SECONDARY ACCESS TO EUROPEAN PASSENGER NAME RECORDS

Sara Roda

Ph.D. Researcher, Vrije Universiteit Brussel, Faculty of Law Criminology, Department of Interdisciplinary Studies of Law – «METAJURIDICA», Law, Science, Technology Society Research Group
Pleinlaan 2, 1050 Elsene, Brussels, BE
Sara.Roda@vub.be; www.vub.ac.be/LSTS/

Keywords: ***Directive 2016/681, data protection, PNR, law enforcement, GDPR***

Abstract: *This article intends to demonstrate that access to the EU PNR data for further use, as defined by Directive 2016/681, is not limited to Member States' competent authorities for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime, Europol and third countries competent authorities, as was probably the legislators' intention. Through other legal instruments, based on a duty of information exchange and sincere collaboration, several Union bodies, agencies and even international organisations may have access to EU PNR data, although limited by their mandate and to the extent necessary for the accomplishment of their tasks. The paper further examines the safeguards and data protection guarantees established in the PNR Directive and, where relevant, compares them to the Law Enforcement Data Protection Directive (LE Directive), the General Data Protection Regulation (GDPR) and the Europol Regulation, focusing on the data subject rights. Depending on the entity that processes EU PNR data, the legal regime of data protection will change. In the area of law enforcement, striking the right balance between the right to privacy and protection of personal data vis-à-vis public security is the cornerstone. The increasing systematic mass collection and processing of personal data by public authorities is cause for concern and sufficient substantive and procedural structures need to be put in place to scrutinise those activities in detail.*

1. Introduction[1]

Directive 2016/681 (PNR Directive)[2] establishes a European Passenger Name Record (EU PNR) system to assist law enforcement (LE) authorities in the fight against terrorist offences and serious crime (e.g. trafficking in human beings, narcotic drugs, weapons, nuclear materials, sexual exploitation of children, etc.), including international crimes (e.g. crimes within the jurisdiction of the International Criminal Court, such as crimes against humanity, torture or genocide). This is a decentralised system, as Member States are obliged to implement their own national PNR systems in accordance with principles and standards laid down in the PNR Directive.[3] PNR data[4] is seen by the European Commission, Member States and law enforcement authori-

[1] This article is based on the first part of my Master Thesis in International and European Law (PILC), Academic year 2017–2018, Vrije Universiteit Brussel / Institute of European Studies. My promotor was Prof. Dr. Gloria González Fuster (VUB) and readers were Prof. Dr. Ben Smoulders and Prof. Dr. Bernd Martenczuk.

[2] European Parliament and Council Directive 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 [2016] OJ L199/132 (hereinafter PNR Directive). The transposition deadline by Member States was 25 May 2018.

[3] Communication to the European Parliament and the Council of 6 April 2016 on Stronger and Smarter Information Systems for Borders and Security [2016] COM(2016) 205 final, p 14.

[4] PNR data is a record of each passenger's travel requirements, for each journey booked by or on behalf of any person, held in air carriers' reservation and departure control systems – Art. 3(5) PNR Directive.

ties as an **important criminal intelligence tool**.[5] It is said to track or identify unsuspected persons capable of carrying out terrorist offences or serious crimes, by checking PNR data against (non-discriminatory) predetermined criteria, the so-called screening, or by comparing PNR data against law enforcement databases at national or EU level on persons or objects wanted or under alert, which would help LE authorities prevent, detect, investigate and prosecute terrorist acts or serious crimes.[6] In other words, it aims at verifying if a person or an object that is about to depart or land in a Member State is not being searched by the police or if a passenger may present a risk considering his/her travel patterns. **The EU PNR data must contain 19 items** which are listed in Annex I of the PNR Directive. These items can contain a **vast amount of personal information from an individual**, such as a passenger's name, address, telephone number, email address, billing address, frequent flyer information (which can amount to include a risk analysis of the passenger with more intrusive screenings to label the passenger as a «trusted traveller» or «high risk»),[7] *general remarks* [which is a very wide term and can include any kind of information, such as meal preferences - e.g. Kosher, Halal, sensitive security information, illnesses, special (medical) service requests, or even specific benefits granted for belonging to a political or religious association], names of other travellers on the PNR and Advanced Passenger Information (API) data.[8] These 19 items cannot contain information on a person's race or ethnic origin, religion or belief, political or any other opinion, trade union membership, health, sexual life or sexual orientation. In the event that any such elements are transferred to the national competent authority responsible for preventing, detecting, investigating or prosecuting terrorist offences and serious crimes, that is the PIU, which could happen through the *general remarks* item, the latter has the responsibility and obligation to delete them.[9]

