500.00

in the name and with the power of attorney of the Plaintiff (attached), we file the following

complaint

and petition,

> to order the Defendant to refrain from storing, processing and transferring the Claimant's passenger data relating to the flight SN 2581 on 2 November 2019 from Brussels (BRU) to Berlin Tegel (TXL) at 9.45 a.m. and the flight SN 2582 from Berlin Tegel (TXL) to Brussels (BRU) at 12.00 noon on 5 November 2019.

Also in the proceedings for a

temporary injunction

pursuant to § 123 (1) of the Rules of the Administrative Courts (VWGO), we petition

> to order to temporarily prohibit the Defendant from storing, processing and transferring of the Plaintiff's passenger data relating to flight SN 2581 on 2 November 2019 from Brussels (BRU) to Berlin Tegel (TXL) at 9.45 a.m. and the flight SN 2582 from Berlin Tegel (TXL) to Brussels (BRU) at 12.00 noon on 5 November 2019.

In view of the fundamental importance of the case, in particular in view of the questions referred to the European Court of Justice, we suggest that the case should not be transferred to a single judge.

We submit the following statement of reasons for the claim and the application:

Outline

A. Preliminary remark

The Plaintiff is a former Head of the Secretariat of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament and a visiting professor at Queen Mary University of London. He opposes the storage, processing and transfer of his personal data on flights from Brussels to Berlin and back in accordance with the Passenger Name Record Act (Fluggastdatengesetz). According to this law, airlines must transfer extensive data records of all passengers flying to or leaving Germany to the Federal Criminal Police Office. In addition to names, addresses and nationalities, these records also contain sensitive data, such as date of birth, telephone number, email address and payment information, as well as information on accompanying persons, baggage, frequent flyer entry and "general information" in a free text field. On the one hand, the Federal Criminal Police Office compares this data with databases, and on the other, it applies "patterns" to them, with which it seeks to gain new grounds for suspicion against individuals. The data remains stored for five years, posing significant security risks for passengers such as the Plaintiff.

This new form of mass surveillance fits seamlessly into the public sector's increasing efforts to completely record citizens. However, passenger data storage stands out from the multitude of safety laws in that its necessity has not even been proven in the first place; rather, the data of millions of innocent citizens is stored and processed for experimental purposes.

Limited personal data (name, date of birth, etc.), as already collected in accordance with § 31a of the Federal Police Act (BPolG) and also deleted 24 hours after entry, would suffice for the comparison of passenger data with databases. By storing and processing considerably more data for a much longer period of time, the new passenger data storage system violates the rights of the Plaintiff. The comparison of passenger data with "patterns" is *a fortiori* contrary to the constitution, because it covers aircraft passengers like the Plaintiff irrespective of whether they have a previous conviction, whether they use a route classified as critical or whether they travel during a particularly hazardous situation. According to an opinion of the ECJ, the pattern comparison also includes a "certain" error rate; the European Data Protection Supervisor even considers this error rate to be "substantial". The risk of unjustified follow-up measures is correspondingly high, with all the associated financial losses and damage to reputation or even loss of freedom.

The EU Directive on which the Passenger Name Record Act is based violates Articles 7 and 8 of the EU Charter of Fundamental Rights as interpreted and applied by the ECJ in its opinion on the Passenger Name Record Agreement between the EU and Canada. According

to the directly applicable observations of the ECJ, the Directive is too vague, in particular through the use of a free text field; it lacks concrete conditions for the storage and further use of the data. Instead, it illegally collects the data indiscriminately; it lacks comprehensible time limits for the storage of the data, in particular it does not provide for the deletion of the data after the departure of the data subjects; it lacks requirements for an independent control of the processing of the mass data collected, and it does not contain sufficient safeguards for the transfer of the data to foreign services. We therefore suggest that, in order to safeguard the Plaintiff's fundamental rights, the procedure should be suspended and the question of the validity of the Directive submitted to the ECJ.

The Federal legislature, however, goes even further with the Passenger Name Record Act than the Directive requires, whereby the storage of passenger data also violates the Plaintiff's right to informational self-determination under Art. 2 (1) in conjunction with Art. 2 (1) of the German Constitution (Grundgesetz): The Directive only requires the transfer of data on flights going to or coming from outside Europe; the Passenger Name Record Agreement extends this obligation to intra-European flights. The standards of the Federal Constitutional Court on the mass storage of personal data are therefore even more violated by the Passenger Name Record Act.

As an active data protector, the Plaintiff has a strong interest in preventing the storage, processing and transfer of his data, although the admissibility does not depend on this particular interest.

B. Facts of the case

The complaint is directed against measures taken by the Defendant to store, process and transfer data on the basis of the Act on the Processing of Passenger Name Record (PNR) Data to Implement Directive (EU) 2016/681 (Passenger Name Record Act - hereinafter "**FlugDaG**"). Most of the law came into force on 10 June 2017. The penalty for non-compliance (§ 18 FlugDaG) as well as the regulations for the transfer of passenger data to foreign authorities (§§ 7-10 FlugDaG) came into force on 25 May 2018.

As its full name suggests, the FlugDaG transposes Directive 2016/681 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 (hereinafter referred to as the "**PNR Directive**") into national law.

The complaint extends to the storage of an extensive data record concerning the Plaintiff, its automated comparison with so-called "patterns" typical of crime and various databases, as well as its possible forwarding to domestic and foreign authorities.

The complaint is related in substance to civil actions brought by the signatory on behalf of other plaintiffs against the transfer of the data records by the airlines to the Defendant and to parallel proceedings brought against the Defendant.

I. The Plaintiff

The Plaintiff is an Italian citizen and lives in Brussels, Belgium. He was head of the Secretariat of the Committee on Civil Liberties, Justice and Home Affairs in the European Parliament (the so-called LIBE Committee), visiting professor at Queen Mary University of London, Department of Law, and Executive Director of the Fundamental Rights European Experts Group – FREE Group. So even after his retirement from the EU Parliament in December 2011, he remained active in the area of the transparency of the public sector and the protection of personal data.

For a working meeting with the Gesellschaft für Freiheitsrechte e.V., the Plaintiff wishes to travel from Brussels to Berlin on 2 November 2019 and back again on 5 November 2019. Documentation of the flight booking attached as

Exhibit K 1

It is completely incomprehensible to the Plaintiff why data from these flights should be transferred to the Federal Criminal Police Office for review in up to 19 categories and stored there for five years. He does not want his data to be used for comparison with "patterns" which are completely opaque to him, in addition to the necessary comparison of data with databases of wanted persons or objects. In particular, the Plaintiff does not see why it should be necessary to store and process his telephone number, his email address, his luggage details, his payment information, ominous "general information" and a lot of other data about an innocent citizen like him at a police station for years. The hope that such new data retention will provide the security authorities with reliable information on suspicious aircraft movements is not sufficiently demonstrated, let alone substantiated, and in any case does not justify the storage and processing of his data or even the transfer of his data to third parties. He is concerned that he will be exposed to unjustified measures, for example, that after the transfer of his data to other states, which he cannot prevent, he will encounter problems when entering these states without having given cause for this.

The Plaintiff therefore considers the planned storage, processing and transfer of his data – confirmed by an opinion of the ECJ on the PNR agreement between Canada and the EU – a violation of his fundamental rights. He considers it even more unacceptable that the FlugDaG covers not only non-European flights, but also intra-European flights such as his own, in addition to the mandatory program of the PNR Directive.

II. European legal background of the challenged measures

On 27 April 2016, the European Parliament and the Council of the European Union adopted the PNR Directive with the stated aim of "preventing, detecting, investigating and prosecuting terrorist offences and serious crime" (see marginal No 10). Until then, Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (hereinafter "the **API Directive**") had essentially regulated the use of PNR data. This required border control authorities to make passenger data available on a case-by-case basis at the request of a Member State for flights into the territory of the European Union. Law enforcement agencies have sometimes used the API Directive as a basis for identifying suspects or persons under investigation. A data record was to be transferred, the scope of which fell short of that provided for in the PNR Directive (cf. Art. 3 (2) API Directive). However, the EU Commission did not see this as a legal basis for recording all passengers for the purpose of obtaining comprehensive information on suspects and suspicions.

> Cf. the proposal of the EU Commission for the Directive, COM/2011/0032, p. 7 et seq.

In 2013, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs rejected an extension of the relevant powers proposed by the EU Commission in 2011 due to constitutional concerns.

> Cf. committee report of 29 April 2013, available at https://bit.ly/2Hoqcmv (last accessed on 3 May 2019).

In the aftermath of the terrorist attacks in Paris in November 2015, the proposal for a comprehensive passenger data directive returned to the EU's political agenda.

The PNR Directive obliges Member States to establish a so-called "PNR unit" (Art. 4 (1) PNR Directive) linked to the purposes of prevention, detection, investigation and prosecution of terrorist offences and serious crime (Art. 6 (2) PNR Directive). According to Art. 3 No. 8 PNR Directive, these are "terrorist offences" which under national law are offences within the meaning of Art. 1 No. 8 and No. 9 of the framework decision 2002/475/JHA, as well as the offences listed in Annex II of the PNR Directive, which are punishable as "serious crime"

under the national law of a Member State by a custodial sentence or a detention order for a maximum period of at least three years.

Under Article 8 (1) PNR Directive, Member States are required to require all air carriers to transfer a data record defined in Annex I to the Directive (hereinafter "**PNR data**") to the (Passenger Information Units of the Member State in whose territory the flights in question arrive or depart, using the "push" method (Article 3(7) of the PNR Directive), for all flights within the scope of the Directive. The "push" method means that the airlines themselves must actively transfer the data record (as opposed to the "pull" method, where the recipient can pull data). The PNR units have to process the PNR data in accordance with Article 6 of the PNR Directive. Annex I No. 12 under "General Information" provides for a free text field which may contain a variety of information not conclusively determined by the legislature.

Pursuant to Art. 9 (2) sentence 1 PNR Directive, the Passenger Information Unit of each Member State may request the transfer of PNR data and processing results stored in the Passenger Information Unit of any other Member State in a reasoned request to the Passenger Information Unit of any other Member State. Pursuant to Art. 9 (2) sentence 2 PNR Directive, it must direct its request at a specific data element or a specific combination of data elements. Under essentially the same conditions, national PNR units may transfer PNR data to Europol, the European law enforcement agency, following a reasoned request, in accordance with Art. 10 (2) sentence 1 PNR Directive.

