Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data

PNR data are information collected by air carriers for commercial and operational purposes in providing air transportation services. PNR data contain different information, such as travel dates, travel itinerary, ticket information, contact details, the travel agent at which the flight was booked, means of payment used, seat number and baggage information. They are provided by the passengers. PNR data are unverified information that are not necessarily accurate, nor is the same information collected for each passenger.

General background

In recent times, PNR data are increasingly used by law enforcement authorities to combat serious crime and terrorism. At the European Union level, the European Commission presented a proposal on the use of Passenger Name Record data in February 2011 (COM(2011) 32 final) which is still subject to discussions between the co-legislators. In the current absence of EU legislation, a growing number of Member States are establishing national PNR systems on the basis of domestic law.

Ensuring the respect of fundamental rights

The collection, storage and processing of PNR data by law enforcement authorities has implications on fundamental rights enshrined in the EU Charter for Fundamental Rights as noted by the opinions to the proposed PNR directive submitted by FRA, the European Data Protection Supervisor (EDPS) and the Article 29 Working Party. Particularly relevant are in this context the right to respect for private life (Article 7), protection of personal data (Article 8), freedom to conduct a business (Article 16); and non-discrimination (Article 21). Processing of PNR data must comply with these rights which according to Article 52 (1) of the Charter can only be limited if this is necessary and proportional and if such limitation is provided by law, respect the essence of the rights and freedoms in question and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Benefit and scope of the operational guidance

In light of efforts by Member States to establish national PNR systems, FRA was requested by the European Commission to provide practical guidance relating to the processing of PNR data for law enforcement purposes. As a result, in informal consultation with European Commission services and the European Data Protection Supervisor (EDPS) and building on FRA's 2011 opinion on PNR, the following twelve considerations have been developed.

They constitute a list of "dos and don'ts" on how to operationalise fundamental rights when establishing national PNR systems. They contribute to promote compliance with fundamental rights. They are a living document to be regularly updated based on experience gathered over time.

The twelve fundamental rights considerations do not address the processing of PNR data by airlines and reservation systems' data controllers.

Limitations of the operational guidance

The twelve fundamental rights considerations are not comprehensive. They do not absolve Member States from their duty to comply with all applicable legal obligations, including those set forth in national law and the relevant EU acquis, and in particular with core data protection principles, including the principles of necessity and proportionality, the principle of lawful processing as well as the principle of purpose specification and limitation. Practitioners can find guidance on these principles in the Handbook on European data protection law published by FRA, the European Court of Human Rights and the Council of Europe in January 2014.

They are without prejudice to any future EU law developments in this area, including conclusions that the EU co-legislator may reach on the necessity and proportionality of processing PNR data for law enforcement purposes.

Cooperation with national data protection authorities

Authorities in charge of establishing national PNR systems should have satisfactory answers to questions, such as whether there is a national legal basis for the processing of PNR data, whether such legal basis covers the purpose pursued and whether the necessity of the system is justified.

In order to ensure full compliance with data protection requirements, authorities responsible for processing PNR data are encouraged to collaborate with national data protection authorities, consulting them at an early stage of the process, including to carry out an impact assessment of the data protection implications of establishing a national PNR system.

For each of the twelve fundamental rights considerations, this guidance offers specific advice.

Twelve fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data:

1. Use PNR data only to combat terrorism and serious transnational crimes
2. Limit access to the PNR database to a specialised unit
3. Do not request direct access to airlines' databases
4. Delete sensitive PNR data
5. Set strict security and traceability safeguards against abuse
6. Reduce likelihood of flagging false positives
7. Be transparent towards passengers
8. Allow persons to access and rectify their PNR data
9. Do not permit identification of data subjects or retention of data for longer than necessary
10. Transfer data extracted from PNR only to competent national public authorities
11. Only transfer data extracted from PNR to third countries under strict conditions
12. Carry out objective and transparent evaluation of the PNR system

1. Use PNR data only to combat terrorism and serious transnational crimes

PNR data should only be used for the prevention, detection, investigation and prosecution of terrorism as set out in Articles 1 to 4 of Council Framework Decision 2002/475/JHA, serious crimes as listed in Article 2 (2) of Council Framework Decision 2002/584/JHA which have a transnational nature as well as international crimes as defined in the Rome Statute of the International Criminal Court. A definition of terrorism and 'serious crime' is indispensable to ensure legal certainty. PNR data should not be processed for any other purpose (*e.g.* migration control).

