Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes

The European Union Agency for Fundamental Rights (FRA)

Having regard to Article 2 of Regulation 168/2007 requesting FRA to provide assistance and expertise relating to fundamental rights to institutions of the Community in order to support them when they take measures or formulate courses of action within their respective spheres of competence to fully respect fundamental rights

Having regard to Article 3/2 of Regulation 168/2007 stating that FRA shall refer to fundamental rights as defined in Article 6/2 of the Treaty on European Union when carrying out its tasks

Having regard to the Treaty on European Union, and in particular its Article 6/2

Having regard to Article 4/2 of Regulation 168/2007 empowering FRA to give opinions and conclusions concerning proposals of the European Commission or positions taken by the institutions to the EU institutions on request

Having regard to the request for an opinion on the proposal for a council framework decision, COM (2007) 654, on the use of Passenger Name Record (PNR) for law enforcement purposes in accordance with Article 4/2 of Regulation 168/2007 received on 18 September 2008 from the Presidency of the European Union,

Having regard to and building upon the following opinions of other institutions and bodies on this proposal: (a) Opinion of the European Data Protection Supervisor; and (b) Joint opinion of the Article 29 Working Party and the Working Party on Police and Justice.

Has adopted the following opinion

A. Introduction

1. The Presidency of the European Union requested on 3 September 2008 an opinion of the FRA within its mandate on the proposed Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, COM (2007) 654 (henceforth the Proposal). The FRA welcomes this request for its opinion.

B. Focus of the opinion

2. This opinion focuses on three fundamental rights:
   I. The right to respect for private life according to Article 8 of the European Convention of Human Rights and Article 7 of the Charter of Fundamental Rights of the European Union;
   II. The right to data protection according to Article 8 of the Charter of Fundamental Rights of the EU;
   III. The prohibition of discrimination according to Article 21 of the Charter of Fundamental Rights of the European Union.

C. Right to respect for private life (Article 8 of the European Convention of Human Rights and Article 7 of the Charter of Fundamental Rights of the EU)

3. The Annex to the proposal of the Commission for a Council Framework Decision on the use of PNR data for law enforcement purposes lists the (19) data concerned:

   (1) PNR record locator;

   (2) Date of reservation/issue of ticket;

   (3) Date(s) of intended travel;

   (4) Name(s);

   (5) Address and Contact information (telephone number, e-mail address);

   (6) All forms of payment information, including billing address;

   (7) All travel itinerary for specific PNR;

   (8) Frequent flyer information;

   (9) Travel agency / Travel agent;

   (10) Travel status of passenger including confirmations, check-in status, no show or go show information;

   (11) Split / Divided PNR information;

   (12) General remarks (excluding sensitive information);

   (13) Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, Automated Ticket Fare Quote fields;

   (14) Seat number and other seat information;

   (15) Code share information;

   (16) All baggage information;

   (17) Number and other names of travellers on PNR;

   (18) Any collected API information;

   (19) All historical changes to the PNR listed in numbers 1 to 18.

4. The processing of such personal data constitutes an interference with the right to respect for private life, under Article 8 of the European Human Rights Convention and Article 7 of the Charter of Fundamental Rights of the EU.[1] Such interference is only permitted under three conditions which are cumulative. Each condition has an autonomous function to fulfil:

   I. The objective must be legitimate and meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others according to Article 52 of the Charter of Fundamental Rights of the EU;

[1] According to the European Court of Human Rights, 'the storing of information relating to an individual's private life in a secret register and the release of such information come within the scope of Article 8 § 1' (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48 ; Kopp v. Switzerland, 25 March 1998, Reports of Judgments and Decisions 1998-II, p. 540, § 53 ; Amann v. Switzerland [GC] judgment (Application no. 27798/95), § 65, ECHR 2000-II ; Rotaru v. Romania judgment of 4 May 2000 (Application no. 28341/95), § 43 ; Segerstedt-Wiberg and Others v. Sweden judgment of 6 June 2006 (Application no. 62332/00), § 73).

II. The conditions under which the restriction is imposed must be provided for by law, in legislation or regulations which must be accessible to the individual concerned and protect that individual from arbitrariness through, inter alia, precision and foreseeability;

III. The means chosen must be proportionate to the end pursued so that they can be considered necessary and genuine. A disproportionate infringement of the right to respect for private life is not allowed, even for the sake of achieving highly desirable objectives.

