.SIAK REPUBLIC OF AUSTRIA
FEDERAL MINISTRY OF THE INTERIOR
SICHERHEITSAKADEMIE

.SIAK-Journal – Journal for Police Science and Practice

Kainz, Viola/Prunner, Marina

Passenger Name Records Data in the Fight Against Serious Crime. The path from the Passenger Name Records Directive to national law

SIAK-Journal − Journal for Police Science and Practice (International Edition/2019), 4-12.

doi: 10.7396/IE_2019_A

Please cite this articel as follows:

Kainz, Viola/Prunner, Marina (2019). Passenger Name Records Data in the Fight Against Serious Crime. The path from the Passenger Name Records Directive to national law, SIAK-Journal − Journal for Police Science and Practice (International Edition Vol. 9), 4-12, Online: http://dx.doi.org/10.7396/IE_2019_A.

published online: 8/2019

Passenger Name Records Data in the Fight Against Serious Crime

The path from the Passenger Name Records Directive to national law

VIOLA KAINZ,
Legal Expert in Department III/1 (Legal Affairs) at the Austrian Federal Ministry of the Interior.

MARINA PRUNNER,
Legal Expert in Department III/1 (Legal Affairs) at the Austrian Federal Ministry of the Interior.

In a modern, highly interconnected world, the activities of organised or terrorist crime do not stop at national borders. In response to the lifting of internal border controls by the Schengen Agreement and fuelled by recent terrorist attacks in Europe, the European Union has established rules for the international exchange of personal Passenger Name Records (PNR) data between law enforcement agencies. The PNR Directive will complement existing tools to prevent, detect, investigate and prosecute terrorist offences and serious crime through the use of PNR data. The processing of PNR data and related specific data analysis has created the ability to not only identify people already in the crosshairs of the law enforcement agencies, but also to find new investigative approaches to identify those individuals who were previously unknown to law enforcement agencies, but could be linked to a terrorist offence or an offence of similar gravity. The PNR Directive was implemented throughout Austria by the Federal Law on the Processing of Passenger Name Records for the Prevention, Hindrance and Resolution of Terrorist and Certain Other Offences (PNR Law). This article aims to give the reader an insight into the background of the processing of PNR data (1) and the European PNR system (2) as well as a comprehensive overview of the essential content of the new PNR Law (3).

1. BACKGROUND

On 17 August 2018, following extensive parliamentary and public discussions, the Federal Law on the Processing of Passenger Name Records for the Prevention, Hindrance and Resolution of Terrorist and Other Serious Crime (PNR Law[1]), Federal Law Gazette I No. 64/2018 entered into force.[2] Thus, the EU Directive 2016/681 on the Use of Passenger Name Records (PNR data) for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime[3] (hereinafter the PNR Directive) was implemented nationwide. A system of national and international processing of passenger data has now been created in the fight against serious crime. It has a long and turbulent history.

1.1 International developments

Since the end of the 20th century, passenger name records have been increasingly used for state purposes. Passenger name records (PNR data) are passenger data collected by airlines for business purposes. Although the data vary, they are always a combination of information such as name, contact details, address, payment and billing information, credit card numbers, booking and flight dates, itinerary, baggage and seat information or any other information – thus,

information that may be of great interest in the prevention and investigation of crime.[4]

Following the terrorist attacks of 11 September 2001, the "Aviation and Transportation Security Act"[5] in the United States required all airlines to provide the authorities with access to their passenger data on all flights into, out of, or across US territory.[6] The EU has also been endeavouring to adopt PNR agreements with third countries and to create an EU-wide PNR system.

