COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 18 May 2016

T-PD-BUR(2015)11rev2

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

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

Directorate General of Human Rights and the Rule of Law

Table of Contents

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 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

[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

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.

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)

[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.

- 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 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.

[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.

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 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.

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

(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[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).

(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

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

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.