COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 24 June / juin 2016 T-PD(2016)12Mos

THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD)

Compilation of comments received

Draft Opinion on the Data protection implications of the processing of Passenger Name Records

****

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL (T-PD)

Compilation des commentaires reçus

Projet d'avis relatif aux dossiers passagers (PNR)

Directorate General / Direction Générale
Human Rights and Rule of Law / Droits de l'Homme et Etat de droit

TABLE / INDEX

AUSTRIA / AUTRICHE

Preliminary remarks: PNR are currently under scrutiny by the ECJ, Case Avis 1/15; the opinion of the Advocate General is scheduled for 8 September 2016; the decision of the ECJ might influence this draft opinion.

The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS n°108, hereinafter referred to as 'Convention 108'),

Recalling the European Convention on Human Rights (ECHR) and in particular Articles 8 (right to respect for private life) and 13 (right to an effective remedy), as further elaborated by the jurisprudence of the European Court of Human Rights and Article 2 (freedom of movement) of Protocol No. 4,

Having regard to Convention 108 and other relevant Council of Europe instruments in the field of data protection such as Recommendation (87)15 regulating the use of personal data in the police sector and Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling,

Noting the rapid spread at global level of information technology systems and legislations concerning the transmission by air carriers of personal data of their passengers to public authorities for law enforcement and national security purposes,

Resolved to support respect for human rights with regard to the processing of personal data of air transport by public authorities responsible for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes,

Adopted the present opinion:

1. Introduction

The 32nd Plenary meeting (1-3 July 2015) of the Consultative Committee of Convention 108 decided, in light of the growing concerns raised by reactions to the recent terrorist attacks and threats, to prepare the present opinion, having notably considered the issues addressed in the report "Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards"[1].

The Bureau of the Committee, during its 36th (6-8 October 2015), 37th (9-11 December 2015) and 38th meetings (22-24 March 2016) worked on the preparation of the Opinion, which was

[1] Report prepared by Mr D. Korff with the contribution of Ms M. Georges: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

examined by the 33rd Plenary meeting of the Committee of Convention 108 after written consultation of the delegations and interested stakeholders.

The Committee of Convention 108 understands that, in the recent context of accrued menace of terrorist attacks, the fight against terrorism must be reinforced. It underlines the importance of combating terrorism efficiently and effectively while ensuring respect for human rights, the rule of law and the common values upheld by the Council of Europe. The Committee notes the willingness of governments to establish systems allowing the screening of personal data of air passengers as one of the means to prevent terrorism and other serious crimes, as an element of their efforts to improve security. In this context, the Committee considers it necessary to recall the data protection principles that are applicable to such systems, underlining that the interference with human rights, including the right to the protection of private life and to the protection of personal data can only occur when the necessary conditions have been fulfilled.

Article 8 of the ECHR and Article 9 of Convention 108 have set the conditions that must be respected when a limitation to the rights to private life and data protection is considered. Such a limitation must be in accordance with a clear law and must be necessary in a democratic society for a legitimate aim (such as national security, public safety or the prevention of crime).

2. The system

Several types of passenger data exist and for the purposes of the present opinion, the Committee will focus on Passenger Name Records (PNRs).

PNRs are records used in the air transport industry for commercial and operational purposes in providing air transportation services. The PNRs are created by airlines and travel agencies[2], relating to travel bookings in order to enable an exchange of information between them and in accordance with the passengers' requests. Such records are captured in many ways as the reservations[3] can be created in Global Distribution Systems (GDS), computer reservation systems (CRS), or the airline's own reservation system. Data fed into an airline's departure control system (DCS) upon check-in by the passenger (i.e. seat and baggage information) can also be added automatically to an existing PNR when the CRS and DCS are integrated in a single system.

[2] In the future, "non-carriers economic operators" (i.e. travel agencies and tour operators) may be obliged to provide PNR data to the national competent authorities.

[3] Among global reservations systems, Amadeus is the only one located in Europe, with Headquarters in Spain, its Data Centre in Germany and its Research and Development Centre in France. It is owned and used notably by Air France, Iberia Airlines, Lufthansa, British airways and Scandinavian airlines and over 60 other carriers across the globe are affiliated to it.

Although PNRs were originally introduced for air travel, CRS can now also be used for bookings of hotels, car rental, boat and train trips.

The format and content of a PNR, due to the common needs of multiple actors, has been progressively harmonised and standardised by the International Air Transport Association (IATA) which provides support in the design of passenger data programs.

The PNR information is collected from passengers and contains part or whole of the following items:

- Full name
- address and contact information (phone number, e-mail address, IP address)
- type of travel document and number
- date of birth
- nationality
- country of residence
- travel itinerary of at least one segment (complete for specific PNR)
- address for the first night spent in the country of destination
- method of payment used, including billing address and credit card details
- frequent flyer data and benefits (free upgrade or ticket)
- an open field with general remarks ("Special Service Request", "Optional Services Instruction" or "Other Service Information") such as all available information on unaccompanied minors, dietary and medical requirements, seating preferences, languages, details of disability, and other similar requests.
- an individual reference (PNR record locator code)
- information on the travel agency/travel agent
- ticket information (number, date of reservation, date of issuance, one-way tickets)
- fare details and the restrictions possibly applying to this fare (and related taxes)
- names and number of other passengers travelling together on the PNR
- travel status of passengers, including confirmations, check-in status, 'no show' or 'go show' information;
- seat number and other seating information
- code share information
- split/divided information (where the itineraries of several passengers under a PNR are not similar and changes must be brought to the booking for one passenger of an existing PNR)
- baggage information
- historic of all changes to PNR information listed above.

In practice, the content of each existing PNR will greatly vary as the number and nature of fields to complete will depend on the itinerary (travel to the USA? roundtrip itinerary covering several towns in a same country or in several countries?), the offer of services by airlines and the reservation system used (over 60 fields to be completed for some of them).

The fact that the information collected is provided by passengers, or by others on their behalf and that such information is not checked, is also an important aspect of the system which needs to be underlined and taken into account as far as the principle of data accuracy is concerned. There is the potential for error: a PNR may contain incorrect information about an individual, which could, in some circumstances, raise suspicion.

Two different methods of transmission of the data from the commercial sector to the competent authorities of the public sector exist:

- the 'pull' method whereby public authorities directly reach into ('access') the reservation system and extract ("pull") a copy of the required data from it;

- the 'push' whereby the operator transmits ('pushes') the required PNR data into the database of the authority requesting them.

3. Legality

While PNRs can be of benefit to the competent public authorities in combatting terrorism and other serious crimes, a number of conditions have to be met in order for the interference with the rights to private life and data protection to be permissible.

Pursuant to the case-law of the European Court of Human Rights relating to Article 8 of the ECHR such interference is only permissible where it is in accordance with the law and is strictly necessary and proportionate to the legitimate aim pursued.

While the assessment of the necessity of the interference, and the proportionality of the measures considered, have to be carefully examined in light of various elements, the Committee will briefly recall what the ECHR considers to be covered by the condition of legality. The requirement that any interference be 'in accordance with the law' (or 'provided for by the law' as prescribed in Article 9 of Convention 108) will only be met when three conditions are satisfied:

- the measure must have some basis in domestic law,
- this law must be clear and precise enough to be accessible to the person concerned (it must obviously be public), and
- have foreseeable consequences (enabling the person, if need be with appropriate

advice, to regulate her or his conduct and act accordingly)[4].

In the context of processing of PNRs by law enforcement authorities, the criterion of the quality of the law implies a very precise and strict definition of the legitimate aim pursued (for instance, no open formulation in the definition of a serious crime can be allowed and examples of what is considered as such – for instance the fight against drug trafficking, human trafficking or child trafficking – are to be spelt out clearly).

4. Necessity and proportionality

Any prescribed or envisaged measures on processing PNR data by the competent public authorities, in light of the interference that they may entail with the rights of the data subjects, must be subject to scrutiny of their necessity and proportionality. The Committee calls for the examination of objective elements enabling to assess such necessity, the proportionality of the measures prescribed as well as the efficiency and effectivity of the system (which should be demonstrable where such systems already exist).

The envisaged processing of PNR data is the general and indiscriminate screening of all passengers by different competent authorities, including individuals who are not suspected of any crime, and concerns data initially collected for commercial purposes by private entities. In light of the degree of interference with the rights to private life and data protection that would arise from such processing, the fact that this processing is a necessary measure in a democratic society for the fight against terrorism and other serious crimes has to be clearly evidenced and the appropriate safeguards must be put in place. A specific demonstration of the necessity is needed for the collection and further use of PNR data. The apparent legitimacy of the aim pursued (preventing, detecting, investigating and prosecuting terrorist offences and other serious crimes) is not sufficient as it appears to be too broad.

The European Court of Human Rights underlined that "while the adjective 'necessary' […] is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'."[5]

While the State has a margin of appreciation in choosing the necessary means to achieve its legitimate and necessary aim, it must assess whether the interference created by such measures corresponds to a 'pressing social need'[6]. The assessment of the proportionality of the

[4] ECHR Kennedy v. the United Kingdom, § 151; Rotaru v. Romania, 28341/95, §§50, 52 and 55; Amann v. Switzerland, § 50; Iordachi and Others v. Moldova; Kruslin v. France, § 27; Huvig v. France, § 26; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, § 71; Liberty and Others v. the United Kingdom, § 59, etc.

[5] Handyside v. UK, 5493/72, §48.

[6] Olsson v. Sweden, 10465/83.

derogation needs to be based on the examination of a wide variety of element such as the definition of clear and limited purposes, of the scope of application of the system, of the nature of the data concerned, its length of conservation, etc.

Deciding on the validity of the Data Retention Directive (regarding the retention of communication data), the Court of Justice of the European Union underlined[7] that "the derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".

In case of existing systems of processing of PNR data, greater transparency on the assessment of the efficacy of such systems should be sought with a view to enabling a sound independent assessment of the necessity of the system. For instance, objective and quantifiable information regarding terrorist threats which could be avoided, other deterrent effects, the modification of criminals' behaviours (e.g. abandoning originally intended criminal acts), the likelihood of substantially increased costs and difficulty of perpetrating crimes (like terrorist attacks) would help inform an assessment as to whether such a PNR system is necessary.

A regular review at periodic intervals of the necessity of the PNR system to pursue its appropriate justification in time should be carried out.

5. Principles and safeguards

(a) Scope of application

The scope of application of the processing of PNR data must be clearly and precisely defined in order to guarantee the proportionality of the interference with the rights of the persons concerned. This notably applies to the competent authorities receiving the data, the type of data processed, and the length of conservation of the data.

Regarding the recipient authorities, national ones in particular, the establishment of dedicated coordination units (such as the proposed 'Passengers Information Units' in the proposed EU scheme) contributes to preventing a mix between judicial and surveillance activities but the competencies of such units need to be strictly and narrowly defined and made public.

The transmission and further dissemination of data to the public authorities need to be relevant, adequate and proportionate (Article 5 of Convention 108) to the purposes for which they are processed. The transmitted data must be clearly defined (the elements of the PNR that are to be transmitted must be exhaustively listed), on the basis of objective criteria, and limits to the subsequent use of such data must also be established. Competent national authorities legally authorised to process PNR data should be listed and that information should be made public.

The period of retention of the PNR data must also be clearly specified and limited to what is justified by objective criteria as it must be "based on objective criteria in order to ensure that it is

[7] Digital Rights Ireland, C-293/12 of 8 April 2014, §52.

limited to what is necessary"[8]. Masking out some elements of the data after a certain period of time can mitigate the risks entailed by a longer period of conservation of the data but it should be recalled that masked out data still permits identification of the individuals and continues as such to constitute personal data.

(b) Purpose limitation

In light of the severity of the interference with the rights to private life and data protection, pose by the processing of PNR data by competent public authorities the purposes need to be clearly and precisely predefined on the basis of objective criteria which limit the transmission of the data only to the competent authorities as well as the further use of such data. The PNR can, in no circumstances, be used beyond these purposes (where it is the case, sanctions must be provided).

PNR systems are generally justified on the basis of the prevention, detection, investigation and prosecution of terrorist offences and other serious crimes and a clear delimitation of those key notions is needed in order to strictly circumscribe the use of such systems.

The definition of 'terrorism' and 'terrorist offences' is of particular complexity (see the relevant UN Conventions, the Council of Europe Convention on the prevention of terrorism of 2005 and its 2015 additional protocol). In the absence of a clear definition, this terminology should be restrictively construed. Should that not be the case, the purpose of the PNR system would remain too vague and the principle of proportionality would not be respected.

The crimes for which PNR data can be used and shared should be strictly limited, clearly defined and particularly serious (for instance, crimes against humanity, torture, or genocide). Any use that is not prescribed by the law establishing a PNR system should be expressly prohibited and the use of any evidence obtained in violation of this law should not be admissible in court.

(c) Data transmission

As regards the transmission of the data from the commercial sector to the competent authorities of the public sector, the Committee considers that the 'push' method, with the operator being fully responsible for the quality of the data and the conditions of transmission, is to be preferred as it offers greater data protection safeguards than the 'pull' one. These guarantees should however not be circumvented by a system whereby all passengers data are systematically sent in an automated way, which would make it eventually similar to a pull system.

The Committee recommends that an initial short period of retention of the PNR be defined, which could be renewed on the basis of a case-by-case examination of the request and its justification by an independent authority. In case of suspicion, the data could be retained for

[8] Digital Rights Ireland, C-293/12 of 8 April 2014 §64.

longer as it may be necessary in the context of legal proceedings (if the suspicion is lifted, the data should be deleted).

(d) Data mining and matching

The processing of personal data concerns all passengers and may not be limited to the collection of data of targeted individuals suspected of involvement in a criminal offence or posing an immediate threat to national security or public order. Instead, the data is processed in order to also be able to identify the persons in contact with potential suspects ('contact chaining') or threats, and anyone who "might" be involved in, or who "might become" involved in the criminal activities defined by the law establishing the sharing of PNRs with the competent authorities.

The data analysis aims to detect 'unknown persons' on the basis of pre-determined criteria and match known suspects against other data sets.

Assessing passengers on the basis of PNRs raises the question of predictability of the measure (the screening is carried out on the basis of predictive algorithms using dynamic criteria which may constantly evolve) and, where the data is linked to other datasets available to the competent authorities, the compatibility of such data matching with the principle of purpose limitation is to be questioned (sole use of datasets created for law enforcement purposes) and the precise subject of 'identification' defined (is the identification aimed at matching an actual suspected or convicted individual or rather at rating the passengers on a risk-scale?) in a manner that complies with the requirement of foreseeability.

The development of data mining and matching algorithms should be based on the results of an assessment of the likely impact of the data processing on the rights and fundamental freedoms of data subjects.

The basic structure of the analyses should be transparent and the matching of different datasets should only be made on the basis of predefined risk indicators which are both sufficiently high and have been clearly identified in advance in relation to an ongoing investigation and only for a predefined period (list of convicted persons for serious crimes, list of persons under investigation for suspicion of terrorist activities).

The results of such automatic assessments of individuals should be carefully examined on a case-by-case basis, by a person in a non-automated manner and the reasoning of the processing should be made known to the data subject objecting to it.