1.2 The EU PNR Agreement

In particular, on the occasion of the US data processing legislation, which also obliged European airlines to submit data to the US authorities, efforts were made by the European Commission (EC) to simplify the transfer of PNR data. As a result, temporary PNR agreements were concluded not only with the USA[7], but also with Canada[8] and Australia[9]. Following the entry into force of the Treaty of Lisbon on 1 December 2009, the European Parliament (EP) renegotiated the PNR agreements in order to adapt them, in particular, to European data protection and privacy standards. While the agreements with the US and Australia could be re-concluded with only a few data protection improvements, the revocation of the Data Retention Directive[10] by the European Court of Justice (ECJ)[11] prompted the EP to appeal to the ECJ regarding the compatibility with EU treaties of the proposed new agreement with Canada. In its Expert Opinion[12], the ECJ stated that the agreement could not be concluded in the form proposed as several of its provisions were incompatible with the fundamental rights recognised by the EU. The proposed agreement would interfere with fundamental rights to privacy and the protection of personal data, which are indeed justified by the objective of common good (ensuring public safety in the fight against terrorist offences and cross-border serious crime) and are suitable for attaining that objective. However, several provisions of the agreement are not limited to what is strictly necessary and there are no clear, precise rules for the application of the measures provided for therein – a reproach that should also be considered in the legislative process of the Austrian PNR law.

1.3 A PNR system for Europe

There were also efforts within the EU to establish a European PNR system. While the EC's initial proposals in 2013 were still rejected by the EP due to grave concerns about respect for fundamental rights and data protection, the issue returned to the European agenda after the attacks in Paris and Brussels. A clear majority of the EP now spoke in favour of the adoption of a PNR directive and thus the EU-wide processing of PNR data. The PNR Directive was published in the Official Journal of the European Union on 25 May 2016; Member States had two years to translate them into national law.

2. IMPLEMENTATION OF THE PNR DIRECTIVE IN AUSTRIA

The aim of the PNR Directive is to combat terrorism and serious crime using PNR data, which is why its implementation fell within the remit of the Austrian Federal Ministry of the Interior (hereinafter BMI). With the establishment of the Passenger Information Unit (PIU), the central hub for the processing of passenger data provided for by the PNR Directive, the Federal Criminal Police was commissioned as an organisational unit of the BMI. The legal, practical and organisational measures to ensure swift national implementation and effective use of the new PNR system were developed in close cooperation with the Legal Affairs Department of the BMI

as well as the specialist departments of other affected Austrian federal ministries – the Federal Ministry for Constitution, Reforms, Deregulation and Justice (BMVRDJ)[13], the Federal Ministry of Finance (BMF)[14] and the Federal Ministry of Food and Agriculture (BMLV)[15]. The draft PNR law was sent out for public review on 25 January 2018[16]; the review period ended on 22 February 2018.

Suggestions and criticisms were expressed as part of the review process; these were examined and, if necessary, were included in further adaptation. In particular, it was argued that the PNR Law should be adopted despite the rejection by the ECJ of the proposed EU PNR agreement with Canada.[17] However, especially with regard to this review, special attention was paid to compliance with the provisions of the ECJ during the drafting of the PNR Law, so that the data protection officers and the judicial authorities could be provided with a proportionate and balanced regulation for the implementation of the PNR Directive based on the narrow purpose limitation of the processing of PNR data, the special nature of the processing period with its (data protection) safeguards, the limited number of authorised processing authorities and the strict scrutiny by the responsible legal protection officers. Further criticisms from the review process will be discussed in the relevant section.

The PNR Law, revised on the basis of the results of the review, was laid before the National Council on 13 June 2018 as a government bill[18] and was approved by Parliament in July 2018.[19] The Federal Law on the Processing of Passenger Name Records for the Prevention, Hindrance and Resolution of Terrorist and Other Serious Crime (PNR Law) entered into force on 17 August 2018, Federal Law Gazette I No. 64/2018.

3. THE PNR LAW IN DETAIL

The details of the PNR Law will be examined in the following.