Member States may also transfer PNR data and processing results to third countries pursuant to Art. 11 (1) PNR Directive if the same conditions apply as to other Member States. In addition, an appropriate level of data protection must be maintained in the respective third country within the meaning of Article 13 (1)(d) of framework decision 2008/977/JHA PNR Directive (Article 11 (1)(a) PNR Directive). Framework decision 2008/977/JHA has now been replaced by Directive 2016/680 (hereinafter referred to as the "**Data Protection Directive**"); references to the framework decision shall be construed as references to the Data Protection Directive (cf. Art. 59 thereof). Thus, the reference in Art. 11 PNR Directive is now to be understood as a reference to Art. 35 et seqq. of the Data Protection Regulation. Consequently, a so-called adequacy decision of the EU Commission is generally required before a transfer to a third country (Art. 36 Data Protection Directive). The transfer must also be necessary for the purposes specified in Article 1 (2) of the PNR Directive (Article 11(1)(b) PNR Directive). Furthermore, the third country must undertake not to transfer the PNR data to another third country without the consent of the respective Member State (Art. 11 (1)(c) PNR Directive). However, there are significant exceptions to these seemingly strict requirements in Art. 38 of the Data Protection Directive. According to this, a Member State may also transfer (PNR) data without a decision on adequacy or

guarantees if the sometimes extremely vague conditions mentioned there (cf. e.g. Art. 38 (1) (d)) of the Data Protection Directive: "... on a case-by-case basis for the purposes referred to in Article 1(1)').

After six months, the PNR data is to be reduced to the core data listed under Art. 12 (2) PNR Directive in the course of "depersonalisation". “Repersonalisation" is, however, possible under the conditions set out in Article 12(3) of the PNR Directive, namely for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious crime (cf. reference to Article 6 (2)(b) PNR Directive).

The storage, processing and transfer of data under the PNR Directive concerns only "third-country flights". According to Article 3 (2) of the PNR Directive, this term covers any scheduled or non-scheduled flight of an airline departing from a third country and bound for the territory of a Member State or departing from the territory of a Member State and bound for the territory of a third country. In both cases, flights with stopovers in the territory of Member States or third countries are included. However, Article 2 (1) of the PNR Directive gives the Member States the option of applying the Directive also to "EU flights", i.e. in accordance with Article 3 (2) of the PNR Directive to any scheduled or non-scheduled flight of an airline departing from the territory of a Member State and bound for the territory of one or more other Member States, without intermediate stops in the territory of a third country.

III. Subject and content of the FlugDaG

The FlugDaG implements the PNR Directive. § 1 (1) FlugDaG stipulates that the Federal Criminal Police Office (BKA) is the national unit for processing passenger name record data (passenger information unit, PIU). The processing of the data takes place at the Federal Administration Office (BVA) as the "contract processor" of the PIU. The modalities of the cooperation are laid down in an agreement pursuant to § 62 of the German Data Protection Act (BDSG). According to § 2 (3) FlugDaG, the obligation to transfer applies to all civil flights which depart in Germany and arrive in another country or which depart from another country and arrive in Germany or stop there, i.e. also intra-EU flights. The FlugDaG thus goes beyond the minimum harmonisation through the PNR Directive, cf. Art. 2 PNR Directive. As a result, the Federal Administration Office for Germany expects around 170 million passengers per year, which would generate 340 million data records.

Cf. the explanatory memorandum, Bundestag Printed Paper 18/11501, p. 23.

According to Eurostat, only around 65 million passengers would be affected excluding intra-EU flights.

Cf. Eurostat, Air Transport Statistics 2016, online at https://bit.ly/2vy5ISK (last accessed 3 May 2019).

The list of PNR data to be transferred is defined in § 2 (2) FlugDaG and corresponds to the list contained in Annex II of the PNR Directive. A free text field is also provided for here (§ 2 (2) No. 16 FlugDaG). Although § 13 (3) FlugDaG provides for immediate deletion obligations for all PNR data containing information on racial or ethnic origin, political opinions, religious or ideological convictions, membership of a trade union, state of health, sexual life or sexual orientation of a person, the PNR data must be deleted immediately. However, neither the FlugDaG itself nor the explanatory memorandum to the Act show how this is to be secured in terms of IT technology or procedure, particularly in the free text field that cannot be classified in a system, since the transferring airline considers that this is the case. Thus it remains conceivable that conclusions about a religious conviction are possible, for example, through special food requests (halal, kosher, etc.).

In the following, we will explain the transfer, processing and transfer process of PNR data in its chronological order:

1. Transfer of PNR data by airlines and storage

Airlines are obliged to transfer PNR data electronically to the PIU using the push method at two separate times in accordance with § 2 (5) sentence 1 No. 1 and 2 FlugDaG – firstly 48 to 24 hours before departure and secondly after boarding the aircraft. Infringement by airlines is punishable by a fine of up to fifty thousand Euro pursuant to § 18 (1) and (2) FlugDaG.

As a rule, this data remains for five years in the central database maintained by the BVA, § 13 (1) FlugDaG. However, the retention period for PNR data forwarded to other authorities and for processing results is separate from this retention period. In accordance with § 13 (4) sentence 3 FlugDaG, the regulations applicable to the respective authority apply to PNR data; in accordance with § 13 (4) sentence 2 FlugDaG, the processing results are not to be deleted until they are no longer required to provide information to other authorities (as defined in § 6 (1) sentence 1, (2) sentence 1 FlugDaG) or the PIUs of other Member States or to generate patterns.

Furthermore, the encroachment intensity of the storage is to be reduced by the fact that the PNR data pursuant to § 5 (1) FlugDaG is "depersonalised" by the Federal Criminal Police Office as the PIU after six months from their transfer by the airlines. This is to be done by redaction (obliteration) of the data points listed in § 5 (1) FlugDaG (name of the traveller and fellow travellers, payment information, frequent flyer entry, free text field, etc.).

However, the designation of this process as "depersonalisation" is inaccurate or at least contrary to the system. Thus, as is required under data protection law and customary in IT technology, a distinction is to be made between "anonymisation" and "pseudonymisation". While anonymisation makes it completely impossible to assign a data record to an individual person, pseudonymisation only replaces certain identity features with pseudonyms (e.g. combinations of numbers), meaning that individual assignment of the data records is more difficult, but remains possible with the aid of a key. As can be seen from §§ 46 No. 5, 71 (1) sentence 4 BDSG, this distinction is also used by the legislature. For example, § 46 No. 5 BDSG describes "pseudonymisation" as a reversible process involving the use of keys, while § 71 (1) sentence 4 BDSG assumes a dichotomy of the terms "pseudonymisation" and "anonymisation".

Although the terms "depersonalisation" and "redaction" suggest otherwise, § 5 (2) FlugDaG only requires pseudonymisation. This is because "depersonalisation" is to be abolished in the sense of a re-enabling the individual assignment of PNR data if the BKA, the state criminal investigation offices, the customs administration, the Federal Police, the Federal and State Office for the Protection of the Constitution, the Military Counter-Intelligence Service or the Federal Intelligence Service (as defined in § 6 (1) and (2) FlugDaG; hereinafter referred to as "**security authorities**") make such a request and this is necessary in the case of a comparison with external data of the security authorities pursuant to § 4 (5) sentence 1 FlugDaG for the prevention or prosecution of criminal offences pursuant to § 4 (1) FlugDaG (§ 5 (2) sentence 1 and sentence 4 FlugDaG). This "repersonalisation" thus restores the original data record and, contrary to § 5 (2) sentence 1 no. 2 FlugDaG, can also be carried out without court approval in the event of imminent danger by order of the President of the BKA (§ 5 (2) sentence 2 FlugDaG).

For the purpose of repersonalisation, the depersonalised PNR data remains accessible to specially authorised staff of the passenger information centre.

2. Processing of PNR data

The BVA receives the PNR data centrally as an order processor, prepares it technically, compares it automatically in accordance with the technical specifications of the PIU (i.e. of the BKA) and inspects it from a technical point of view, § 1 (3) FlugDaG.

After the data records have been received by the BVA, they are compared with existing databases and at the same time with so-called "patterns" in accordance with § 4 (2) FlugDaG. This comparison is carried out automatically before the aircraft arrives in Germany or before departure from Germany. Before being forwarded to other authorities as a result of

a hit, the processing results are individually checked in accordance with § 4 (2) sentence 2 FlugDaG.

(a) Purpose of the comparison

The purpose of data processing declared in § 4 (1) FlugDaG is to identify persons who have committed one of the offences listed in this catalogue or who will do so within a foreseeable period of time. While § 4 (1) No. 1 to 4 FlugDaG lists concrete criminal offences, § 4 (1) No. 5 and 6 FlugDaG only refer to EU standards, in particular to the list of punishable acts in Annex II of the PNR Directive, without specifying this list in more detail or establishing a materiality threshold.

The comparisons are intended to achieve two things: On the one hand – hence the comparison with already existing databases – the identification of persons who have already appeared in connection with terrorist offences or serious crime. On the other hand, a "different, new way" of fighting crime is to be found in the comparison with so-called "patterns".

> As in the explanatory memorandum, Bundestag Printed Paper 18/11501, p. 28.

The aim is to filter out those persons from the mass of air passengers who have never before become suspicious or conspicuous under criminal law, but whose flight behaviour – whether accidental or not –, according to experience in criminology, corresponds to the flight behaviour of those persons who have already appeared in connection with relevant criminal offences. So this is an attempt to find new suspects.

b) Comparison with existing databases

In § 4 (2) No. 1 FlugDaG it is stipulated in the abstract that the comparison with such databases is permissible if they serve the purpose of tendering for persons or property. The legislature assumes that a comparison will be made with the databases "Schengen Information System", "INPOL Central" and the "Automated Search Facility - Stolen and Lost Travel Documents Database" (hereinafter "**ASF-SLTD**"). The Schengen Information System and the INPOL Central are search lists for persons and objects searched for inside and outside the Schengen area. In particular, the ASF-SLTD registers objects reported as stolen so that it can be recorded when a passenger travels with a stolen or forged identity or passport document.

