From: Paulien de Morree [mailto:P.DeMorree@Forum.nl]
Sent: 21 June 2011 17:08
To: BUZEK Jerzy, President
Subject: Note of the Meijers Committee on the Proposal for a Directive on the use of PNR data regarding terrorist offences and serious crime

Dear Mr Buzek,

Please find attached a copy of a letter and a note at the attention of the Commissioner for Home Affairs, Ms Malmström, by the Meijers Committee - the standing committee of experts on international immigration, refugee and criminal law - regarding the Commission proposal for a Directive on the use of PNR the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)32). In this note, the Meijers Committee shares some of its concerns regarding this recent proposal.

Kind regards,
Paulien de Morree.

P.E. de Morree, MSc LLM
secretary

Meijers Committee
Standing committee of experts on
internationaal immigration, refugee
and criminal law

Postbus 201, 3500 AE Utrecht
The Netherlands
Tel: +31 (0)30 297 4328
Fax: +31 (0)30 296 0050
p.demorree@forum.nl
http://www.commissie-meijers.nl

Meijers Committee
Standing committee of experts on
international immigration, refugee
and criminal law

Secretariat
p.o. box 201, 3500 AE Utrecht/The Netherlands
phone 0031 30 297 43 28/43 21
fax 0031 30 296 00 50
e-mail cie.meijers@forum.nl
http://www.commissie-meijers.nl

[redacted] [redacted]

To (by e-mail) Ms Cecilia Malmström
Commissioner for Home Affairs
EUROPEAN COMMISSION
B-1049 BRUSSELS

Reference CM1108
Regarding Directive on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)32)
Date Utrecht, 21 June 2011

Dear Commissioner, Ms Malmström,

Please find attached a note of the Meijers Committee, the Standing committee of experts on international immigration, refugee and criminal law, regarding the proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)32 final) of 2.2.2011.
A somewhat adjusted version of this note is recently published by the Centre for European Policy Studies (CEPS).[1]

Considering the risks of violation of the right to non-discrimination, privacy and data protection, the freedom of movement of EU citizens and lawfully resident third-country nationals, and the high costs for the individual Member States and air transport organisations, the Meijers Committee recommends the withdrawal of the proposed PNR Directive.

The Meijers Committee notes that earlier criticisms of the European Parliament, the EDPS, and other stakeholders with regard to the necessity and proportionality of the 2007 PNR Directive has not or only partially been taken into account. The new proposal (COM(2011)32) does not offer clear rules with regard to the powers of national authorities to use PNR data or to transfer these data to other countries, nor does it include sufficient safeguards to protect the fundamental rights of individuals. The proposal lacks in particular harmonised rules with regard to the following subjects:

- purpose limitation;
- data retention;
- transfer of data to third countries;
- individual rights;
- legal remedies;
- powers of supervisory and judicial authorities.

[1] E. Brouwer, "Ignoring Dissent and Legality: The EU's proposal to share the personal information of all passengers", in: *Justice and Home Affairs, CEPS Liberty and Security in Europe*, 17 June 2011.

Furthermore, the Commission does not provide real evidence of the necessity or added value of the current PNR proposal for the prevention or prosecution of terrorist offences or serious crime also taking into account existing measures such as the API Directive, the Schengen information System, and the exchange of information based on the Prüm Treaty. The Meijers Committee underlines that these measures should be evaluated first to establish the existence of any 'security gap'. Without this information on the necessity or added value, it must be concluded that this proposal does not meet the general principle of proportionality, which is one of the general principles of European Union law requiring that measures implemented by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it.

Any new draft on the transfer of PNR data should include an extended impact assessment with reliable and up-to-date information on the efficiency, financial costs, and consequences with regard to the aforementioned fundamental rights.

If the aforementioned requirements are met, any future proposal on the use of PNR data should include precise criteria limiting the discretionary powers of national authorities, limitative grounds on which data may be collected, the authorities 'competent' to receive and use such data, time limits for data retention, and applicable safeguards and sanctions for misuse or incorrect use of data. Furthermore, the rights and legal remedies for individuals with regard to the collection and use of their data should be formulated more precisely, including the right to information and the right to financial repair. Should any questions arise, the Meijers Committee is prepared to provide you with further information on this subject.