For the purpose of matching, data should flow to the PNR system, but not from the PNR system to other databases. Matching should only be possible when a hit occurs based on sufficiently elevated risk score associated with an incoming data.

(e) Prohibition of the systematic use of sensitive data

While PNRs should only contain information that is needed to facilitate a passenger's travel, a number of sensitive data which would serve to indicate racial origin, political opinions or religious or other beliefs or data relating to a person's health or sexual orientation may be included in the PNR, not only under the 'coded' data but also under the open field containing general remarks (such as dietary or medical requirements, or the fact that a political association benefited from reduced fares for the travel of its members) which could lead to direct discrimination.

While the competent authorities receiving such data in the PNRs are not allowed to process it (no assessment can be run on the basis of a criteria linked to any sensitive data) and must therefore mask or delete it, the Committee considers that a clear prohibition of the systematic use of such sensitive data should be established, implying there should be an obligation on the competent public authorities to mask or erase this type of data.

(f) Rights of information, access, rectification and deletion

The Committee recalls that according to Article 1 of both the ECHR and Convention 108, the rights to privacy and data protection have to be secured for every individual within the jurisdiction respectively in the territory of the contracting Parties, irrespective of her or his nationality or residence.

Comment [SM1]: Art. 1 of Convention 108 speaks of "territory" and not of "jurisdiction"

The person whose PNR data is being shared with the competent authorities is entitled to know what happens with her or his data (what type of data, for which purpose, for how long, processed by whom, transmitted to whom), has a right of access and to ask for rectification or deletion of personal data. While such rights can be limited under the restrictive conditions previously mentioned (where it is in accordance with the law and necessary in the interest of a legitimate aim), the Committee recommends that persons who are not suspected of having committed, or being about to commit, a terrorist offence or other serious crime enjoy the full exercise of those rights. Persons who are suspected of having committed, or being about to commit such offences may at least request the correction of inaccurate data and the deletion of unlawful data. If such persons are removed from suspicion, they should be able to exercise their full rights of access, rectification or deletion of personal data.

Any limitation of those rights must be made known to passengers at the time of collection of their data and during the whole processing activity by the competent public authorities.

Where data concerning a passenger have been collected without her or his knowledge, and unless the data are deleted, that person should be informed, where practicable, that information is held about her or him as soon as the object of the purpose for collection is no longer likely to be prejudiced. The persons concerned should also be informed on how to exercise their rights and what remedies are available.

(g) Security

As required by Article 7 of Convention 108, appropriate security measures shall be taken for the protection of personal data. This notably implies that the PNR system shall be held in a secure physical environment, with high-level intrusion controls and a strict access (to a limited number of persons) control (such as layered logins and the production of an audit record of access). Furthermore, communication of the PNR data to the competent authorities must be protected by technical and procedural means (strong cryptography, effective procedures for managing keys, etc).

(h) Transborder Data flows

In light of the international nature of PNRs systems (where data will not be flowing transborder in the communication phase between the reservation system and the competent authorities it may simply flow at the sole level of the reservation system as several of them are not based in Europe while the passengers are), the Committee recalls that to be legal, such transfers to States, where the PNR data is stored or transferred, that are not Parties to Convention 108 must satisfy the conditions established to guarantee the appropriate protection of data subjects.

(i) Remedies

It is an essential requirement of the case law of the European Court of Human Rights that "effective remedies" against violations of fundamental rights exist and be available to individuals (and not solely to nationals of the particular country concerned). While the Court of Justice of the European Union expressly mentions the requirement for redress before a tribunal, the European Court of Human Rights ruled[9] that the absence of judicial control does not necessarily constitute a violation of the rights at stake as long as other strong safeguards are provided for by the legislation (for instance independent oversight by authorities vested with sufficient powers and competence to exercise an effective and continuous control).

Article 10 of Convention 108 requires that Parties "establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection" set out in the Convention.

The Committee highlights the importance, as a pre-condition to an effective remedy, for the person concerned to be fully informed regarding the processing of her or his personal data and underlines the difficulties which exist in providing effective remedies against algorithm-based decisions and challenging inferences based on data analysis (false positives and other discriminatory measures).

[9] Klass and Others v. Germany, §§ 55-56; Kennedy v. the United Kingdom, § 167.

(j) Oversight and transparency

It is clear from the case law of the European Court of Human Rights that the oversight of the authorities responsible for surveillance should be performed by an independent and external body.

The Committee underlines the role of the competent data protection authorities, which should not only be consulted in the normative process of adoption of the related laws and regulations but could also assess the compliance of a PNR system with data protection rules on the basis of individual complaints that they could receive, or on their own initiative.

Other specialised independent authorities (such as a parliamentary commission) in charge of overseeing law enforcement and intelligence agencies also have a role in controlling the scope of application of the system, its efficiency and perform case-by-case controls regarding the rationale of the retention of the passenger's data and the duration of this retention.

Supervision by independent data protection authorities, by specialised independent authorities in charge of overseeing law enforcement and intelligence agencies, as well as through independent assessments of the efficiency by the competent authorities themselves could lead to greater transparency and accountability of the powers and competencies of a PNR system.

Dedicated data protection officers should be designated within the competent authorities processing PNR data with a view to ensuring compliance and accountability of the system (with a regular evaluation of the risks at stake and systematic audits of the PNR), the data processing and communication of the data, its updating and deletion, as well as the information provided to passengers. Data protection officers could also have a role as contact points in case of complaints or requests by the persons concerned. They are encouraged to raise awareness on "good practices".

6. Conclusions

In view of the special interference with the rights to data protection and privacy that PNR measures may represent, the legality, proportionality and necessity of a PNR system need to be strictly respected and demonstrated, thus implying notably the following:

- transparent demonstration in a measurable form of the necessity and proportionality of the system in light of the legitimate aim pursued;

- accurate and strict definitions of the legitimate aim pursued are required and PNR data is only allowed for the defined limited grounds (prevention, detection, investigation and prosecution of terrorist offences and other serious crimes);

- transparent assessment of the efficacy of the PNR system;

- publicity of the competent public authorities (ideally dedicated coordination units);

- transmission of data via ‘push method’ with a clear definition of the initial retention period and appropriate security measures;

- prohibition of the systematic use of sensitive data;

- limitation of the data mining to risk indicators sufficiently high and clearly identified in relation to an ongoing investigation and for a predefined period, with case-by-case examination of the results in a non-automatic manner;

- legal and necessary limitations only to the rights of information, access, rectification and deletion of the individuals;

- competence of the data protection authorities (to be consulted and able to assess the PNR system as well as to deal with individual complaints);

- availability of effective remedies for the individuals;

- independent and external oversight of the PNR system;

- periodic review of the PNR systems by the competent authorities.

BELGIUM / BELGIQUE

The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS n°108, hereinafter referred to as 'Convention 108'),

Recalling the European Convention on Human Rights (ECHR) and in particular Articles 8 (right to respect for private life) and 13 (right to an effective remedy), as further elaborated by the jurisprudence of the European Court of Human Rights and Article 2 (freedom of movement) of Protocol No. 4,

Having regard to Convention 108 and other relevant Council of Europe instruments in the field of data protection such as Recommendation (87)15 regulating the use of personal data in the police sector and Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling,

Noting the rapid spread at global level of information technology systems and legislations concerning the transmission by air carriers of personal data of their passengers to public authorities for law enforcement and national security purposes,

Resolved to support respect for human rights with regard to the processing of personal data of air transport by public authorities responsible for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes,

Adopted the present opinion:

1. Introduction

The 32nd Plenary meeting (1-3 July 2015) of the Consultative Committee of Convention 108 decided, in light of the growing concerns raised by reactions to the recent terrorist attacks and threats, to prepare the present opinion, having notably considered the issues addressed in the report "Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards"[10].

The Bureau of the Committee, during its 36th (6-8 October 2015), 37th (9-11 December 2015) and 38th meetings (22-24 March 2016) worked on the preparation of the Opinion, which was examined by the 33rd Plenary meeting of the Committee of Convention 108 after written consultation of the delegations and interested stakeholders.

The Committee of Convention 108 understands that, in the recent context of accrued menace of terrorist attacks, the fight against terrorism must be reinforced. It underlines the importance of

[10] Report prepared by Mr D. Korff with the contribution of Ms M. Georges: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

combating terrorism efficiently and effectively while ensuring respect for human rights, the rule of law and the common values upheld by the Council of Europe. The Committee notes the willingness of governments to establish systems allowing the screening of personal data of air passengers as one of the means to prevent terrorism and other serious crimes, as an element of their efforts to improve security. In this context, the Committee considers it necessary to recall the data protection principles that are applicable to such systems, underlining that the interference with human rights, including the right to the protection of private life and to the protection of personal data can only occur when the necessary conditions have been fulfilled.

Comment [GC2]: PNR also includes advanced passenger information (e.g. number of seat), so not only 'personal data'

Article 8 of the ECHR and Article 9 of Convention 108 have set the conditions that must be respected when a limitation to the rights to private life and data protection is considered. Such a limitation must be in accordance with a clear law and must be necessary in a democratic society for a legitimate aim (such as national security, public safety or the prevention of crime).

2. The system

Several types of passenger data exist and for the purposes of the present opinion, the Committee will focus on Passenger Name Records (PNRs).

PNRs are records used in the air transport industry for commercial and operational purposes in providing air transportation services. The PNRs are created by airlines and travel agencies[11], relating to travel bookings in order to enable an exchange of information between them and in accordance with the passengers' requests. Such records are captured in many ways as the reservations[12] can be created in Global Distribution Systems (GDS), computer reservation systems (CRS), or the airline's own reservation system. Data fed into an airline's departure control system (DCS) upon check-in by the passenger (i.e. seat and baggage information) can also be added automatically to an existing PNR when the CRS and DCS are integrated in a single system.

Although PNRs were originally introduced for air travel, CRS can now also be used for bookings of hotels, car rental, boat and train trips.

[11] In the future, "non-carriers economic operators" (i.e. travel agencies and tour operators) may be obliged to provide PNR data to the national competent authorities.

[12] Among global reservations systems, Amadeus is the only one located in Europe, with Headquarters in Spain, its Data Centre in Germany and its Research and Development Centre in France. It is owned and used notably by Air France, Iberia Airlines, Lufthansa, British airways and Scandinavian airlines and over 60 other carriers across the globe are affiliated to it.

The format and content of a PNR, due to the common needs of multiple actors, has been progressively harmonised and standardised by the International Air Transport Association (IATA) which provides support in the design of passenger data programs.

Comment [GC3]: But still deem to be very diverse.

The PNR information is collected from passengers and contains part or whole of the following items:

- Full name
- address and contact information (phone number, e-mail address, IP address)
- type of travel document and number
- date of birth
- nationality
- country of residence
- travel itinerary of at least one segment (complete for specific PNR)
- address for the first night spent in the country of destination
- method of payment used, including billing address and credit card details
- frequent flyer data and benefits (free upgrade or ticket)
- an open field with general remarks (“Special Service Request”, "Optional Services Instruction" or "Other Service Information”) such as all available information on unaccompanied minors, dietary and medical requirements, seating preferences, languages, details of disability, and other similar requests.
- an individual reference (PNR record locator code)
- information on the travel agency/travel agent
- ticket information (number, date of reservation, date of issuance, one-way tickets)
- fare details and the restrictions possibly applying to this fare (and related taxes)
- names and number of other passengers travelling together on the PNR
- travel status of passengers, including confirmations, check-in status, ‘no show’ or ‘go show’ information;
- seat number and other seating information
- code share information
- split/divided information (where the itineraries of several passengers under a PNR are not similar and changes must be brought to the booking for one passenger of an existing PNR)
- baggage information
- historic of all changes to PNR information listed above.

In practice, the content of each existing PNR will greatly vary as the number and nature of fields to complete will depend on the itinerary (travel to the USA? roundtrip itinerary covering several towns in a same country or in several countries?), the offer of services by airlines and the reservation system used (over 60 fields to be completed for some of them).

The fact that the information collected is provided by passengers, or by others on their behalf and that such information is not checked, is also an important aspect of the system which needs

to be underlined and taken into account as far as the principle of data accuracy is concerned. There is the potential for error: a PNR may contain incorrect information about an individual, which could, in some circumstances, raise suspicion.

Two different methods of transmission of the data from the commercial sector to the competent authorities of the public sector exist:

- the 'pull' method whereby public authorities directly reach into ('access') the reservation system and extract ("pull") a copy of the required data from it;

- the 'push' whereby the operator transmits ('pushes') the required PNR data into the database of the authority requesting them.

Comment [GC4]: Most MS, as BE, will choose for the push option.

3. Legality

While PNRs can be of benefit to the competent public authorities in combatting terrorism and other serious crimes, a number of conditions have to be met in order for the interference with the rights to private life and data protection to be permissible.

Pursuant to the case-law of the European Court of Human Rights relating to Article 8 of the ECHR such interference is only permissible where it is in accordance with the law and is strictly necessary and proportionate to the legitimate aim pursued.

While the assessment of the necessity of the interference, and the proportionality of the measures considered, have to be carefully examined in light of various elements, the Committee will briefly recall what the ECHR considers to be covered by the condition of legality. The requirement that any interference be 'in accordance with the law' (or 'provided for by the law' as prescribed in Article 9 of Convention 108) will only be met when three conditions are satisfied:

- the measure must have some basis in domestic law,
- this law must be clear and precise enough to be accessible to the person concerned (it must obviously be public), and
- have foreseeable consequences (enabling the person, if need be with appropriate advice, to regulate her or his conduct and act accordingly)[13].

[13] ECHR Kennedy v. the United Kingdom, § 151; Rotaru v. Romania, 28341/95, §§50, 52 and 55; Amann v. Switzerland, § 50; Iordachi and Others v. Moldova; Kruslin v. France, § 27; Huvig v. France, § 26;

In the context of processing of PNRs by law enforcement authorities, the criterion of the quality of the law implies a very precise and strict definition of the legitimate aim pursued (for instance, no open formulation in the definition of a serious crime can be allowed and examples of what is considered as such – for instance the fight against drug trafficking, human trafficking or child trafficking – are to be spelt out clearly).

Comment [GC5]: This is the case in the BE draft law where a specific list has been drafted, in line with the EU directive.

4. Necessity and proportionality

Any prescribed or envisaged measures on processing PNR data by the competent public authorities, in light of the interference that they may entail with the rights of the data subjects, must be subject to scrutiny of their necessity and proportionality. The Committee calls for the examination of objective elements enabling to assess such necessity, the proportionality of the measures prescribed as well as the efficiency and effectivity of the system (which should be demonstrable where such systems already exist).

The envisaged processing of PNR data is the general and indiscriminate screening of all passengers by different competent authorities, including individuals who are not suspected of any crime, and concerns data initially collected for commercial purposes by private entities. In light of the degree of interference with the rights to private life and data protection that would arise from such processing, the fact that this processing is a necessary measure in a democratic society for the fight against terrorism and other serious crimes has to be clearly evidenced and the appropriate safeguards must be put in place. A specific demonstration of the necessity is needed for the collection and further use of PNR data. The apparent legitimacy of the aim pursued (preventing, detecting, investigating and prosecuting terrorist offences and other serious crimes) is not sufficient as it appears to be too broad.