3.1 Passenger Information Unit

The PNR Law created a system for processing PNR data and established the Austrian PIU at the BMI (Section 1(2)). This collects, stores and processes the PNR data transmitted by the airlines, forwards them or the results of the data processing to the competent authorities and is, in principle, responsible for the exchange of information with the PIUs of other EU Member States and with Europol (Sections 2, 4 and 7).[20] This function is performed by the Federal Criminal Police Office as an organisational unit of the Austrian Federal Minister of the Interior.

3.1.1 PNR data

The individual PNR data to be provided by the airlines are listed exhaustively in Section 3 and correspond to Annex I of the PNR Directive.[21] However, only PNR data that the airlines have collected for business purposes during the booking process are to be transmitted.[22] Consequently, airlines are not required to collect more passenger information than they have already collected through their PNR data. The concerns about this expressed in the review process[23] are therefore unfounded. Since the PNR data to be transmitted are listed in the law, those data transmitted by the airlines which are not PNR data as laid out in Section 3 should be deleted immediately after being noticed. Likewise, the processing of special categories of personal data pursuant to Section 39 of the Data Protection Act (DSG), Federal Law Gazette I No. 165/1999 as amended by Federal Law Gazette I No. 120/2017 (previously "sensitive data") is not permitted; data containing such information must be deleted immediately after being noticed

in the event of their transmission (Section 3(2)).

3.1.2 Scope of application

The PNR Law and thus the obligatory transmission of PNR data by the airlines to the Austrian PIU applies only to flights with reference to a third country (Section 2(1)). This includes every scheduled or non-scheduled flight by an airline which is taking off from a third country and has the territory of Austria as its destination or is taking off in Austria and has a third country as its destination, including flights with a stopover in a Member State or third country.[24] The draft review also provided for the application to both flights from and to third countries and intra-European flights (i.e. from one Member State to Austria or from Austria to another Member State). With the now standardised restriction to flights from and to third countries, the criticism of the "gold plating" expressed in the review – that the PNR Law went further than the PNR Directive, since the PNR Directive only requires the processing of passenger data for flights from or to third countries whereas the processing of passenger data on intra-European flights is exempted for Member States[25] – was acted on and the scope of the PNR Law was restricted to flights from or to third countries.

However, due to the current high level of abstract risk in Europe and especially regarding Austria's EU Council Presidency in the second half of 2018, the Federal Minster of the Interior provided for an authorisation to extend the scope of application also to international intra-European flights from and to Austria (Section 2(5)). Coinciding with the entry into force of the PNR Law, a six-month PNR regulation, Federal Law Gazette II No. 208/2018, was issued for the period of the Austrian Presidency in order to provide as much protection as possible during this politically sensitive period.[26]

3.1.3 Data transmission by airlines

Pursuant to Section 2(1), airlines are required to transmit PNR data to the PIU at specific times.[27] The PNR data must be sent to the PIU within a period of 24 to 48 hours prior to the scheduled departure time and immediately after completion of the passenger-related formalities (completion of boarding). This enables the timely examination of the respective data records and the possible timely preparation and taking of necessary (police) measures as well as the information as to whether a specific person is or was on a flight. However, regardless of the times mentioned above, airlines are also obliged to provide prompt and free information on passenger data, if necessary, to avert a specific, current danger as laid down in the PNR Law (Section 2(4)). Due to the purpose limitation of preventing or hindering the criminal offences covered by the PNR Law, only the security authorities, customs authorities and bodies and authorities of the military intelligence services entrusted with defence or military law enforcement are entitled to make such a request. Both the request to the airline and the transmission of the data are made via the PIU.[28]

In order to ensure sufficient protection of the data during electronic transmission, airlines are obliged to transmit the data in the agreed manner only (Section 2(1)). The possible technical formats were determined by the EC.[29] Only in the event of technical disruptions and in exceptional circumstances can transmissions also take place in other appropriate ways, which must in any case ensure an adequate level of data protection as laid down in Section 54(2) of the Austrian Data Protection Act (Section 2(2)).