C.1. Legitimacy

5. At a general level, preventing and fighting terrorist offences and organised crime are legitimate objectives, and they correspond to a "pressing social need" and objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others according to Article 52 of the Charter of Fundamental Rights of the EU.

C.2. Accordance with the law

6. Article 52 of the Charter of Fundamental Rights requires that any restriction to the right to respect for private life be 'in accordance with the law'. This 'not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects'.2 According to the European Court of Human Rights, a rule is 'foreseeable' 'if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct'.
7. This requirement of precision constitutes an essential guarantee against arbitrariness in the imposition of restrictive measures, and such protection is even more important as regards secret surveillance measures, due to the heightened risks of arbitrariness in such circumstances.[3]
8. Therefore, any measure giving the authorities a power to interfere with the right to respect for private life by collecting and further processing personal data should contain explicit, detailed provisions concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information thus obtained.[4]
9. The Proposal contains a few open-ended formulations which do not provide the required degree of certainty:

I. Among the PNR data to be collected, the proposal refers under 'item 12' 'General remarks (excluding sensitive information)' to the list of PNR data

---

[2] Rotaru v. Romania judgment of 4 May 2000 (Application no. 28341/95), § 52

[3] Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82, p. 32, § 67 ('Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference') ; reiterated in Segerstedt-Wiberg and Others v. Sweden judgment of 6 June 2006 (Application no. 62332/00), § 76.

[4] Rotaru v. Romania judgment of 4 May 2000 (Application no. 28341/95), § 57.

appended to the proposal). The content of what may be indicated under this item should be further specified.

II. In the Proposal, any retention of PNR data by law enforcement authorities and any exchange of such data between them should be done exclusively for the purpose of preventing and combating terrorist offences and organised crime, and these expressions are in turn defined by reference. Concerning the definition of "terrorist offences" the Proposal refers to the very broad catalogue in Articles 1 to 4 of the Council Framework Decision 2002/475/JHA on combating terrorism. In order to clarify the term "organised crime" the Proposal refers to "Article 2 of the Council Framework Decision (xx/xx) on the fight against organised crime". As this Council Framework Decision has not been adopted, the reference made in the Proposal has no substance.

III. According to the Proposal, PNR data may be processed to identify associates of persons who are or may be involved in offences related to terrorism or organised crime. However, nowhere is the term "associate" defined. The term "associate" is an imprecise term which could encompass family, friends, but also acquaintances or, more distant, colleagues.

10. Since such open-ended formulations do not provide the required degree of certainty, they need to be avoided. In all cases identified, wording should also be added to improve the precision of these provisions and to identify those fundamental rights applicable for data subjects. Furthermore, such open-ended formulations are also incompatible with the two requirements, first that data can only be collected for specified and explicit purposes and, second, that data to be collected and transmitted for the purpose of combating terrorism and organised crime should, in a democratic society, be necessary, proportionate and not excessive.

11. According to Article 3(3) of the proposed Framework Decision, the PIU to be designated in each Member State shall be responsible for 'analysing the PNR data' and for 'carrying out a risk assessment of the passengers in order to identify the persons requiring further examination'. This processing of PNR data should serve to 'identify persons who are or may be involved in a terrorist or organised crime offence, as well as their associates'; 'to create and update risk indicators for the assessment of such persons'; 'to provide intelligence on travel patterns and other trends relating to terrorist offences and organised crime'; 'to be used in criminal investigations and prosecutions of terrorist offences and organised crime' (Art. 3(5)).

12. Thus, the objective is not merely to identify known terrorists or individuals known to be involved in organized crime. The added value of PNR data is justified by the European Commission, in its proposal, precisely because of the proactive nature of the system it intends to establish – a system which, indeed, seeks to develop 'profiles' and associate, for example, individuals known to be linked to terrorist organisations and others, who might be linked by following the same travel routes or having the same travel patterns or history.

13. The use made of data concerning any specific individual will depend on the comparison between the data relating to that individual and other individuals, whether known or not known to be linked to terrorist organisations or to organised crime. This results in a situation in which it is not possible for any individual to know which use shall be made of his/her PNR data, a situation incompatible with the requirement of "foreseeability" imposed under Article 8(2) of the European

Convention on Human Rights, which stipulates that any restriction to the right to respect for private life should be 'in accordance with the law'.