Yours sincerely,

C.A. Groenendijk

Prof. C.A. Groenendijk
chairman

cc. The President of the European Parliament, Mr J. Buzek
The member of the LIBE-committee of the European Parliament
Director-General for Justice and Home Affairs of the Council of the EU, Mr I. Bizjak
Commissioner for Justice, Ms V. Reding
EDPS

Reference CM1108
Regarding Directive on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)32)
Date Utrecht, 21 June 2011

1 Purpose and necessity of the PNR proposal

In February 2011, the European Commission published a proposal for a new Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.[2] This proposal follows and replaces an earlier draft for a Framework Decision of 2007 on the use of PNR for law enforcement purposes.[3] The draft Framework Decision, which primary goal was the fight against terrorism and organised crime, has been critically received by the European Parliament, the EDPS, the EU Agency for Fundamental Rights, Article 29 Working Party, and other organisations. In their comments, these organisations criticised in particular the lack of evidence on the necessity and proportionality of the proposed measure, the insufficient level of data protection, and the risks of profiling and transfer of data to third countries. With regard to the new proposal of the Commission, the EDPS, the Article 29 Working Party and the European Economic and Social Committee repeated many of their earlier criticisms.[4]

Comparing the current proposal with the earlier draft of 2007, the Commission took into account some criticisms of the aforementioned stakeholders. With regard to the data retention periods the original time limit of thirteen years has been reduced to five years. Furthermore, in response to the criticism of European Parliament and EDPS with regard to the differentiation between pull- and push methods in the 2007 proposal (push method for EU carriers, and a combination of push and pull for third country carriers) the Commission proposal now provides for an exclusive use of the push method.[5] However, despite these improvements, the new proposal does not really narrow the scope of its application, nor does it provide extra safeguards. On the contrary, in stead of limiting the goals for which Member States may use PNR data, the current proposal further extends the purpose of this instrument. Whereas the earlier draft Framework Decision on the use of PNR data was limited for the purpose of 'preventing and combating terrorist offences and organised crime', this has been changed in the new PNR proposal into 'the prevention, detection, investigation and prosecution of terrorist offences and serious crime'. Especially the use of the definition 'prevention, detection, and investigation' and of 'serious crimes' leaves the national authorities a wide margin of appreciation, which will result in large differences between the Member States implementing this Directive.

For the definition of serious crime and serious transnational crime, the proposal refers to the Framework Decision 2002/584 on the European Arrest Warrant, which could be considered as a positive delimitation of crimes for which PNR data may be processed. However, the list of offences in Article 2 (2) of the Framework Decision still includes the possibility for a divergent practice in the Member States, including general definitions such as 'terrorism', 'participation in a criminal organisation', 'corruption', 'computer-related crime', 'facilitation of unauthorised entry and residence', or 'sabotage'. Furthermore, according to the explanatory memorandum, Member States may exclude minor offences if this would not be proportionate: this implies that in general PNR

[2] COM (2011) 32, 2.2.2011.
[3] COM (2007) 654.
[4] Opinion of the EDPS, 25 March 2011; Opinion 10/2011 of the Article 29 Data Protection Working Party, 5 April 2011; Opinion of European Economic and Social Committee, 5 May 2011, Council document 10169/11, 13 May 2011. See also the opinion of the European Union Agency for Fundamental Rights (FRA) of 14 June 2011.
[5] "Push method" means that carriers forward by own means the PNR data to the national authorities of the arrival or departure state, whereas "pull method" implies that the national authorities obtain the PNR data by having direct access to the reservation systems of the air carriers.

data may be processed for minor offences as well. Also, this possibility of exemption will result in a differentiated implementation of this Directive by the Member States. Finally, recital 28 of the preamble provides that the possibility remains for Member States to oblige air carriers to transfer PNR data for other purposes than those specified in the Directive.

According to the Meijers Committee, the reasons for the (extended) use of PNR data are not clarified. In the explanatory memorandum, the Commission refers to trafficking in human beings and drugs crime and illustrates the human and economic costs of these crimes, using rather random data of different sources, including for example data of the UK Home Office of costs incurred 'in anticipation of crime' of 2003. Furthermore, the Commission does not provide real evidence of the added value of using PNR data for the prevention or prosecution of these crimes. The European Commission only refers to examples of three countries (Belgium, Sweden, UK) in which a substantial number of drugs seizures would have been 'exclusively or predominantly' due to the processing of PNR data. These data are not further specified and, surprisingly, not mentioned at all in the impact assessment to this proposal. Furthermore, it seems odd that according to the Commission, Belgium reported that 95 % of all drugs seizures in 2009 were exclusively or predominantly due to processing PNR data, while according to the same impact assessment Belgium would not have implemented any PNR scheme yet.