2. The applicable EU legal framework for the use of EU PNR data

2.1. Scope of the PNR Directive

The Directive regulates the **transfer of PNR data of passengers of extra-EU flights**[10] by air carriers (private companies) to the so-called Passenger Information Units (PIUs), and the processing operations of that data by Member States, including collection, use and retention by public authorities, exchange between Member States or with the European Union Agency for Law Enforcement Cooperation (Europol) (Art. 4(2)(b) PNR

5 Communication from the Commission of 21 September 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries [2010] COM(2010) 492, p 3-4. For De Hert, Paul and Papakonstantinou, Vagelis, Repeating the mistakes of the past will do little good for air passengers in the EU: The comeback of the EU PNR Directive and a lawyer's duty to regulate profiling, [2015] Vol 6 Issue 2 New Journal of European Criminal Law 160-165, p 162, *«(...) PNR processing is an aggressive type of processing in the hands of law enforcement.*», it constitutes a mass surveillance tool as it aims at blacklisting and profiling individuals.

6 Commission proposal for a Directive of the European Parliament and of the Council of 2 February 2011 on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2011] COM(2011) 32 final. For the Council's position see https://www.consilium.europa.eu/en/policies/fight-against-terrorism/passenger-name-record/, accessed 11 November 2018.

7 Matthias Leese, Blurring the dimensions of privacy? Law enforcement and trusted traveller programs, [2003] 29 No. 5 Computer Law & Security Review p 480-490.

8 API data, regulated under Council Directive 2004/82/EC of 29 August 2004 on the obligation of carriers to communicate passenger data (API Directive), consists of biographical information taken from the machine-readable part of a passport. API data is held by Member States for 24 hours and is made available to border control authorities for improving border controls and combating illegal immigration in relation to flights entering the EU. Their use for other law enforcement purposes is allowed by the Directive to identify suspects or wanted persons – COM(2010) 492, p 3-4.

9 Recital 15 and Art. 13(4) PNR Directive.

10 For full definition of an extra-EU flight see Art. 3(2) PNR Directive. The Directive also contains an enabling provision extending the PNR transfer to intra-EU flights or to selected intra-EU flights Art. 2 PNR Directive. For full definition of an intra-EU flight see Art. 3(3) PNR Directive. All Member States declared their intention of extending the PNR transfer to intra-EU flights, Council Statement of 16 April 2016, http://data.consilium.europa.eu/doc/document/ST-7829-2016-ADD-1/en/pdf, accessed on 18 March 2018 – however only 19 Member States have notified the Commission of their decision to apply the PNR to intra-EU flights – Communication from the Commission to the European Parliament, the European Council and the Council of 13 June 2018 / Fifteenth progress report towards an effective and genuine Security Union [2018] COM(2018) 470 final, p 11.

Directive)and transfer to third countries (Arts. 1(a) and (b) and 11 PNR Directive). In addition, operations identified in the «processing» definition of the Law Enforcement Data Protection Directive (LE Directive),[11] such as recording, consultation, organisation, structuring, restriction, etc. are also included.[12] The **purpose of collecting and processing PNR data** is limited to preventing, detecting, investigating and prosecuting terrorist offences and serious crime (Art. 1(2) PNR Directive). The definition of «**terrorist offences»** is provided by national law in relation to Arts. 1 to 4 of the Council Framework Decision 2002/475/JHA.[13] The latter has been repealed by the Combating Terrorism Directive,[14]which considerably changed the scope and dimension of the offences identified in the Framework Decision, criminalising new conducts. The absence of a correlation table in the Combatting Terrorism Directive or of a specific provision in the latter amending the PNR Directive, can raise certain questions as to whether a conduct should be qualified as criminal and as to the subsequent definition of the rights of suspects of criminal offences.[15]The offences that fall under the definition of «**serious crime»,** are identified in the exhaustive list of Annex II of the PNR Directive, which are punishable at national level by a custodial sentence or a detention order for a maximum period of at least three years (Art. 3(9) PNR Directive). By 25 May 2020, the Commission is required to **review the necessity, proportionality and effectiveness** of broadening the *ratione personae* scope of collection and transfer of PNR data to include non-carrier economic operators, such as travel agencies and tours operators, that provide travel-related services, including the booking of flights (Art. 19(3) PNR Directive).Since Member States have already expressed their intention to extend under national law the same obligations to those entities,[16] such a review will be of limited interest. The material scope can also be extended to other transportation providers, such as rail, road and maritime international transport (recital 33 PNR Directive).