3.2 Processing of the PNR data

3.2.1 Strict purpose limitation

The use of passenger data as laid down in Article 1(2) of the PNR Directive is limited to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. The processing of PNR data is exclusively permissible for the prevention, hindrance and investigation of terrorist acts for which legal punishment is prescribed[30] as well as of such actions for which legal punishment is prescribed which belong to one of the categories listed in the annex to the PNR Law and are punishable with imprisonment, the upper limit of which is at least three years (Section 1(1))[31] – PNR data are not used for low-threshold offences. Despite the corresponding proposal in the review process[32], adapting the list of offences in the annex to the PNR Law to Austrian terminology was ruled out in order to ensure full implementation of the PNR Directive – an approach that also applies to the catalogue of offences for the Federal Law on Judicial Cooperation in Criminal Matters with the Member States of the European Union – EU-JZG[33], Federal Law Gazette I No. 36/2004.

3.2.2 Comparison of PNR data

After the PNR data are transmitted, they are processed in a separate PNR database and automatically compared with the search and security police data processing, which aids the prevention or prosecution of judicial offences in accordance with Section 1(1) and on the basis of certain criteria (Section 4(1)).[34] While comparison with existing search evidence enables the identification of persons and documents or means of payment already known to the authorities, the purpose of comparison with the abovementioned criteria is to identify persons who are not yet known to the security or law enforcement authorities and who could be connected to a criminal offence as laid down in the PNR Law.[35]

These criteria are composed of inspection properties which arouse and relieve suspicion and are created by the PIU based on the expertise of the competent authorities and their criminal experience (Section 5). In order not to run counter to the purpose of the PNR Directive, these criteria are not – as repeatedly suggested in the review process[36] – laid down by regulation. If these criteria were promulgated by regulation, they would be obsolete immediately after the adoption of such a regulation, since offenders could adapt their approach to the established criteria. Such a regulation would almost represent a guide on how to evade discovery. Likewise, there would no longer be the necessary flexibility regarding the rapid adaptation of the criteria needed to keep pace with developments on the side of offenders. The parameters were specified in greater detail in the law in order to take account of the concerns raised (Section 5(2)).

3.2.3 Verification of hits

If the automated comparison results in a hit, an individual check by a PIU employee is always carried out in order to take further measures only after verification that it is indeed a person associated with serious crime as laid down in the PNR Directive. This ensures that only those data records that have been individually checked by a person are forwarded, if necessary, to the competent authorities.[37] The processing of PNR data can thus never automatically lead to a stigmatisation of persons who appear as hits as a result of the processing mechanism. Contrary to the contentions in the review procedure[38], to protect those concerned, no hits are thus forwarded which were generated solely on the basis of the automated comparison.

3.3 Data protection

The processing of PNR data is subject to special data protection in accordance with the requirements of the PNR Directive.[39] Special legal provisions have also been made to comply with these requirements in view of the ECJ's expert opinion on the proposed agreement between Canada and the European Union on the transmission of PNR data. Thus, the PNR Law provides for a narrow purpose limitation so that PNR data may only be processed for the purposes defined in the PNR Directive and the PNR Law (prevention, hindrance and investigation of terrorist and certain other serious criminal offences (Section 1(1) and Section 4). Processing for other purposes is prohibited.[40] Furthermore, the transmission of this data is only permitted to those authorities which are responsible for the prevention, hindrance and investigation of terrorist and certain other criminal offences under the PNR Law (Section 7).[41]

3.3.1 Depersonalisation

The PNR data are to be depersonalised six months after being transmitted by the airlines (Section 6).[42] Depersonalisation is the process of rendering unrecognisable all data with which a person can be unequivocally identified. The cancellation of such depersonalisation is only permitted for the reasons explicitly stated in Section 6(2):[43] however, on the basis of a reasonable request from a competent authority, the depersonalisation will be cancelled only after authorisation by the respective legal protection officer or by order of the public prosecutor on the basis of a judicial approval or by court order pursuant to the provisions of the Criminal Procedure Code, Federal Law Gazette No. 631/1975.[44]