The European Court of Human Rights underlined that "while the adjective 'necessary' […] is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'."[14]

While the State has a margin of appreciation in choosing the necessary means to achieve its legitimate and necessary aim, it must assess whether the interference created by such measures corresponds to a 'pressing social need'[15]. The assessment of the proportionality of the derogation needs to be based on the examination of a wide variety of element such as the definition of clear and limited purposes, of the scope of application of the system, of the nature of the data concerned, its length of conservation, etc.

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, § 71; Liberty and Others v. the United Kingdom, § 59, etc.

[14] Handyside v. UK, 5493/72, §48.

[15] Olsson v. Sweden, 10465/83.

Deciding on the validity of the Data Retention Directive (regarding the retention of communication data), the Court of Justice of the European Union underlined[16] that "the derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".

In case of existing systems of processing of PNR data, greater transparency on the assessment of the efficacy of such systems should be sought with a view to enabling a sound independent assessment of the necessity of the system. For instance, objective and quantifiable information regarding terrorist threats which could be avoided, other deterrent effects, the modification of criminals' behaviours (e.g. abandoning originally intended criminal acts), the likelihood of substantially increased costs and difficulty of perpetrating crimes (like terrorist attacks) would help inform an assessment as to whether such a PNR system is necessary.

A regular review at periodic intervals of the necessity of the PNR system to pursue its appropriate justification in time should be carried out.

5. Principles and safeguards

(a) Scope of application

The scope of application of the processing of PNR data must be clearly and precisely defined in order to guarantee the proportionality of the interference with the rights of the persons concerned. This notably applies to the competent authorities receiving the data, the type of data processed, and the length of conservation of the data.

Regarding the recipient authorities, national ones in particular, the establishment of dedicated coordination units (such as the proposed 'Passengers Information Units' in the proposed EU scheme) contributes to preventing a mix between judicial and surveillance activities but the competencies of such units need to be strictly and narrowly defined and made public.

The transmission and further dissemination of data to the public authorities need to be relevant, adequate and proportionate (Article 5 of Convention 108) to the purposes for which they are processed. The transmitted data must be clearly defined (the elements of the PNR that are to be transmitted must be exhaustively listed), on the basis of objective criteria, and limits to the subsequent use of such data must also be established. Competent national authorities legally authorised to process PNR data should be listed and that information should be made public.

The period of retention of the PNR data must also be clearly specified and limited to what is justified by objective criteria as it must be "based on objective criteria in order to ensure that it is limited to what is necessary"[17]. Masking out some elements of the data after a certain period of time can mitigate the risks entailed by a longer period of conservation of the data but it should be recalled that masked out data still permits identification of the individuals and continues as such to constitute personal data.

[16] Digital Rights Ireland, C-293/12 of 8 April 2014, §52.

[17] Digital Rights Ireland, C-293/12 of 8 April 2014 §64.

(b) Purpose limitation

In light of the severity of the interference with the rights to private life and data protection, pose by the processing of PNR data by competent public authorities the purposes need to be clearly and precisely predefined on the basis of objective criteria which limit the transmission of the data only to the competent authorities as well as the further use of such data. The PNR can, in no circumstances, be used beyond these purposes (where it is the case, sanctions must be provided).

PNR systems are generally justified on the basis of the prevention, detection, investigation and prosecution of terrorist offences and other serious crimes and a clear delimitation of those key notions is needed in order to strictly circumscribe the use of such systems.

The definition of 'terrorism' and 'terrorist offences' is of particular complexity (see the relevant UN Conventions, the Council of Europe Convention on the prevention of terrorism of 2005 and its 2015 additional protocol). In the absence of a clear definition, this terminology should be restrictively construed. Should that not be the case, the purpose of the PNR system would remain too vague and the principle of proportionality would not be respected.

The crimes for which PNR data can be used and shared should be strictly limited, clearly defined and particularly serious (for instance, crimes against humanity, torture, or genocide). Any use that is not prescribed by the law establishing a PNR system should be expressly prohibited and the use of any evidence obtained in violation of this law should not be admissible in court.

(c) Data transmission

As regards the transmission of the data from the commercial sector to the competent authorities of the public sector, the Committee considers that the 'push' method, with the operator being fully responsible for the quality of the data and the conditions of transmission, is to be preferred as it offers greater data protection safeguards than the 'pull' one. These guarantees should however not be circumvented by a system whereby all passengers data are systematically sent in an automated way, which would make it eventually similar to a pull system.

Comment [GC6]: Directive and BE draft law forbid to keep other data as it has been described. If other data are sent in this systematically system, these have to be deleted.

The Committee recommends that an initial short period of retention of the PNR be defined, which could be renewed on the basis of a case-by-case examination of the request and its justification by an independent authority. In case of suspicion, the data could be retained for longer as it may be necessary in the context of legal proceedings (if the suspicion is lifted, the data should be deleted).

(d) Data mining and matching

The processing of personal data concerns all passengers and may not be limited to the collection of data of targeted individuals suspected of involvement in a criminal offence or posing an immediate threat to national security or public order. Instead, the data is processed in

order to also be able to identify the persons in contact with potential suspects ('contact chaining') or threats, and anyone who "might" be involved in, or who "might become" involved in the criminal activities defined by the law establishing the sharing of PNRs with the competent authorities.

The data analysis aims to detect 'unknown persons' on the basis of pre-determined criteria and match known suspects against other data sets.

Assessing passengers on the basis of PNRs raises the question of predictability of the measure (the screening is carried out on the basis of predictive algorithms using dynamic criteria which may constantly evolve) and, where the data is linked to other datasets available to the competent authorities, the compatibility of such data matching with the principle of purpose limitation is to be questioned (sole use of datasets created for law enforcement purposes) and the precise subject of 'identification' defined (is the identification aimed at matching an actual suspected or convicted individual or rather at rating the passengers on a risk-scale?) in a manner that complies with the requirement of foreseeability.

The development of data mining and matching algorithms should be based on the results of an assessment of the likely impact of the data processing on the rights and fundamental freedoms of data subjects.

The basic structure of the analyses should be transparent and the matching of different datasets should only be made on the basis of predefined risk indicators which are both sufficiently high and have been clearly identified in advance in relation to an ongoing investigation and only for a predefined period (list of convicted persons for serious crimes, list of persons under investigation for suspicion of terrorist activities).

The results of such automatic assessments of individuals should be carefully examined on a case-by-case basis, by a person in a non-automated manner and the reasoning of the processing should be made known to the data subject objecting to it.

For the purpose of matching, data should flow to the PNR system, but not from the PNR system to other databases. Matching should only be possible when a hit occurs based on sufficiently elevated risk score associated with an incoming data.

(e) Prohibition of the systematic use of sensitive data

While PNRs should only contain information that is needed to facilitate a passenger's travel, a number of sensitive data which would serve to indicate racial origin, political opinions or religious or other beliefs or data relating to a person's health or sexual orientation may be included in the PNR, not only under the 'coded' data but also under the open field containing general remarks (such as dietary or medical requirements, or the fact that a political association benefited from reduced fares for the travel of its members) which could lead to direct discrimination.

While the competent authorities receiving such data in the PNRs are not allowed to process it (no assessment can be run on the basis of a criteria linked to any sensitive data) and must

therefore mask or delete it, the Committee considers that a clear prohibition of the systematic use of such sensitive data should be established, implying there should be an obligation on the competent public authorities to mask or erase this type of data.

(f) Rights of information, access, rectification and deletion

The Committee recalls that according to Article 1 of both the ECHR and Convention 108, the rights to privacy and data protection have to be secured for every individual within the jurisdiction of the contracting Parties, irrespective of her or his nationality or residence.

The person whose PNR data is being shared with the competent authorities is entitled to know what happens with her or his data (what type of data, for which purpose, for how long, processed by whom, transmitted to whom), has a right of access and to ask for rectification or deletion of personal data. While such rights can be limited under the restrictive conditions previously mentioned (where it is in accordance with the law and necessary in the interest of a legitimate aim), the Committee recommends that persons who are not suspected of having committed, or being about to commit, a terrorist offence or other serious crime enjoy the full exercise of those rights. Persons who are suspected of having committed, or being about to commit such offences may at least request the correction of inaccurate data and the deletion of unlawful data. If such persons are removed from suspicion, they should be able to exercise their full rights of access, rectification or deletion of personal data.

Any limitation of those rights must be made known to passengers at the time of collection of their data and during the whole processing activity by the competent public authorities.

Where data concerning a passenger have been collected without her or his knowledge, and unless the data are deleted, that person should be informed, where practicable, that information is held about her or him as soon as the object of the purpose for collection is no longer likely to be prejudiced. The persons concerned should also be informed on how to exercise their rights and what remedies are available.

(g) Security

As required by Article 7 of Convention 108, appropriate security measures shall be taken for the protection of personal data. This notably implies that the PNR system shall be held in a secure physical environment, with high-level intrusion controls and a strict access (to a limited number of persons) control (such as layered logins and the production of an audit record of access). Furthermore, communication of the PNR data to the competent authorities must be protected by technical and procedural means (strong cryptography, effective procedures for managing keys, etc).

(h) Transborder Data flows

In light of the international nature of PNRs systems (where data will not be flowing transborder in the communication phase between the reservation system and the competent authorities it may simply flow at the sole level of the reservation system as several of them are not based in Europe while the passengers are), the Committee recalls that to be legal, such transfers to

States, where the PNR data is stored or transferred, that are not Parties to Convention 108 must satisfy the conditions established to guarantee the appropriate protection of data subjects.

(i) Remedies

It is an essential requirement of the case law of the European Court of Human Rights that "effective remedies" against violations of fundamental rights exist and be available to individuals (and not solely to nationals of the particular country concerned). While the Court of Justice of the European Union expressly mentions the requirement for redress before a tribunal, the European Court of Human Rights ruled[18] that the absence of judicial control does not necessarily constitute a violation of the rights at stake as long as other strong safeguards are provided for by the legislation (for instance independent oversight by authorities vested with sufficient powers and competence to exercise an effective and continuous control).

Article 10 of Convention 108 requires that Parties "establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection" set out in the Convention.

The Committee highlights the importance, as a pre-condition to an effective remedy, for the person concerned to be fully informed regarding the processing of her or his personal data and underlines the difficulties which exist in providing effective remedies against algorithm-based decisions and challenging inferences based on data analysis (false positives and other discriminatory measures).

(j) Oversight and transparency

It is clear from the case law of the European Court of Human Rights that the oversight of the authorities responsible for surveillance should be performed by an independent and external body.

The Committee underlines the role of the competent data protection authorities, which should not only be consulted in the normative process of adoption of the related laws and regulations but could also assess the compliance of a PNR system with data protection rules on the basis of individual complaints that they could receive, or on their own initiative.

Other specialised independent authorities (such as a parliamentary commission) in charge of overseeing law enforcement and intelligence agencies also have a role in controlling the scope of application of the system, its efficiency and perform case-by-case controls regarding the rationale of the retention of the passenger's data and the duration of this retention.

Supervision by independent data protection authorities, by specialised independent authorities in charge of overseeing law enforcement and intelligence agencies, as well as through

[18] Klass and Others v. Germany, §§ 55-56; Kennedy v. the United Kingdom, § 167.

independent assessments of the efficiency by the competent authorities themselves could lead to greater transparency and accountability of the powers and competencies of a PNR system.

Dedicated data protection officers should be designated within the competent authorities processing PNR data with a view to ensuring compliance and accountability of the system (with a regular evaluation of the risks at stake and systematic audits of the PNR), the data processing and communication of the data, its updating and deletion, as well as the information provided to passengers. Data protection officers could also have a role as contact points in case of complaints or requests by the persons concerned. They are encouraged to raise awareness on "good practices".

6. Conclusions

In view of the special interference with the rights to data protection and privacy that PNR measures may represent, the legality, proportionality and necessity of a PNR system need to be strictly respected and demonstrated, thus implying notably the following:

- transparent demonstration in a measurable form of the necessity and proportionality of the system in light of the legitimate aim pursued;

- accurate and strict definitions of the legitimate aim pursued are required and PNR data is only allowed for the defined limited grounds (prevention, detection, investigation and prosecution of terrorist offences and other serious crimes);

- transparent assessment of the efficacy of the PNR system;

- publicity of the competent public authorities (ideally dedicated coordination units);

- transmission of data via 'push method' with a clear definition of the initial retention period and appropriate security measures;

- prohibition of the systematic use of sensitive data;

- limitation of the data mining to risk indicators sufficiently high and clearly identified in relation to an ongoing investigation and for a predefined period, with case-by-case examination of the results in a non-automatic manner;

- legal and necessary limitations only to the rights of information, access, rectification and deletion of the individuals;

- competence of the data protection authorities (to be consulted and able to assess the PNR system as well as to deal with individual complaints);

- availability of effective remedies for the individuals;

- independent and external oversight of the PNR system;

- periodic review of the PNR systems by the competent authorities.

DENMARK / DANEMARK

Denmark acknowledges that the draft opinion on PNR is drafted exclusively from a data protection point of view. However, we must state the importance of striking the right balance between the requirements of data protection with the necessity for flexibility for the member states to set up their own detailed rules for the processing of PNR data in accordance with Convention 108.

Specific comment on (b) purpose limitation

First of all the text of this paragraph should be simplified and shortened.

Secondly, Denmark is of the view that the paragraph would entail too strict limitations to the processing of PNR data. The text should consequently - more clearly - establish that PNR data may only be collected for the prevention, detection, prosecution and investigation of serious crime and terrorist offences. Any further use of the PNR data that is not prescribed by law should be expressly prohibited.

FRANCE / FRANCE

The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS n°108, hereinafter referred to as 'Convention 108'),

Recalling the European Convention on Human Rights (ECHR) and in particular Articles 8 (right to respect for private life) and 13 (right to an effective remedy), as further elaborated by the jurisprudence of the European Court of Human Rights and Article 2 (freedom of movement) of Protocol No. 4,

Having regard to Convention 108 and other relevant Council of Europe instruments in the field of data protection such as Recommendation (87)15 regulating the use of personal data in the police sector and Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling,

Noting the rapid spread at global level of information technology systems and legislations concerning the transmission by air carriers of personal data of their passengers to public authorities for law enforcement and national security purposes,

Resolved to support respect for human rights with regard to the processing of personal data of air transport by public authorities responsible for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes,

Adopted the present opinion:

1. Introduction

The 32nd Plenary meeting (1-3 July 2015) of the Consultative Committee of Convention 108 decided, in light of the growing concerns raised by reactions to the recent terrorist attacks and threats, to prepare the present opinion, having notably considered the issues addressed in the report "Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards"[19].

The Bureau of the Committee, during its 36th (6-8 October 2015), 37th (9-11 December 2015) and 38th meetings (22-24 March 2016) worked on the preparation of the Opinion, which was examined by the 33rd Plenary meeting of the Committee of Convention 108 after written consultation of the delegations and interested stakeholders.