The processing of PNR data should apply to flights departing from or going to a third country.

2. Limit access to the PNR database to a specialised unit

Access to the PNR database should be limited to national Passengers Information Units. Staff working in these units should be given the level of access to the data that is necessary to carry out their individual tasks (for example, analysts working only on drug-related crimes should not have access to the terrorism-related alerts). Analysis of PNR data should not be outsourced to private service providers.

Due to the sensitive character of PNR data processing Passengers Information Units should appoint a data protection officer with special expertise in the field of data protection for the internal supervision of data processing activities, without prejudice to the external independent supervision by national data protection authorities. Staff deployed to Passengers Information Units must offer guarantees in terms of competence, integrity and respect of fundamental rights. Prior to their assignment they should be trained on processing PNR data in compliance with fundamental rights, including data protection.

3. Do not request direct access to airlines' databases

PNR data should be actively transmitted by the airlines to Passenger Information Units (*push-method*), and not "pulled" by these units through direct access to the airlines' database. Transmission should be based on a clear and precise request which defines the receiving authority, the data elements to be transmitted and, where applicable, the categories of passengers and flights concerned. This is justified by the necessity to ensure that only authorised law enforcement authorities receive PNR data and that they only access the amount of data they are legally authorised to access. Besides, this *push method* allows airlines some control to ensure that they can verify compliance with their data protection obligations.

4. Delete sensitive PNR data

Sensitive PNR data revealing individual characteristics listed in Article 6 of the Council Framework Decision 2008/977/JHA, namely racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and data concerning health or sex life should not be processed by Passenger Information Units. To achieve this, the following should be undertaken:

- Upon receipt of the data and before any further processing, the Passenger Information Unit should filter out and remove automatically the following data from

the "General remarks" field of PNR, when this has not already been done by the airlines or reservation systems' data controller:

- Codes relating to food preferences[1]
- Codes relating to medical information[2]
- Certain codes relating to children[3]
- SSR code LANG relating to language(s) spoken.

- Specifically authorised staff within the Passenger Information Unit should verify if the above sensitive data have been removed and, if not, delete them completely and irrevocably. As a good practice, this should be complemented by running a matching and removal program with a regularly updated glossary of "sensitive terms" (e.g. *trade union*) over the database to detect and effectively delete non-standardised SSR codes as well as sensitive data hidden in free text.

- Before any manual processing of PNR data (e.g. in reaction to an alert based on automated processing) or any onward forwarding to third parties (see considerations 10 and 11), PNR data should be manually reviewed by the Passenger Information Unit to verify if they contain any sensitive information. Any remaining sensitive information should be removed before further processing. In doing this, pay particular attention to the following PNR fields, which may contain free text:

  - "Salutations" field (e.g. MR/MRS/MISS/MSTR/DR)
  - "General remarks" field
  - Field "All historical changes".

5. Set strict security and traceability safeguards against abuse

The PNR database must be separated from other databases. A comprehensive set of security rules, including logical measures such as authentication and multilayer access control, secured storage media, backup systems *etc.* should be in place in order to prevent accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any unlawful forms of processing.

Every access to PNR data by the Passenger Information Unit staff should be logged in a comprehensive audit trail. The log records should be available for internal and external monitoring purposes. They should contain all information necessary to reconstruct the operations performed on the data, e.g. the user name, the work location of the user, the date and the time of access, the content of the query, the number of records returned, the justification for accessing the database and any action taken. Modifications or deletions of data shall also be logged in a way that allows identifying the exact effect of the change in the data. Audit trails should be maintained at all levels that allow modification or access to the data. Automatic log analysis procedures should be in place.

The log record should be accessible to national data protection authorities who should be entitled to audit the work of the Passenger Information Unit on a regular basis.

As a good practice, internal control mechanism should include automated checks to identify unusual behaviour as well as well as sample random checks of processed PNR data.

[1] See list in annex 1.
[2] See list in annex 2.
[3] See list in annex 3.

Any breach of data security should be notified to national competent authorities and should be subject to effective, proportionate and dissuasive sanctions in accordance with national law. The competent national data protection authority should be informed without delay.

6. Reduce likelihood of flagging false positives

Sensitive data as defined in consideration 4 should never be used as assessment criteria or to run PNR data against watch lists.