Cf. the explanatory memorandum, Bundestag Printed Paper 18/11501, p. 28.

c) Comparison with “patterns”

The patterns are based on empirical experience in criminology. They are intended to store profiles of known offenders whose itineraries, stopovers, length of stay, etc. are considered typical for certain offences. The dynamic approach of the perpetrators and the associated fast-moving nature of patterns stand in the way of a further legal definition of the content of the patterns. The idea is that it is necessary to prevent perpetrators from being able to adapt their procedures to patterns in such a way that they would be rendered useless due to rigid legal requirements. The legislature uses a drug courier as an example of a delinquent, from whose flight behaviour one can draw conclusions to justify suspicious about passengers behaving in a similar manner.

Cf. the explanatory memorandum, Bundestag Printed Paper 18/11501, p. 29.

In accordance with § 4 (3) sentence 1 FlugDaG, the patterns are prepared by the PIU under the guidance of the security authorities. The PNR data itself can also be analysed (§ 4 (4) FlugDaG). The patterns are then be reviewed at least every six months in cooperation with the security authorities and the PIU's data protection officer(s). The data protection officer of the PIU is identical to the data protection officer of the BKA (§ 12 (1) FlugDaG). The Federal Commissioner for Data Protection and Freedom of Information reviews the preparation and application of the patterns at least every two years (§ 4 (4) sentence 8 FlugDaG).

The effectiveness of the use of patterns to combat crime has not been proven by studies – it is experimental. The PIU is not obliged to report to parliament or the public. Instead, only the Federal Commissioner for Data Protection and Freedom of Information is obliged to report to the Federal Government (§ 4 (4) sentence 9 FlugDaG).

During the automated comparison of the data records with the patterns, plausibility checks are first carried out, i.e. matches are sought with the flight behaviour of known offenders. Subsequently, “negative plausibilities" are formed, i.e. the data records are compared with the inspection characteristics contained in the patterns (within the meaning of § 4(3) sentence 5 FlugDaG). The BVA forwards the data records with plausibilities that have not been refuted by negative plausibilities to the BKA for individual validation. The legislature assumes that this will affect a total of approx. 0.1% of all data records, while 99.9% of the data records will remain with the BVA. However, these expected values fluctuate. At a demonstration of the technical system that the BVA intends to use for data processing at *CeBIT 2017*, 0.07% of the data records were positively identified.

Cf. the explanatory memorandum, Bundestag Printed Paper 18/11501, p. 26, and *Alexander Sander* in the statement of opinion of the Digitale Gesellschaft e.V. (p. 4) in the committee's printed document 18(4)869 B.

With approximately 170 million people travelling to and from Germany by air every year, a positive rate of approximately 0.1% corresponds to 170,000 positive hits.

3. Follow-up measures, in particular forwarding of data and processing results

With regard to these positively identified data records, the PIU will consider the next steps. In particular, those persons who have not yet become suspicious before the PNR data is processed should then be "further investigated" by the security authorities within the framework of preventive or repressive police or secret service measures.

Cf. the explanatory memorandum, Bundestag Printed Paper 18/11501, p. 25.

The PIU forwards the data records and processing results to the security authorities to initiate such measures pursuant to § 6 (1), (2) FlugDaG. For the authorities mentioned in § 6 (1) FlugDaG, the purpose limitation contained in § 1 (2) and § 6 (3) FlugDaG pursuant to § 6 (4) FlugDaG is waived to the extent that they may also use the transferred data for other purposes, in particular for the prosecution of other criminal offences not contained in § 4 (1) FlugDaG, insofar as they perform criminal prosecution tasks.

Pursuant to § 7 (3) FlugDaG, the PNR unit may also transfer both the PNR data records and the processing results to the PNR units of other Member States if it becomes apparent that the transfer is necessary following a comparison or if a reasoned request is received from the Member State to the PNR Unit which indicates that the transfer is necessary to prevent or prosecute the offences listed in § 4 (1) FlugDaG, or if the airline receives a corresponding request. The criterion of necessity is not specified in detail, but the explanatory memorandum of the Act gives as an example that necessity exists if, on the basis of an analysis of passenger data, it appears that smuggling gangs are using new routes to or via another Member State, or if a greater number of people linked to terrorist offences have travelled to a particular Member State.

Cf. the explanatory memorandum, Bundestag Printed Paper 18/11501, p. 33.

If a similar request has been made by Europol, the PIU may also transfer the PNR data records and the processing results pursuant to § 9 sentence 1 FlugDaG to Europol.

In addition, the PIU may also transfer PNR data and processing results to the authorities of countries which are not EU Member States (hereinafter referred to as "**third countries**") in accordance with § 10 (1) FlugDaG. The requirements for this essentially correspond to those of §§ 7, 9 FlugDaG. In addition, however, pursuant to § 10 (1) No. 2 FlugDaG, these authorities must undertake to transfer the data to the authorities of a third country only if this is necessary to prevent or prosecute terrorist offences or serious crime, and if the consent of the PIU is obtained prior to further transfer. Furthermore, the PIU must comply with §§ 78-80 BDSG. This presupposes that the EU Commission has taken a decision on the appropriateness of the third country in accordance with Art. 36 (3) of Directive 2016/680. This is currently the case for Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA.

List available at https://bit.ly/2Jnzlbo (last accessed 3 May 2019).

Furthermore, PNR data can also be transferred to third countries without a decision on adequacy or guarantees – under the same vague conditions as under Art. 38 of the Data Protection Directive, cf. § 80 (1) BDSG.

4. No obligation to inform

The FlugDaG does not provide for passengers affected to be informed of PNR processing and transfer or of any follow-up measures. A passenger who has not previously been the subject of criminal proceedings may, as a result of positive identification, be the subject of an investigation and data concerning him or her may be transferred to third countries without his or her knowledge.

IV. Course of proceedings

By letter of 26 March 2019, the Claimant asked the Defendant to state that it would refrain from storing, processing and transferring passenger data relating to him in respect of the flight at issue.

Exhibit K 2

Subsequently, by letter of 4 April 2019, the Defendant declared to the signatory that it intended to apply the law in force and to store and process the Claimant's passenger data.

Exhibit K 3

The present complaint was therefore necessary.

C. Legal evaluation

The preventive injunction action is admissible (see section I.). It is also justified because, in the absence of a lawful legal basis, the Plaintiff has a public-law right to an injunction to prohibit the collection, storage and processing of his PNR data. The PNR Directive on which the FlugDaG is based violates higher-ranking European law and is therefore invalid (see section II). Consequently, the FlugDaG itself violates European fundamental rights (see section III.). To the extent that it makes full use of the leeway granted by the PNR Directive, the FlugDaG also violates the German Constitution (see section IV.).

I. Admissibility

A preventive injunction action presupposes a well-founded concern that the Defendant will in future illegally interfere with the Plaintiff's legal sphere through its sovereign acts.

> BVerwG, judgment of 22 October 2014 - 6 C 7.13 (= ZD 2015, 322), marginal No. 20.

This action must already be so concrete that it has the certainty required for a review of legality.

> BVerwG, judgment of 13 December 2017 - 6 A 6.16 (= DÖV 2018, 378), marginal No. 12 with further references.

This is the case here, because the PNR data storage and processing in question will surely occur. In particular, the Plaintiff's flights fall within the material scope of § 2 (3) FlugDaG. In addition, the Plaintiff unsuccessfully asked the Defendant to declare that it would not store and process the PNR data at issue (see Exhibit K2).

The granting of preventive legal protection also presupposes a special interest worthy of protection in the sense that it is not reasonable for the data subject to be referred to the subsequent legal protection provided by the administrative court order for the normal case.

> BVerwG, judgment of 13 December 2017 - 6 A 6.16 (= DÖV 2018, 378), marginal No. 15 with further references.

This is also the case here. PNR data storage and processing will take place at least 24 hours before departure. There is also a possibility that this information will be forwarded to other authorities, including foreign authorities. *a posteriori* legal protection could no longer eliminate the effect of these encroachments.

The Plaintiff is also entitled to sue for the preventive claim to cease and desist PNR data storage and processing analogous to § 42 (2) VwGO, as if there is relevant data encroachment by state authorities covered by the scope of protection of the right of informational self-determination, without this being covered by an effective basis of authorisation, this may – directly supported by Art. 2 (1) in conjunction with Art. 1 (1) of the German Constitution – lead to legal claims for defence (public law injunctive relief).

> OVG Lüneburg, judgment of 12 February 1991 - 9 L 246/89 (= NJW 1992, 192, 193); cf. also BVerwG, judgment of 13 December 2017 – 6 A 6.16 (= DÖV 2018, 378) – , marginal No. 22.

The lack of an effective legal basis for the storage and processing of PNR data is explained below.

II. PNR Directive violates higher-level European law

The collection, storage and processing of PNR data by the Defendant on the basis of the FlugDaG is already unlawful and prohibited because the PNR Directive on which the law is based violates higher-ranking European law, in particular Articles 7 and 8 Charter of Fundamental Rights (see No. 2.). If this court comes to the same conclusion, it must refer the issue to the ECJ as to whether the PNR Directive is compatible with Art. 7, 8 CFR (see No. 3).

1. Binding to the Charter of Fundamental Rights

The bodies of the European Union are bound to the fundamental rights guaranteed in the Charter pursuant to Art. 51 (1) sentence 1 CFR. In particular, Directives issued by them must therefore be measured against these fundamental rights.

2. Violation of Art. 7 and 8 CFR in connection with Art. 52 (1) sentence 2 CFR

The ECJ has repeatedly commented on the standards of Art. 7 and 8 CFR for the handling of personal data (see a) below). According to these standards, PNR data storage and processing encroaches on these fundamental rights (see b) below) without being justified (see c) below).

a) Case law of the ECJ

aa) General standards

Art. 7 CFR protects private life, among other things. This includes in particular the free decision of the individual on his personal lifestyle, as well as whether or not to make it the subject of public knowledge and discussion.

> *Kingreen* in: Calliess/Ruffert, TEU/TFEU, 5th ed. 2016, marginal No. 3.

According to Art. 8 CFR, every person also has a right to the protection of personal data relating to them. This fundamental right is closely linked to the fundamental right to respect for private life.

> ECJ, judgment of 9 November 2010, Volker and Markus Schecke GbR and Eifert, C-92/09 and C-93/09, EU:C:2010:662, marginal No. 47.