The Committee of Convention 108 understands that, in the recent context of accrued menace of terrorist attacks, the fight against terrorism must be reinforced. It underlines the importance of

[19] Report prepared by Mr D. Korff with the contribution of Ms M. Georges: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

combating terrorism efficiently and effectively while ensuring respect for human rights, the rule of law and the common values upheld by the Council of Europe. The Committee notes the willingness of governments to establish systems allowing the screening of personal data of air passengers as one of the means to prevent terrorism and other serious crimes, as an element of their efforts to improve security. In this context, the Committee considers it necessary to recall the data protection principles that are applicable to such systems, underlining that the interference with human rights, including the right to the protection of private life and to the protection of personal data can only occur when the necessary conditions have been fulfilled.

Article 8 of the ECHR and Article 9 of Convention 108 have set the conditions that must be respected when a limitation to the rights to private life and data protection is considered. Such a limitation must be in accordance with a clear law and must be necessary in a democratic society for a legitimate aim (such as national security, public safety or the prevention of crime).

2. The system

Several types of passenger data exist and for the purposes of the present opinion, the Committee will focus on Passenger Name Records (PNRs).

PNRs are records used in the air transport industry for commercial and operational purposes in providing air transportation services. The PNRs are created by airlines and travel agencies[20], relating to travel bookings in order to enable an exchange of information between them and in accordance with the passengers' requests. Such records are captured in many ways as the reservations[21] can be created in Global Distribution Systems (GDS), computer reservation systems (CRS), or the airline's own reservation system. Data fed into an airline's departure control system (DCS) upon check-in by the passenger (i.e. seat and baggage information) can also be added automatically to an existing PNR when the CRS and DCS are integrated in a single system.

Although PNRs were originally introduced for air travel, CRS can now also be used for bookings of hotels, car rental, boat and train trips.

[20] In the future, "non-carriers economic operators" (i.e. travel agencies and tour operators) may be obliged to provide PNR data to the national competent authorities.

[21] Among global reservations systems, Amadeus is the only one located in Europe, with Headquarters in Spain, its Data Centre in Germany and its Research and Development Centre in France. It is owned and used notably by Air France, Iberia Airlines, Lufthansa, British airways and Scandinavian airlines and over 60 other carriers across the globe are affiliated to it.

The format and content of a PNR, due to the common needs of multiple actors, has been progressively harmonised and standardised by the International Air Transport Association (IATA) which provides support in the design of passenger data programs.

The PNR information is collected from passengers and contains part or whole of the following items:

- Full name
- address and contact information (phone number, e-mail address, IP address)
- type of travel document and number
- date of birth
- nationality
- country of residence
- travel itinerary of at least one segment (complete for specific PNR)
- address for the first night spent in the country of destination
- method of payment used, including billing address and credit card details
- frequent flyer data and benefits (free upgrade or ticket)
- an open field with general remarks (“Special Service Request”, "Optional Services Instruction" or "Other Service Information”) such as all available information on unaccompanied minors, dietary and medical requirements, seating preferences, languages, details of disability, and other similar requests.
- an individual reference (PNR record locator code)
- information on the travel agency/travel agent
- ticket information (number, date of reservation, date of issuance, one-way tickets)
- fare details and the restrictions possibly applying to this fare (and related taxes)
- names and number of other passengers travelling together on the PNR
- travel status of passengers, including confirmations, check-in status, ‘no show’ or ‘go show’ information;
- seat number and other seating information
- code share information
- split/divided information (where the itineraries of several passengers under a PNR are not similar and changes must be brought to the booking for one passenger of an existing PNR)
- baggage information
- historic of all changes to PNR information listed above.

La directive PNR du 27 avril 2016 dresse, en son annexe I, la liste des données PNR que les Etat membres recueillent et peuvent exploiter selon les finalités définies par ladite directive.

In practice, the content of each existing PNR will greatly vary as the number and nature of fields to complete will depend on the itinerary (travel to the USA? roundtrip itinerary covering several towns in a same country or in several countries?), the offer of services by airlines and the reservation system used (over 60 fields to be completed for some of them).

The fact that the information collected is provided by passengers, or by others on their behalf and that such information is not checked, is also an important aspect of the system which needs to be underlined and taken into account as far as the principle of data accuracy is concerned. There is the potential for error: a PNR may contain incorrect information about an individual, which could, in some circumstances, raise suspicion.

Il est exact que les données PNR ne sont pas fiables à 100% car elles sont transmises aux compagnies aériennes par les passagers ou des tiers. Toutefois, la nature des données PNR a un intérêt opérationnel très important pour les services qui seront autorisés à les exploiter.

Il convient de souligner qu'aucune action par les autorités compétentes n'est possible sur la seule base du traitement automatisée de données PNR (article 7§6.de la directive)

En outre, l'article12§5 de la directive permet aux Etats membres de conserver le résultat du traitement automatisé d'une donnée, lorsque ce résultat s'est révélé négatif, tant que les données de base n'ont pas été effacées, afin d'éviter de futures « fausses » concordances positives. Cette mesure contribue à la protection des libertés individuelles.

Par ailleurs, toujours selon la directive PNR, lorsque des transporteurs aériens recueillent des données API (lesquelles sont fiables puisque tirées de la bande de lecture optique des documents de voyage des passagers), ils doivent les transmettre, que ces données API aient été collectées par ces transporteurs aériens en même temps ou séparément des données PNR (article 8§2 de la directive). En effet, comme le souligne le considérant 9 de la directive *« l'utilisation combinée des données PNR et des données API présent une valeur ajoutée en ce qu'elle aide les Etats-membres à vérifier l'identité d'une personne, renforçant ainsi la valeur du résultat en termes de prévention détection et de répression des infractions et réduisant au minimum le risque de soumettre des personnes innocentes à des vérifications et à des enquêtes* » .

Two different methods of transmission of the data from the commercial sector to the competent authorities of the public sector exist:

- the 'pull' method whereby public authorities directly reach into ('access') the reservation system and extract ("pull") a copy of the required data from it;

- the 'push' whereby the operator transmits ('pushes') the required PNR data into the database of the authority requesting them.

La directive PNR prévoit l'utilisation unique de la méthode Push, plus protectrice en matière de protection des données. Cette méthode permet également aux transporteurs aériens de savoir quelles données sont concernées.

3. Legality

While PNRs can be of benefit to the competent public authorities in combatting terrorism and other serious crimes, a number of conditions have to be met in order for the interference with the rights to private life and data protection to be permissible.

Pursuant to the case-law of the European Court of Human Rights relating to Article 8 of the ECHR such interference is only permissible where it is in accordance with the law and is strictly necessary and proportionate to the legitimate aim pursued.

While the assessment of the necessity of the interference, and the proportionality of the measures considered, have to be carefully examined in light of various elements, the Committee will briefly recall what the ECHR considers to be covered by the condition of legality. The requirement that any interference be 'in accordance with the law' (or 'provided for by the law' as prescribed in Article 9 of Convention 108) will only be met when three conditions are satisfied:

- the measure must have some basis in domestic law,
- this law must be clear and precise enough to be accessible to the person concerned (it must obviously be public), and
- have foreseeable consequences (enabling the person, if need be with appropriate advice, to regulate her or his conduct and act accordingly)[22].

In the context of processing of PNRs by law enforcement authorities, the criterion of the quality of the law implies a very precise and strict definition of the legitimate aim pursued (for instance, no open formulation in the definition of a serious crime can be allowed and examples of what is considered as such – for instance the fight against drug trafficking, human trafficking or child trafficking – are to be spelt out clearly).

Les dispositions de la directive PNR **qui devront être transposées en droit national (d'ici le 25 mai 2018),** prennent en compte ces éléments :

[22] ECHR Kennedy v. the United Kingdom, § 151; Rotaru v. Romania, 28341/95, §§50, 52 and 55; Amann v. Switzerland, § 50; Iordachi and Others v. Moldova; Kruslin v. France, § 27; Huvig v. France, § 26; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, § 71; Liberty and Others v. the United Kingdom, § 59, etc.

- L'article 1§2 de la directive PNR limite strictement les finalités d'exploitation des données PNR : « *les données PNR recueillies conformément à la présente directive ne peuvent être traitées qu'à des fins de prévention et de détection des infractions terroristes et formes graves de criminalité ainsi que d'enquêtes et de poursuite en la matière comme prévu à l'article 6, paragraphe 2, points a), b) et c)* ».

- L'article 3 §8 de la directive précise la définition des infractions terroristes : ce sont celles qui sont visées aux articles 1er à 4 de la décision-cadre 2002/475/JAI.

- L'article 3§9 et l'annexe II de la directive indiquent ce qu'il faut entendre par formes graves de criminalité.

4. Necessity and proportionality

Any prescribed or envisaged measures on processing PNR data by the competent public authorities, in light of the interference that they may entail with the rights of the data subjects, must be subject to scrutiny of their necessity and proportionality. The Committee calls for the examination of objective elements enabling to assess such necessity, the proportionality of the measures prescribed as well as the efficiency and effectivity of the system (which should be demonstrable where such systems already exist).

The envisaged processing of PNR data is the general and indiscriminate screening of all passengers by different competent authorities, including individuals who are not suspected of any crime, and concerns data initially collected for commercial purposes by private entities. In light of the degree of interference with the rights to private life and data protection that would arise from such processing, the fact that this processing is a necessary measure in a democratic society for the fight against terrorism and other serious crimes has to be clearly evidenced and the appropriate safeguards must be put in place. A specific demonstration of the necessity is needed for the collection and further use of PNR data. The apparent legitimacy of the aim pursued (preventing, detecting, investigating and prosecuting terrorist offences and other serious crimes) is not sufficient as it appears to be too broad.

En sus des finalités visées par la directive PNR à l'article 1§2, la directive précise également les fins auxquelles l'UIP peut traiter les données collectées à l'article 6§2, répondant ainsi aux exigences exposées en lien avec les principes de nécessité et de proportionnalité.

De surcroît, de nombreux exemples concrets ont été apportés par les Etats membres de l'Union européenne pour démontrer la nécessité de la collecte et de l'exploitation des données PNR dans le cadre de la lutte contre le terrorisme et les formes graves de criminalité.

Les garanties offertes par la directive PNR en matière de respect de la vie privée et des droits fondamentaux sont considérées par la France comme permettant de remplir les objectifs de nécessité et de proportionnalité.

The European Court of Human Rights underlined that "while the adjective 'necessary' […] is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'."[23]

While the State has a margin of appreciation in choosing the necessary means to achieve its legitimate and necessary aim, it must assess whether the interference created by such measures corresponds to a 'pressing social need'[24]. The assessment of the proportionality of the derogation needs to be based on the examination of a wide variety of element such as the definition of clear and limited purposes, of the scope of application of the system, of the nature of the data concerned, its length of conservation, etc.

Outre qu'elle définit clairement et de manière limitative les finalités (article 1) et la nature des données (annexe I), la directive PNR interdit le traitement et par conséquent l'exploitation et la conservation des données sensibles (article 13§4). De même, la durée de conservation est limitée à 5 ans (article 12§1).

Par ailleurs, à l'issue d'une période de six mois, les données PNR, les données qui peuvent servir à identifier directement le passager, sont masquées (article 12§2 de la directive). Les autorités compétentes doivent formuler une requête motivée et fondée sur des raisons suffisantes, auprès de leur de leur UIP nationale (Unité d'informations passagers), afin de pouvoir exploiter les données démasquées au cas par cas (article 12§5). Dans la première période de conservation de six mois, les demandes des autorités compétentes doivent également être motivées en vue d'un traitement au cas par cas.

Il est précisé qu'à l'issue de la période de conservation de 5 ans, les données PNR doivent être effacées de manière définitive (article 12§4).

Enfin, les garanties en matière de protection des données sont détaillées à l'article 13. Aux termes de l'article 5, chaque UIP doit nommer un délégué à la protection des données chargé de contrôler les traitements des données PNR et de mettre en œuvre les garanties pertinentes. Le délégué à la protection des données doit pouvoir accomplir ses tâches en toute indépendance.

Deciding on the validity of the Data Retention Directive (regarding the retention of communication data), the Court of Justice of the European Union underlined[25] that "the derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".

In case of existing systems of processing of PNR data, greater transparency on the assessment of the efficacy of such systems should be sought with a view to enabling a sound independent assessment of the necessity of the system. For instance, objective and quantifiable information

[23] Handyside v. UK, 5493/72, §48.

[24] Olsson v. Sweden, 10465/83.

[25] Digital Rights Ireland, C-293/12 of 8 April 2014, §52.

regarding terrorist threats which could be avoided, other deterrent effects, the modification of criminals' behaviours (e.g. abandoning originally intended criminal acts), the likelihood of substantially increased costs and difficulty of perpetrating crimes (like terrorist attacks) would help inform an assessment as to whether such a PNR system is necessary.

L'article 19 de la directive prévoit que, sur la base des informations communiquées par les Etats membres, la Commission européenne procédera à un réexamen précis de tous les éléments de la directive et établira un rapport. Cette mesure sera très utile pour évaluer la pertinence des dispositions de la directive.

En lien avec cet article 19, l'article 20 prévoit que les Etats membres fournissent chaque année à la Commission européenne certains éléments statistiques, comme le nombre de passagers identifiés en vue d'un examen plus approfondi par les autorités compétentes. Ces éléments permettront, entre autres, d'évaluer l'utilité de ce dispositif.

A regular review at periodic intervals of the necessity of the PNR system to pursue its appropriate justification in time should be carried out.

5. Principles and safeguards

(a) Scope of application

The scope of application of the processing of PNR data must be clearly and precisely defined in order to guarantee the proportionality of the interference with the rights of the persons concerned. This notably applies to the competent authorities receiving the data, the type of data processed, and the length of conservation of the data.

CF remarques précédentes sur la directive PNR

Regarding the recipient authorities, national ones in particular, the establishment of dedicated coordination units (such as the proposed 'Passengers Information Units' in the proposed EU scheme) contributes to preventing a mix between judicial and surveillance activities but the competencies of such units need to be strictly and narrowly defined and made public.

En application de la directive PNR (article 4), chaque Etat membre met en place ou désigne une « unité d'informations passagers »(UIP). Ainsi, les autorités compétentes n'auront pas d'accès direct aux données PNR. Cette organisation est un élément important pour respecter le principe de proportionnalité.

The transmission and further dissemination of data to the public authorities need to be relevant, adequate and proportionate (Article 5 of Convention 108) to the purposes for which they are processed. The transmitted data must be clearly defined (the elements of the PNR that are to be transmitted must be exhaustively listed), on the basis of objective criteria, and limits to the subsequent use of such data must also be established. Competent national authorities legally authorised to process PNR data should be listed and that information should be made public.

La directive PNR décrit précisément la manière dont les autorités compétentes pourront avoir accès aux données PNR (articles 4 et 7). Cet accès devra toujours être motivé et sera contrôlé.

The period of retention of the PNR data must also be clearly specified and limited to what is justified by objective criteria as it must be "based on objective criteria in order to ensure that it is limited to what is necessary"[26]. Masking out some elements of the data after a certain period of time can mitigate the risks entailed by a longer period of conservation of the data but it should be recalled that masked out data still permits identification of the individuals and continues as such to constitute personal data.

Cf observations précédentes.