3.3.2 Control by the data protection officer

In addition, the data protection authority is an independent data protection officer who is responsible for checking the legality of all processing operations in the databases and who must be informed of any (non-judicially approved)[45] cancellation of depersonalisation (Section 8).[46]

3.3.3 Storage period

The PNR data in the PNR data processing systems shall be deleted five years after the date of transmission by the airlines (Section 4(5)). If the PNR data have already resulted in a verified hit (see 3.2.3) and if the data have been or will be used in a legal proceeding, the storage or deletion obligations are based on the legal provisions applicable to this proceeding.[47]

3.3.4 Right to information

All air passengers, of course, have a right to information (Section 9). They must cooperate to the appropriate extent (for example, by providing proof of identity or details of their flights) in an information procedure in order to avoid any unjustified or disproportionate effort on the part of the PIU. However, for data protection reasons, there is no right of information to data that have already been depersonalised (see 3.3.1 above), as the removal of depersonalisation would disproportionately affect the data protection interests of other potentially concerned persons. Moreover, the removal is only admissible for the reasons laid out in the exhaustive list in Article 12(3) of the PNR Directive – which does not include the right to information.[48]

3.4 International data exchange

An essential aspect of the PNR system is the exchange of information between Member States and with Europol, which should be carried out through existing, secure technical channels.[49] This exchange of information should, in principle, be carried out by

the PIUs of the various Member States. Only in the event of imminent danger – if a specific and present threat connected to terrorist offences or serious crime has to be averted – is the direct contact of another Member State with the Austrian PIU and the corresponding information or data transfer provided for (Section 7(1) last sentence).[50] A list published in the Official Journal of the EU states which national authorities of other Member States are to be regarded as "competent authorities" and are therefore eligible to apply[51]. The transmission of passenger data to third countries is governed by the provisions of Section 8 ff of the Police Cooperation Act, Federal Law Gazette No. 104/1997.

3.5 Effective enforcement

The PNR Directive stipulates that Member States must provide for effective, proportionate and deterrent sanctions, including fines, to ensure the required effectiveness.[52] According to Section 112(1) of the Alien's Police Act 2005, Federal Law Gazette I No. 100/2005, and in concretisation of Article 14 of the PNR Directive, an airline commits an administrative offence if it fails to provide PNR data in the prescribed manner (e.g. if the data is not transmitted in the appropriate protocols and data formats to the PIU), in full or on time (Section 10); a fine of 5,000 to 15,000 EUR is prescribed, in the event of recurrence of up to 30,000 EUR.[53] However, according to the Administrative Penal Act 1991, Federal Law Gazette No. 52/1991, only behaviour for which it is also responsible is relevant. Therefore, it is only responsible for technical defects if measures are not taken immediately to rectify the fault. The competent authorities for conducting the administrative penalty procedures are the State Police Directorates.

4. CONCLUSION

The PNR Law will complement existing tools with more meaningful investigative measures in order to combat cross-border terrorism and certain other forms of crime more effectively. Thus, it will now be easier to identify previously unknown potential threats, accomplices and informants. The competent authorities are given professional opportunities to identify terrorist threats and activities as well as threats by organised crime in advance and to take appropriate measures. In times of global networking, in order to deal with cross-border crime, it is particularly relevant that close cooperation and rapid exchange of information across national borders are guaranteed in order to keep abreast of current developments on the offenders' side. At the same time, such necessary measures must be implemented with the utmost care and diligence to protect the individual. In order to take this protection into account, the PNR Law provides for a large number of important special data protection regulations.

