Council of the European Union

Brussels, 8 September 2016
(OR. en)

11794/16

LIMITE

JAI 710
DAPIX 133
ENFOPOL 259
COMIX 574
ENFOCUSTOM 120
CRIMORG 93
SCHENGEN 15
VISA 276
SIRIS 118
COPEN 247
ASIM 113
FRONT 329

NOTE

From:	General Secretariat of the Council
To:	Working Party on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	6704/16
Subject:	Manual on Law Enforcement Information Exchange - Draft update 2016

The Manual on Law Enforcement Information Exchange (6704/16), drafted in the framework of the Information Management Strategy (IMS) for EU internal security, aims at supporting, streamlining and facilitating cross-border in formation exchange. Since the manual is intended as a tool for police officers working in this area, both structure and content of the manual are focussed on the practical day-to-day cooperation between national authorities involved in information exchange, and their training purposes.

It has to be noted that in order to further enhance its practical value, the manual has been translated and exists meanwhile in all official languages of the Union. Furthermore, it was agreed to update the manual twice a year, as necessary in the light of new legislation, practical experiences, or changes to the contact details of the authorities concerned.

The update for 2016 has to take account of the new legislation adopted in 2016, that is the Passenger Name Record (PNR) Directive and the Data Protection Directive, and to changes to the national factsheets. However, for the sake of readability and in order to deal with the update exercise in the most pragmatic way, the current draft only deals with changes concerning Part II (General Information) of the manual and sets out the information about the new legislation. After agreement by DAPIX on the content of this draft, the text will be incorporated in the final version of the updated manual, together with the changes to the contact details contained in Part III of the manual (National Fact Sheets).

In order to be as close as possible to the existing manual, the numbering of the text presented in annex to this note follows the structure of the manual. Thus, chapter 1.12 of the updated manual would set out information about Passenger Information Units (PIUs), the new communication channel in the framework of the PNR Directive, whereas chapter 3.16 would set out information about the PNR legislation in general. A request for contact details on the future PIUs is submitted in a different document (CM 3713/16).

As to the information on the Data Protection Directive, the Working Party should agree on the right place with a view to the "umbrella" relevance of the Directive. For the time being, the draft suggests 3.0, that is at the very beginning of the chapter on legislation.

DAPIX is invited to discuss the draft set out in annex to this note at its meeting on 13 September 2016 with a view to finalising the update of the manual in due time.

PART II - General information

1. CHANNELS OF CONTACT

1.12. Passenger Information Unit (PIU)

In the framework of Directive 2016/681[1], each Member State establishes or designates an authority competent for law enforcement to act as its passenger information unit (PIU)[2]. Such units are competent for processing passenger name record (PNR) data received from air carriers and, furthermore, are the lynchpin for the cross-border information exchange among themselves and with Europol. Two or more Member States may establish or designate a single authority to serve as their common PIU.

The processing of PNR data serves mainly the assessment of passengers in order to identify persons who require further examination by law enforcement authorities. The directive applies to extra-EU flights and may be applied to intra-EU flights as well if a Member State decides to do so.

PNR data should be compared against various databases in order to support the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The assessment of PNR data facilitates the identification of persons who were, prior to such assessment, unsuspected of involvement in terrorist offences or such crime. In line with EU data protection policy, the processing of such data should be proportionate to the specific security goals pursued by the Directive.

---

[1] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119/132, 4.5.2016.

[2] Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with the Directive by 25 May 2018.

The PIU is responsible for:

- at domestic level, collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the national competent law enforcement authorities;

- at Union level, exchanging both PNR data and the result of processing those data with the corresponding PIUs of other Member States and with Europol.

The storage, processing and analysis of PNR data by the PIU shall be carried out exclusively within a secure location or location within the territory of a Member State. Moreover, the PNR data provided to the PIUs have to be retained in a database at the PIU for a period of five years after their transfer to the PIU of the Member State of arrival or departure. However, six months after their transfer, all PNR data have to depersonalised through masking out of data elements which could serve to identify directly the data subject. The result of processing shall be kept by the PIU only as long as necessary to inform the relevant national competent law enforcement authorities and to inform the PIUs of other Member States of a positive match.

The PIU processes only those data listed in Annex I of the directive, and for the following purposes:

- carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State in order to identify persons who require further examination by national law enforcement authorities and, where required, by Europol;

- responding, on a case-by-case basis, to a request from the competent authorities to provide and process PNR data for law enforcement purposes in specific cases, and to provide these authorities and, where appropriate, Europol with the results of such processing;

- analysing PNR data for the purpose of updating or creating new criteria applied for the identification of passengers that may be involved in a terrorist offence of serious crime.

When carrying out such assessments, the PIU may compare PNR data against law enforcement databases in accordance with Union, international and national rules applicable to such databases, or process PNR data against pre-determined criteria. These predetermined criteria must be targeted, proportionate and specific. It is up to the PIUs to set up and regularly review those criteria in cooperation with the relevant law enforcement authorities. The criteria shall not be based on sensitive personal data such as race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

With regard to persons identified, the PIU transmits all relevant and necessary PNR or the result of processing thereof to the corresponding PIU of the other Member States. These PIUs will transmit the information received to their own competent authorities.

The data protection officer appointed to monitor the processing of PNR data has access to all data processed by the PIU. A data subject is entitled to contact the data protection officer on all issues relating the processing of that data subject's PNR data.

All transfers of PNR data by air carriers to the PIUs are to be made by electronic means that provide sufficient guarantees in respect of technical security measures. To that effect, the Commission will adopt common protocols air carriers have to comply with when electronically transferring data, and, furthermore, supported data formats to ensure the readability of the data by all relevant parties.