2.2. Key features of the PNR Directive

Member States are not given direct access to the airlines database. The PNR data is sent by air carriers to the PIU of the Member State concerned, the so-called «push method» (deliberate transfer),[17] 24 to 48 hours before the scheduled flight departure time and immediately after flight closure (Art. 8(3) PNR Directive). The data is then processed and assessed by the Member State's PIU for the sole purpose of identifying persons requiring further examination by competent authorities and by Europol (where relevant and if within its com-

[11] European Parliament and Council Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (hereinafter LE Directive).

[12] Recital 27 and Arts. 1 and 11 PNR Directive and Recital 34 and Art. 3(1) LE Directive.

[13] Art. 3(8) PNR Directive. Before the Lisbon Treaty, police cooperation was a competence under the third pillar and framework decisions (FDs) were the legal instruments used. FDs bound Member States on the results to be achieved leaving the form and methods to national authorities (similar to first pillar Directives at the time). Under the third pillar, Member States compliance to FDs escaped the control of the Commission and of the CJEU. A Member State could voluntary opt-in to be under the CJEU's jurisdiction, but the role of the Court was limited to the interpretation of FDs via the preliminary ruling procedure. When the Lisbon Treaty entered into force, and after the five-year transitional period, FDs on police cooperation on criminal matters became enforceable by the Commission – Art. 10 of Protocol n° 36 on Transitional Provisions of the Lisbon Treaty.

[14] European Parliament and Council Directive (EU) 2017/541 of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L88/6.

[15] The main question is whether «terrorist offences» under Art. 3(8) of the PNR Directive should still be interpreted as referring to Arts. 1 to 4 of the repealed Framework Decision or rather to the corresponding articles of the repealing Combatting Terrorism Directive. If the latter is not transposed by a Member State, or correctly done so, legal uncertainty can occur at the time when the acts are committed. The debate is out of this article's scope, but EU case-law precludes a Directive from having the effect of determining or aggravating the liability in criminal law of accused persons. In this sense: Case C-105/03 of 15 June 2005 *Maria Pupino* ECLI:EU:C:2005:386 (16 June 2005), §44-45, Joined Cases C-387/02, C-391/02 and C-403/02 *Berlusconi and Others* (3 May 2005) ECLI:EU:C:2005:270, §73-74.

[16] Council Statement from 16 April 2016 (7829/16 ADD 1).

[17] For full definition see Art. 3(7) PNR Directive.

petence).[18] Further examination implies that the person in question may be involved in or is a suspect of a terrorist offence or serious crime, or that the crime is being committed with the journey itself (e.g. drug smuggling or money laundering through cash transport). **The exchange of information between Member States' PIUs is the general rule** (Art. 9(1) and (3) final sentence PNR Directive), although in case of urgency a national competent authority may, if duly reasoned, request information directly to the PIU of another Member State (Art. 9(3) PNR Directive). If a person is identified for further examination, this information needs to be shared with the PIUs of other Member States, who in turn will share it with their national competent authorities in due time to allow border controls (recital 13 and Art. 9 PNR Directive). **Data provided by airline carriers can be stored in the PIU's database for 5 years** after being transferred to the PIU of another Member State, after which it must be deleted. PNR data is «depersonalised» after 6 months to mask out any information that can serve to identify directly the passenger.[19] Access to the full PNR data after this period is only admitted when it is reasonably believed to be necessary to respond to requests made, on a case-by-case basis, by competent authorities or Europol, and is approved by a judicial authority or another national authority competent under national law to verify whether the conditions for PNR data disclosure are met (recital 37 and Art. 12 PNR Directive). Any subsequent transfer of data between LE and judicial authorities is regulated by national legislation and the period of retention is no longer under the scope of the PNR Directive (recital 26 PNR Directive). **Any decision having an adverse legal effect on or that significantly affects a person cannot be taken by automated processing of PNR data.** The PNR Directive provides that an «individual review» by a «human» is mandatory (recital 20 and Arts. 6(5)(6) and 7(6) PNR Directive). The extent of the review is not specified further, giving a wide margin of manoeuvre for LE authorities to decide.[20] The only limit introduced was the prohibition of taking decisions based on a person's race, ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, health, sexual life or sexual orientation.[21] Another important guarantee established in the PNR Directive is the assurance that any assessment made before the arrival of a flight or its departure from a Member State cannot jeopardise the free movement principle and the right of entry of EU citizens in the EU (Art. 6(9) PNR Directive) or be used to deny asylum or the statute of a refugee to non-EU nationals (recital 21 PNR Directive). A Member State may transfer PNR data to a third country, on a case-by-case basis and in accordance with the provisions laid down by Member States pursuant to Council Framework Decision 2008/977/JHA.[22] Transfers of PNR data without prior consent of the Member State from which the data was obtained are permitted in exceptional circumstances (Art. 11 PNR Directive). **All processing of PNR data should be logged or documented** for verifying its legality, self-monitoring and ensuring proper data integrity and secure processing (recital 37 PNR Directive). This is key to detect and track who had access for subsequent control. Passengers must be informed that their PNR data is being collected