With regard to the treatment of personal data, the ECJ has therefore uniformly drawn the scope of protection of both fundamental rights.

> Cf. intuitively the opinion of the European Court of Justice 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 121 et seq. with further references; further judgment of 17 October 2013, Schwarz, C-291/12, EU:C:2013:670, marginal No. 24 et seqq.

In this respect, the two fundamental rights cover any information concerning an identified or identifiable natural person.

> ECJ, judgment of 9 November 2010, Volker and Markus Schecke GbR and Eifert, C-92/09 and C-93/09, EU:C:2010:662, marginal No. 52; judgment of 24 November 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 and C-469/10, EU:C:2011:777, marginal No. 42; judgment of 17 October 2013, Schwarz, C-291/12, EU:C:2013:670, marginal No. 26; cf. also Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 122.

This also includes data relating to the professional sphere of the data subject.

> Cf. ECJ, judgment of 20 May 2003, Österreichischer Rundfunk et al., C-465/00, C-138/01, C-139/01, EU:C:2003:294, marginal No. 73 et seq. to Art. 8 ECHR.

According to the case law of the ECJ, the disclosure of personal data to a third party, such as a public authority, already constitutes an encroachment on the fundamental right pursuant to Art. 7 CFR, irrespective of the subsequent use of the transferred information. The same applies to the storage of personal data and access to the data for its use by the authorities. In order to establish such an encroachment, it is irrelevant whether the information transferred is to be regarded as sensitive or whether the data subjects suffer any disadvantages as a result of the procedure.

> ECJ, judgment of 20 May 2003, Österreichischer Rundfunk et al., C-465/00, C-138/01 and C-139/01, EU:C:2003:294, marginal No. 74 and 75; judgment of 8 April 2014, Digital Rights Ireland et al., C-293/12 and C-594/12, EU:C:2014:238, marginal No. 33 et seqq.; judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, marginal No. 87; cf. also Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 124.

This applies accordingly to Art. 8 CFR.

> ECJ, judgment of 17 October 2013, Schwarz, C-291/12, EU:C:2013:670, marginal No. 25; judgment of 8 April 2014, Digital Rights Ireland et al., C-293/12 and C-594/12, EU:C:2014:238, marginal No. 36; Opinion of the ECJ 1/15, of 26 July 2017, EU:C:2017:592, marginal No. 126.

However, the rights set out in Articles 7 and 8 of the Charter cannot claim absolute validity, but rather must be seen in the light of their social function.

> ECJ, judgment of 9 November 2010, Volker and Markus Schecke and Eifert, C-92/09 and C-93/09, EU:C:2010:662, marginal No. 48; judgment of 17 October 2013, Schwarz, C-291/12, EU:C:2013:670, marginal No. 33; judgment of 5 May 2011, Deutsche Telekom AG, C-543/09, EU:C:2011:279, marginal No. 51; cf. also Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 136.

In particular, the guarantee of public security is an objective serving the common good which can also justify serious encroachment with the fundamental rights laid down in Articles 7 and 8 CFR.

> ECJ, judgment of 8 April 2014, Digital Rights Ireland et al., C-293/12 and C-594/12, EU:C:2014:238, marginal No. 42 and 44; judgment of 15 February 2016, N., C-601/15 PPU, EU:C:2016:84, marginal No. 53; cf. also Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 148 et seq.

However, the protection of the fundamental right to respect for private life requires that exceptions to the protection of personal data be limited to what is strictly necessary,

> ECJ, judgment of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU:C:2008:727, marginal No. 56; of 9 November 2010, Volker and Markus Schecke GbR and Eifert, C-92/09 and C-93/09, EU:C:2010:662, marginal No. 77; of 8 April 2014, Digital Rights and Others, C-293/12 and C-594/12, EU:C:2014:238, marginal No. 52; of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, marginal No. 92; of 21 December 2016, Tele2 et al., C-203/15 and C-698/15, EU:C:2016:970, marginal No. 96; cf. also Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 140,

which also results from the principle of proportionality in Art. 52 (1) sentence 2 CFR.

With regard to the storage of personal data, the legislation in question must always satisfy objective criteria which establish a link between the personal data to be stored and the objective pursued.

> ECJ, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, marginal No. 93; judgment of 21 December 2016, Tele2 Sverige and Watson et al., C-203/15 and C-698/15, EU:C:2016:970, marginal No. 110; cf. also Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 191.

For the use of lawfully stored personal data, Union legislation must not be limited to ensuring that access to such data fulfils one of the purposes set out in the legislation, but must also lay down the substantive and procedural conditions for the use of the data.

> ECJ, judgment of 21 December 2016, Tele2 Sverige and Watson et al., C-203/15 and C-698/15, EU:C:2016:970, marginal No. 117 et seq. with further references.; see also Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 192.

In order to meet these requirements, the provision containing the encroachment must lay down clear and precise rules on the scope and application of the measure in question and establish minimum requirements so that the persons whose data has been transferred have sufficient guarantees to ensure effective protection of their personal data against misuse. In particular, it must indicate the circumstances and conditions under which a measure providing for the processing of such data may be taken in order to ensure that the encroachment is limited to what is strictly necessary. The need to have such safeguards is all the more important where personal data is processed automatically. This applies in particular to the protection of the special category of sensitive personal data.

> ECJ, judgment of 8 April 2014, Digital Rights Ireland et al., C-293/12 and C-594/12, EU:C:2014:238, marginal No. 54 and 55; judgment of 21 December 2016, Tele2 Sverige and Watson et al., C-203/15 and C-698/15, EU:C:2016:970, marginal No. 109 and 117; Opinion of the ECJ 1/15 of 26 July

2017, EU:C:2017:592, marginal No. 141; cf. in this sense also ECHR, 4 December 2008, S. and Marper/UK, 30562/04 and 30566/04, CE:ECHR:2008:1204JUD003056204, § 103.

The ECJ has further differentiated this case law, in particular in its rulings on data retention and in its expert opinion on the PNR agreement between the EU and Canada.

bb) ECJ judgments on data retention

Directive 2006/24 (hereinafter referred to as the "**Data Retention Directive**") originally obliged all EU Member States to introduce the retention of telecommunications connection data. On 8 April 2014, the ECJ declared it invalid as it infringed Articles 7, 8 and 52 of the CFR.

ECJ, judgment of 8 April 2014, Digital Rights Ireland et al., C-293/12 and C-594/12, EU:C:2014:238

The ECJ affirmed an encroachment on these fundamental rights with the consideration that very precise conclusions can be drawn on the private life of the persons whose data has been stored from all the telecommunications connection data covered by the Data Retention Directive, such as habits of daily life, permanent or temporary whereabouts, daily or other rhythmic changes of location, activities carried out, social relations of these persons and the social environment in which they operate.

ECJ, judgment of 8 April 2014, Digital Rights Ireland et al., C-293/12 and C-594/12, EU:C:2014:238, marginal No. 27, 32 et seqq.

The ECJ did not consider this encroachment for the purposes of combating international terrorism and serious crime to be justified. In doing so, the ECJ justified the lack of necessity of the Data Retention Directive under the following aspects, among others:

- The material scope of the Data Retention Directive covers all forms of electronic communications, the use of which is widespread and increasingly important in the daily lives of individuals; thus it encroached on the fundamental rights of almost the entire European population (marginal No. 56 of the judgment). The data collected would also not have to be related to a particular threat, for example by location or period of time (marginal No. 59).
- The personal scope of the Data Retention Directive covers all persons who use electronic means of communication, including persons for whom there is no indication whatsoever that their conduct might be connected, even indirectly or remotely, with

serious criminal offences, and even persons subject to professional secrecy would be covered (marginal No. 58 of the judgment).

- The Data Retention Directive does not contain sufficient procedural safeguards to make access to retained data subject to prior control by a court or independent administrative body (marginal No. 62 of the judgment).
- In addition, the retention periods would apply to all data without any distinction being made as to their possible usefulness or the data subjects (marginal No. 63 et seq. of the judgment).

These findings on the disproportionate nature of the retention of telecommunications connection data were confirmed by the ECJ in a second judgment.

> ECJ, judgment of 21 December 2016, Tele2 Sverige and Watson et al., C-203/15 and C-698/15, EU:C:2016:970, marginal No. 99 et seqq., esp. marginal No. 105 et seq.

cc) Opinion of the ECJ on PNR data

The ECJ has also issued a detailed opinion specifically on the handling of PNR data.

> Opinion of the ECJ 1/15 of 26 July 2017 (hereinafter the "**Opinion**").

The Opinion concerned the PNR Agreement between the EU and Canada (hereinafter the "**EU-Canada Agreement**"). The European Parliament had asked the ECJ whether the processing and transfer of PNR data provided for in the EU-Canada Agreement was compatible with Articles 7, 8 and 52 (1) CFR.

In order to protect personal data, the ECJ requires that, where it is transferred from the Union to a third country, the high level of protection of fundamental freedoms and rights afforded by Union law is maintained. Although the means of ensuring such a level of protection may differ from those used in the Union to safeguard requirements arising from Union law, they must nevertheless prove effective in practice.

> Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 134; cf. also ECJ, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, marginal No. 72 et seqq.

That means: What the European Court of Justice has already recognised as contrary to Union law in connection with an international PNR agreement applies all the more to purely intra-European regulations ("equivalent").

The Opinion concluded that the EU-Canada Agreement as submitted to the ECJ is incompatible with Articles 7, 8 and 52(1) CFR because

- Parts of the EU-Canada Agreement were not formulated clearly enough (more about this below);
- the models and criteria used in the automated processing of PNR data were not specific and reliable, discrimination was not excluded and it was not ensured that Canada only uses databases related to the fight against terrorism and serious crime;
- the use of the data beyond the date of arrival does not require any new circumstances and is not subject to an independent review;
- PNR data may be transferred to third countries without the EU-Canada Agreement ensuring that third countries provide an adequate level of protection in accordance with Union law; and
- data subjects are not informed about the storage and use of their data after a hit.