C.3. Proportionality

14. Only an interference which is necessary to achieve a legitimate objective is proportionate. The main difficulty in evaluating the necessity and proportionality of the restrictions to the right to respect for private life and the protection of personal data brought about by the processing of PNR data, as currently envisaged, is that the Fundamental Rights Agency has received very little information about the usefulness of such processing for the purposes of combating terrorism or organised crime.

15. In the Explanatory Memorandum (under 1. General Context) the European Commission states that: "Currently, arrangements for the transmission of PNR data in the context of the fight against terrorism and transnational organised crime have been concluded between the EU and the United States and Canada and are limited to travel by air. These require that air carriers, which were already capturing the PNR data of passengers for their own commercial purposes, are obliged to transmit these data to the competent authorities of the USA and Canada. On the basis of an exchange of information with these third countries, the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes. The EU has further been able to learn from the experiences of such third countries in the use of PNR data, as well as from the experience of the UK from its pilot project. More specifically, the UK was able to report numerous arrests, identification of human trafficking networks and gaining of valuable intelligence in relation to terrorism in the two years of the operation of its pilot project."

16. While FRA has no specific reason to doubt the claims of the European Commission, it was not provided with, nor does it have, the necessary evidence in order to formulate a conclusive and independent opinion on the necessity of processing PNR data in the EU Member States. FRA can only confirm that the necessity and added value of the use of PNR for law enforcement purposes in order to fight terrorism and organised crime would need to be demonstrated clearly and beyond doubt using robust and convincing evidence in order for the interference to be proportionate.

17. PNR data are 'a record of each passenger's travel requirements containing all the information necessary to enable reservations to be processed and controlled by the air carriers for each journey booked by or on behalf of any person.' (Art. 2(c) of the Proposal for a Framework Decision). This data processing operation, however, was originally not designed for law enforcement purposes, but for commercial purposes.

18. It is required under Article 7 of the Charter of Fundamental Rights of the EU that any measure restricting the right to respect for private life be strictly tailored to the legitimate aims justifying such restrictions. It follows that, in principle, the author of any such measure should clearly define the objective served by the collection and processing of personal data, and only then decide which of these personal data should be processed, and by what means. This method would ensure that proportionality is taken into account from the outset.

19. In this instance the contrary has happened: As it was found that airline companies were already processing PNR data for commercial purposes, it was considered that the transfer of these data to PIUs and, subsequently, to other law enforcement

agencies, could be justified as contributing to their intelligence-gathering and – processing capacities.[5] Thus, instead of being guided by a clear understanding of what type of data are required in order to combat terrorism and organised crime, the choice of the personal data to be processed as well as the scope of the processing were guided by other considerations – including the minimisation of costs and administrative burdens for the air carriers concerned – rather than by a concern for limiting the restrictions to the right to respect for private life and to the protection of personal data to the minimum compatible with the objective of providing EU citizens with a high level of security.

20. In the light of this it is necessary to scrutinise exactly how processing of personal data contributes to the aim of combating terrorism and organised crime in order to ensure proportionality.

21. Furthermore, in order to minimise the restrictive impact of any new instrument on PNR data on the right to respect for private life of individuals and the protection of personal data, the adoption of any such instrument should be preceded by a detailed review of existing measures, which already provide for the processing of data relating to individuals travelling to the EU from abroad, in order to specify why these measures do not suffice to provide the additional intelligence required.

22. These instruments are the Visa Information System[6] and the Schengen Information System, now entering its second generation.[7] Similarly, a review of the implementation of the obstacles facing the implementation of Directive 2004/82/EC of 29 April 2004 on the obligation of air carriers to communicate passenger data would be advisable in order to frame adequately new proposals concerning the processing of more data by air carriers for law enforcement purposes.

23. In conclusion, in order to ensure proportionality, it is essential to demonstrate effectively that all personal data collected under the PNR proposal are beyond any doubt absolutely necessary for combating terrorism and organised crime. In particular, it is important to demonstrate that these data would have to be collected, even if they were not readily available from air carriers, as essential elements for effective law enforcement against terrorism and organised crime.