[1] *Paragraphs without further designation refer to the PNR Law.*

[2] *Federal Law Gazette I No. 64/2018, promulgated on 16 August 2018.*

[3] *OJ L 119, 04/05/2016, 132 ff.*

[4] *Haller (2016) 86 f.*

[5] *Public Law 107–71, 19 November 2001, 115 STAT. 597, Online: https://www.gpo.gov/fdsys/pkg/PLAW-107publ71/pdf/PLAW-107publ71.pdf (28/08/2018).*

[6] *This example was followed by several countries, such as Canada, Australia, New Zealand and the United Kingdom; mwN Haller (2016) 87.*

[7] *Council Decision 2006/729/ CFSP/JHA of 05/10/2006, OJ L 298 of 27/10/2006, 27 ff, and Council Decision 2007/551/ CFSP/JHA of 23/07/2007, OJ L 204 of 04/08/2007, 16 ff.*

[8] *Council Decision 2006/230/EC of 18/07/2005, OJ L 82 of 21/03/2006, 14 ff.*

[9] *Council Decision 2008/651/CFSP/ JHA of 30/06/2008, OJ L 213 of 08/08/2008, 47 ff.*

[10] *Directive 2006/24/EC of the European Parliament and of the Council on the retention of data relating to the provision or processing of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC, OJ L 105 of 13/04/2006, 54 ff.*

[11] *ECJ, Joined Cases 293/12 and C 594/12, Digital Rights Ireland and others, ECLI:EU: C:2014:238.*

[12] *ECJ 26/07/2017, Opinion 1/15, online: http://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&doclang=DE (28/08/2018).*

[13] *Austrian Federal Ministry of Constitutional Affairs, Reforms, Deregulation and Justice.*

[14] *Austrian Federal Ministry of Finance.*

[15] *Austrian Federal Ministry of Defence.*

[16] *4/ME XXVI. GP.*

[17] *Austrian Chamber of Labour (BAK), 6/SN-4/MEXXVI. GP; epicenter.works, 10/SN-4/ ME XXVI. GP.*

[18] *186 BlgNR XXVI. GP.*

[19] *Decision in the National Council on 5 July 2018, in the Federal Council on 12 July 2018.*

[20] *Article 4(2) of the PNR Directive.*

[21] *PNR data according to the PNR Law are 1. PNR data booking code details, 2. date of booking and ticket issuance, 3. scheduled departure date or scheduled departure dates, 4. passenger's surname, name at birth and first name, 5. passenger's address and contact details, including telephone number and email address, 6. all types of payment information, including billing address, 7. entire itinerary for specific PNR data, 8. frequent flyer entry details, 9. details of the travel agency and clerk, 10. travel status of the passenger with details of travel confirmations, check-in status, flights not taken and passengers with a ticket but without reservation, 11. details of split and shared PNR data, 12. general information, including all available information on unaccompanied minors, such as the name, gender, age and languages of the minor, name and contact details of the escort on departure and the relationship of that person to the minor, name and contact details of the person collecting them and the relationship of that person to the minor, accompanying airport staff on departure and arrival, 13. ticketing field information, including ticket number, date of ticket issuance, one-way tickets, Automated Ticket Fare Quote fields, 14. seat number and other seating information, 15. code sharing details, 16. complete luggage details, 17. number and name of fellow passengers in the PNR data, 18. any extended passenger data (API data) collected, including type, number, country of issue and expiration date of identity documents, nationality, surname, departure and arrival dates, departure and arrival airports, departure and arrival times and 19. all previous changes to the PNR data listed under points 1 to 18.*

[22] *See EBRV 186 BlgNR XXVI. GP 2, 3; also Recital 8 of the PNR Directive.*

[23] *Austrian Airlines, 4/SN-4/ME XXVI. GP; Industrial Association, 8/SN-4/ME XXVI. GP; Austrian Economic Chambers, 19/SN-4/ME XXVI. GP.*

[24] *See EBRV 186 BlgNR XXVI. GP 2.*

[25] *Data Protection Authority, 7/SN-4/ME XXVI. GP; The Austrian Bar Association, 20/SN-4/ME XXVI. GP; Austrian Chamber of Labour (BAK), 6/SN-4/ME XXVI. GP; epicenter.works, 10/SN-4/ME XXVI.GP.*