2 Relationship with the API Directive

The Commission does not provide information on the implementation of the Directive on the use of Advanced Passenger Information (API) which has been adopted in 2004 and which implementation date exceeded in September 2006.[6] This Directive concerns the obligation of air carriers to transfer API data to border officials for immigration law purposes. The Meijers Committee notes that with regard to the added value for law enforcement and migration control purposes, it is important to differentiate between API and PNR data. Whereas API concerns data from the machine readable zone of the passport including name, date of birth, passport number, nationality, PNR data includes data which are registered by the airline companies or travel agencies when a traveller makes a reservation: including name of the person, seat number, travelling route, booking agent, credit card number etc. These PNR data collected for reservation purposes may differ for each air carrier organisation and do not always include the same categories of information. The most important difference between API and PNR is that the information which can be extracted from PNR data mainly depends from the data the passenger submits him- or herself to the ticket reservation system. Related to the passport information, API data offer national officers more objective and permanently valid information, permitting the identification of individuals. Whereas PNR data, including variable information on the passenger, including meals, contact information, travel agency may be useful for profiling, it is also less reliable information, being dependent on what the traveller submitted him- or herself when making a reservation. Furthermore, as has been pointed out as well by the AEA, Association of European Airlines, with respect to the identification of passengers the PNR data is not always consistent with the persons actually on board of the air carrier. The Meijers Committee notes in this regard, that the category (10) of PNR data to be collected, as described in the annex to the current proposal, is rather pointless. Referring to 'travel status of passenger, including confirmations, check-in status, no show or go show information', this includes data which is by definition not included in the PNR data, because this information will only be available when the passenger has (or not) checked in for his or her flight.

During negotiations on earlier drafts of the API Directive, the use of API was originally planned for immigration control purposes only. However, shortly before the final adoption of the Directive, a

[6] Directive 2004/82/EC of 29 August 2004. In June 2010, the Commission started an infraction procedure against Poland for failure to adopt necessary laws implementing the Directive, C-304/10, *OJ* C 246/22, 11.9. 2010.

provision has been added allowing Member States to use the passenger data for law enforcement purposes (Article 6). One would have expected an evaluation by the Commission of the current use of the API Directive, together with the existing large-scale databases in the EU, before proposing new measures of data collection. Although the Directive 2004/82/EC does not include a sunset clause or obligation for the Commission to evaluate this instrument it self, it is in line with the general policy of the Commission to assess 'the initiative's expected impact on individuals' right to privacy and personal data protection and set out why such an impact is necessary and why the proposed solution is proportionate to the legitimate aim of maintaining internal security within the European Union, preventing crime or managing migration however'. [7] This failure of identifying first the security gaps prior of existing systems and methods of cooperation, has been pointed out by the Article 29 Working Party in its opinion of April 2011 as well.[8] According to the Working Party, even if any gap would exist, then the next step should be to analyse the best way to fill this gap by exploiting and improving existing mechanisms, without necessarily introducing a whole new system.

3 Lack of harmonisation

According to the European Commission, the PNR proposal is necessary to harmonise national legislation on obligations for air carriers, preventing the creation of 27 'considerably diverging systems', which could result in 'uneven levels of data protection across the Union, security gaps, increased costs and legal uncertainty for carriers'. The goal of the current proposal is to guarantee 'a uniform standard of protection of personal data under any proposal, and provide legal certainty for individuals, commercial operators and law enforcement authorities'.[9]

Firstly, the Meijers Committee questions the claim of the Commission that this proposal is necessary to prevent '27 diverging systems' in the EU. At this time only three Member States provide legislation for the use of PNR.[10] This means that, rather than harmonising existing rules, this proposal will result in forcing a large majority of the EU Member States to adopt a new law enforcement measure. Secondly, with regard to important issues on the collection and use of PNR, the current proposal does not provide for harmonisation at all. As mentioned above, the purpose of using PNR data has not been narrowly defined and the proposal leaves the Member States a wide margin of interpretation by referring to 'serious crime' and 'serious transnational crime' and by including the aforementioned recital 28 of the preamble. In the next sections we will see that the proposal does not offer harmonised rules with regard to other important subjects as well, including:

- time limits;
- extension to internal flights;
- functioning of PIU's;
- authorities entitled to request or receive PNR data, and;
- transfer of data to third countries.