(b) Purpose limitation

In light of the severity of the interference with the rights to private life and data protection, pose by the processing of PNR data by competent public authorities the purposes need to be clearly and precisely predefined on the basis of objective criteria which limit the transmission of the data only to the competent authorities as well as the further use of such data. The PNR can, in no circumstances, be used beyond these purposes (where it is the case, sanctions must be provided).

Cf. observations précédentes.

PNR systems are generally justified on the basis of the prevention, detection, investigation and prosecution of terrorist offences and other serious crimes and a clear delimitation of those key notions is needed in order to strictly circumscribe the use of such systems.

The definition of 'terrorism' and 'terrorist offences' is of particular complexity (see the relevant UN Conventions, the Council of Europe Convention on the prevention of terrorism of 2005 and its 2015 additional protocol). In the absence of a clear definition, this terminology should be restrictively construed. Should that not be the case, the purpose of the PNR system would remain too vague and the principle of proportionality would not be respected.

CF observations précédentes sur la définition des infractions terroristes telle que prévue dans la directive PNR.

The crimes for which PNR data can be used and shared should be strictly limited, clearly defined and particularly serious (for instance, crimes against humanity, torture, or genocide). Any use that is not prescribed by the law establishing a PNR system should be expressly prohibited and the use of any evidence obtained in violation of this law should not be admissible in court.

La liste des infractions graves est définie dans l'annexe II de la directive. Cette liste est plus large que celle précédemment indiquée à titre illustratif (crimes contre l'humanité, génocide,

[26] Digital Rights Ireland, C-293/12 of 8 April 2014 §64.

torture). Les infractions visées à cette annexe II de la directive doivent être passibles d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale de trois ans au titre du droit national des Etats-membres.

(c) Data transmission

As regards the transmission of the data from the commercial sector to the competent authorities of the public sector, the Committee considers that the 'push' method, with the operator being fully responsible for the quality of the data and the conditions of transmission, is to be preferred as it offers greater data protection safeguards than the 'pull' one. These guarantees should however not be circumvented by a system whereby all passengers data are systematically sent in an automated way, which would make it eventually similar to a pull system.

Cf. remarques précédentes sur le système Push, choisi par la directive PNR. Ce système permet aux transporteurs aériens de garder la main sur les données transmises, en d'autres termes, de savoir exactement quelles sont les données de leurs clients, transmises aux UIP.

Enfin, si toutes les données PNR relevant de l'annexe I de la directive PNR sont transmises aux autorités des Etats membres, cela ne signifie pas qu'elles seront toutes exploitées par les services opérationnels. Toutefois, leur conservation est nécessaire car il n'est pas possible d'identifier par avance les données qui seront éventuellement nécessaires dans le cadre d'une enquête pénale.~~.~~

The Committee recommends that an initial short period of retention of the PNR be defined, which could be renewed on the basis of a case-by-case examination of the request and its justification by an independent authority. In case of suspicion, the data could be retained for longer as it may be necessary in the context of legal proceedings (if the suspicion is lifted, the data should be deleted).

Cf Observations ci-dessus sur le masquage des données après une période de rétention de 6 mois.

En revanche, cette proposition est peu compatible avec les nécessités opérationnelles des services qui exploitent les données PNR. Leur conservation est nécessaire car elle peut se révéler utile dans le cadre d'une enquête. Les enquêteurs ont besoin de pouvoir consulter pendant un certain laps de temps. En effet, la constitution, puis le mode opératoire de groupes criminels ou terroristes prennent un certain temps pouvant aller jusqu'à plusieurs années. A titre d'exemple, les individus liés à des groupes terroristes peuvent ne pas se déplacer pendant une période assez longue pour ensuite effectuer des déplacements vers ou à partir de zones à risque.

D'ailleurs, comme cela a déjà été indiqué, l'article 12 de la directive PNR prévoit que toutes les données PNR seront conservées pendant une durée significative, de 5 ans après leur transfert, et que cette conservation ne sera assortie d'un masquage qu'au bout de 6 mois.

(d) Data mining and matching

The processing of personal data concerns all passengers and may not be limited to the collection of data of targeted individuals suspected of involvement in a criminal offence or posing an immediate threat to national security or public order. Instead, the data is processed in order to also be able to identify the persons in contact with potential suspects ('contact chaining') or threats, and anyone who "might" be involved in, or who "might become" involved in the criminal activities defined by the law establishing the sharing of PNRs with the competent authorities.

The data analysis aims to detect 'unknown persons' on the basis of pre-determined criteria and match known suspects against other data sets.

Assessing passengers on the basis of PNRs raises the question of predictability of the measure (the screening is carried out on the basis of predictive algorithms using dynamic criteria which may constantly evolve) and, where the data is linked to other datasets available to the competent authorities, the compatibility of such data matching with the principle of purpose limitation is to be questioned (sole use of datasets created for law enforcement purposes) and the precise subject of 'identification' defined (is the identification aimed at matching an actual suspected or convicted individual or rather at rating the passengers on a risk-scale?) in a manner that complies with the requirement of foreseeability.

The development of data mining and matching algorithms should be based on the results of an assessment of the likely impact of the data processing on the rights and fundamental freedoms of data subjects.

The basic structure of the analyses should be transparent and the matching of different datasets should only be made on the basis of predefined risk indicators which are both sufficiently high and have been clearly identified in advance in relation to an ongoing investigation and only for a predefined period (list of convicted persons for serious crimes, list of persons under investigation for suspicion of terrorist activities).

Ceci est prévu par la directive PNR : article 6

The results of such automatic assessments of individuals should be carefully examined on a case-by-case basis, by a person in a non-automated manner and the reasoning of the processing should be made known to the data subject objecting to it.

Les articles 6§5 et 6§6 de la directive PNR prévoient le réexamen individuel par des moyens non automatisés.

For the purpose of matching, data should flow to the PNR system, but not from the PNR system to other databases. Matching should only be possible when a hit occurs based on sufficiently elevated risk score associated with an incoming data.

Les données PNR sont confrontées aux bases de données utiles aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité comme, par exemple, en France, le FPR (fichier des personnes recherchées), le SIS et la base de données SLTD d'Interpol.

Il est nécessaire de confronter tous les données des passagers afin de savoir si une concordance positive apparaît.

(e) Prohibition of the systematic use of sensitive data

While PNRs should only contain information that is needed to facilitate a passenger's travel, a number of sensitive data which would serve to indicate racial origin, political opinions or religious or other beliefs or data relating to a person's health or sexual orientation may be included in the PNR, not only under the 'coded' data but also under the open field containing general remarks (such as dietary or medical requirements, or the fact that a political association benefited from reduced fares for the travel of its members) which could lead to direct discrimination.

While the competent authorities receiving such data in the PNRs are not allowed to process it (no assessment can be run on the basis of a criteria linked to any sensitive data) and must therefore mask or delete it, the Committee considers that a clear prohibition of the systematic use of such sensitive data should be established, implying there should be an obligation on the competent public authorities to mask or erase this type of data.

Comme cela a déjà été indiqué, la directive PNR interdit clairement la conservation et l'exploitation des données sensibles (article 13§4)

(f) Rights of information, access, rectification and deletion

The Committee recalls that according to Article 1 of both the ECHR and Convention 108, the rights to privacy and data protection have to be secured for every individual within the jurisdiction of the contracting Parties, irrespective of her or his nationality or residence.

The person whose PNR data is being shared with the competent authorities is entitled to know what happens with her or his data (what type of data, for which purpose, for how long, processed by whom, transmitted to whom), has a right of access and to ask for rectification or deletion of personal data. While such rights can be limited under the restrictive conditions previously mentioned (where it is in accordance with the law and necessary in the interest of a legitimate aim), the Committee recommends that persons who are not suspected of having committed, or being about to commit, a terrorist offence or other serious crime enjoy the full exercise of those rights. Persons who are suspected of having committed, or being about to

commit such offences may at least request the correction of inaccurate data and the deletion of unlawful data. If such persons are removed from suspicion, they should be able to exercise their full rights of access, rectification or deletion of personal data.

Any limitation of those rights must be made known to passengers at the time of collection of their data and during the whole processing activity by the competent public authorities.

Where data concerning a passenger have been collected without her or his knowledge, and unless the data are deleted, that person should be informed, where practicable, that information is held about her or him as soon as the object of the purpose for collection is no longer likely to be prejudiced. The persons concerned should also be informed on how to exercise their rights and what remedies are available.

L'article 13§1de la directive PNR confère à tous les passagers une série de droits : droit à l'information, droit d'accès, de rectification, d'effacement et de limitation, droits à réparation et à un recours juridictionnel. Ces droits sont ceux qui sont prévus, notamment, dans la réglementation de l'Union européenne, à l'application de laquelle il est renvoyé. Par conséquent, la directive 2016/680, du 27 avril 2016, en matière de protection des données, a vocation à s'appliquer dans le domaine des données PNR (une fois transposée en droit interne par les Etats membres).

(g) Security

As required by Article 7 of Convention 108, appropriate security measures shall be taken for the protection of personal data. This notably implies that the PNR system shall be held in a secure physical environment, with high-level intrusion controls and a strict access (to a limited number of persons) control (such as layered logins and the production of an audit record of access). Furthermore, communication of the PNR data to the competent authorities must be protected by technical and procedural means (strong cryptography, effective procedures for managing keys, etc).

L'article 13§2 de la directive dispose que « Chaque État membre veille à ce que les dispositions adoptées en droit national en application des articles 21 et 22 de la décision-cadre 2008/977/JAI concernant la confidentialité du traitement et la sécurité des données s'appliquent également à tous les traitements de données à caractère personnel effectués en vertu de la présente directive ».

(h) Transborder Data flows

In light of the international nature of PNRs systems (where data will not be flowing transborder in the communication phase between the reservation system and the competent authorities it may simply flow at the sole level of the reservation system as several of them are not based in Europe while the passengers are), the Committee recalls that to be legal, such transfers to States, where the PNR data is stored or transferred, that are not Parties to Convention 108 must satisfy the conditions established to guarantee the appropriate protection of data subjects.

(i) Remedies

It is an essential requirement of the case law of the European Court of Human Rights that "effective remedies" against violations of fundamental rights exist and be available to individuals (and not solely to nationals of the particular country concerned). While the Court of Justice of the European Union expressly mentions the requirement for redress before a tribunal, the European Court of Human Rights ruled[27] that the absence of judicial control does not necessarily constitute a violation of the rights at stake as long as other strong safeguards are provided for by the legislation (for instance independent oversight by authorities vested with sufficient powers and competence to exercise an effective and continuous control).

Article 10 of Convention 108 requires that Parties "establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection" set out in the Convention.

The Committee highlights the importance, as a pre-condition to an effective remedy, for the person concerned to be fully informed regarding the processing of her or his personal data and underlines the difficulties which exist in providing effective remedies against algorithm-based decisions and challenging inferences based on data analysis (false positives and other discriminatory measures).

Cf. Observations précédentes : les droits à réparation et à un recours juridictionnel prévus dans le droit de l'Union seront applicables pour la directive PNR (article 13.1).

(j) Oversight and transparency

It is clear from the case law of the European Court of Human Rights that the oversight of the authorities responsible for surveillance should be performed by an independent and external body.

The Committee underlines the role of the competent data protection authorities, which should not only be consulted in the normative process of adoption of the related laws and regulations but could also assess the compliance of a PNR system with data protection rules on the basis of individual complaints that they could receive, or on their own initiative.

Other specialised independent authorities (such as a parliamentary commission) in charge of overseeing law enforcement and intelligence agencies also have a role in controlling the scope of application of the system, its efficiency and perform case-by-case controls regarding the rationale of the retention of the passenger's data and the duration of this retention.

Supervision by independent data protection authorities, by specialised independent authorities in charge of overseeing law enforcement and intelligence agencies, as well as through independent assessments of the efficiency by the competent authorities themselves could lead to greater transparency and accountability of the powers and competencies of a PNR system.

[27] Klass and Others v. Germany, §§ 55-56; Kennedy v. the United Kingdom, § 167.

Dedicated data protection officers should be designated within the competent authorities processing PNR data with a view to ensuring compliance and accountability of the system (with a regular evaluation of the risks at stake and systematic audits of the PNR), the data processing and communication of the data, its updating and deletion, as well as the information provided to passengers. Data protection officers could also have a role as contact points in case of complaints or requests by the persons concerned. They are encouraged to raise awareness on "good practices".

Dans ce domaine également, la directive PNR, aux termes de l'article 15 b) prévoit que l'autorité de contrôle nationale de chaque Etat membre vérifie la licéité du traitement des données, effectue des enquêtes des inspections et des audits conformément au droit national, de sa propre initiative ou en se fondant sur une réclamation.

6. Conclusions

In view of the special interference with the rights to data protection and privacy that PNR measures may represent, the legality, proportionality and necessity of a PNR system need to be strictly respected and demonstrated, thus implying notably the following:

- transparent demonstration in a measurable form of the necessity and proportionality of the system in light of the legitimate aim pursued;

- accurate and strict definitions of the legitimate aim pursued are required and PNR data is only allowed for the defined limited grounds (prevention, detection, investigation and prosecution of terrorist offences and other serious crimes);

- transparent assessment of the efficacy of the PNR system;

- publicity of the competent public authorities (ideally dedicated coordination units);

- transmission of data via 'push method' with a clear definition of the initial retention period and appropriate security measures;

- prohibition of the systematic use of sensitive data;

- limitation of the data mining to risk indicators sufficiently high and clearly identified in relation to an ongoing investigation and for a predefined period, with case-by-case examination of the results in a non-automatic manner;

- legal and necessary limitations only to the rights of information, access, rectification and deletion of the individuals;

- competence of the data protection authorities (to be consulted and able to assess the PNR system as well as to deal with individual complaints);

- availability of effective remedies for the individuals;

- independent and external oversight of the PNR system;

- periodic review of the PNR systems by the competent authorities.

IRELAND / IRLANDE

Ireland will implement a PNR system when giving effect to Directive (EU) 2016/681 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

Insofar as the Council of Europe draft opinion on PNR is compatible with Directive 2016/281 Ireland can be supportive of that opinion. We are of the view that the Directive provides the appropriate balance between protections for personal data while also ensuring that PNR systems will be an effective tool in the fight against terrorism and serious transnational crime.

UNITED KINGDOM / ROYAUME-UNI

Introduction

The Bureau of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD-BUR) have requested comments on the Draft Opinion on the Data protection implications of the processing of Passenger Name Records (T-PD-BUR (2015) 11rev2).

UK's response

The EU PNR Directive provides sufficient safeguards and limitations on the use of the data. The PNR Directive was agreed by the EU only once all three institutions (Commission, Council for the EU and the European Parliament) were satisfied it meets the high European Data Protection standards and compatible with the European Convention on Human Rights.

'Severity' of the Interference

We do not agree that the interference with the passenger's rights to 'private life and data protection' is 'severe' (para.4(b) on page 7). The Council of Europe applies the incorrect test. Article 8 ECHR does not provide a 'right to private life' as suggested in their document; it provides a 'right to *respect* for family life'. Family life can therefore be interfered with, providing it is for a legitimate aim. Furthermore, the interference is not "severe" as it is simply information a passenger provides to the carrier as part of their booking process and passengers expect a level of interference during travel in return for their safety (e.g. searches, passport checks, etc). The interference with the passenger's privacy must be for a legitimate aim.

