COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 4 December 2015

T-PD-BUR(2015)05

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

Preliminary draft Opinion on the Data protection implications of the processing of Air Transport Passenger Information

Directorate General of Human Rights and the Rule of Law

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,

Concerned about 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 the respect of human rights with regard to the processing of personal data right to data protection in the context of the processing of air transport passengers' personal data by public authorities responsible for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes,

Adopted the present opinion:

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 have an opinion prepared, notably based on 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) and 37th (9-11 December 2015) meetings, worked on the preparation of the Opinion, which …

The Committee of Convention 108 notes the current shift operated by governments towards further security and their growing willingness to establish systems allowing the screening of personal data of air passengers as one of the means to prevent and fight terrorist offences and serious crimes. In this context, the Committee considers necessary to recall the data protection principles applicable to such systems, underlining the interference with the human rights to the protection of private life and to the protection of personal data that they represent, and the conditions that have to be compulsorily fulfilled in order to render such interference acceptable.

[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

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

The system

Several types of passenger data exist and for the purposes of the present opinion, the Committee will focus on Passenger Name Records, with due regard also being paid to Advanced Passenger Information.

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 can be created in Global Distribution Systems (GDS) or computer reservation system (CRS, such as Amadeus[3], Sabre, Travelport) 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 CDS 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, and train trips.

The layout 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.

A PNR will contain part or whole of the following information on the passenger:

- 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 (EU/US PNR)
- travel itinerary of at least one segment (complete for specific PNR)
- address for the first night spent in the US (EU/US PNR)
- 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.

[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] Amadeus is the only CRS 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 PNR will also contain:

- 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 on their behalf, is also an important feature of the system which needs to be underlined.

Advanced Passenger Information (API)
For more formal purposes (immigration, customs, security) other records exist containing the passenger's identity (full name, date of birth and nationality) obtained from travel document information (passport details also recorded) and the basic information about the flights concerned (departure point, entry point on the territory, code of transport and departure and arrival times of the transport): they are the Advanced Passenger Information (API) contained in the API System (APIS).
API contains data relating to each individual passenger (Item Data)

- Surname/Given Names
- Nationality
- Date of Birth
- Gender
- Official Travel Document Number
- Issuing State or Organization of the Official Travel Document
- Travel Document Type
- Expiration Date of Travel Document
- Seating information
- Baggage Information

And data relating to the flight (Header Data)

- Flight Identification
- Scheduled Departure Date and time
- Scheduled Arrival Date and time
- Last Place/Port of Call of Aircraft
- Place/Port of Aircraft Initial Arrival
- Subsequent Place/Port of Call within the country
- Number of Passengers on the flight

Directive 2004/82/EC of 29 April 2004 on "the obligation of carriers to communicate passenger data" to authorities responsible for carrying out checks on persons at external borders of the European Union prescribes a slightly shorter list of data (see Article 3.2).

API is collected at the time of check-in, for border control purposes, shared with border control agencies through APIS prior to a flight arrival (not shared earlier than 30 minutes before departure, i.e. preferably when the aircraft doors have been closed and the aircraft readied for departure).

Part of API data and PNR data evidently overlap in practice and the Committee is of the opinion that a better articulation between both systems could be beneficial for the protection of individuals with regard to the processing of personal data (see page 7).

Data transmission
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.

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.

While both PNRs and API can be of high interest to the competent authorities in ensuring a sound border control management and in fighting against terrorism and serious crimes, a number of conditions have to be met in order for such an interference with the rights to private life and data protection be permissible.

According to the case-law of the European Court of Human Rights relating to Article 8 of the ECHR such interference can only be accepted where it is in accordance with the law, 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, has to be carefully examined in light of a variety of elements, the Committee will briefly recall what the ECHR considers to be covered by the condition relating to the law.
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].

[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.

In the context of the 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 – is to be spelt out clearly).

The necessity

In light of the degree of interference with the rights to private life and data protection that would arise from the processing of PNR data (general and indiscriminate screening of all passengers, individuals who are not suspected of any crime), initially collected for commercial purposes, by different competent authorities, the evidence that such processing is a necessary measure in a democratic society for the fight against terrorism and against serious crimes has to be clearly established and the appropriate safeguards put in place.

The necessity of the limitation, and the fact than no other less intrusive means exist, must be substantiated with objective elements and a mere formulation justifying that such a processing is necessary and proportionate to the specific aim pursued by the legal act in question is not acceptable.