---

[5] See, e.g., the justification for limiting the scope of the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes to air transport, excluding for the moment sea, rail and road transport : this option, preferred by the majority of those consulted by the Commission, 'is generally based on the fact that air carriers already have systems with which they capture PNR data and it would therefore be easier for them to comply with the proposal' (Summary of the Impact Assessment of the proposal for a Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, SEC(2007) 1422, p. 6).

[6] See Council Decision (2004/512/EC) of 8 June 2004 establishing the Visa Information System (VIS) (OJ L 213, 15.6.2004, p. 5), and the following extensions : Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129 ; Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60) ; Proposal for a Regulation of the European Parliament and of the Council of [...] amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code (COM/2008/0101 final, of 22.2.2008).

[7] See Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63), Council Regulation (EC) No 189/2008 of 18 February 2008 on the tests of the second generation Schengen Information System (SIS II) (OJ L 57, 1.3.2008, p. 1), and the Proposal for a Council Regulation on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) (COM(2008)197 final, of 16.4.2008).

D. Protection of personal data (Article 8 of the Charter of Fundamental Rights of the EU)

24. The protection of personal data also involves positive obligations. As illustrated by the case of Sari and Colak v. Turkey at the European Court of Human Rights, where national legislation should organise the regime for the exercise of fundamental rights, it may not be sufficient to disregard any provision or set of provisions, which are incompatible with the requirements of international human rights. Instead, a positive obligation is imposed on States to provide the necessary legislative framework, which a judge will normally not find it within his/her power to establish.[8]

25. The proportionality of the substantive provisions of any legal instrument for processing of PNR data for law enforcement purposes cannot be adequately evaluated without considering its procedural safeguards. This is clear from relevant case-law of the European Court of Human Rights.9 As noted by the Court, this applies to an even greater extent as regards secret surveillance measures, since secrecy 'carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole (...). This being so, the resultant interference can only be regarded as "necessary in a democratic society", if the particular system of secret surveillance adopted contains adequate guarantees against abuse.'[10]

26. Regarding the automated processing of personal data, reference should be made to the guarantees listed in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which may be seen as making explicit, in its specific field of application, the requirements which follow from the right to respect for private life and the protection of personal data. It is important to ensure that the instrument prescribing the processing of PNR data for law enforcement purposes describe in detail which guarantees will apply.

27. In this regard, a general reference to the principles regulating processing of personal data, or to the future Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which does not as yet exist, will probably not suffice. Firstly, because the scope of application of this latter instrument is expected to be narrow and may not cover all the processing of PNR data for combating terrorism and organised crime; and, secondly, because the scope of application of this latter instrument and of Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data is uncertain. Even more importantly, the procedural rights of the data subject should be spelled out explicitly in any instrument prescribing the processing of PNR data for law enforcement, because the effective exercise of these rights under personal data

---

[8] Eur. Ct. HR (2nd sect.), *Sari and Colak v. Turkey* (Appl. N° 42596/98 and 42603/98) judgment of 4 April 2006, § 37.

[9] See Klass and others v. Germany judgment of 6 September 1978, §§ 50-60 ; Malone and Others v. the United Kingdom judgment of 2 August 1984, § 81; Segerstedt-Wiberg and Others v. Sweden judgment of 6 June 2006 (Application no. 62332/00), § 103.

[10] Malone and Others v. the United Kingdom judgment of 2 August 1984, § 81. See also the Rotaru v. Romania judgment of 4 May 2000, § 59 : 'In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure'.

protection law (e.g., right to information about the identity of the controller and about the purposes of the processing for which the data are intended, the right of access to data, and the right to rectification) requires that the data subject must be well informed about the procedures which should be followed and the respective obligations of the data collector, for example the air carriers, and the PIU.

28. The Commission proposal on the use of PNR for law enforcement purposes is silent on the right of access of data subjects to data which has been collected concerning him or her, and the right to have it rectified. The proposal also does not specify which independent authority shall control compliance with data protection standards. Both are required under Article 8 of the Charter of Fundamental Rights.