The use of PNR does not have to be 'indispensable' to meet this test, but there does need to be a '*pressing social need'* (Handyside v UK 1976). Essentially, the reasons given for collecting PNR must justify the interference and to do this, they must be '*proportionate*' and the reasons given to justify the interference must be '*relevant and sufficient*'. PNR has a unique functionality that enables law enforcement to identify previously unknown individuals that would not otherwise be possible without much more intrusive methods.

Limitation of offences to crimes against humanity, torture and genocide

It is wrong to suggest that terrorist offences should be restrictively construed. It is a common misconception that the more restrictive the use of PNR the more the passenger is protected. The reality is that the same amount of PNR is processed irrespective of the limitation of the offences it can be used for. In fact the more limited the scope of PNR, the less offences will be picked up, the less proportionate and necessary the processing is. It is therefore bad data protection to limit the use of PNR to crimes against humanity, torture and genocide.

Retention

The EU PNR Directive permits retention of PNR for five years and this is consistent with other country's systems. It is important Passenger Information Units can retain data for these periods as PNR's greatest benefit is being able to identify individuals previously unknown; it is therefore not possible to simply retain PNR on those who are known. Also, retaining PNR enables rules to be tested and refined so the interventions are targeted at a smaller group of individuals. Without this testing ability the interventions will be less targeted.

CANADA / CANADA

The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS n°108, hereinafter referred to as 'Convention 108'),

Recalling the European Convention on Human Rights (ECHR) and in particular Articles 8 (right to respect for private life) and 13 (right to an effective remedy), as further elaborated by the jurisprudence of the European Court of Human Rights and Article 2 (freedom of movement) of Protocol No. 4,

Having regard to Convention 108 and other relevant Council of Europe instruments in the field of data protection such as Recommendation (87)15 regulating the use of personal data in the police sector and Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling,

Noting the rapid spread at global level of information technology systems and legislations concerning the transmission by air carriers of personal data of their passengers to public authorities for law enforcement and national security purposes,

Resolved to support respect for human rights with regard to the processing of personal data of air transport by public authorities responsible for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes,

Adopted the present opinion:

1. Introduction

The 32nd Plenary meeting (1-3 July 2015) of the Consultative Committee of Convention 108 decided, in light of the growing concerns raised by reactions to the recent terrorist attacks and threats, to prepare the present opinion, having notably considered the issues addressed in the report "Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards"[28].

The Bureau of the Committee, during its 36th (6-8 October 2015), 37th (9-11 December 2015) and 38th meetings (22-24 March 2016) worked on the preparation of the Opinion, which was examined by the 33rd Plenary meeting of the Committee of Convention 108 after written consultation of the delegations and interested stakeholders.

The Committee of Convention 108 understands that, in the recent context of accrued menace of terrorist attacks, the fight against terrorism must be reinforced. It underlines the importance of

[28] Report prepared by Mr D. Korff with the contribution of Ms M. Georges: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

combating terrorism efficiently and effectively while ensuring respect for human rights, the rule of law and the common values upheld by the Council of Europe. The Committee notes the willingness of governments to establish systems allowing the screening of personal data of air passengers as one of the means to prevent terrorism and other serious crimes, as an element of their efforts to improve security. In this context, the Committee considers it necessary to recall the data protection principles that are applicable to such systems, underlining that the interference with human rights, including the right to the protection of private life and to the protection of personal data can only occur when the necessary conditions have been fulfilled.

Article 8 of the ECHR and Article 9 of Convention 108 have set the conditions that must be respected when a limitation to the rights to private life and data protection is considered. Such a limitation must be in accordance with a clear law and must be necessary in a democratic society for a legitimate aim (such as national security, public safety or the prevention of crime).

2. The system

Several types of passenger data exist and for the purposes of the present opinion, the Committee will focus on Passenger Name Records (PNRs).

PNRs are records used in the air transport industry for commercial and operational purposes in providing air transportation services. The PNRs are created by airlines and travel agencies[29], relating to travel bookings in order to enable an exchange of information between them and in accordance with the passengers' requests. Such records are captured in many ways as the reservations[30] can be created in Global Distribution Systems (GDS), computer reservation systems (CRS), or the airline's own reservation system. Data fed into an airline's departure control system (DCS) upon check-in by the passenger (i.e. seat and baggage information) can also be added automatically to an existing PNR when the CRS and DCS are integrated in a single system.

Although PNRs were originally introduced for air travel, CRS can now also be used for bookings of hotels, car rental, boat and train trips.

[29] In the future, "non-carriers economic operators" (i.e. travel agencies and tour operators) may be obliged to provide PNR data to the national competent authorities.

[30] Among global reservations systems, Amadeus is the only one located in Europe, with Headquarters in Spain, its Data Centre in Germany and its Research and Development Centre in France. It is owned and used notably by Air France, Iberia Airlines, Lufthansa, British airways and Scandinavian airlines and over 60 other carriers across the globe are affiliated to it.

The format and content of a PNR, due to the common needs of multiple actors, has been progressively harmonised and standardised by the International Air Transport Association (IATA) which provides support in the design of passenger data programs.

The PNR information is collected from passengers and contains part or whole of the following items:

- Full name
- address and contact information (phone number, e-mail address, IP address)
- type of travel document and number
- date of birth
- nationality
- country of residence
- travel itinerary of at least one segment (complete for specific PNR)
- address for the first night spent in the country of destination
- method of payment used, including billing address and credit card details
- frequent flyer data and benefits (free upgrade or ticket)
- an open field with general remarks (“Special Service Request”, "Optional Services Instruction" or "Other Service Information”) such as all available information on unaccompanied minors, dietary and medical requirements, seating preferences, languages, details of disability, and other similar requests.
- an individual reference (PNR record locator code)
- information on the travel agency/travel agent
- ticket information (number, date of reservation, date of issuance, one-way tickets)
- fare details and the restrictions possibly applying to this fare (and related taxes)
- names and number of other passengers travelling together on the PNR
- travel status of passengers, including confirmations, check-in status, ‘no show’ or ‘go show’ information;
- seat number and other seating information
- code share information
- split/divided information (where the itineraries of several passengers under a PNR are not similar and changes must be brought to the booking for one passenger of an existing PNR)
- baggage information
- historic of all changes to PNR information listed above.

In practice, the content of each existing PNR will greatly vary as the number and nature of fields to complete will depend on the itinerary (travel to the USA? roundtrip itinerary covering several towns in a same country or in several countries?), the offer of services by airlines and the reservation system used (over 60 fields to be completed for some of them).

The fact that the information collected is provided by passengers, or by others on their behalf and that such information is not checked, is also an important aspect of the system which needs

to be underlined and taken into account as far as the principle of data accuracy is concerned. There is the potential for error: a PNR may contain incorrect information about an individual, which could, in some circumstances, raise suspicion.

Two different methods of transmission of the data from the commercial sector to the competent authorities of the public sector exist:

- the 'pull' method whereby public authorities directly reach into ('access') the reservation system and extract ("pull") a copy of the required data from it;

- the 'push' whereby the operator transmits ('pushes') the required PNR data into the database of the authority requesting them.

3. Legality

While PNRs can be of benefit to the competent public authorities in combatting terrorism and other serious crimes, a number of conditions have to be met in order for the interference with the rights to private life and data protection to be permissible.

Pursuant to the case-law of the European Court of Human Rights relating to Article 8 of the ECHR such interference is only permissible where it is in accordance with the law and is strictly necessary and proportionate to the legitimate aim pursued.

While the assessment of the necessity of the interference, and the proportionality of the measures considered, have to be carefully examined in light of various elements, the Committee will briefly recall what the ECHR considers to be covered by the condition of legality. The requirement that any interference be 'in accordance with the law' (or 'provided for by the law' as prescribed in Article 9 of Convention 108) will only be met when three conditions are satisfied:

- the measure must have some basis in domestic law,
- this law must be clear and precise enough to be accessible to the person concerned (it must obviously be public), and
- have foreseeable consequences (enabling the person, if need be with appropriate advice, to regulate her or his conduct and act accordingly)[31].

[31] ECHR Kennedy v. the United Kingdom, § 151; Rotaru v. Romania, 28341/95, §§50, 52 and 55; Amann v. Switzerland, § 50; Iordachi and Others v. Moldova; Kruslin v. France, § 27; Huvig v. France, § 26;

In the context of processing of PNRs by law enforcement authorities, the criterion of the quality of the law implies a very precise and strict definition of the legitimate aim pursued (for instance, no open formulation in the definition of a serious crime can be allowed and examples of what is considered as such – for instance the fight against drug trafficking, human trafficking or child trafficking – are to be spelt out clearly).

4. Necessity and proportionality

Any prescribed or envisaged measures on processing PNR data by the competent public authorities, in light of the interference that they may entail with the rights of the data subjects, must be subject to scrutiny of their necessity and proportionality. The Committee calls for the examination of objective elements enabling to assess such necessity, the proportionality of the measures prescribed as well as the efficiency and effectivity of the system (which should be demonstrable where such systems already exist).

The envisaged processing of PNR data is the general and indiscriminate screening of all passengers by different competent authorities, including individuals who are not suspected of any crime, and concerns data initially collected for commercial purposes by private entities. In light of the degree of interference with the rights to private life and data protection that would arise from such processing, the fact that this processing is a necessary measure in a democratic society for the fight against terrorism and other serious crimes has to be clearly evidenced and the appropriate safeguards must be put in place. A specific demonstration of the necessity is needed for the collection and further use of PNR data. The apparent legitimacy of the aim pursued (preventing, detecting, investigating and prosecuting terrorist offences and other serious crimes) is not sufficient as it appears to be too broad.

The European Court of Human Rights underlined that "while the adjective 'necessary' […] is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'."[32]

While the State has a margin of appreciation in choosing the necessary means to achieve its legitimate and necessary aim, it must assess whether the interference created by such measures corresponds to a 'pressing social need'[33]. The assessment of the proportionality of the derogation needs to be based on the examination of a wide variety of element such as the definition of clear and limited purposes, of the scope of application of the system, of the nature of the data concerned, its length of conservation, etc.

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, § 71; Liberty and Others v. the United Kingdom, § 59, etc.

[32] Handyside v. UK, 5493/72, §48.

[33] Olsson v. Sweden, 10465/83.

Deciding on the validity of the Data Retention Directive (regarding the retention of communication data), the Court of Justice of the European Union underlined[34] that "the derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".

In case of existing systems of processing of PNR data, greater transparency on the assessment of the efficacy of such systems should be sought with a view to enabling a sound independent assessment of the necessity of the system. For instance, objective and quantifiable information regarding terrorist threats which could be avoided, other deterrent effects, the modification of criminals' behaviours (e.g. abandoning originally intended criminal acts), the likelihood of substantially increased costs and difficulty of perpetrating crimes (like terrorist attacks) would help inform an assessment as to whether such a PNR system is necessary.

A regular review at periodic intervals of the necessity of the PNR system to pursue its appropriate justification in time should be carried out.

5. Principles and safeguards

(a) Scope of application

The scope of application of the processing of PNR data must be clearly and precisely defined in order to guarantee the proportionality of the interference with the rights of the persons concerned. This notably applies to the competent authorities receiving the data, the type of data processed, and the length of conservation of the data.

Regarding the recipient authorities, national ones in particular, the establishment of dedicated coordination units (such as the proposed 'Passengers Information Units' in the proposed EU scheme) contributes to preventing a mix between judicial and surveillance activities but the competencies of such units need to be strictly and narrowly defined and made public.

The transmission and further dissemination of data to the public authorities need to be relevant, adequate and proportionate (Article 5 of Convention 108) to the purposes for which they are processed. The transmitted data must be clearly defined (the elements of the PNR that are to be transmitted must be exhaustively listed), on the basis of objective criteria, and limits to the subsequent use of such data must also be established. Competent national authorities legally authorised to process PNR data should be listed and that information should be made public.

The period of retention of the PNR data must also be clearly specified and limited to what is justified by objective criteria as it must be "based on objective criteria in order to ensure that it is limited to what is necessary"[35]. Masking out some elements of the data after a certain period of time can mitigate the risks entailed by a longer period of conservation of the data but it should be recalled that masked out data still permits identification of the individuals and continues as such to constitute personal data.

[34] Digital Rights Ireland, C-293/12 of 8 April 2014, §52.

[35] Digital Rights Ireland, C-293/12 of 8 April 2014 §64.

(b) Purpose limitation

In light of the severity of the interference with the rights to private life and data protection, pose by the processing of PNR data by competent public authorities the purposes need to be clearly and precisely predefined on the basis of objective criteria which limit the transmission of the data only to the competent authorities as well as the further use of such data. The PNR can, in no circumstances, be used beyond these purposes (where it is the case, sanctions must be provided).

PNR systems are generally justified on the basis of the prevention, detection, investigation and prosecution of terrorist offences and other serious crimes and a clear delimitation of those key notions is needed in order to strictly circumscribe the use of such systems.

The definition of 'terrorism' and 'terrorist offences' is of particular complexity (see the relevant UN Conventions, the Council of Europe Convention on the prevention of terrorism of 2005 and its 2015 additional protocol). In the absence of a clear definition, this terminology should be restrictively construed. Should that not be the case, the purpose of the PNR system would remain too vague and the principle of proportionality would not be respected.

The crimes for which PNR data can be used and shared should be strictly limited, clearly defined and particularly serious (for instance, crimes against humanity, torture, ~~or~~ genocide, human trafficking, drug smuggling, or money laundering). Any use that is not prescribed by the law establishing a PNR system should be expressly prohibited and the use of any evidence obtained in violation of this law should not be admissible in court.

Comment [FS--7]: Canada recommends the addition of other serious criminal offence that are transnational in nature, to illustrate other serious crimes.

(c) Data transmission

As regards the transmission of the data from the commercial sector to the competent authorities of the public sector, the Committee considers that the 'push' method, with the operator being fully responsible for the quality of the data and the conditions of transmission, is to be preferred as it offers greater data protection safeguards than the 'pull' one. These guarantees should however not be circumvented by a system whereby all passengers data are systematically sent in an automated way, which would make it eventually similar to a pull system.

Comment [TJG7018]: Canada disagrees with this statement. The safeguards inherent to 'Push" are that the data owner retains control over their system and whose data is transmitted (single flight to one country, vs all flights to all countries). PNR processing is not effective without the ability to process the data for all inbound travellers. Without that ability to establish a baseline of normal travel patterns, exceptions cannot / will not be effectively identified. This statement seems to be in conflict with this acknowledged practice in (d), below.

The Committee recommends that an initial short period of retention of the PNR be defined, which could be renewed on the basis of a case-by-case examination of the request and its justification by an independent authority. In case of suspicion, the data could be retained for longer as it may be necessary in the context of legal proceedings (if the suspicion is lifted, the data should be deleted).