The ECJ considered the following categories of PNR data in the EU-Canada Agreement to be too vague:

- Category 5 (“Available frequent flyer and bonus data [free tickets, upgrades, etc.]”), because the term “etc.” is too vague and because it remains unclear whether it refers solely to information on passengers' participation in bonus programmes or to all information on flights and bookings operated under such programmes (see marginal No. 157 of the Opinion).
- Category 17 ("General entries including OSI (Other Supplementary Information), SSI (Special Service Information) and SSR (Special Service Request) information") because it is a free text field. Such a category does not contain information on the nature and extent of the information to be transferred and may itself contain information which is not related to the purpose of the transfer of PNR data. Since the information referred to under this heading would only be given as an example, as shown by the use of the word “including”, it would not limit the nature and scope of the information it could collect (marginal No. 160 of the Opinion).

b) PNR Directive encroaches on Art. 7 and 8 CFR

The PNR Directive deeply encroaches on the right to respect for private life and the right to protection of personal data. What the European Court of Justice has ruled with regard to the storage of telecommunications data,

> ECJ, judgment of 8 April 2014, Digital Rights Ireland et al., C-293/12 and C-594/12, EU:C:2014:238, marginal No. 27,

also applies to the storage of PNR data: The data allows comprehensive conclusions to be drawn about the private and – likewise protected – professional life of the data subjects, namely who travelled where and when, in whose company, what means of payment they used, what contact details they provided or whether they travelled with light or heavy luggage. The free text field can also be used to generate various other data, and the contents of that data are not clear. In this way, detailed personality profiles can be created – especially for frequent flyers, but not only for them. All this data is stored centrally for months and – in "depersonalised" form – years, it is automatically cross-checked with databases and samples and can be forwarded to domestic authorities as well as to authorities of other EU countries and even third countries. The data subjects must therefore expect that all of their air journeys will be or may become known to various public authorities and that they may be subject to further measures by the security authorities due to a data processing procedure which they cannot foresee and which may entail substantial hardships.

c) Encroachment is not justified

The encroachment upon these fundamental rights is not justified because it goes beyond the limits of what is necessary.

The PNR Directive pursues legitimate objectives, namely the prevention and prosecution of terrorist offences and serious crime (cf. Article 1(2) PNR Directive). However, it is doubtful whether the collection, storage and processing of PNR data are actually appropriate to achieve this objective. This is because the PNR Directive does not explain how exactly the comparison with pre-defined criteria should lead to new suspects, i.e. which data should be related to which other data and with what result.

However, the encroachment is not necessary or appropriate to achieve the objective. The PNR Directive is already too vague in parts (see aa)). Nevertheless, the planned storage and processing of PNR data without cause is inadmissible because its objective and personal scope of application is too broad (see bb)) and the duration of storage is not subject to comprehensible limits (see cc)). Finally, the procedural rights of data subjects are not respected (see dd)) and there is insufficient protection for data subjects when PNR data is transferred to third countries (see ee)).

aa) PNR Directive too vague in parts

According to the standards of the ECJ, the PNR Directive is not sufficiently defined insofar as it provides in Annex I that the "frequent flyer entry" (No. 8) and "general information (including all available information on ...)" (No. 12) also belong to the PNR data and must therefore be collected, stored and processed.

The general information referred to in point 12 of Annex I is a free text field. Like Category 17 of the EU-Canada Agreement, the requirements for the filling of this field do not contain exhaustive information on the nature and quantity of the information to be provided, as is apparent from the use of the word “including”, and may themselves include information which is not related to the purpose of the transfer of PNR data.

> See, for example, the Opinion of the ECJ on the EU-Canada Agreement 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 160; see a) cc) above.

With regard to the frequent flyer entry, the uncertainty arises from the fact that it is unclear whether it refers solely to information on passengers' participation in bonus schemes or to all information on flights and bookings operated under such schemes.

> See, for example, the Opinion of the ECJ on the EU-Canada Agreement 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 157; see a) cc) above.

bb) Material and personal scope of application too broad

The scope of the PNR Directive is too broad and goes beyond what is necessary.

The PNR Directive does not contain any objective restrictions: All international flights of all airlines are recorded, regardless of their country of origin and destination or a specific or even increased threat situation in one country or another. In addition, in the case of an extension to EU flights, cf. Art. 2 PNR Directive, PNR data on flights between neighbouring EU countries is also collected and stored, although the EU Member States can be regarded as safe compared to many other regions in the world. Furthermore, all data transferred to the PNR Unit is stored and subjected to automated comparison with databases and patterns.

A milder measure of equivalent effect would be readily conceivable: For example, the pre-defined criteria (Article 6 (2)(b) of the PNR Directive) could be applied to the selection of flights on which airlines are required to push PNR data to the PNR Unit rather than to PNR data collected and stored by the PNR Unit.

The PNR Directive also does not contain any restrictions on personal scope: All passengers are covered, regardless of their personal history – and also without an exception for those bearing professional secrets, who may have an interest in the secrecy of certain journeys. According to estimates by the Federal Government, 99.9% of the PNR data records collected in Germany do not produce hits, i.e. they are stored and processed unnecessarily from the outset (cf. B.III.2.c above).

This is not in line with the ECJ's requirement that the storage of data must always satisfy objective criteria which establish a link between the personal data to be stored and the objective pursued.

> Cf. in particular the Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 191 and further references in a) aa) above.

There is no connection between the storage of PNR data of objectively non-dangerous and non-suspected persons and the fight against terrorism. This does not change the fact that a small percentage of the PNR data stored relates to unidentified dangerous persons and that mass storage is used to (also) identify them, as only this circumstance can establish the connection between the PNR data of these persons and the objective pursued. The connection is also does established from the fact that, for example, the non-dangerous and non-suspected persons knowingly move within a certain area of suspicion, for example by travelling to a crisis area; the PNR Directive applies without exception to all international flights.

The recording of persons for whom there is no indication whatsoever that their conduct might be even indirectly or remotely connected with serious criminal offences, and in particular the registration of persons carrying professional secrets, are also incompatible with Articles 7 and 8 CFR according to the ECJ case law on data retention.

> Cf. ECJ, judgment of 8 April 2014, Digital Rights Ireland et al., C-293/12 and C-594/12, EU:C:2014:238, marginal No. 58.

However, even if the collection and storage of data were considered necessary, the PNR Directive does not comply with the ECJ's requirement that substantive conditions must be laid down for the use of the data.

> See Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 192 and further references in a) aa) above.

Because the use is not subject to any further requirements: All PNR data is cross-checked with existing databases and with "pre-established criteria" (Art. 6 (3) PNR Directive).

The PNR Directive thus goes even further than the use of retained telecommunications connection data, because this has always had to be related to a specific case – a specific suspicion – whereas PNR data processing does not need a reason, but rather is automatic without any further conditions.

While the comparison of PNR data with databases containing persons suspected of having committed a criminal offence or found to be dangerous may still have at least an abstract factual connection with the objective of the PNR Directive, this is not guaranteed for comparison with pre-established models. Because the current state of the art does not guarantee that patterns, however defined they may be, are likely to indicate a dangerous person. On the contrary, the EU Commission has already admitted to the ECJ on the occasion of the EU-Canada Agreement that there is a "certain" error rate; the European Data Protection Supervisor even considers this error rate to be "substantial".

> Cf. the Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 169 et seq.

However, as long as there is a "certain" to "substantial" error rate, it is not necessary to check all passengers uniformly on the basis of these patterns, because classical investigation methods are just as promising. However, it is also inappropriate because a "certain" to “substantial" error rate leads to a high number of innocent victims who have to expect unjustified follow-up measures.

Accordingly, the ECJ has found that automated processing using models and criteria must ensure that they are specific, reliable and non-discriminatory by taking into account statistical data and the results of international research in their production and verification.

> Cf. the Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 174.

The PNR Directive does not make such provisions. Although Art. 6 (4) sentence 3 PNR Directive stipulates that the criteria must be "targeted, proportionate and defined", it does not specify how this is to be achieved. Furthermore, it is unclear how it is to be guaranteed that racial or ethnic origin may not serve as the basis for the designs in accordance with the provisions of Art. 6 (4) sentence 4 PNR Directive, which is intended to protect against discrimination (cf. Art. 21 (1) CFR). It seems likely that certain international routes will be considered more sensitive than others and that people of a certain racial or ethnic origin will make greater use of these routes. For example, the proportion of Turkish people or people of Turkish origin on flights from Germany to Turkey is very high and it is to be expected that a criterion which considers flights from Germany to Turkey to be relevant to security will

systematically affect Turkish people or people of Turkish origin and thus have an indirect discriminatory effect.

(cc) Insufficient time limits for the storage and use of PNR data

Measured against the time limits set by the ECJ for the storage of PNR data, the PNR Directive also exceeds the limits of what is necessary in this respect.

The Directive allows the retention of PNR data of all passengers for a period of five years and their use for the purposes set out in Article 6(2) of the PNR Directive for the duration of the retention of the PNR data of all passengers (after six months, however, only under the further conditions of Article 6 (3) of the PNR Directive). In particular, it has no influence on this possibility of use if the data subjects have left the target country again.

This does not meet the requirements of Art. 7 and 8 CFR as developed by the ECJ. With regard to the EU-Canada Agreement, the Court has ruled that passengers checked on entry and exit do not, in principle, pose a threat to Canada in the area of terrorism or serious cross-border crime if neither these checks and verifications nor any other circumstance would have provided objective indications of this. In such cases, after their departure, there would no longer be a link between PNR data and public security and the continued storage of all passengers' data would no longer be necessary. Other provisions could only apply if, in specific cases, there were objective indications that certain passengers could pose a threat of terrorism or serious cross-border crime even after their departure.

> Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 204 et seqq.; cf. also ECJ, judgement of 08 April 2014, EU:C:2014:238, marginal No. 63 et seq.; ECJ, judgment of 21 December 2016, EU:C:2016:970, marginal No. 119.

Applied to the PNR Directive, this means that the retention of PNR data – particularly qualified data, cf. bb) above – from the outset can be considered necessary only for the duration of the stay in the country of destination. The PNR data of persons who have not been identified as relevant to security either before or during the journey are to be deleted immediately. Although it may theoretically be possible that the data might become relevant again at some point, according to the ECJ's assessments, it is out of proportion to the far-reaching, massive encroachment on the fundamental rights of the data subjects to store data beyond the journey in response to this eventuality.