[18] Recital 23 and Art. 6(2) PNR Directive. The express mention to real-time access by Europol to PNR data, that is prior to the arrival and departure of passengers to prevent a crime, was not in the 2011 Commission Proposal for the PNR Directive. This feature was introduced by the co-legislators during the legislative procedure. The Commission had only envisaged the re-active use of PNR data, i.e. in case of an on-going investigation, Europol would formulate a request to the Member State (Recital 20, COM(2011) 32 final).

[19] This includes name and number of travellers on the PNR travelling together, address and contact information, all payment information including billing address, frequent flyer information, *general remarks* and API data – Art. 12(2) PNR Directive.

[20] WP29 provided some guidelines concerning the qualification of «human involvement» for the purposes of the GDPR which could be used in the context of the PNR Directive. «Human involvement» means that the review cannot consist in applying automatically the decision based on automated processing and that it must be made by someone that has the authority and competence to change the decision - WP29 Opinion on «Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679» adopted on 3 October 2017 and later revised and adopted on 6 February 2018 (WP251rev.01) p 20-21.

[21] An additional reasonable safeguard which could have been added would have been to make the LE decision dependent on the obtention of material proof against a person (e.g. detection of falsified visa, of drugs or undeclared cash).

[22] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60 has been repealed by the LE Directive with effect from 6 May 2018. References to this Framework Decision should be construed as references to the LE Directive - Art. 59 LE Directive.

and about their rights (recital 37 PNR Directive). The PIU must keep records of several processing operations, in particular collection, consultation, disclosure and erasure (Art. 13(6) PNR Directive).

2.3. Compliance with which EU privacy and data protection rules: Directive (EU) 2016/680 (LE Directive), Regulation (EU) 2016/679 (GDPR) or Regulation (EU) 2016/794 (Europol)?

This section considers which legal instrument the entities who process PNR data in the context of the EU PNR system are subject to and must comply with when they process personal data. This illustrates the variety of processing activities taking place and the different applicable data protection regimes. I point out **two types of access: «primary access»,** where the legitimacy to process such data stems directly from the PNR Directive; and «**secondary access»,** where other entities in the LE and border management area might have access to personal PNR data indirectly, through other legal instruments, e.g. Europol Regulation, LE Directive, EPPO Regulation and national legislation, or even the TFEU [Art. 86(2)] and TEU [Art. 4(3)]. **Entities with primary access** are air carriers, PIUs, national competent authorities under Art. 7 of the PNR Directive (which could be LE and judicial authorities, such as police, courts and customs), Europol and third countries' competent authorities pursuant to Art. 11 of the PNR Directive. **Entities with secondary access** can be the European Union Agency for Criminal Justice Cooperation (Eurojust), the European Anti-Fraud Office (OLAF), the European Public Prosecutor's Officer (EPPO) and the International Criminal Police Organisation (Interpol).

2.3.1. Primary access

2.3.1.1. Air carriers

Air carriers are private entities who initially process PNR data for commercial purposes and are now legally obliged to handover that data to PIUs. The processing operations related to personal data, including appropriate technical and organisational measures to ensure data security and confidentiality of processing are governed by the GDPR.[23] This is due to the fact that the main and original purpose of collection by air carriers is not the same as the one established in Art. 1(2) of the PNR Directive, which is to prevent, detect, investigate and prosecute terrorist offences and serious crime. The express mention to the application of the GDPR reinforces the distinction between processing operations (and consequently of legal regimes) of EU PNR data by private entities and by public authorities. As a result, individuals wishing to enforce their rights to privacy and protection of personal data against air carriers will be subject to the rules and safeguards of the GDPR.

2.3.1.2. PIUs and Member States' competent authorities

PIUs and competent authorities that fit the definition of Art. 7(2) of the PNR Directive are namely public authorities with LE competences (e.g. police, customs), but also judicial authorities, or even any other body or entity entrusted by Member States to exercise public powers under the PNR Directive, namely prevention, detection, investigation or prosecution of terrorist offences and serious crime. These entities, when processing personal PNR data, are subject to Art. 13 of the PNR Directive, which then refers to Arts. 17 to 22 of Council Framework Decision 2008/977/JHA. The latter has been repealed by the LE Directive, which has considerably changed some of those rights.[24] Despite the absence of a correlation table concerning both legal

[23] European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L199/1 (hereinafter GDPR). References made to the repealed Directive are construed as references to the GDPR – Art. 94 GDPR; Arts. 13(3) and 21(2) PNR Directive.