29. Article 8 of the Proposal extends the application of the data protection framework decision to the transfer of PNR data to third countries. The Article also provides for some specific conditions and safeguards as regards to the transfer of PNR data to third countries. It requires the consent of the Member State in case of onward transfer and, in addition, introduces the requirement that the transfer should comply with the national legislation of the Member State concerned, as well as any applicable international agreement.

30. A matter of principle that is raised by the transfer of PNR data to third countries is that of ensuring an adequate level of protection of PNR data in the recipient country. The European standard of data protection cannot always be ensured when personal data are processed outside the European Union. Given also the lack of binding international rules regarding processing of data for law enforcement purposes, the transfer of PNR data to third countries creates the risk of serious infringements of fundamental rights.

31. In this light, it is particularly problematic that Article 8 of the Commission's proposal makes no reference to the most fundamental principle pertaining to conditions of transfer to third countries, i.e. the principle that an adequate level of protection of data protection must be ensured and monitored. The "adequate level of protection" as required in the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data is not requested in the Proposal. In this respect, reference is only made to the "the requirements and guarantees according to the Council Framework Decision on the protection of personal data processed in the context of police and judicial cooperation in criminal matters". This Council Framework Decision, however, does not yet exist. The requirement in Article 8 lacks precision and purpose. Article 8(1)(a) simply states that a Member State may relay PNR-data to the investigating authorities of a third country "if it is sure that the authorities of the third country will use the data exclusively for the purpose of preventing and combating terrorism and organised crime". The reference to "organised crime" is too broad. Furthermore, no control mechanisms are set up which could provide an indication as to when the member state can "be sure". As European Union data protection standards do not apply in third countries, it is essential to have corresponding safeguard mechanisms which are as strong as possible, or risk an uncontrolled dissemination of data outside the European Union. Moreover, even if such strong safeguards are included, a safeguard mechanism may be breached by the authorities of a third country and an aggrieved individual may not have an effective remedy.

32. This is precisely why Directive 95/46/EC considers that 'the transfer of personal data to a third country which does not ensure an adequate level of protection must be

prohibited'.[11] In particular, the adequacy of the level of protection to be guaranteed in the State to which personal data are transferred is to be assessed taking into account 'all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country'.[12]

33. It could be argued that the data are given freely by the passengers; passengers could be seen to have consented to the data collection and processing. According to the data protection regulation of many Member States and the European Union, it is significant whether the data subject has given his or her consent unambiguously and voluntarily to the proposed transfer of personal data (see for example Article 26 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data). Such consent can indeed justify the collection and processing of data. Nonetheless, Article 2(h) of Directive 95/46/EC provides that "'the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." Accordingly, consent can hardly justify the measures foreseen in the Proposal since the legal framework is too vague, as mentioned above. More importantly though, as denying consent will inevitably lead to the consequence of not being allowed to travel, it is questionable, if this form of consent can really be interpreted as voluntary.

E. Prohibition of discrimination (Article 21 of the Charter of Fundamental Rights of the EU)

34. Under the Proposal, PNR data can and would be used for 'profiling' purposes; this is actually among the very reasons why the PNR data are processed in the first place. Although PNR data as such does not qualify as sensitive data, the profiling of such data for law enforcement purposes can reveal a number of sensitive information about the individual, particularly when combined with information obtained from other sources.

35. 'Profiling' is generally defined as the systematic association of sets of physical, behavioural or psychological characteristics with particular offences and their use as a basis for making law-enforcement decisions. Profiles can be either descriptive, i.e. designed to identify those likely to have committed a particular criminal act and thus reflecting the evidence the investigators have gathered concerning this act; or they may be predictive, i.e. designed to identify those who may be involved in some future, or as-yet-undiscovered, crime.[13]

---

[11] 57th recital in the preamble to Directive 95/46.

[12] Article 25(2) of Directive 95/46. See also Article 29 Working Party, Working Document *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24th July 24 1998, WP 12 ; and see, as regards the adequacy of the level of protection of personal data in the United States, Article 29 Working Pary, Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to be Transferred to the United States Bureau of Customs and Border Protection (US CBP), at:
http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2004_en.htm.

[13] See Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/4/26, 29 January 2007, at paragraph 33. See also E.U. Network of Independent Experts on Fundamental Rights, *Ethnic profiling*, CFR-CDF.Opinion4-2006, p. 9-13.