3.1 Time limits

Despite the shortening of the data retention periods from a maximum of thirteen years to a maximum of five years, the 2011 proposal still includes some questionable provisions extending the further use of PNR data. The proposed Article 9 differentiates between a period of 30 days after the transfer of PNR data in which they are retained in a database of the national Passenger Information Unit (PIU). After this period, the data will be stored for a further five years by the PIU's. In principle, during this period, all elements serving to identify persons will be 'masked' out,

[7] European Commission, COM (2010) 835, *Communication on Overview of information management in the area of freedom, security and justice*, p. 25.
[8] Opinion 10/2011, 5 April 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_en.pdf.
[9] Staff Working Paper Impact Assessment SEC (2011) 132, 2.2.2011, see p. 15 and 20.
[10] UK, France, and Denmark, with the remark that it is still unclear whether UK will decide for an opt in to this proposal. See Commission Staff Working Document on Impact Assessment, 2 February 2011, SRC (2011) 132.

meaning that after 30 days after the transfer of their data, passengers can no longer be identified on the basis of these data. However, during the period of five years access to full PNR data will remain possible for 'a limited number of personnel of national PIU's' specifically authorised to carry out analysis of PNR data and to develop assessment criteria according to Article 4(d) of the proposal. This latter provision allows the analysing of PNR data for the purpose of updating or creating new criteria for carrying out assessments in order to identify persons who may be involved in a terrorist offence or serious transnational crime. In other words, during these five years, personnel of PIU's may use non-anonymised data for the purpose of setting up new profiles. Furthermore, during the same period of five years, each head of the national PIU's may have access to the full data 'where it could be reasonably believed that it is necessary to carry out an investigation and in response to a specific and actual threat or risk or a specific investigation or prosecution.' Both the description of 'limited number of personnel' and 'specific investigation or prosecution' is too vague and allows disproportional use of passenger's data.

The Meijers Committee also notes that the proposed Directive allows the aforementioned time limit of 30 days cq. five years to be set aside by the Member States. Article 9 (3) of the proposal includes an exception to the obligation to delete PNR data after five years, where they have been transferred to national competent authorities and are used 'in the context of specific criminal investigations or prosecutions, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State'.

Finally, Article 9 (4) allows the PIU's to keep the results of matching based on PNR data for an indefinite period, namely 'as long as necessary to inform the competent authorities of a positive match'. Important is the provision which obliges the PIU's to keep data on so-called 'false' positive matches: these data should be kept for a maximum period of three years to avoid future false matches: however the proposal does not provide safeguards on the further retention of these data and on how other national authorities will be informed there has been a false match.

3.2 International and/or internal flights?

On the basis of the proposed Article 6, Member States will have the choice to decide whether the obligation on air carriers applies only to international flights arriving on their territory or also to departing flights. Currently, the Member States are negotiating the (optional) extension of this Directive to internal flights. This means that air carriers will have to deal with divergent rules applying in each Member States. This will result not only in high costs for each air carrier organisation, but also in a different treatment of travellers flying in or into the EU.

3.3 The functioning of the PIU's

The draft Directive does not offer harmonised rules on the functioning of the national PIU's. The PNR proposal allows differences between the Member States with regard to the assessments carried out on passenger data, the use and new creation of 'pre-determined criteria' for the PNR assessments, and the further transfer of data to law enforcement authorities, other Member States, or third parties. As will be set out below, the use of profiling and the assessment of individual behaviour solely based on PNR imply risks for the fundamental rights of travellers. The lack of harmonised criteria will increase these risks.

3.4 Authorities entitled to request or receive PNR data

Article 5 (1) of the proposal obliges Member States to adopt a list of competent national authorities entitled to request or receive PNR data or the result of processing PNR data by the PIU's. The Directive does not however give any further specification other than that these authorities should be 'competent for the prevention, detection, investigation or prosecution of terrorist offences and

serious crime'. The Meijers Committee notes that a comparable mechanism is chosen in the Data Retention Directive.[11] The list of authorities having access to telecommunications data, published in the recent evaluation report on the implementation of the Data Retention Directive of the European Commission, establishes many differences between the Member States.[12] These differences concern in the first place the scope of 'competent national authorities'. According to this evaluation, fourteen Member States include security and intelligence services, six Member States list tax and/or customs authorities and three list border authorities. Secondly, the list establishes many differences with regard to the procedure of gaining access to the telecommunication data. Eleven Member Sates require judicial authorisation for each request for access to retained data and in three Member States judicial authorisation is required in 'most cases'. In four Member States the authorisation of a senior officer is required but not of a judge and in two Member States the only condition is that the request is made in writing. In the evaluation report, the Commission states it is necessary to assess the need for a greater degree of harmonisation with respect to the authorities having and the procedure for obtaining access to retained data. The Meijers Committee recommends that the outcome of such an evaluation should be awaited before adopting comparable mechanisms with regard to PNR data or other proposals granting national law enforcement authorities access to personal data (for example Eurodac).