This assessment is not affected by the fact that the PNR data is to be depersonalised after six months from its transfer in accordance with Article 12 (2) of the PNR Directive. It can be

left open here whether such (reversible) depersonalisation (while maintaining full access for a qualified group of persons, cf. explanatory memorandum to the Act, Bundestag Printed Paper 18/11501, p. 30) has any added value at all from the point of view of fundamental rights -–especially since the data can already be held by other authorities in the meantime and is subject to their own rules there. In any case, depersonalisation does not change the fact that the ECJ only allows the storage of PNR data to continue beyond the duration of the journey if there are objective indications that specific persons could pose a threat in connection with terrorism or cross-border serious crime even after their departure.

dd) Insufficient procedural guarantees

Furthermore, the PNR Directive does not provide sufficient procedural protection.

The PNR Directive does not include any provisions which state that the storage and use of PNR data is subject to independent checks. Only the cancellation of depersonalisation requires the approval of a "judicial authority" or another qualified national authority, Art. 12 (3) PNR Directive.

This does not meet the requirements of Art. 7 and 8 CFR as developed by the ECJ. With regard to the EU-Canada Agreement, the ECJ found that the use of the PNR data stored after entry into the country of destination (there: Canada) is only permissible if, in principle, it is subject to prior review by a court or an independent administrative body, except in duly substantiated cases of urgency, and if the decision is taken following a reasoned request made by the competent authorities, in particular in connection with procedures for the prevention, detection or prosecution of criminal offences.

> Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 202 with further references.

The PNR Directive does not comply with these requirements. This is not changed by the examination of the cancellation of depersonalisation by a judicial authority. Firstly, it is already questionable whether all "judicial authorities" of the Member States are independent in the sense of the ECJ Opinion; and secondly, the examination by a judicial authority is not intended for the case that a data record is to be further used after successful arrival on the basis of new concrete indications (see cc) above).

In its Opinion, the ECJ also emphasised the necessity of an obligation to notify data subjects. To that end, it stated that it was necessary to provide passengers with individual information – retroactively – where there was objective evidence justifying the use of PNR data beyond systematic/automated checks, and that prior authorisation by a court or an independent

administrative body was also required. The same would apply in cases where PNR data would be disclosed to other authorities or to individuals. However, such a notification could only be made if it could no longer interfere with the investigations of the authorities.

> Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 223 et seq.

The PNR Directive does not contain any such obligation to notify. It therefore also violates Art. 7 and 8 CFR for this reason.

ee) Insufficient safeguards during the transfer of PNR data to third countries

Finally, the PNR Directive does not provide sufficient safeguards for the transfer of PNR data to third countries.

The ECJ has found that a transfer of personal data to third countries requires that a Commission decision pursuant to Article 25(6) of Directive 95/46 (now: Article 36 of the Data Protection Directive), according to which the third country guarantees an adequate level of protection for the data.

> Opinion of the ECJ 1/15 of 26 July 2017, EU:C:2017:592, marginal No. 214.

However, as outlined above (see section B.III.3), PNR data may also be transferred to third countries under other conditions, namely on the basis of guarantees (Art. 37 Data Protection Directive) or vague exceptions (Art. 38 Data Protection Directive). An adequate level of data protection is then not guaranteed.

ff) Overall assessment

The PNR Directive also does not withstand an overall assessment within the context of the proportionality test pursuant to Art. 52 (1) sentence 2 CFR.

Its objective is to prevent and prosecute terrorist or other serious criminal offences by collecting, storing and processing PNR data of all international passengers, outside specific high-risk situations, in order to register the movements of persons entered in databases and to obtain new suspects by means of pre-defined criteria, the latter having a "certain" to "substantial" error rate and furthermore the value of a successful investigation of a suspicion for public security being unclear.

On the other hand:

- the mass storage and processing of retained PNR data by the state, and, above all, by automated means, of persons whose previous behaviour did not give rise to their monitoring;
- the excessively long retention of PNR data (five years);
- the likelihood, bordering on certainty, of unjustified follow-up action against falsely suspected persons, such as further government investigation measures or refusal of entry;
- the risk of the intimidating effect of secret mass surveillance on the exercise of other fundamental rights, such as the fundamental right to freedom of movement; and
- the risk of stigmatising certain groups of the population which, because of their origin, could be disproportionately covered by the pre-defined criteria.

3. Legal consequence: Submission to the ECJ

Should this court follow the submissions made here and have doubts about the compatibility of the PNR Directive – and thus of the FlugDaG – with the EU Charter of Fundamental Rights, it must refer the question of the validity of the PNR Directive to the ECJ pursuant to Art. 267 (2) TFEU. If a national court considers secondary law to be incompatible with higher-ranking European law, it must refer the matter to the ECJ, even if appeals against its decision were still admissible; the margin of discretion granted under Article 267(2) TFEU is then reduced to zero because the Member State courts are not themselves empowered to declare acts of the Union institutions invalid.

> Fundamentally ECJ, judgment of 22 October 1987, Foto-Frost, C-314/85, EU:C:1987:452, marginal No. 11 et seq.; expressly confirmed in the judgment of 6 December 2005, Gaston Schul, C-461/03, EU:C:2005:742, marginal No. 17 et seqq.

We propose to refer the following questions:

1. *Is Directive 2016/681 compatible with the right to privacy enshrined in Article 7 CFR?*
2. *Is Directive 2016/681 compatible with the right to protection of personal data enshrined in Article 8 CFR?*

III. FlugDaG violates Art. 7 and 8 CFR

Under Art. 51 (1) sentence 1 2nd half sentence CFR, Member States are bound to the EU Charter of Fundamental Rights when implementing directives.

ECJ, judgment of 12 December 1996, X, C-74/95, EU:C:1996:491, marginal No. 25 et seq. (on Art. 7 ECHR); judgment of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, marginal No. 68.

Insofar as the FlugDaG implements the PNR guideline one to one, it is subject to Art. 7 and 8 in conjunction with Art. 51 (1) sentence 2 CFR, it is accordingly also invalid (cf. section II. above) and it is not to be applied.

IV. FlugDaG violates the German Constitution insofar as the German legislature makes use of the scope of the PNR Directive

By extending the obligation to transfer data to also include intra-European flights, § 2 (3) FlugDaG makes full use of the scope granted by the PNR Directive, which activates the test standard of the German Constitution (see 1. below). The law fails against this standard because it violates the Plaintiff's fundamental right to informational self-determination (see 2.).

1. Part of the FlugDaG to be measured based on the German Constitution

If a national implementation act implements the requirements of an EU Directive, it must be measured primarily against European law; these requirements are violated by the FlugDaG to the same extent as the PNR Directive (cf. sections II. and III. above).

National constitutional law remains applicable only to the extent that the form of the national transposition law is not prescribed by EU law.

Thus especially regarding the EU Directives, Federal Constitutional Court (BVerfGE) 118, 79 <95> with further references

This is the case for the following regulations of the FlugDaG (hereinafter referred to as the "**challenged FlugDaG regulations**"):

- the extension of PNR data storage and processing to intra-EU flights pursuant to § 2 (3) FlugDaG, which is not mandatory under Art. 2 PNR Directive;
- the possibility of changing the purpose of data use in accordance with § 6 (4) FlugDaG;
- to refer the decision in § 4 (1) No. 5 and 6 FlugDaG to European regulations instead of listing the criminal offences from the German Criminal Code.

The first point in particular opens up a comprehensive obligation to check whether the storage and processing of PNR data of intra-EU flights is compatible with the German Constitution. The associated extension of the objective scope of PNR data storage and processing has the effect of an independent, national PNR legislation, which must prove itself against the standards of the German Constitution.

2. Violation of Article 2 (1) in connection with Article 1 (1) of the German Constitution

The challenged FlugDaG regulations violate the Plaintiff's fundamental right to informational self-determination.

a) Benchmark

Art. 2 (1) in connection with Article 1 (1) of the German Constitution guarantees a fundamental right to informational self-determination. This right guarantees the right of the individual, which follows from the principle of self-determination, to decide for himself in principle when and within what limits personal circumstances in life are revealed.

> Cf. Federal Constitutional Court 65, 1 <43>; 84, 192 <194>; 96, 171 <181>; 103, 21 <32 et seq.>; 113, 29 <46>; 115, 320 <341>.

In particular, it shall protect its institutions against the unlimited collection, storage, use and disclosure of data relating to them which have been individualised or can be individualised.

> Cf. Federal Constitutional Court 65, 1 <43>; 67, 100 <143>; 84, 239 <279>; 103, 21 <33>; 115, 320 <341>.

For those who cannot monitor with sufficient certainty which information concerning them is known in certain areas of their social environment, and who is unable to assess the knowledge of possible communication partners to some extent, can be substantially inhibited in their freedom to plan or decide on their own.

> Cf. Federal Constitutional Court 65, 1 <42 et seq.>; 115, 320 <341 et seq.>.

The monitoring or observing activity of the police can affect the scope of protection of fundamental rights and gain the legal quality of encroachments on fundamental rights.

> Cf. Federal Constitutional Court 110, 33 <56>; 115, 320 <342>.

This applies in particular if personal information is collected and stored for the purpose of electronic data processing. As a result, this data can not only be retrieved at any time and in

a matter of seconds, regardless of distance, it can also be merged with other data collections, especially when integrated information systems are being set up, thus creating a wide range of possible uses and links.

Cf. Federal Constitutional Court 65, 1 <42>; 115, 320 <342>.

However, the basic right to informational self-determination is not guaranteed without limits. On the contrary, the individual must accept such limitations of his right as are justified by overriding general interests.

Cf. Federal Constitutional Court 65, 1 <43 et seq.>; 115, 320 <344 et seq.>.

However, these restrictions require a constitutional legal basis, which must comply in particular with the principle of proportionality and the requirement of the clarity of standards.

Cf. Federal Constitutional Court 65, 1 <43 et seq.>; 115, 320 <345>.

For the legal assessment of the nature of the encroachment made possible by the authorisation, it is important, among other things, how many holders of fundamental rights are exposed to such intensive impairments and under what conditions this happens, in particular whether these persons have given cause for this.

Cf. Federal Constitutional Court 100, 313 <376>; 109, 279 <353>; 115, 320 <347>.

The weight of the individual impairment depends on whether the data subjects remain anonymous as persons, what personality-related information is recorded and what disadvantages the holders of fundamental rights are threatened with as a result of the measures or they fear not without reason.