36. Profiling is, in principle and at least in its descriptive form, a permissible means of law-enforcement activity. Detailed profiles based on factors that are statistically proven to correlate with certain criminal conduct may be effective tools in order to better target limited law-enforcement resources. However, when law-enforcement authorities use broad profiles that reflect untested generalisations, their practices may constitute disproportionate interferences with fundamental rights. In particular, profiling based on stereotypical assumptions that persons of a certain 'race', national or ethnic origin, religion, intellectual disabilities or mental illness are particularly likely to commit crime may lead to practices that are incompatible with the prohibition of discrimination.

37. Profiling can also be used in the context of data-mining initiatives, i.e. searches of personal data sets according to presumed characteristics of suspects. As already noted, profiling is actually among the very reasons why the PNR data are processed in the first place. Thus, profiling within the context of PNR data raises concerns with regard to the prohibition of discrimination on grounds such as race, national or ethnic origin and religion.

38. Reports published on earlier measures of profiling in e.g. Germany and the United Kingdom, do not confirm at all at this stage the efficiency of profiling of personal data on grounds based on or associated with ethnicity, national origin or religion.[14] Rather, the available evidence suggests that profiling practices based directly on, or factually targeting, ethnicity, national origin or religion are an unsuitable and ineffective, and therefore a disproportionate, means of countering terrorism and organised crime: they affect thousands of innocent people, without producing concrete results. There is evidence to indicate that profiling practices, based on stereotypes, have not been any more successful than other crime prevention and law enforcement approaches in identifying offenders with respect to criminal activity.[15]

39. Moreover, even if the classifications underlying these methods did correspond to a higher risk posed by some categories of persons, this would still not mean that their use is justified. Some infringements of fundamental rights are unjustifiable irrespective of the aim they pursue and their effectiveness. Article 52(1) of the Charter of Fundamental Rights of the European Union provides that any "limitation (...) must (...) respect the essence of those rights and freedoms. (...)." Substantial interferences into the essence of a right are not "necessary in a democratic society" under the European Convention of Human Rights. Any mass profiling using stereotypical assumptions based on racial or religious criteria should be conceived as unjustifiable. Moreover, any form of ethnic profiling is likely to be illegal also in terms of international law because it infringes the guarantees of the International Convention on the Elimination of all Forms of Racial Discrimination. All Member States of the EU are bound by this Convention.

40. Terrorist-profiling practices entail considerable negative effects that must also be considered. The most significant adverse effect of profiling based on ethnicity, national origin and religion tends to be that it alienates and victimises certain ethnic and religious groups which in turn may have significant negative implications for law-

---

[14] For an overview of various studies and reports, see Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/4/26, 29 January 2007, especially at paragraphs 47-58.

[15] Empirical research from the United States indicates that the resultant 'hit rate' from ethnic profiling practices, that is the apprehension of criminals through ethnic profiling, is not as high as one would assume, and can be challenged as an efficient tool for identifying criminals (Harris, D.A. (2006) 'US Experiences with Racial and Ethnic Profiling: History, Current Issues, and the Future' *Critical Criminology*, Vol.14, No.3, pp.213-239.

enforcement efforts, as it involves a deep mistrust of the police. There is a wealth of evidence by researchers to indicate the negative social consequences of discriminatory profiling practices, which may serve to enhance reactions and actions against the State as, in part, a reflection of perceived and real discrimination against certain communities.

41. Despite the human rights concerns stemming from e.g. the principle of non-discrimination, the use of terrorist profiles that include criteria associated with ethnicity, national origin and religion is not always forbidden. If, in the context of an investigation into a terrorist crime already committed, there are reasonable grounds to assume that the suspect fits a certain descriptive profile, then the reliance on characteristics such as ethnic appearance, national origin or religion is justified. Similarly, these factors can be employed to target search efforts where there is specific intelligence suggesting that an identifiable individual fulfilling these characteristics is preparing a terrorist act.

42. The situation is different, however, in the case of preventive counter-terrorism efforts that are not intelligence-led. While profiles used for such efforts may include behavioural or psychological characteristics, they must not be based on stereotypical generalisations that certain ethnic or religious groups pose a greater terrorist risk than others. Profiling based on behavioural patterns is significantly more efficient than reliance on ethnicity, national origin or religion. Any profiling related to PNR data must therefore be based on more specific individual, preferable behavioural, factual parameters. To this end, the FRA is conducting research on discriminatory profiling practices in the EU, which will result in the publication of a Handbook identifying practical measures to target and respond to discriminatory profiling. (The results of this work will be published by the Agency at the beginning of 2009).