In light of the nature of such a massive and non-targeted collection of personal data, an exceptional demonstration of the necessity is needed and the apparent legitimacy of the aim pursued (preventing, detecting, investigating and prosecuting terrorist offences and serious crimes) is not sufficient. In order to reach public justification of the need of the processing of PNR data by law enforcement, greater transparency on the assessment of the efficiency of this kind of massive and non-targeted surveillance is to be sought.

Would an alternative and less intrusive system based on the screening of API data be effective? How many terrorist threats have been avoided on the basis of the use of API or PNRs, etc.?

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]

The Court of Justice of the European Union also underlined[6] that the "the derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".

And proportionality

While the State has a margin of appreciation in choosing the necessary means, it has to assess whether the interference created by such measures corresponds to a 'pressing social need'[7].

The assessment of the proportionality of the derogation needs to be based on an examination of the purposes of that derogation and its scope of application. Various elements, such as the nature of the data concerned, how long it is stored for and the nature

[5] Handyside v. UK, 5493/72, §48.
[6] Digital Rights Ireland, C-293/12 of 8 April 2014, §52.
[7] Olsson v. Sweden, 10465/83.

of the processing will also have to be examined when assessing the proportionality of a PNR system.

In light of the severity of the interference with the rights to private life and data protection, the **purposes** need to be clearly and precisely defined on the basis of objective criteria which delimit the transmission to or access by the competent authorities to the data. The PNR can in no circumstances be used beyond such purposes (where it is the case, sanctions must be provided).

PNR systems' are generally being justified on the basis of the prevention, detection, investigation and prosecution of terrorist offences and 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 a particular complexity (see the relevant UN Conventions, the Council of Europe Convention on the prevention of terrorism of 2005 and its 2015 additional protocol) and in the absence of a clear definition, this terminology should be restrictively understood.

The crimes for which PNR data can be shared should be clearly defined as being serious crimes of a transnational nature (with a precise list of such crimes as previously mentioned) and/or of a particular gravity (for instance, crimes against humanity, torture, genocide or a crime entailing a custodial sentence or detention superior to a specified number of years).

In light of the degree of surveillance implied by such an indiscriminate system, an alternative could be a case-by-case use of passenger information where a serious and actual threat is objectively established.

The scope of application must also be clear and precise in order to allow a sound assessment of the proportionality. 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, the national ones in particular, the setting-up of dedicated coordination units (such as the proposed 'Passengers Information Units' in the proposed EU scheme) enables to prevent a mix between judicial and surveillance activities but the competencies of such units need to be strictly and narrowly defined and made public.

The data transmitted or accessed by the public authorities need to be adequate and proportionate according to their mission. They must be clearly defined, on the basis of objective criteria, and limits to the subsequent use of such data must also be established.

In order to demonstrate proportionality, a strict delimitation of the scope of application as regards the travel data shared is necessary. Will the PNR of all air passengers be shared with public authorities or only the ones relating to individuals who are being looked for? In the future will it also include data related to other forms of travel (train, boat, bus?). Will non air transport data only be shared where no other means of transport exist? Should all data relating to a crossing of frontiers, whichever transport is used, be shared? Or only for certain destinations and origins?

A time-limitation could also be considered, as for instance allowing for the sharing of information solely during defined periods (state of emergency, maximum alert level, etc.).

When should such data be 'pushed' (90, 72 or 24 hours before the departure time?) and how many times?

Which data will be requested (which fields of the PNR?)

Bearing in mind that PNR data is provided by the passengers or on their behalf, it is important to underline that someone knowing that such a surveillance system exists will adapt the itinerary of the travel, the method of payment and for instance the services requested to a non-suspicious pattern.

In light of the above, the Committee is of the opinion that a three-fold system could be considered, allowing for a first transmission of a basic list of passengers at the reservation stage (dates and time of travel, location of departure and destination and full name of the passenger).

Once this data is being transferred to the competent authorities, in case of positive match and concrete suspicion, a more detailed list of information related to the passenger concerned could be requested.

Finally, prior to the departure of the plane (once the aircraft doors have been closed), on the basis of the API, competent authorities could operate a final check.

The length of retention of the PNR data must also be clearly defined and limited to what is justified by objective criteria as its determination must be "based on objective criteria in order to ensure that it is limited to what is necessary"[8].

The Committee recommends that an initial short period (maximum of 30 days) 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). The Committee recalls that masked out data still permits identification of the individuals and continues as such to constitute personal data.

As previously mentioned, the assessment of the proportionality of the derogation needs to be based on a variety of elements, such as the type of data processed and the nature of the processing, which also brings the Committee to underline the risks arising from the data mining and data matching operated by the competent authorities on the basis of the PNR.