(d) Data mining and matching

The processing of personal data concerns all passengers and may not be limited to the collection of data of targeted individuals suspected of involvement in a criminal offence or posing an immediate threat to national security or public order. Instead, the data is processed in

order to also be able to identify the persons in contact with potential suspects ('contact chaining') or threats, and anyone who "might" be involved in, or who "might become" involved in the criminal activities defined by the law establishing the sharing of PNRs with the competent authorities.

The data analysis aims to detect 'unknown persons' on the basis of pre-determined criteria and match known suspects against other data sets.

Assessing passengers on the basis of PNRs raises the question of predictability of the measure (the screening is carried out on the basis of predictive algorithms using dynamic criteria which may constantly evolve) and, where the data is linked to other datasets available to the competent authorities, the compatibility of such data matching with the principle of purpose limitation is to be questioned (sole use of datasets created for law enforcement purposes) and the precise subject of 'identification' defined (is the identification aimed at matching an actual suspected or convicted individual or rather at rating the passengers on a risk-scale?) in a manner that complies with the requirement of foreseeability.

The development of data mining and matching algorithms should be based on the results of an assessment of the likely impact of the data processing on the rights and fundamental freedoms of data subjects.

The basic structure of the analyses should be transparent and the matching of different datasets should only be made on the basis of predefined risk indicators which are both sufficiently high and have been clearly identified in advance in relation to an ongoing investigation and only for a predefined period (list of convicted persons for serious crimes, list of persons under investigation for suspicion of terrorist activities).

The results of such automatic assessments of individuals should be carefully examined on a case-by-case basis, by a person in a non-automated manner and the reasoning of the processing should be made known to the data subject objecting to it.

For the purpose of matching, data should flow to the PNR system, but not from the PNR system to other databases. Matching should only be possible when a hit occurs based on sufficiently elevated risk score associated with an incoming data.

(e) Prohibition of the systematic use of sensitive data

While PNRs should only contain information that is needed to facilitate a passenger's travel, a number of sensitive data which would serve to indicate racial origin, political opinions or religious or other beliefs or data relating to a person's health or sexual orientation may be included in the PNR, not only under the 'coded' data but also under the open field containing general remarks (such as dietary or medical requirements, or the fact that a political association benefited from reduced fares for the travel of its members) which could lead to direct discrimination.

While the competent authorities receiving such data in the PNRs are not allowed to process it (no assessment can be run on the basis of a criteria linked to any sensitive data) and must

therefore mask or delete it, the Committee considers that a clear prohibition of the systematic use of such sensitive data should be established, implying there should be an obligation on the competent public authorities to mask or erase this type of data.

(f) Rights of information, access, rectification and deletion

The Committee recalls that according to Article 1 of both the ECHR and Convention 108, the rights to privacy and data protection have to be secured for every individual within the jurisdiction of the contracting Parties, irrespective of her or his nationality or residence.

The person whose PNR data is being shared with the competent authorities is entitled to know what happens with her or his data (what type of data, for which purpose, for how long, processed by whom, transmitted to whom), has a right of access and to ask for rectification or deletion of personal data. While such rights can be limited under the restrictive conditions previously mentioned (where it is in accordance with the law and necessary in the interest of a legitimate aim), the Committee recommends that persons who are not suspected of having committed, or being about to commit, a terrorist offence or other serious crime enjoy the full exercise of those rights. Persons who are suspected of having committed, or being about to commit such offences may at least request the correction of inaccurate data and the deletion of unlawful data. If such persons are removed from suspicion, they should be able to exercise their full rights of access, rectification or deletion of personal data.

Any limitation of those rights must be made known to passengers at the time of collection of their data and during the whole processing activity by the competent public authorities.

Where data concerning a passenger have been collected without her or his knowledge, and unless the data are deleted, that person should be informed, where practicable, that information is held about her or him as soon as the object of the purpose for collection is no longer likely to be prejudiced. The persons concerned should also be informed on how to exercise their rights and what remedies are available.

(g) Security

As required by Article 7 of Convention 108, appropriate security measures shall be taken for the protection of personal data. This notably implies that the PNR system shall be held in a secure physical environment, with high-level intrusion controls and a strict access (to a limited number of persons) control (such as layered logins and the production of an audit record of access). Furthermore, communication of the PNR data to the competent authorities must be protected by technical and procedural means (strong cryptography, effective procedures for managing keys, etc).

(h) Transborder Data flows

In light of the international nature of PNRs systems (where data will not be flowing transborder in the communication phase between the reservation system and the competent authorities it may simply flow at the sole level of the reservation system as several of them are not based in Europe while the passengers are), the Committee recalls that to be legal, such transfers to

States, where the PNR data is stored or transferred, that are not Parties to Convention 108 must satisfy the conditions established to guarantee the appropriate protection of data subjects.

(i) Remedies

It is an essential requirement of the case law of the European Court of Human Rights that "effective remedies" against violations of fundamental rights exist and be available to individuals (and not solely to nationals of the particular country concerned). While the Court of Justice of the European Union expressly mentions the requirement for redress before a tribunal, the European Court of Human Rights ruled[36] that the absence of judicial control does not necessarily constitute a violation of the rights at stake as long as other strong safeguards are provided for by the legislation (for instance independent oversight by authorities vested with sufficient powers and competence to exercise an effective and continuous control).

Article 10 of Convention 108 requires that Parties "establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection" set out in the Convention.

The Committee highlights the importance, as a pre-condition to an effective remedy, for the person concerned to be fully informed regarding the processing of her or his personal data and underlines the difficulties which exist in providing effective remedies against algorithm-based decisions and challenging inferences based on data analysis (false positives and other discriminatory measures).

(j) Oversight and transparency

It is clear from the case law of the European Court of Human Rights that the oversight of the authorities responsible for surveillance should be performed by an independent and external body.

The Committee underlines the role of the competent data protection authorities, which should not only be consulted in the normative process of adoption of the related laws and regulations but could also assess the compliance of a PNR system with data protection rules on the basis of individual complaints that they could receive, or on their own initiative.

Other specialised independent authorities (such as a parliamentary commission) in charge of overseeing law enforcement and intelligence agencies also have a role in controlling the scope of application of the system, its efficiency and perform case-by-case controls regarding the rationale of the retention of the passenger's data and the duration of this retention.

Supervision by independent data protection authorities, by specialised independent authorities in charge of overseeing law enforcement and intelligence agencies, as well as through

[36] Klass and Others v. Germany, §§ 55-56; Kennedy v. the United Kingdom, § 167.

independent assessments of the efficiency by the competent authorities themselves could lead to greater transparency and accountability of the powers and competencies of a PNR system.

Dedicated data protection officers should be designated within the competent authorities processing PNR data with a view to ensuring compliance and accountability of the system (with a regular evaluation of the risks at stake and systematic audits of the PNR), the data processing and communication of the data, its updating and deletion, as well as the information provided to passengers. Data protection officers could also have a role as contact points in case of complaints or requests by the persons concerned. They are encouraged to raise awareness on "good practices".

6. Conclusions

In view of the special interference with the rights to data protection and privacy that PNR measures may represent, the legality, proportionality and necessity of a PNR system need to be strictly respected and demonstrated, thus implying notably the following:

- transparent demonstration in a measurable form of the necessity and proportionality of the system in light of the legitimate aim pursued;

- accurate and strict definitions of the legitimate aim pursued are required and PNR data is only allowed for the defined limited grounds (prevention, detection, investigation and prosecution of terrorist offences and other serious crimes);

- transparent assessment of the efficacy of the PNR system;

- publicity of the competent public authorities (ideally dedicated coordination units);

- transmission of data via 'push method' with a clear definition of the initial retention period and appropriate security measures;

- prohibition of the systematic use of sensitive data;

- limitation of the data mining to risk indicators sufficiently high and clearly identified in relation to an ongoing investigation and for a predefined period, with case-by-case examination of the results in a non-automatic manner;

- legal and necessary limitations only to the rights of information, access, rectification and deletion of the individuals;

- competence of the data protection authorities (to be consulted and able to assess the PNR system as well as to deal with individual complaints);

- availability of effective remedies for the individuals;

- independent and external oversight of the PNR system;

- periodic review of the PNR systems by the competent authorities.

EUROPEAN DATA PROTECTION SUPERVISOR / CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES

The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS n°108, hereinafter referred to as 'Convention 108'),

Recalling the European Convention on Human Rights (ECHR) and in particular Articles 8 (right to respect for private life) and 13 (right to an effective remedy), as further elaborated by the jurisprudence of the European Court of Human Rights and Article 2 (freedom of movement) of Protocol No. 4,

Having regard to Convention 108 and other relevant Council of Europe instruments in the field of data protection such as Recommendation (87)15 regulating the use of personal data in the police sector and Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling,

Noting the rapid spread at global level of information technology systems and legislations concerning the transmission by air carriers of personal data of their passengers to public authorities for law enforcement and national security purposes,

Resolved to support respect for human rights with regard to the processing of personal data of air transport by public authorities responsible for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes,

Adopted the present opinion:

1. Introduction

The 32nd Plenary meeting (1-3 July 2015) of the Consultative Committee of Convention 108 decided, in light of the growing concerns raised by reactions to the recent terrorist attacks and threats, to prepare the present opinion, having notably considered the issues addressed in the report "Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards"[37].

The Bureau of the Committee, during its 36th (6-8 October 2015), 37th (9-11 December 2015) and 38th meetings (22-24 March 2016) worked on the preparation of the Opinion, which was examined by the 33rd Plenary meeting of the Committee of Convention 108 after written consultation of the delegations and interested stakeholders.

[37] Report prepared by Mr D. Korff with the contribution of Ms M. Georges: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

The Committee of Convention 108 understands that, in the recent context of accrued menace of terrorist attacks, the fight against terrorism must be reinforced. It underlines the importance of combating terrorism efficiently and effectively while ensuring respect for human rights, the rule of law and the common values upheld by the Council of Europe. The Committee notes the willingness of governments to establish systems allowing the screening of personal data of air passengers as one of the means to prevent terrorism and other serious crimes, as an element of their efforts to improve security. In this context, the Committee considers it necessary to recall the data protection principles that are applicable to such systems, underlining that the interference with human rights, including the right to the protection of private life and to the protection of personal data can only occur when the necessary conditions have been fulfilled.

Article 8 of the ECHR and Article 9 of Convention 108 have set the conditions that must be respected when a limitation to the rights to private life and data protection is considered. Such a limitation must be in accordance with a clear law and must be necessary in a democratic society for a legitimate aim (such as national security, public safety or the prevention of crime).

2. The system

Several types of passenger data exist and for the purposes of the present opinion, the Committee will focus on Passenger Name Records (PNRs).

PNRs are records used in the air transport industry for commercial and operational purposes in providing air transportation services. The PNRs are created by airlines and travel agencies[38], relating to travel bookings in order to enable an exchange of information between them and in accordance with the passengers' requests. Such records are captured in many ways as the reservations[39] can be created in Global Distribution Systems (GDS), computer reservation systems (CRS), or the airline's own reservation system. Data fed into an airline's departure control system (DCS) upon check-in by the passenger (i.e. seat and baggage information) can also be added automatically to an existing PNR when the CRS and DCS are integrated in a single system.

Although PNRs were originally introduced for air travel, CRS can now also be used for bookings of hotels, car rental, boat and train trips.

[38] In the future, "non-carriers economic operators" (i.e. travel agencies and tour operators) may be obliged to provide PNR data to the national competent authorities.

[39] Among global reservations systems, Amadeus is the only one located in Europe, with Headquarters in Spain, its Data Centre in Germany and its Research and Development Centre in France. It is owned and used notably by Air France, Iberia Airlines, Lufthansa, British airways and Scandinavian airlines and over 60 other carriers across the globe are affiliated to it.

The format and content of a PNR, due to the common needs of multiple actors, has been progressively harmonised and standardised by the International Air Transport Association (IATA) which provides support in the design of passenger data programs.

The PNR information is collected from passengers and contains part or whole of the following items:

- Full name
- address and contact information (phone number, e-mail address, IP address)
- type of travel document and number
- date of birth
- nationality
- country of residence
- travel itinerary of at least one segment (complete for specific PNR)
- address for the first night spent in the country of destination
- method of payment used, including billing address and credit card details
- frequent flyer data and benefits (free upgrade or ticket)
- an open field with general remarks (“Special Service Request”, "Optional Services Instruction" or "Other Service Information”) such as all available information on unaccompanied minors, dietary and medical requirements, seating preferences, languages, details of disability, and other similar requests.
- an individual reference (PNR record locator code)
- information on the travel agency/travel agent
- ticket information (number, date of reservation, date of issuance, one-way tickets)
- fare details and the restrictions possibly applying to this fare (and related taxes)
- names and number of other passengers travelling together on the PNR
- travel status of passengers, including confirmations, check-in status, ‘no show’ or ‘go show’ information;
- seat number and other seating information
- code share information
- split/divided information (where the itineraries of several passengers under a PNR are not similar and changes must be brought to the booking for one passenger of an existing PNR)
- baggage information
- historic of all changes to PNR information listed above.

In practice, the content of each existing PNR will greatly vary as the number and nature of fields to complete will depend on the itinerary (travel to the USA? roundtrip itinerary covering several towns in a same country or in several countries?), the offer of services by airlines and the reservation system used (over 60 fields to be completed for some of them).

The fact that the information collected is provided by passengers, or by others on their behalf and that such information is not checked, is also an important aspect of the system which needs

to be underlined and taken into account as far as the principle of data accuracy is concerned. There is the potential for error: a PNR may contain incorrect information about an individual, which could, in some circumstances, raise suspicion.

Two different methods of transmission of the data from the commercial sector to the competent authorities of the public sector exist:

- the 'pull' method whereby public authorities directly reach into ('access') the reservation system and extract ("pull") a copy of the required data from it;

- the 'push' whereby the operator transmits ('pushes') the required PNR data into the database of the authority requesting them.

3. Legality

While PNRs can be of benefit to the competent public authorities in combatting terrorism and other serious crimes, a number of conditions have to be met in order for the interference with the rights to private life and data protection to be permissible.

Pursuant to the case-law of the European Court of Human Rights relating to Article 8 of the ECHR such interference is only permissible where it is in accordance with the law and is strictly necessary and proportionate to the legitimate aim pursued.

While the assessment of the necessity of the interference, and the proportionality of the measures considered, have to be carefully examined in light of various elements, the Committee will briefly recall what the ECHR considers to be covered by the condition of legality. The requirement that any interference be 'in accordance with the law' (or 'provided for by the law' as prescribed in Article 9 of Convention 108) will only be met when three conditions are satisfied:

- the measure must have some basis in domestic law,
- this law must be clear and precise enough to be accessible to the person concerned (it must obviously be public), and
- have foreseeable consequences (enabling the person, if need be with appropriate advice, to regulate her or his conduct and act accordingly)[40].

[40] ECHR Kennedy v. the United Kingdom, § 151; Rotaru v. Romania, 28341/95, §§50, 52 and 55; Amann v. Switzerland, § 50; Iordachi and Others v. Moldova; Kruslin v. France, § 27; Huvig v. France, § 26;

In the context of processing of PNRs by law enforcement authorities, the criterion of the quality of the law implies a very precise and strict definition of the legitimate aim pursued (for instance, no open formulation in the definition of a serious crime can be allowed and examples of what is considered as such – for instance the fight against drug trafficking, human trafficking or child trafficking – are to be spelt out clearly).