Cf. Federal Constitutional Court 100, 313 <376>; 109, 279 <353>; 115, 320 <347>.

The Federal Constitutional Court has developed these criteria for the assessment of the intensity of encroachment on information-related encroachments on fundamental rights, particularly in decisions on telecommunications secrecy under Article 10 (1) of the German Constitution and on the fundamental right of the inviolability of the home under Article 13 (1) of the German Constitution. Since these fundamental rights represent special manifestations of the fundamental right to informational self-determination,

Cf. Federal Constitutional Court 51, 97 <105>; 100, 313 <358>; 109, 279 <325 et seq.>,

these standards shall also apply to the more general fundamental right unless they are characterised by the special features applicable to the special guarantees.

Cf. Federal Constitutional Court 115, 320 <347>.

The intensity of information-related encroachments on fundamental rights also depends on what disadvantages those affected are threatened with as a result of the encroachments or are not feared by them without reason.

Cf. Federal Constitutional Court 100, 313 <376>; 115, 320 <351>.

Thus, the transfer and use of data may create a risk for data subjects that they become subject to state investigation measures, which goes beyond the general risk of being exposed to unjustified suspicion.

Cf. Federal Constitutional Court 115, 320 <351>.

Information-related investigation measures can also have a stigmatising effect on those concerned if they become known, thereby indirectly increasing the risk of discrimination in everyday or professional life.

Cf. Federal Constitutional Court 115, 320 <351>.

Encroachments on fundamental rights which are characterised both by a lack of suspicion and by a wide dispersion – i.e. in which numerous persons are included in the scope of action of a measure who have no link to a concrete misconduct and have not initiated the encroachment through their behaviour – generally exhibit a high intensity of encroachment.

Cf. Federal Constitutional Court 100, 313 <376, 392>; 109, 279 <353>; 113, 29 <53>; 113, 348 <383>; 115, 320 <354>.

For the individual's freedom as a fundamental right is affected all the more intensively the less he himself has given cause for state intervention. Such interventions and encroachment may also have intimidating effects which may lead to impairment of the exercising of fundamental rights.

Cf. Federal Constitutional Court 65, 1 <41 et seq.>; 113, 29 <46>; 115, 320 <354>.

A deterrent effect to the exercise of fundamental rights must not only be avoided in order to protect the subjective rights of the individuals concerned. The common good is also affected because self-determination is an elementary functional condition of a free democratic community based on the ability of its citizens to act and participate.

Cf. Federal Constitutional Court 113, 29 <46>; 115, 320 <354 et seq.>.

It endangers the impartiality of behaviour if the dispersion of investigative measures contributes to the risks of abuse and a sense of being monitored.

Cf. Federal Constitutional Court 115, 320 <355>.

The principle of proportionality also means that the legislature may only provide for intensive encroachment on fundamental rights based on certain levels of suspicious or danger.

Cf. Federal Constitutional Court 100, 313 <383 et seq.>; 109, 279 <350 et seqq.>; 115, 320 <361>.

Whether an encroachment on a fundamental right can be proportionate to averting future threats of impairment of a legal interest, even in the run-up to concrete dangers, does not only depend on whether there is a sufficient prospect that the encroachment will be successful,

on the requirement of suitability for success Federal Constitutional Court 42, 212 <220>; 96, 44 <51>; 115, 320 <361>,

but also on the requirements of the mandatory provision with regard to the proximity of the data subjects to the legal interest threat in question.

Cf. Federal Constitutional Court 100, 313 <395>; 110, 33 <60 et seq.>; 113, 348 <385 et seqq., 389>; 115, 320 <361 et seq.>.

If the legislature renounces limiting requirements in relation to the probability of the occurrence of danger and the proximity of those affected to the threat to be averted, and if it nevertheless provides for a power to intervene with substantial severity, this is not sufficient under constitutional law.

Cf. Federal Constitutional Court 115, 320 <362>.

According to these standards, the Federal Constitutional Court determined, for example, with regard to computer-assisted police data mining techniques (dragnet search), that it should not be made possible already in advance of a concrete danger, because it would lead to

encroachments, completely without suspicions, on fundamental rights with a high degree of variability, which would be able to record information with an intensive personal reference.

Cf. Federal Constitutional Court 115, 320 <362>.

b) Violation of fundamental rights through PNR data storage and processing

According to these standards, the challenged FlugDaG regulations violate the basic right to informational self-determination.

aa) Application of the FlugDaG to intra-EU flights

PNR data storage and processing encroaches on the right to informational self-determination, as personal information is collected, stored and processed for the purpose of electronic data processing.

Cf. Federal Constitutional Court 115, 320 <342>; 120, 378 <397 et seq.>; cf. as above section II.2.b) on Art. 7, 8 CFR with the same structure.

Such an encroachment must, in order to be justified, comply with the principle of proportionality, i.e. it must pursue a legitimate aim and be appropriate, necessary and proportionate to that aim.

Like the PNR Directive itself, the FlugDaG pursues legitimate objectives by preventing and prosecuting terrorist offences and serious crime (§ 1 (2) FlugDaG).

However, it is questionable whether the measure is actually appropriate to achieve these objectives, even more so than in the case of the processing of PNR data for flights to and from non-EU countries. This would require evidence that patterns applied to intra-EU flights and comparison with databases can contribute to the prevention and prosecution of these crimes. The legislature does not provide any justification for this.

On this crit. *Arzt,* DÖV 2017, 1013 (1026).

In any case, however, the measure is not necessary to achieve the objective. In this respect, the above comments on the disproportionality of the PNR Directive can be applied to the FlugDaG in the light of Art. 7, 8 CFR: The objective and personal scope of application of the FlugDaG is too broad, because it does not differentiate, for example, according to certain travel routes or suspect status (see II.2.c)bb above); the time limits for storage and processing are also insufficient, because after the successful entry or exit of the data

subjects, the reason for the encroachment on fundamental rights has ceased to exist and the law does not react to this (see II.2.c)cc above)).

In addition, the encroachment on fundamental rights associated with PNR data storage and processing is inappropriate according to the standards of the Federal Constitutional Court's case law.

The FlugDaG serves the protection of high-ranking constitutional assets, namely the protection of legal assets threatened by terror and serious crimes. However, this abstract purpose is not sufficient. Rather, the concrete contribution of the inclusion of intra-EU flights in PNR data storage and processing to the protection of these legal interests must be assessed and weighed against the encroachment on fundamental rights in question. It should be borne in mind that in only 0.1% of cases the legislature expects positive hits from the comparison with databases and patterns (see B.III.2.c above), although it is unclear whether the hit rate for the group of intra-EU flights is different to this. Regardless of this, positive hits do not yet mean that the new suspicions are well-founded (or that arrests of suspects are justified); rather, a "certain" to "substantial" error rate (see II.2.c)bb above) should be subtracted out. Even after deducting this quota, only a new suspicion has been gained in the area of hazard prevention, and this can vanish once again. Finally, it is unclear in how many cases a suspicion is actually established that a crime is prevented, even if the suspicion is confirmed.

> Cf. also the explanations of the Federal Constitutional Court on the unsuccessfulness of the dragnet search for so-called terrorist sleepers, for which data records of 5.2 million people were processed, which led to a sleeper file with 32,000 people, the searching of which in itself did not lead to any concrete suspicion of encroachment, Federal Constitutional Court 115, 320 <356>.

On the other hand, there is the continuous, governmental, protracted, mass and above all inconsequential storage and processing of PNR data of individuals. The associated encroachments are of substantial importance, as can be seen in particular from the case law of the Federal Constitutional Court on the dragnet search and the retention of telecommunications data.

> Regarding the significance of the Federal Constitutional Court case law on the dragnet search for the assessment of the FlugDaG, see also *Arzt*, DÖV 2017, 1023 et seqq.

The FlugDaG does, however, define the data affected by storage and processing (cf. § 2 (2) FlugDaG), in contrast to the regulation of the North Rhine-Westphalian police law on the

dragnet search, which was at issue at the time. But PNR data in itself contains a lot of important information, such as name, address, nationality, date of birth, telephone number, email address and payment information, as well as details of escorts, baggage and frequent flyer record (much more on this below). It is also unclear which further "general information" the airlines will provide through the free text field (§ 2 (2) No. 16 FlugDaG). There are also no exceptions for people carrying professional secrets.

It is also problematic that PNR data – unlike telecommunications data retention – is immediately consolidated centrally by the state, without any reason.

> For the Federal Constitutional Court, decentralised storage by private individuals was an essential criterion for the constitutionality of the retention of telecommunications data, Federal Constitutional Court 125, 260 <321 et seq.>.

All this data is now to be compared with other databases and "patterns", from which – as in the case of the dragnet search,

> Cf. BVerfGE 115, 320 <349> –

new and diverse information can be gleaned. This in itself is a profound encroachment on the fundamental right to informational self-determination.

The intensity of this encroachment is further affected by any consequences for the data subjects resulting from the comparison:

- The reconciliation creates an increased risk for the data subjects of becoming the target of further official investigation measures and of coming under pressure to explain.

  > On this aspect in connection with the retention of telecommunications data BVerfGE 125, 260 <320>.

  Follow-up measures can also have a stigmatising effect, for example in the case of refusal of entry at passport control at the airport.
- Those affected by positive hits are not notified – not even after the investigations following a hit have been completed (cf. on the inapplicability of § 56 BDSG above III.).
- The data remains stored for five years without exception even after the comparison on entry or exit – i.e. even if no suspicion has arisen – and is kept ready for further comparisons (after six months, however, only subject to further conditions). This time

limit by far exceeds the six months that the Federal Constitutional Court saw "at the upper limit of what is justifiable under considerations of proportionality” in connection with the retention of telecommunications data.

BVerfGE 125, 260 <322>.

In contrast to the retention of telecommunications data, the data subject cannot "rely on the fact that his data will be deleted [after the deadline] and can no longer be reconstructed by anyone",

BVerfGE 125, 260 <322>,

because there are many possibilities of transfer, i.e. the data could already have become independent (cf. section B.III.3 above).

- Finally, it should also be borne in mind that the theft of the data collected can never be ruled out with certainty, which can have far-reaching consequences for data subjects, particularly in the event of misuse of payment information.

In addition, there is the already mentioned wide dispersion of the measure, as it covers all passengers arriving or departing, including systematically non-suspected persons, and the comparison is not made in the context of specific threats but on an ongoing basis.