Data mining and matching

The processing of personal data is massive and indiscriminate as it concerns all passengers and may not be limited to a matching of data with the one 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 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.

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

The assessment aims both at detecting 'unknown persons' on the basis of pre-determined criteria and matching known suspects against other data sets.

Assessing passengers on the basis of PNRs data 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 (for which purposes were the other datasets created?) 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 its 2015 report[9], the European Commission for Democracy through law ('Venice Commission') noted that one "implication of the European Court of Human Rights' approach is that there must be legal authority for issuing selectors as regards the content of the data, and as regards metadata [communication data], for issuing instructions for contact-chaining and otherwise analyzing this data." The basic structure of the analyses should be transparent.

The Committee notes that the data mining exercise is by its very nature of a dubious reliability, as looking for a small number of persons amongst millions of passengers will inevitably induce a high rate of false positives, i.e. people being wrongly labelled as "high risk" by the system and/or false negatives (actual criminals and terrorists not being identified as their behaviour is adapted to correspond to a 'normal' one).

It is worth repeating that the accuracy and relevance of the raw data on which the analysis is based can be questioned (provided by the passengers themselves, having the possibility to choose an ordinary and non-suspicious itinerary for instance).

Matching data of different datasets should only be allowed in specific cases, such as suspicion of guilt of a targeted individual, and on the basis of data sets which have been clearly listed beforehand (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 reviewed on a case-by-case basis, in a non-automated manner and the reasoning of the processing should be known of the data subject objecting to it.

Finally, the Committee recalls that the criteria used for the data mining and matching can in no circumstances be based on the following special categories of data (Article 6 of Convention 108): racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life.

[9] Report on the Democratic oversight of the security services and of signal intelligence agencies, §96. https://www.coe.int/t/dghl/standardsetting/media/conf-foe-2015/Venice%20Commission_Study%20No%20719_2013.pdf

Prohibition of the transmission of sensitive data

While PNRs should not contain any information that is not needed to facilitate a passenger's travel, a number of sensitive data (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 under the open field containing general remarks (such as dietary or medical requirements) which can 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 have a duty to delete it, the Committee considers that a clear prohibition of the transmission of such sensitive data to the competent authorities should be established.

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 to every individual within the jurisdiction of the contracting Parties, whatever 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 non-suspected persons enjoy a full exercise of those rights and that for suspected persons, they may at least request the correction of inaccurate data and the deletion of unlawful data.

Any limitation of those rights must be made pro-actively available to the passengers at the time of collection of their data.

Passengers whose data is collected must be informed on how to exercise their rights and remedies available.

Security

As foreseen under Article 7 of Convention 108, appropriate security measures shall be taken for the protection of personal data which implies that the communication of the PNR and API data to the competent authorities must be protected by hard cryptography and that logs of the various accesses and uses of the data be kept.

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 is in the obligation to raise concerns as to possible gaps in the protection of data subjects if no effective laws of equivalent effect exist in the countries where the PNR data is stored or transferred.

In this respect, the Committee underlines that in its judgment of 6 October 2015 Maximillian Schrems v. Data Protection Commissioner (case C362/14), the Court of Justice of the European Union has invalidated the EU-US "Safe Harbour" agreement on the basis that the European Commission "did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments"[10].

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 but the Court ruled[11] that the absence of judicial control does not necessarily constitute a violation of the rights at stake as other strong safeguards could be provided for by the legislation (for instance independent oversight by authorities vested with sufficient powers and competence to exercise an effective and continuous control).

The Committee highlights the difficulties which exist in providing effective remedies against algorithm-based decisions and challenging inferences (false positives and other discriminatory measures).

The Committee considers that both an administrative and judicial remedy should be made available to persons concerned.

Oversight and transparency

It is clear from the case-law of the European Court of Human Rights that an oversight of the authorities performing 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 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.

[10] §94.
[11] Klass and Others v. Germany, §§ 55-56; Kennedy v. the United Kingdom, § 167.

Transparency on the powers and competencies of the PNR system can be achieved through the control of the data protection authorities, of specialised independent authorities in charge of overseeing intelligence agencies as well as through independent assessments of the efficiency by the competent authorities themselves.

Data protection officers should be designated within the competent authorities processing PNR and API data with a view to control the compliance of the system, the data processing and communication of the data, its updating and deletion, as well as the information provided to passengers. Data protection officers are encouraged to raise awareness on “good practices”

Conclusions

(…)