43. In conclusion, the techniques using the profiling of PNR data must comply with a number of human rights guarantees, particularly the guarantees of non-discrimination. Given that no information clearly confirms at this stage the efficiency and utility of profiling practices based on ethnicity, national origin or religion, such practices should be considered to constitute unlawful discrimination. Therefore, they should be explicitly banned.

44. It is to be welcomed that the draft Framework Decision includes a clause (Article 3 (3) in fine) according to which 'No enforcement action shall be taken by the Passenger Information Units and the competent authorities of the Member States only by reason of the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation." Accordingly, profiling "by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation" as such is not excluded, just enforcement action on this basis.

45. However, while such a clause may bar enforcement action under the stated conditions, it is likely that the 'analysis and risk assessment' called for under the same provision and based directly on notions such as 'associates', 'risk indicators' 'travel patterns and other trends' would indirectly and in fact be related to at least some of the prohibited or at least suspect parameters in question. Therefore, it would be important to add wording which explicitly prevents this and to closely monitor who in fact becomes targeted by the proposed risk assessment and whether the implementation of the Framework Decision will result in indirect discrimination on account of ethnicity, national origin or religion.

46. The protection from discriminatory profiling also calls for procedural safeguards. This is clear from the relevant case-law of the European Court of Human Rights.16 As noted by the Court, this applies even to a greater extent as regards secret surveillance measures, since secrecy 'carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole (...). This being so, the resultant interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse.'17 In this context, it could be considered that the Proposal explicitly should provide for control by an independent authority.

F. Summary of Conclusions

47. The proposal contains open-ended and imprecise formulations (e.g. "general remarks", "associates", "terrorist offences", "organised crime"). The data processing operations to be undertaken by authorities should be defined and specified precisely in order to ensure that data processing operations on the basis of PNR data are foreseeable by data subjects. This requirement of precision constitutes an essential guarantee against arbitrariness in the imposition of restrictive measures, and such protection is even more important as regards secret surveillance measures, due to the heightened risks of arbitrariness in such circumstances.

48. More explanation and evidence is needed to demonstrate beyond doubt that the collection and use of PNR data for law enforcement purposes is necessary and adds value to the fight against terrorism and organised crime in order to meet the requirement of proportionality inherent in the right to respect for private life.

49. Before adoption of this measure to create a system to collect and use PNR data for law enforcement purposes, a detailed review of the already existing measures (Visa Information System, Schengen Information System, Directive 2004/82/EC) should be completed with a view to determining why these existing measures do not suffice to provide the additional intelligence required.

50. The proposal should contain sufficient procedural safeguards. As it stands, the proposal provides neither for mandatory rights of data subjects according to Article 8 of the Charter of Fundamental Rights (right of access, right of rectification), nor for control by an independent authority. A general reference to another data protection instrument will not suffice in this regard. Effective exercise of rights of data subjects requires that the data subject be clearly informed about the applicable procedures.

51. Article 8 of the proposal should ensure that data transfers to third countries are only possible if an adequate level of protection of PNR data is ensured and monitored in the recipient country.

---

[16] See Klass and others v. Germany judgment of 6 September 1978, §§ 50-60 ; Malone and Others v. the United Kingdom judgment of 2 August 1984, § 81; Segerstedt-Wiberg and Others v. Sweden judgment of 6 June 2006 (Application no. 62332/00), § 103.

[17] Malone and Others v. the United Kingdom judgment of 2 August 1984, § 81. See also the Rotaru v. Romania judgment of 4 May 2000, § 59 : 'In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure'.

52. Wording should be added which ensures that profiling based on PNR data is intelligence-led, based on more specific individual, preferably behavioural, factual parameters. Profiling based on stereotypical generalisations about ethnic, national or religious groups should be explicitly banned and there is a need to closely monitor who in fact becomes targeted by the proposed risk assessment to ensure compatibility with the prohibition of discrimination.