> Cf. regarding automated license plate recognition BVerfGE 120, 378 <430>: “Automated license plate recognition, which affects everyone indiscriminately only because a vehicle passes through a place set up without any special reason or even permanently for automated registration of vehicle license plates, also conveys the impression of constant control. The emerging feeling of being watched can [...] lead to intimidation and consequently to encroachment in the exercise of fundamental rights."

However, if the legislature renounces limiting requirements in relation to the probability of the occurrence of danger and the proximity of those affected to the threat to be averted, and if it nevertheless provides for a power to intervene with substantial severity, this is not sufficient under constitutional law.

> Cf. Federal Constitutional Court 115, 320 <362>.

Such intensive encroachments on fundamental rights as here are only appropriate in the case of a concrete danger.

> Cf. accordingly on the dragnet search in detail BVerfGE 115, 320 <357 et seqq.>; similarly also (data retention) BVerfGE 125, 260 <330>: "The legal

basis for authorisation must at least require actual indications of a concrete danger to the legal interests to be protected. This requirement leads to the fact that assumptions or general principles of experience are not sufficient to justify access to the data."

Although a permanent threat may also be considered, a general threat situation, which allegedly existed practically uninterruptedly after 11 September 2001 at the latest, is not sufficient for this. The encroachment on the right to informational self-determination brought about by PNR data storage and processing presupposes the existence of further facts, from which a concrete danger arises, for example because there are actual indications for the preparation of terrorist attacks or that persons in Germany are prepared for terrorist attacks which are to be carried out in Germany itself or elsewhere in the foreseeable future.

Also regarding the dragnet search, BVerfGE 115, 320 <364 et seq.>.

bb) Possibility of changing the purpose of PNR data and processing results

§ 6 FlugDaG regulates the transfer of data resulting from a comparison pursuant to § 4 (2) or (5) FlugDaG, as well as the results of the processing of this data, to various domestic authorities. According to § 6 (3) FlugDaG, these authorities may only process the transferred data for the purposes of § 4 (1) FlugDaG. § 6 (4) FlugDaG restricts this purpose limitation in favour of criminal prosecution if findings "give rise to suspicion of a particular other criminal offence".

This possibility of a change of purpose violates the right of the data subjects to informational self-determination.

According to the case law of the Federal Constitutional Court, changes in purpose must be measured against the fundamental rights that were decisive for data collection. This applies to any use of data for a purpose other than that for which they were collected, whether as evidence or as an investigative approach.

Cf. Federal Constitutional Court 109, 279 <377>; 141, 220 <327>.

The legislature may indeed permit further use of the data for purposes other than those for which the data was originally collected. However, it must then ensure that the severity of the encroachment from the data collection is also taken into account with regard to the new use.

Cf. BVerfGE 100, 313 <389 et seq.>; 109, 279 <375 et seq.>; 120, 378 <408>; 130, 1 <33 et seq.>; 133, 277 <372 et seq.>; 141, 220 <326 et seq.>.

A prerequisite for a change of purpose is that the new use of the data serves to protect legal interests or to uncover crimes of such severity that could constitutionally justify their new collection by comparably serious means.

> Cf. BVerfGE 100, 313 <360 et seqq.>; 109, 279 <377>; 110, 33 <73>; 120, 378 <408>; 130, 1 <34>; 141, 220 <328>.

This is not guaranteed under the current system, as this speaks only of the use of data to pursue suspicions of a "particular other offence". This formulation does not satisfy the requirements of the Federal Constitutional Court because the comparable severity of the criminal offences is not guaranteed.

> So also *Wollenschläger*, statement on the draft of the FlugDaG of 24 April 2017, p. 53 et seq.

cc) Catalogue of offences does not comply with constitutional requirements

§ 4 (1) No. 1 to 4 FlugDaG refer to specific criminal offences, while § 4 (1) No. 5 and 6 FlugDaG refer to EU norms which only list certain criminal offences – but not German criminal offences. In addition, Annex II of the PNR Directive referred to contains a number of offences which are less serious than the other offences and are often committed in less serious forms, such as corruption (No. 6), fraud (No. 7), money laundering. (No. 8 variation 1), computer offences (No. 9), facilitation of illegal entry and residence (No. 11), trafficking in cultural goods (No. 16) or fraudulent counterfeiting and piracy (No. 17).

This also violates the fundamental right of the data subjects to informational self-determination.

§ 4 (1) No. 5 and 6 FlugDaG are initially not sufficiently defined. According to the case law of the Federal Constitutional Court, the more serious the encroachment based on the storage is, the more restrictive the requirements for the use of data and their scope in the relevant legal bases must be. The reason, purpose and extent of the respective encroachment as well as the corresponding encroachment thresholds must be regulated by the legislature in an area-specific, precise and clear manner.

> Cf. BVerfGE 100, 313 <359 et seq.>; 110, 33 <53>; 113, 29 <51>; 113, 348 <375>; 115, 320 <365>; 118, 168 <186 et seq.>; 125, 260 <328>.

As regards criminal prosecution, it follows from this that a search of the data presupposes at least the suspicion of a serious criminal offence based on certain facts. Which criminal offences are to be covered by this, the legislature has to determine conclusively with the

obligation of the data storage. It has a margin of judgment in this respect. It can either use existing catalogues or create its own, for example to record crimes for which telecommunications traffic data is of particular importance. The qualification of an offence as serious must, however, be expressed objectively in the criminal provision, particularly in terms of its scope. However, a general clause or simply a reference to offences of major importance is not sufficient.

Cf. BVerfGE 125, 260 <328 et seq.>.

According to these standards, a mere reference to an EU catalogue of criminal offences is not sufficient, as it is not clear to the security authorities which German criminal offences correspond to the criminal offences listed in Annex II of the PNR Directive and open up the scope of application of the FlugDaG. Consequently, the legislature would have had to "translate" the offences referred to therein and listed them in § 4 (1).

Thus probably also *Arzt*, DÖV 2017, 1023 (1025).

However, there is also no guarantee that the comparison under § 4 (2) and (5) FlugDaG will be made with regard to sufficiently serious criminal offences. The Federal Constitutional Court requires the legislature to ensure, beyond the abstract definition of a corresponding catalogue of criminal offences, that recourse to data stored as a precaution is only permissible if the criminal offence being prosecuted weighs heavily in the individual case and the use of the data is proportionate.

Cf. Federal Constitutional Court 125, 260 <329>.

In particular, this is not guaranteed for the criminal offences listed at the beginning of this section, which also know less serious forms of offence. In this respect, there is no materiality threshold in individual cases, in particular for data transfer to other authorities (§§ 6 et seqq. FlugDaG).

It cannot be argued against all this that, as far as intra-European flights are concerned, the punishable acts listed in Annex II of the PNR Directive are prescribed by European law. The German legislature could and should have drawn up its own list of offences with regard to intra-European flights.

3. Legal consequence: Application for judicial review pursuant to Article 100 (1) of the German Constitution

In the event that the court considers the PNR Directive to be compatible with Articles 7 and 8 CFR or the ECJ should determine the invalidity of the PNR Directive by way of prior review, we propose, on behalf of the Plaintiff, a referral to the Federal Constitutional Court pursuant to Article 100 (1) sentence 1 of the German Constitution.

V. Application for a temporary injunction

The application for a temporary injunction pursuant to § 123 (1) VwGO is admissible. In particular, despite the preventive legal protection asserted here, there is a sufficient interest in legal protection. Against the background of the constitutional principle of the separation of powers and the principle of effective legal protection in Article 19 (4) of the German Constitution, which was conceived in a reactive way from the outset, administrative judicial legal protection is fundamentally not designed as a preventive measure. A deviation from this basic decision can only be considered in exceptional cases if the subsequent legal protection would be associated with unreasonable disadvantages for the data subject, in particular if without the recourse to preventive legal protection there would be a danger that accomplished actions which can no longer be reversed would be created or if irreparable damage would result.

> Cf. Higher Administrative Court (OVG) Münster, decision of 22 June 2017 - 13 B 238/17 -, marginal No. 27 with further references; OVG Münster, decision of 1 August 2013 – 4 B 608/13 (= NVwZ 2014, 92); Higher Administrative Court (VGH) Kassel, decision of 14 July 1988 – 11 TG 1736/85 (= NJW 1989, 470, 472); *Schoch*, in: Schoch/Schneider/Bier, VwGO, as at: March 2014, § 123 marginal No. 46.

That is the case here. PNR data storage and processing will take place at least 24 hours before departure. There is also a possibility that this information will be forwarded to other authorities, including foreign authorities. *a posteriori* legal protection could no longer eliminate the effect of these encroachments.

The application for a temporary injunction is also well-founded. Please refer to the above for a description of the application for a judicial order: The storage and processing of the Plaintiff's PNR data would be unlawful because the PNR Directive on which the FlugDaG is based is invalid because it violates Articles 7 and 8 CFR and thus the PNR data storage and processing itself violates the CFR (see sections C.II and C.III above); insofar as the Federal legislature exhausts the scope of the PNR Directive (PNR data storage and processing also

for intra-European flights) or the entire Flight Data Act is to be measured against the German Constitution because the PNR Directive is invalid, the PNR data storage and processing also violates Art. 2 (1) in conjunction with Art. 1 (1) of the German Constitution (cf. C.IV above).

The reason for the order results from the fact that the Plaintiff's reference to the final conclusion of the main proceedings would in any event irreversibly frustrate his rights to be secured in view of the forthcoming flight.

VI. Summary

The following can therefore be summarised:

1. The action is admissible and well founded.

2. The application for a temporary injunction is also admissible and well-founded.

The Plaintiff has a claim under public law to an injunction against the storage, processing and transfer of PNR data to be pursued by way of a general action for performance (preventive action for injunction).

It follows from all this that the proceedings should be stayed and the question of the validity of the PNR Directive should be referred to the ECJ for a preliminary ruling.

We ask for an immediate decision on the request for a judicial order.

We politely request that the case be heard before the court in the near future.

Two certified copies attached.

Prof. Dr. Remo Klinger
(Attorney-at-law)

List of appendices

Appendix 1: Flight booking

Appendix 2: Letter of formal notice to the Defendant

Appendix 3: Response of the Defendant