Assessment criteria should be pre-defined, targeted, specific, proportionate and fact-based, *i.e.* based on experience and on criminal intelligence. Assessment criteria should be tested on anonymised samples. They should be subject to regular reviews by an internal auditor to determining whether the assessment rules remain justified for the specific crime they are aimed to combat.

Before transmitting to law enforcement authorities at border crossing points an alert based on the automated processing of PNR data, the Passenger Information Unit should manually review the PNR data in conjunction with other information to determine whether the passenger effectively poses a security risk and eliminate false positive results due, in particular, to homonyms.

Law enforcement authorities at border crossing points should provide feedback to the Passenger Information Unit on the action taken on the basis of the alert received, if any. Consideration should be given to allow law enforcement authorities at border crossing points discretion on what action to take following receipt of a PNR alert.

To ensure transparency and foreseeability, the list of databases against which PNR data may be run should be established in advance.

7. Be transparent towards passengers

Member States should set up a publicly available webpage as well as other effective information materials (such as leaflets and posters displayed in travel agencies, at airport counters and at border crossing points) – possibly in cooperation with data protection authorities – to provide accurate information to passengers on the collection, storage and processing of PNR data and on the applicable data protection principles and their rights,[4] especially on the redress mechanisms available to passengers under the laws of the Member State.[5] Similarly, airlines should be requested to be transparent and provide such information to passengers, preferably at the time of booking and at the time of check-in.

8. Allow persons to access and rectify their PNR data

Member States should ensure that Passenger Information Units and other authorities with access to PNR data provide an appropriate level of data protection. Without prejudice to restrictions laid down by national law, any person regardless of whether he/she is physically in the Member State or not should have the rights to

[4] Right of access and rights to rectification, erasure and blocking, as possibly restricted under the applicable national legal framework.

[5] See, for example, the following statements on the webpage by the Australian Customs and Border Protection Service at http://www.customs.gov.au/privacy/default.asp and http://www.customs.gov.au/webdata/resources/files/PNRPrivacyStatement.doc.

- access his/her PNR data (including when these have been masked out) and whether and to whom such data have been disclosed and be informed of any refusal or restriction of access;
- seek rectification of his/her PNR data, where the data are inaccurate and be informed whether his/her PNR data have been rectified or erased;
- effective administrative and judicial redress in case any of his/her data protection rights have been violated, including if access has been denied or inaccurate PNR data not rectified or erased; and
- compensation in case of damage as a result of unlawful processing or of any other violation of fundamental rights.

To make these rights effective, passengers who wish to lodge a complaint for having been subjected to an intervention at the border (*e.g.* second-line check) should receive information about the processing of data involved and, if this includes PNR data, of the possibility to request access to and rectification of such data.

9. Do not permit identification of data subjects or retention of data for longer than necessary

PNR data should be retained by the Passenger Information Unit for a period of maximum 30 days from when they were provided by the air carrier.

After that time PNR data should be pseudonimysed by masking out the following PNR elements: name, address and contact information, general remarks and any collected Advance Passenger Information. Pseudonimysed PNR data should be kept separately from active PNR data.

Pseudonimysed PNR data should only be accessible to a limited number of personnel of the Passenger Information Unit specifically authorised to carry out analysis of PNR data and develop assessment criteria.

Only the Head of the Passenger Information Unit should be able to permit access to data elements which have been masked out, when this is required to comply with formal requests submitted in the framework of specific investigations or to comply with data protection rules, *e.g.* in case of request of access by the data subject or by the data protection authority for auditing purposes.

Upon expiry of the data retention period established under national law, PNR data should be permanently deleted by the system. PNR data used in the context of specific criminal investigations or prosecutions may be kept by law enforcement and judicial authorities under the conditions allowed by national law.

10. Transfer data extracted from PNR only to competent national public authorities

Data extracted from PNR should only be shared on a case-by-case basis with competent national public authorities who have been legally authorised to access PNR data. A list of such authorities should be made public. It should only include national authorities with a mandate to combat terrorism and serious crimes, or the national data protection authorities.

Public authorities entitled to receive data extracted from the PNR database should establish a contact point to whom the Passenger Information Unit forwards such data. Correspondence by the Passenger Information Unit with such contact points should be traceable.