[26] *See also the presentation of the Council of Ministers 21/20 of 13 June 2018.*

[27] *When two or more airlines share a flight in a cooperation relationship (so-called "code sharing"), the airline operating the flight is obliged to transmit the PNR data to the PIU.*

[28] *As laid down in Article 9(1) of the PNR Directive, the PIU basically undertakes any communication between the airlines and the national and international authorities within the scope of the PNR Law.*

[29] *Implementation Decision (EU) 2017/759 on the common protocols and data formats to be used by airlines for the transmission of PNR data to the PIUs, OJ L 113, 29/04/2017, 48.*

[30] *These are terrorist acts for which legal punishment pursuant to Section 165(3) second case, Sections 278b to 278f and Section 282a of the Criminal Code, Federal Law Gazette No. 60/1974.*

[31] *Pursuant to Article 3(8) of the PNR Directive, terrorist offences are punishable by national law under Articles 1 to 4 of the Framework Decision on combatting terrorism, while under Article 3(9) of the PNR Directive, those offences*

stipulated in Annex II to the PNR directive are covered by the term of serious crime, which are punishable under national law by imprisonment of at least three years.

32 *Federal Ministry of Finance, 15/SN-4/ME XXVI. GP; Data Protection Authority, 7/SN-4/ME XXVI.GP.*

33 *See Annex I of the EU-JZG, Federal Law Gazette I No. 36/2004.*

34 *See Article 6(2) of the PNR Directive.*

35 *EBRV 186 BlgNR XXVI. GP 4.*

36 *Data Protection Authority, 7/SN-4/ME XXVI. GP; Data Protection Council, 25/SN-4/ME XXVI. GP.*

37 *See Article 6(5) of the PNR Directive.*

38 *Data Protection Authority, 7/SN-4/ME XXVI. GP; Austrian Chamber of Labour (BAK), 6/SN-4/ME XXVI. GP; epicenter.works, 10/SN-4/ME XXVI. GP.*

39 *Article 1(2) and Article 12 f of the PNR Directive.*

40 *See Article 1(2) of the PNR Directive.*

41 *See Article 7 of the PNR Directive.*

42 *See Article 12(2) and (3) of the PNR Directive.*

43 *See Article 12(3) of the PNR Directive.*

44 *EBRV 186 BlgNR XXVI. GP 6.*

45 *Due to the separation of the judiciary and dministration as well as pursuant to Article 12(3)(b)(ii) of the PNR Directive, the data protection officer only has control of those cancellations of depersonalisation which have not been investigated by the judiciary.*

46 *See also Article 5 and Article 12(3)(b)(ii) of the PNR Directive.*

47 *See EBRV 186 BlgNR XXVI. GP 5 as well as Article 12(4) of the PNR Directive and Recital 26 of the PNR Directive.*

48 *See Sections 6(2) and 9 and EBRV 186 BlgNR XXVI. GP 7; Article 12(3) of the PNR Directive and Article 15(1)(e) of Directive (EU) 2016/680 on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offences or the execution of sentences and on the free movement of data and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 04/05/2016, 89.*

49 *See Recital 24 of the PNR Directive.*

50 *Article 9(3) of the PNR Directive.*

51 *List of competent authorities referred to in Article 7 of Directive (EU) 2016/681 on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ C 194, 06/06/2018, 1.*

52 *Article 14 of the PNR Directive and Recital 18 of the PNR Directive.*

53 *The imposition of fines on legal persons is based on the applicable regulation of Section 99d of the Austrian Banking Act, Federal Law Gazette No. 532/1993.*

Sources of information

Haller, Matthias (2016). EU-Fluggastdatensystem und die Grundrechte. Die neue Richtlinie über die Nutzung von Fluggastdaten zur Kriminalitätsbekämpfung im Lichte der Grundrechtecharta, SIAK-Journal — Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3), 86–101, Online: http://dx.doi.org/10.7396/2016_3_H.