[24] For example, the LE Directive has enlarged the information that can be accessed by the data subject under the right of access (Art. 14 LE Directive), changed the scope of the right to rectification, erasure and restriction of processing, which was previously called «right to rectification, erasure and blocking» (Art. 16 LE Directive) and is more detailed concerning the right to administrative and judicial remedies (Arts. 52 to 54 LE Directive).

instruments, Art. 59 of the LE Directive provides that the applicable law should be the LE Directive. One could either adopt a restrictive interpretation, applying to the data subject only the precise rights that still coincide with the repealed Framework Decision, or adopt an extensive interpretation, applying new and extended rights which are more favourable to the data subject. Since the processing of personal PNR data can have negative consequences for the data subject, legal certainty requires defending an extensive interpretation. In short, individuals wishing to enforce their right of privacy and protection of personal data against PIUs and competent authorities falling under the definition of Art. 7 of the PNR Directive will be subject, by reference of Art. 13 of the PNR Directive, to the new and extended rights of the LE Directive.

2.3.1.3. Europol

Established in 1995, Europol became an EU agency in 2009 to support and strengthen Member States' actions and their cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States (recitals 1 and 6 Europol Regulation). Its main tasks include the collection, storage, processing, analysis and exchange of information and intelligence, assistance with investigations, and provision of intelligence and analytical support to Member States. Its processing operations are governed by the Europol Regulation.[25] The processing of personal data by Europol is under the supervision of the European Data Protection Supervisor (recital 50 Europol Regulation)and has specific and autonomous rules regarding the protection of personal data.[26] Europol can request access to PNR data or analytical information to the PIUs of Member States through the Europol National Unit under strict conditions: case-by-case basis, electronic and duly reasoned request, when strictly necessary to support and strengthen Member States' action, respecting the purpose limitation principle of the transfer to prevent, detect or investigate a specific terrorist offence or serious crime which falls within the scope of Europol's competences. Europol's request should still demonstrate that the access to the data will substantially contribute to the prevention, detection or investigation of those offences (Art. 10 PNR Directive). Europol's right of access can still be restricted by Member States' PIUs to ensure the respect of the principle of ownership of data and the protection of personal data (recitals 26 and 27 Europol Regulation). Consequently, an individual wishing to enforce his/her right to privacy and protection of personal data against Europol, will have to do so under the Europol Regulation (Art. 47 and onwards Europol Regulation). If Europol processes non-operational data, which is not related to criminal investigations (e.g. staff data, visitors, service providers), then the processing of such data is subject to Regulation (EU) 2018/1725,[27] which entered into force on 11 December.

2.3.1.4. Third countries' competent authorities

The access by third countries'[28] competent authorities to EU PNR data can be regulated either by the PNR Directive, with the subsidiary application of the LE Directive, or by the GDPR. The difference depends on who transfers the EU PNR data to the third country, either Member States or air carriers. **For air carriers**, as mentioned in subsection 2.3.1.1, the legal regime applied is the GDPR (Art. 21(2) PNR Directive). Hence,

---

25 European Parliament and Council Regulation (EU) 2016/674 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53 (hereinafter Europol Regulation). The latter has been amended by Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS). The analysis of ETIAS implications is beyond the scope of this paper.

26 Recital 40 Europol Regulation and in this sense recitals 11, 12 and Arts. 2(3), 98(2) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39.

27 Recital 53 Europol Regulation; references to Regulation (EC) N° 45/2001 (OJ L8/1, 12.01.2001) should be construed as references to Regulation (EU) 2018/1725 (OJ L295/39, 21.11.2018) – recital 86 and Art. 99 of Regulation (EU) 2018/1725.