The transfer of PNR data to another EU Member State should be channelled through the respective national Passenger Information Units. Any transfer of PNR data to Europol and Eurojust must be done in accordance with their mandate and legal basis. Any onward transfer of received PNR data should be done in accordance with considerations 10 and 11.

11. Only transfer data extracted from PNR to third countries under strict conditions

Transfer of individual data extracted from PNR to third countries should only be allowed on a case-by-case basis and when it is necessary for the prevention, detection, investigation and prosecution of terrorism or serious international or transnational crime. Data should be exclusively shared with relevant national public authorities competent for the prevention, investigation, detection or prosecution of the aforementioned crimes.

Such data transfers should either occur in the framework of existing EU agreements ensuring an adequate level of data protection or, in their absence, be based on applicable bilateral or multilateral agreements or other written understandings that ensure an adequate level of data protection.

Before the transfer, the data protection officer of the Passenger Information Unit must be satisfied that the third country fulfils the conditions for data transfer required under national and EU law.

Transfer of PNR data to the country of origin of persons who have requested or who were found to be in need of international protection must be prohibited.

12. Carry out objective and transparent evaluation of the PNR system

The PNR system should be subject to regular reviews. Based on collected statistics, the necessity and proportionality of processing PNR data should be assessed, ideally after one or maximum two years of operation. The PNR system should be reviewed or adapted based on the results of such assessment. Evaluation results should be made public.

In order to assess the efficiency of the PNR system and to monitor whether persons are flagged by the system as "false positives" appropriate statistics and other evidence should be collected from the outset. This evidence should at least include:

- number of persons whose PNR data were collected;
- number of persons whose PNR data were transferred to competent national public authorities (see consideration 10);
- number of criminal proceedings started on the basis of PNR data (among others) and number of convictions broken down by type of crime;
- number of persons flagged as "false positives", broken down by type of crime.

Vienna, February 2014

Annex 1: Special Service Requirement (SSR) codes relating to food preferences

SSR Code	Definition/Description	Free Text in Request
AVML	Vegetarian Hindu Meal	Not permitted
BBML	Baby Meal	Not permitted
BLML	Bland Meal – Bland/Soft Meal	Not permitted
CHML	Child Meal	Optional
DBML	Diabetic Meal	Not permitted
FPML	Fruit Platter Meal	Not permitted
GFML	Gluten Intolerant Meal	Not permitted
HNML	Hindu Meal	Not permitted
KSML	Kosher Meal	Not permitted
LCML	Low Calorie Meal	Not permitted
LFML	Low Fat Meal	Not permitted
LSML	Low Salt Meal	Not permitted
MOML	Moslem Meal	Not permitted
NLML	Low Lactose Meal	Not permitted
RVML	Vegetarian Raw Meal	Not permitted
SFML	Sea Food Meal	Not permitted
SPML	Special Meal	Mandatory
VGML	Vegetarian Vegan Meal	Not permitted
VJML	Vegetarian Jain Meal	Not permitted
VLML	Vegetarian Lacto – Ovo Meal	Not permitted
VOML	Vegetarian Oriental Meal	Not permitted

Annex 2: Special Service Requirement (SSR) codes relating to medical information

SSR Code	Definition/Description	Free Text in Request
BLND	Blind passenger	Optional
DEAF	Deaf passenger	Optional
DPNA	Disabled Passenger with intellectual or developmental disability needing assistance.	Mandatory
MAAS	Meet And Assist	Mandatory
MEDA	Medical Case	*Not available*
WCBD	Wheelchair – dry cell battery to be transported by a passenger which may require advance notification/preparation/ (dis)assembly	Optional
WCBW	Wheelchair – wet cell battery to be transported by a passenger. May require advance notification/preparation/ (dis)assembly	Optional
WCHC	Wheelchair – C for Cabin seat	Optional
WCHR	Wheelchair – R for Ramp	Optional
WCHS	Wheelchair – S for Steps	Optional
WCMP	Wheelchair – manual power to be transported by a passenger	Optional
WCOB	On Board Wheelchair	Optional

Annex 3: Special Service Requirement (SSR) codes relating to children

SSR Code	Definition/Description	Free Text in Request
BSCT	Bassinet/Carry cot/Baby Basket	Not permitted
EXST	Extra seat	Mandatory
INFT	Infant SSR Code	Mandatory