4. Necessity and proportionality

Any prescribed or envisaged measures on processing PNR data by the competent public authorities, in light of the interference that they may entail with the rights of the data subjects, must be subject to scrutiny of their necessity and proportionality. The Committee calls for the examination of objective elements enabling to assess such necessity, the proportionality of the measures prescribed as well as the efficiency and effectivity of the system (which should be demonstrable where such systems already exist).

The envisaged processing of PNR data is the general and indiscriminate screening of all passengers by different competent authorities, including individuals who are not suspected of any crime, and concerns data initially collected for commercial purposes by private entities. In light of the degree of interference with the rights to private life and data protection that would arise from such processing, the fact that this processing is a necessary measure in a democratic society for the fight against terrorism and other serious crimes has to be clearly evidenced and the appropriate safeguards must be put in place. A specific demonstration of the necessity is needed for the collection and further use of PNR data. The apparent legitimacy of the aim pursued (preventing, detecting, investigating and prosecuting terrorist offences and other serious crimes) is not sufficient as it appears to be too broad.

The European Court of Human Rights underlined that "while the adjective 'necessary' […] is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'."[41]

While the State has a margin of appreciation in choosing the necessary means to achieve its legitimate and necessary aim, it must assess whether the interference created by such measures corresponds to a 'pressing social need'[42]. The assessment of the proportionality of the derogation needs to be based on the examination of a wide variety of element such as the definition of clear and limited purposes, of the scope of application of the system, of the nature of the data concerned, its length of conservation, etc.

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, § 71; Liberty and Others v. the United Kingdom, § 59, etc.

[41] Handyside v. UK, 5493/72, §48.

[42] Olsson v. Sweden, 10465/83.

Deciding on the validity of the Data Retention Directive (regarding the retention of communication data), the Court of Justice of the European Union underlined[43] that "the derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".

In case of existing systems of processing of PNR data, greater transparency on the assessment of the efficacy of such systems should be sought with a view to enabling a sound independent assessment of the necessity of the system. For instance, objective and quantifiable information regarding terrorist threats which could be avoided, other deterrent effects, the modification of criminals' behaviours (e.g. abandoning originally intended criminal acts), the likelihood of substantially increased costs and difficulty of perpetrating crimes (like terrorist attacks) would help inform an assessment as to whether such a PNR system is necessary.

A regular review at periodic intervals of the necessity of the PNR system to pursue its appropriate justification in time should be carried out.

5. Principles and safeguards

(a) Scope of application

The scope of application of the processing of PNR data must be clearly and precisely defined in order to guarantee the proportionality of the interference with the rights of the persons concerned. This notably applies to the competent authorities receiving the data, the type of data processed, and the length of conservation of the data.

Regarding the recipient authorities, national ones in particular, the establishment of dedicated coordination units (such as the proposed 'Passengers Information Units' in the proposed EU scheme) contributes to preventing a mix between judicial and surveillance activities but the competencies of such units need to be strictly and narrowly defined and made public.

The transmission and further dissemination of data to the public authorities need to be relevant, adequate and proportionate (Article 5 of Convention 108) to the purposes for which they are processed. The transmitted data must be clearly defined (the elements of the PNR that are to be transmitted must be exhaustively listed), on the basis of objective criteria, and limits to the subsequent use of such data must also be established. Competent national authorities legally authorised to process PNR data should be listed and that information should be made public.

The period of retention of the PNR data must also be clearly specified and limited to what is justified by objective criteria as it must be "based on objective criteria in order to ensure that it is limited to what is necessary"[44]. Masking out some elements of the data after a ~~certain~~ limited period of time (a few weeks) can mitigate the risks entailed by a longer period of conservation of the data, such as for instance abusive access, but it should be recalled that masked out data still permits identification of the individuals and continues as such to constitute personal data.

Comment [ACL9]: This is still limited compared to previous version. We would support stricter wording. For instance keeping the data directly identifiable for a few weeks before maskling them.

[43] Digital Rights Ireland, C-293/12 of 8 April 2014, §52.

[44] Digital Rights Ireland, C-293/12 of 8 April 2014 §64.

(b) Purpose limitation

In light of the severity of the interference with the rights to private life and data protection, pose by the processing of PNR data by competent public authorities the purposes need to be clearly and precisely predefined on the basis of objective criteria which limit the transmission of the data only to the competent authorities as well as the further use of such data. The PNR can, in no circumstances, be used beyond these purposes (where it is the case, sanctions must be provided).

PNR systems are generally justified on the basis of the prevention, detection, investigation and prosecution of terrorist offences and other serious crimes and a clear delimitation of those key notions is needed in order to strictly circumscribe the use of such systems.

The definition of 'terrorism' and 'terrorist offences' is of particular complexity (see the relevant UN Conventions, the Council of Europe Convention on the prevention of terrorism of 2005 and its 2015 additional protocol). In the absence of a clear definition, this terminology should be restrictively construed. Should that not be the case, the purpose of the PNR system would remain too vague and the principle of proportionality would not be respected.

The crimes for which PNR data can be used and shared should be strictly limited, clearly defined and particularly serious (for instance, crimes against humanity, torture, or genocide). Any use that is not prescribed by the law establishing a PNR system should be expressly prohibited and the use of any evidence obtained in violation of this law should not be admissible in court.

(c) Data transmission

As regards the transmission of the data from the commercial sector to the competent authorities of the public sector, the Committee considers that the 'push' method, with the operator being fully responsible for the quality of the data and the conditions of transmission, is to be preferred as it offers greater data protection safeguards than the 'pull' one. These guarantees should however not be circumvented by a system whereby all passengers data are systematically sent in an automated way, which would make it eventually similar to a pull system.

The Committee recommends that an initial short period of retention of the PNR be defined, which could be renewed on the basis of a case-by-case examination of the request and its justification by an independent authority. In case of suspicion, the data could be retained for longer as it may be necessary in the context of legal proceedings (if the suspicion is lifted, the data should be deleted).

Comment [ACL10]: Shouldn't this be in the end of 5a)?

(d) Data mining and matching

The processing of personal data concerns all passengers and may not be limited to the collection of data of targeted individuals suspected of involvement in a criminal offence or posing an immediate threat to national security or public order. Instead, the data is processed in

order to also be able to identify the persons in contact with potential suspects ('contact chaining') or threats, and anyone who "might" be involved in, or who "might become" involved in the criminal activities defined by the law establishing the sharing of PNRs with the competent authorities.

The data analysis aims to detect 'unknown persons' on the basis of pre-determined criteria and match known suspects against other data sets.

Assessing passengers on the basis of PNRs raises the question of predictability of the measure (the screening is carried out on the basis of predictive algorithms using dynamic criteria which may constantly evolve) and, where the data is linked to other datasets available to the competent authorities, the compatibility of such data matching with the principle of purpose limitation is to be questioned (sole use of datasets created for law enforcement purposes) and the precise subject of 'identification' defined (is the identification aimed at matching an actual suspected or convicted individual or rather at rating the passengers on a risk-scale?) in a manner that complies with the requirement of foreseeability.

Comment [ACL11]: Could this be clarified?

The development of data mining and matching algorithms should be based on the results of an assessment of the likely impact of the data processing on the rights and fundamental freedoms of data subjects.

The basic structure of the analyses should be transparent and the matching of different datasets should only be made on the basis of predefined risk indicators which are both sufficiently high and have been clearly identified in advance in relation to an ongoing investigation and only for a predefined period (list of convicted persons for serious crimes, list of persons under investigation for suspicion of terrorist activities).

The results of such automatic assessments of individuals should be carefully examined on a case-by-case basis, by a person in a non-automated manner and the reasoning of the processing should be made known to the data subject objecting to it.

For the purpose of matching, data should flow to the PNR system, but not from the PNR system to other databases. Matching should only be possible when a hit occurs based on sufficiently elevated risk score associated with an incoming data.

(e) ~~Prohibition~~ Processing ~~of the systematic use~~ of sensitive data

While PNRs should only contain information that is needed to facilitate a passenger's travel, a number of sensitive data which would serve to indicate racial origin, political opinions or religious or other beliefs or data relating to a person's health or sexual orientation may be included in the PNR, not only under the 'coded' data but also under the open field containing general remarks (such as dietary or medical requirements, or the fact that a political association benefited from reduced fares for the travel of its members) which could lead to direct discrimination.

While the competent authorities receiving such data in the PNRs are not allowed to process it (no assessment can be run on the basis of a criteria linked to any sensitive data) and must

therefore mask or delete it, the Committee considers that a ~~clear~~ prohibition of the ~~systematic~~ use of such sensitive data should be established as a principle~~, implying there should be an obligation on the competent public authorities to mask or erase this type of data~~.

(f) Rights of information, access, rectification and deletion

The Committee recalls that according to Article 1 of both the ECHR and Convention 108, the rights to privacy and data protection have to be secured for every individual within the jurisdiction of the contracting Parties, irrespective of her or his nationality or residence.

The person whose PNR data is being shared with the competent authorities is entitled to know what happens with her or his data (what type of data, for which purpose, for how long, processed by whom, transmitted to whom), has a right of access and to ask for rectification or deletion of personal data. While such rights can be limited under the restrictive conditions previously mentioned (where it is in accordance with the law and necessary in the interest of a legitimate aim), the Committee recommends that persons who are not suspected of having committed, or being about to commit, a terrorist offence or other serious crime enjoy the full exercise of those rights. Persons who are suspected of having committed, or being about to commit such offences may at least be able to request the correction of inaccurate data and the deletion of unlawful data. If such persons are removed from suspicion, they should be able to exercise their full rights of access, rectification or deletion of personal data.

Any limitation of those rights must be made known to passengers at the time of collection of their data and during the whole processing activity by the competent public authorities.

Where data concerning a passenger have been collected without her or his knowledge, and unless the data are deleted, that person should be informed, where practicable, that information is held about her or him as soon as the object of the purpose for collection is no longer likely to be prejudiced. The persons concerned should also be informed on how to exercise their rights and what remedies are available.

(g) Security

As required by Article 7 of Convention 108, appropriate security measures shall be taken for the protection of personal data. This notably implies that the PNR system shall be held in a secure physical environment, with high-level intrusion controls and a strict access (to a limited number of persons) control (such as layered logins and the production of an audit record of access). Furthermore, communication of the PNR data to the competent authorities must be protected by technical and procedural means (strong cryptography, effective procedures for managing keys, etc).

(h) Transborder Data flows

In light of the international nature of PNRs systems (where data will not be flowing transborder in the communication phase between the reservation system and the competent authorities it may simply flow at the sole level of the reservation system as several of them are not based in Europe while the passengers are), the Committee recalls that to be legal, such transfers to

Comment [ACL12]: The previous version read 'transmission'.
What do we mean here by prohibition of systematic use? That case by case use of sensitive data is allowed, as well as the use of masked sensitive data? Under which justification?

Why not keep the idea of prohibition but in a slightly softer way, i.e. prohibition of use of sensitive data should be established as a principle?

States, where the PNR data is stored or transferred, that are not Parties to Convention 108 must satisfy the conditions established to guarantee the appropriate protection of data subjects.

(i) Remedies

It is an essential requirement of the case law of the European Court of Human Rights that "effective remedies" against violations of fundamental rights exist and be available to individuals (and not solely to nationals of the particular country concerned). While the Court of Justice of the European Union expressly mentions the requirement for redress before a tribunal, the European Court of Human Rights ruled[45] that the absence of judicial control does not necessarily constitute a violation of the rights at stake as long as other strong safeguards are provided for by the legislation (for instance independent oversight by authorities vested with sufficient powers and competence to exercise an effective and continuous control).

Article 10 of Convention 108 requires that Parties "establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection" set out in the Convention.

The Committee supports the need to provide for effective redress to the individual, which would cover both administrative and judicial remedy. The Committee also highlights the importance, as a pre-condition to an effective remedy, for the person concerned to be fully informed regarding the processing of her or his personal data and underlines the difficulties which exist in providing effective remedies against algorithm-based decisions and challenging inferences based on data analysis (false positives and other discriminatory measures).

Comment [ACL13]: The sentence on judicial remedy in the previous version has disappeared.
'The Committee considers that both an administrative and judicial remedy should be made available to persons concerned '
While the jurisprudence of the ECHR and the ECJ is not fully aligned on this, shouldn't we still support this conclusion as giving the best chances to individuals to exercise their rights?

The way it stands now, this chapter does not include an effective recommendation (apart from 'informing' the individual).

(j) Oversight and transparency

It is clear from the case law of the European Court of Human Rights that the oversight of the authorities responsible for surveillance should be performed by an independent and external body.

The Committee underlines the role of the competent data protection authorities, which should not only be consulted in the normative process of adoption of the related laws and regulations but could also assess the compliance of a PNR system with data protection rules on the basis of individual complaints that they could receive, or on their own initiative.

Other specialised independent authorities (such as a parliamentary commission) in charge of overseeing law enforcement and intelligence agencies also have a role in controlling the scope of application of the system, its efficiency and perform case-by-case controls regarding the rationale of the retention of the passenger's data and the duration of this retention.

Supervision by independent data protection authorities, by specialised independent authorities in charge of overseeing law enforcement and intelligence agencies, as well as through

[45] Klass and Others v. Germany, §§ 55-56; Kennedy v. the United Kingdom, § 167.

independent assessments of the efficiency by the competent authorities themselves could lead to greater transparency and accountability of the powers and competencies of a PNR system.

Dedicated data protection officers should be designated within the competent authorities processing PNR data with a view to ensuring compliance and accountability of the system (with a regular evaluation of the risks at stake and systematic audits of the PNR), the data processing and communication of the data, its updating and deletion, as well as the information provided to passengers. Data protection officers could also have a role as contact points in case of complaints or requests by the persons concerned. They are encouraged to raise awareness on "good practices".

6. Conclusions

In view of the special interference with the rights to data protection and privacy that PNR measures may represent, the legality, proportionality and necessity of a PNR system need to be strictly respected and demonstrated, thus implying notably the following:

- transparent demonstration in a measurable form of the necessity and proportionality of the system in light of the legitimate aim pursued;

- accurate and strict definitions of the legitimate aim pursued are required and PNR data is only allowed for the defined limited grounds (prevention, detection, investigation and prosecution of terrorist offences and other serious crimes);

- transparent assessment of the efficacy of the PNR system;

- publicity of the competent public authorities (ideally dedicated coordination units);

- transmission of data via 'push method' with a clear definition of the initial retention period and appropriate security measures;

- prohibition of the systematic use of sensitive data;

Comment [ACL14]: Same comment as above. Suggestion to delete 'systematic'.

- limitation of the data mining to risk indicators sufficiently high and clearly identified in relation to an ongoing investigation and for a predefined period, with case-by-case examination of the results in a non-automatic manner;

- legal and necessary limitations only to the rights of information, access, rectification and deletion of the individuals;

- competence of the data protection authorities (to be consulted and able to assess the PNR system as well as to deal with individual complaints);

- availability of effective administrative and judicial remedies for the individuals;

- independent and external oversight of the PNR system;

- periodic review of the PNR systems by the competent authorities.