28 For the notion of a «third country» see Van den Bulck, Paul, Transfers of personal data to third countries, [2017] vol. 18 no. *2 ERA Forum* Springer Berlin Heidelberg 229-247, p 230.

transfers of EU PNR data by air carriers directly to third countries' competent authorities are subject to the GDPR rules on transfers of personal data to third countries.[29] **For Member States**, the transfer of EU PNR data to a third country is made pursuant to Art. 11 of the PNR Directive, which is not clear as to who is responsible within the Member State to carry out the transfer – Member States' PIU or competent authorities under Art. 7 of the PNR Directive. The transfer must be necessary and can only occur on a case-by-case basis for the same purpose as that of Art. 1(2) of the PNR Directive. It must be duly reasoned and comply with the conditions set out in Art. 9(2) of the PNR Directive as well as with the general principles for transfers of personal data under the LE Directive.[30] These principles establish a **three-step protocol to be followed** by the transferring Member State. First, consider the existence of an adequacy decision, recognised by the Commission, applied to the third country (this requirement is constantly monitored by the Commission). Second, in its absence, verify if appropriate safeguards have been provided or exist regarding the protection of personal data. Third, if the previous two conditions are absent, derogations can be allowed in specific circumstances. In short, Member States need to ensure that the same conditions and safeguards set out in the PNR Directive are observed by the third country, and that the level of protection of personal data is «essentially equivalent»[31] to that guaranteed within the EU, including in cases of onward transfers by the third country to competent authorities of another third country, where express authorisation of the Member State is required. It is important to note that the third country can have access not only to the EU PNR data, but also to the result of processing such data by the PIU (a feature that does not exist in the GDPR).

2.3.2. Secondary access

The question in this subsection is whether Eurojust, OLAF, Interpol and the EPPO can have access to EU PNR data via the cooperation they have with Europol and with national competent authorities.[32] If so, which legal framework should be applicable in connection to the enforcement by an individual of his/her right to privacy and data protection? Or should it be considered that the PNR Directive does not allow such subsequent transfers to international organisations, Union bodies or agencies at all? **Art. 11 of the PNR Directive** regulates the transfers of PNR data to third countries and is **silent regarding possible transfers (or subsequent transfers) to international organisations, union bodies or agencies.** No express general permission or prohibition exists in the PNR Directive in relation to international organisations, Union bodies or agencies (with the exception of Europol). However, several EU legal instruments, including the TFEU [Art. 86(2)] and the TEU, under the **principle of sincere cooperation** [Art. 4(3) TEU], encourage the exchange of information and collaboration between Union agencies or bodies as well as with national competent authorities in order to improve efficiency in combatting crime and avoid duplication of resources.

---

29 Arts. 44 and onwards GDPR. The procedure is similar to the one foreseen in the LE Directive in the sense that an adequacy decision of the Commission is required (Art. 45 GDPR), in its absence, appropriate safeguards have to be provided, including the existence of effective legal remedies to enforce data subject rights (Art. 46 GDPR), and if the previous mechanisms are absent, derogations are allowed under certain situations (Art. 49 GDPR). For further detail see the EDPB Guidelines 2/2018 on derogations of Art. 49 under Regulation 2016/679 adopted on 25 May 2018.

30 Art. 11(1)(a) PNR Directive makes express reference to Art. 13 of the Council Framework Decision 2008/977/JHA. As mentioned above, in the absence of a correlation table and for the sake of legal certainty, one should adopt an extensive interpretation construing the reference to Arts. 35 to 38 of the LE Directive.

31 Notion resulting from the Schrems case, §73 and 74, ECLI:EU:C:2015:650.

32 For national competent authorities, through the application of Art. 39 of the LE Directive by way of derogation from Art. 35(1)(b) of the said Directive.

2.3.2.1. Eurojust and OLAF

Art. 21 of the Europol Regulation provides access to Eurojust[33] and to OLAF[34] to information held by Europol, within their respective mandates. The **access is indirect**, based on a hit/no hit system, and is **subject to possible restrictions**, including authorisation and degree of right of access, indicated by the entity providing the information in question, that is Member States, Union bodies, third country or international organisation.[35] A question that could be raised in connection to **Eurojust** is whether through its unique structure one could consider that National Members, who are also heads of the respective national desks offices (submitted to the national law of their Member State), **holding a double «hat»** of national judicial authority,[36] fit the category of national competent authorities under Art. 7 of the PNR Directive, having access to PNR data in that capacity. Either way, there are reasons to believe that Eurojust will be able to have access and process PNR data for the purposes of investigating and prosecuting crimes and offences in which Europol is competent to act. At first sight, it seems that only four offences under Annex II the PNR Directive are not included in Annex I of the Europol Regulation. Those criminal offences are rape, unlawful seizure of aircrafts/ships, sabotage and industrial espionage. Rape could however be subsumed to sexual abuse and sexual exploitation under Annex I of the Europol Regulation, reducing then the list to three. **OLAF** can conduct external investigations, carrying out on-the-spot checks and inspections in Member States, including access to all information and documents relating to the matter under investigation (Art. 3(1) and (5) OLAF Regulation). The cooperation and exchange of information, including personal data and classified information, with Eurojust and Europol is recognised by Art. 13 of the OLAF Regulation. Being a Union body, it is subject to Regulation (EU) 2018/1725. Hence, the processing operations and protection of personal data will be governed by the OLAF Regulation (Art. 10) and by Chapter IX of Regulation (EU) 2018/1725.[37] The offences for which it may have access to and process PNR data are limited to its mandate.[38] Pursuant to Annex II of the PNR Directive, those offences may include i) participation in a criminal organisation, ii) corruption, iii) fraud, including against the financial interests of the Union, iv) laundering of the proceeds of crime and counterfeiting of currency, including the euro, and v) forgery of administrative documents and trafficking therein.