3. LEGISLATION - THE LEGAL CONTEXT, RULES AND GUIDELINES RELATED TO THE MAIN COMMUNICATION METHODS AND SYSTEMS

3.16. PNR (Passenger Name Record) Directive

Legislation

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

Key provisions

The directive establishes at Union level a common legal framework for the transfer and processing of PNR data and provides:

a) for the transfer by air carriers of passenger name record (PNR) data of passengers of extra-EU flights. If a Member decides to apply the directive to intra-EU flights, all provisions apply to intra-EU flights as if they were extra-EU flights;

b) the processing of PNR data, including its collection, use and retention by the Member States and its exchange between Member States.

PNR data, including advance passenger information (API), to be transferred by air carriers are set out in Annex I of the directive. Annex II contains the list of offences defining the scope of applicability of the directive. For the purpose of processing PNR data, each Member State establishes or designates a competent law enforcement authority to act as its passenger information unit (PIU). Two or more Member States may establish or designate a single authority to serve as their common PIU.

At cross-border level, the PIUs exchange among themselves and with Europol both PNR data collected from air carriers and the result of processing those data. The processing of PNR data serves mainly the assessment of passengers prior to their arrival in or departure from a Member State in order to identify persons who require further examination by law enforcement authorities and, where relevant, by Europol.

PIUs may (a) compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such databases, or (b)process PNR data against pre-determined criteria.

At domestic level, the PIUs transmit PNR data or the result of their processing to the competent national law enforcement authorities entitled to further examine the file or to take appropriate action.

PNR data are to be retained in a database at the PIU for a period of five years after their transfer from the Member State of arrival or departure of the flight. However, all PNR data shall be depersonalised after a period of six months. This is to be done through masking out of data elements which could serve to identify directly the passenger to whom those data relate. After five years, PNR data are to be deleted unless they have been transferred for special purposes and, in this case, their retention is governed by national law.

3.17 Advance Passenger Information (API)

Legislation

Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data

Key Provisions

The directive aims at improving border controls and combating illegal immigration. To that end, the directive requires the Member States to establish an obligation for air carriers to communicate certain information concerning their travellers in advance of their entering the European Union Such information is referred to as Advance Passenger Information (API). Under certain conditions and circumstances, Member States may also use API data for law enforcement purposes.

The information is supplied, at the request of authorities responsible for carrying out checks on persons at the external borders of the EU.

Air carriers should transmit API data electronically, or in case of failure by any other appropriate means, to the authorities carrying out the border checks where the passenger enters the EU. API data are checked against national and European databases such as the Schengen Information System (SIS) and the Visa Information System (VIS).

When API data match an entry in a database, an alert is sent to the border police and the corresponding passenger is targeted for examination on arrival.

Collected and transmitted API data have to be deleted by carriers and authorities within 24 hours of transmission or arrival. However, the border authorities can retain the temporary files longer than 24 hours if the data are needed later for the purpose of exercising the statutory functions of the border authorities or for the enforcement of laws and regulations on entry and immigration, including their provisions on the protection of public policy (*ordre public*) and national security.

3.0 Data Protection Directive [3]

Directive (EU) 2016/680, which repeals Council Framework Decision 2008/977/JHA, lays down the specific rules relating to

- the protection of natural persons, whatever their nationality or place of residence, with regard to the processing, whether by automated means or otherwise, of personal data by the police or other law enforcement authorities within the remit of their activities, and
- the free flow, of personal data between competent authorities,

and aims at ensuring the same level of protection for natural person through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities.

The term 'competent authorities' covers public authorities such as the judicial authorities, the police or other law enforcement authorities as well as any other body or entity entrusted by Member State law to exercise public authority and public powers law for the purposes of this Directive. The activities of law enforcement authorities focus mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities. Such activities can also include police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on them where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society which may lead to a criminal offence.

---

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89, 4.5.2016

Processing of personal data for purposes out of the scope of the activities mentioned above and which with Member States may additionally entrust law enforcement authorities, the processing of personal data, in so far as it is within the scope of Union law, is governed by Regulation (EU) 2016/679[4]. Furthermore, Directive (EU) 2016/680 does not cover the processing of personal data with regard to activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities with regard to the common foreign and security policy[5].

For the purposes of the Data Protection Directive:

- **'personal data'** means any information relating to a natural person ('data subject') identified or identifiable, directly or indirectly, in particular by reference to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. A clear distinction shall be drawn between personal data of (a) suspects, (b) convicts, (c) victims and (d) other parties to a criminal offence, such as witnesses.

- **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016

[5] Chapter 2 of Title V of the Treaty on European Union (TEU)

Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. In order to be lawful, such processing should be necessary for the performance of a task carried out by a competent authority for the above mentioned law enforcement purposes. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamentals Freedoms. Personal data are to be adequate and relevant for the purposes for which they are processed.

Processing of particularly sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only under well defined and restrictive conditions.

The establishment of national supervisory authorities that are able to exercise their functions with complete independence is an essential component of the protection of natural persons with regard to the processing of their data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this directive and should contribute to their consistent application throughout the Union. The protection of rights and freedoms of data subjects as well as the responsibility and liability of controllers, that is national competent authorities, and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of responsibilities.

Moving personal data across borders may put jeopardise the ability of natural persons to legally protect themselves from unlawful use or disclosure of those data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative ore remedial powers and inconsistent legal regimes. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information with their foreign counterparts.