---

33 Eurojust is a body of the Union created in 2002 to reinforce the fight against serious cross-border crimes and improve closer co-operation between national judicial authorities (prosecutors and investigative judges). Its competences were strengthened by the Lisbon Treaty in 2009, which granted Eurojust with investigative powers. Its legal framework was recently changed by Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), replacing and repealing Council Decision 2002/187/JHA of 28 February 2002 [2018] OJ L295/138. The latter and Regulation (EU) 2018/1725 will only apply to Eurojust from 19 December 2019.

34 OLAF is an EU body established in 1999 to detect, investigate and stop fraud, corruption and any other illegal activity against the financial interests of the Union. The current legal framework is Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (hereinafter OLAF Regulation), [2013] OJ L248/1.

35 See also recitals 28, 31, 32 and 34 Europol Regulation.

36 Eurojust is composed by 28 national members seconded by each Member State being either a judge, a prosecutor or a police officer. National members have a double dimension: they are part of the European body, carrying out tasks of Eurojust as provided by Art. 6 of the 2002 Council Decision as amended, but they are also granted powers in their capacity as national judicial authorities (Arts. 9 to 9f of the said Council Decision). - Gutiérrez Zarza, Ángeles, Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe (Springer 2015) p 62-64. Regulation (EU) 2018/1727 maintained the double dimension – see Arts. 7, 8, 20 and 21.

37 For transfers to third countries and international organisations see Chapter V and Art. 94 of Regulation (EU) 2018/1725.

38 See footnote 35.

2.3.2.2. The European Public Prosecutor's Office (EPPO)[39]

The EPPO is a Union body established in 2017 under the mechanism of enhanced cooperation referred to in Art. 20(2) TEU and Art. 329(1) TFEU, but its foundations rely on Art. 86 TFEU.[40] It will be responsible for investigating, prosecuting and bringing to judgment perpetrators and accomplices of criminal offences affecting the financial interests of the Union.[41] The offences for which it may have access and process PNR data, according to its mandate, seem identical to OLAF's. EPPO's investigations and prosecutions will be governed by the EPPO Regulation. The principles and rules related to the protection of personal data are extensively specified in Art. 47 and onwards of the EPPO Regulation. According to recital 93 of the EPPO Regulation, such rules should be interpreted and applied in accordance with the interpretation and application of the LE Directive. National law will be applied only to the extent that the matter is not governed by the Regulation. In case of conflict, the EPPO Regulation prevails.[42] The exchange of information between Eurojust, OLAF and Europol are governed respectively by Arts. 3(3), 100, 101 and 102 of the EPPO Regulation.[43] Exchange of information can also take place with other Union institutions and bodies (Art. 103), with third countries and international organisations (Art. 104) as well as with Member States that do not take part in the enhanced cooperation mechanism (Art. 105). Regulation (EU) 2018/1725 applies to the processing of administrative personal data performed by the EPPO.[44] Hence, in the performance of its tasks, the EPPO might have secondary access to PNR data not only through its relations with Europol, but also with national competent authorities, as per Art. 99(1) and (2) on common provisions for EPPO relations with its partners of the EPPO Regulation.

2.3.2.3. International Criminal Police Organisation (Interpol)

Interpol is an international police organisation composed by 194 member countries, each represented by a National Central Bureau.[45] Interpol developed special relations with several partners, including the European Union. All EU Member States are affiliated to Interpol. Specific recitals in each regulation governing Europol, OLAF, EPPO and Eurojust, address the transfers of personal data to Interpol. The reason is that police cooperation, mutual assistance and exchange of information to prevent and fight crime between criminal law enforcement authorities are core activities of Interpol. **An example:** the possibility to exchange personal data between Europol and Interpol is recognised under recitals 32 and 33 of the Europol Regulation and further regulated by Art. 25 of the Europol Regulation on international transfers. Art. 25(1) of the Europol Regulation provides a flexible regime to Europol since the transfer can be based on one of the three conditions below:

– an «adequacy decision» issued by the Commission, meaning that the country or international organisation offers an adequate level of protection to personal data. This decision allows the free flow of

---

39 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office («the EPPO») [2017] OJ L283/1. The enhanced cooperation is open to all Member States wishing to join. The Regulation is binding in its entirety and directly applicable for participating Member States. These are Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Finland, France, Germany, Greece, Lithuania, Luxembourg, Portugal, Romania, Slovakia, Slovenia and Spain.

40 Art. 86 (2) (4)TFEU: «*2. The European Public Prosecutor's Office shall be responsible for investigating, prosecuting and bringing to judgment, where appropriate* ***in liaison with Europol****, the perpetrators of, and accomplices in, offences against the Union's financial interests (…). It shall exercise the* ***functions of prosecutor*** *in the competent courts of the Member States in relation to such offences. 4. The European Council may, (…) extend the powers of the European Public Prosecutor's Office to include* ***serious crime having a cross-border dimension*** *(…)»* (emphasis added).

41 Art. 4 EPPO Regulation, which refers to offences listed in Directive (EU) 2017/1371 of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law [2017] OJ L198/29.

42 Art. 5(3) EPPO Regulation. The latter, together with the Europol Regulation, is seen as *lex specialis* in relation to the general rules of Chapter IX of Regulation (EU) 2018/1725 – recitals 11 and 12 of Regulation (EU) 2018/1725.

43 See also recitals 69 and 100 EPPO Regulation.

44 Recital 90 EPPO Regulation and recital 14 Regulation (EU) 2018/1725.

45 https://www.interpol.int/About-INTERPOL/Overview, accessed 1 January 2019.

personal data from the EU without further need to implement additional safeguards or being subject to further conditions;
- an international agreement providing «adequate safeguards»[46] concluded between the Union and the international organisation pursuant to Art. 218 TFEU; or,
- a cooperation agreement between Europol and the third country or the international organisation allowing the exchange of personal data if concluded before 1 May 2017.

In this case, Interpol has signed a cooperation agreement with Europol on 5 November 2001, which continues to be in force.[47] Therefore, there are reasons to believe that Interpol could have access to PNR data not only via Europol, within their respective mandates, but also via national LE authorities under Art. 35 of the LE Directive, where national LE authorities receive PNR data from the Member State PIUs and then transfer it to international organisations via the LE Directive. Member States, as members of Interpol, have certain **duties of cooperation and information sharing** with this entity (e.g. respond to Interpol notices or information requests). This can be a point for the CJEU to clarify in the future.

3. Conclusion

This paper illustrated the variety of processing activities and applicable data protection regimes that the EU PNR data will be subject to, creating a degree of complexity which is not desirable when data subjects wish to enforce their rights. It further demonstrated that the access to EU PNR data is not limited to entities that have primary access, as provided by the PNR Directive. **Through other EU legal instruments and under the principle of sincere cooperation**, national competent authorities and Europol are encouraged to exchange information with Union agencies and bodies in the area of police and judicial cooperation in criminal matters (Eurojust, OLAF, EPPO), as well as Interpol. **This secondary access was not considered and therefore not tackled in the PNR Directive.** The review of the PNR Directive by the Commission (Art. 19) should also address the consistency between these legal instruments. Moreover, the PNR Directive does not clearly reflect on the different access and use that LE authorities (police and customs) and judicial authorities (court and prosecutors) have in relation to PNR data. They are treated the same way, although their access and use will vary substantially.[48] As a result, Member States can be clearer and stricter about the degree of access by competent authorities and their staff to PNR data, in order to reduce the interference with the right to privacy and protection of personal data.[49] Transparency, responsibility and accountability for the processing operations of personal data are critical to avoid abuse and misuse.

[46] In the LE Directive, the term used is «appropriate safeguards», as per Art. 37.

[47] https://www.europol.europa.eu/sites/default/files/documents/agreement_between_Interpol_and_Europol.pdf, accessed on 1 January 2019.

[48] For example, LE authorities i) may have access to the screening assessment made by the PIU, ii) may complement such assessment by «human involvement», iii) may implement a preventive measure (e.g. thorough baggage control or passport), and iv) are entitled to receive information specific to an on-going investigation. Judicial authorities, however, may only have a mandate to act for a specific case.

[49] For example, i) not all public entities should have access to the same level of information (e.g. police services during an investigation may have broader access than a judge in a specific case); ii) a mandatory requirement on a need-to-know-basis for information exchange between public authorities could be introduced [inspiration could be drawn from the Europol Regulation – recital 27 and Arts. 7(5), 19(2) and 20]; and iii) the capacity (functions or mandate) under which officials are authorised to process PNR data should be defined and their number limited.