3.5 Transfer of PNR data to third countries

Article 8 of the 2011 proposal allows Member States to transfer PNR data and the results of the processing of PNR data, on a case-by-case basis, if:

- in accordance with the conditions of Article 13 of the Framework Decision 2008/977;
- the transfer is necessary for the purposes of this Directive specified in Article 1 (2) and;
- the third country agrees to transfer to third states only when necessary for the purpose of this Directive and only with express authorisation of the Member State.

The inclusion of the condition of 'case-by-case basis' prohibits the systematic transfer to third states. However to ensure its effective application, this provision will need close supervision. Whereas the 2007 proposal only provided for the further transfer of PNR data, this draft also allows for the transfer of the results of the PNR analysis by the PIU's or national authorities. The reference to Article 1(2) of the proposal excludes the transfer of PNR data for 'other purposes' as mentioned in the preamble, however it does include the very wide definition of purposes as provided in Article 4 (2) of the Directive.

Whereas the 2007 proposal explicitly stated that transmission to third states may only take place in accordance with national laws of the Member State concerned and any applicable international standard, the 2011 proposal only refers to the Framework Decision 2008/977.[13] This Framework Decision includes data protection rules in the field of police and judicial cooperation. From the perspective of a uniform scheme of data protection law in the EU, the Meijers Committee considers it illogical to refer in this Directive on the transfer of passenger data to the rules of a former third pillar instrument, when the Commission is expected to replace this instrument (and the Directive 95/46) by a new general instrument on EU data protection law in the near future. Furthermore, the Meijers Committee notes that the Framework Decision 2008/977 does not guarantee a harmonised approach by the EU Member States.

Article 13 of the aforementioned Framework Decision allows the transfer to competent authorities in third States or to international bodies if:
(a) it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

[11] Article 4 Directive 2006/24.
[12] Evaluation report on the Data Retention Directive, COM (2011) 225, 18.4.2011, see p. 9-12.
[13] OJ L 350, 30.12.2008.

(b) the receiving authority in the third State or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
(c) the Member State from which the data were obtained has given its consent to transfer in compliance with its national law; and
(d) the third State or international body concerned ensures an adequate level of protection for the intended data processing.
The Framework Decision allows transfer without prior consent in accordance with paragraph 1(c) if transfer of the data is essential for 'the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State and the prior consent cannot be obtained in good time'.

The adequacy of the level of protection referred to in paragraph 1(d) must be assessed 'in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations'. According to the Framework Decision, 'particular consideration' must be given to 'the nature of the data, the purpose and duration of the proposed processing operation or operations, the State of origin and the State or international body of final destination of the data, the rules of law, both general and sectoral, in force in the third State or international body in question and the professional rules and security measures which apply'. This provision will also result in a differentiated approach by the Member States.

Furthermore, the Meijers Committee notes that Article 13 (3) of the Framework Decision provides a very wide derogation from the aforementioned conditions and allows transfer of personal data if:
(a) the national law of the Member State transferring the data so provides because of:
(i) legitimate specific interests of the data subject; or
(ii) legitimate prevailing interests, especially important public interests; or
(b) the third State or receiving international body provides safeguards which are deemed adequate by the Member State concerned according to its national law.

Finally, the draft Directive allows the further transfer of personal data from the third state to other third countries. Even if this requires the explicit consent of the Member State concerned, it does not give other Member States, national supervisory authorities, the EDPS or the Commission, any power to control this further dissemination of passenger data.

4 PNR, profiling, and fundamental rights of individuals

According to the explanatory memorandum, the draft PNR Directive is aimed to achieve information on 'unknown criminals or terrorist'. Different from other databases such as the Schengen Information System (SIS) or Visa Information Systems providing only information on identified persons, whether or not reported for a specific goals (arrest warrant, to be refused entry), the transfer and especially analysis of PNR data should assist national authorities of the Member States to identify criminal offenders, associates or suspects of terrorism or serious crimes. The Commission differentiates between three possible ways of using PNR data: re-actively, real time, and pro-actively. 'Re-actively' means the use of the data in investigations, prosecutions, unravelling of networks after a crime has been committed. With 'real time use', the Commission refers to national authorities using data prior to the arrival or departure of passengers in order to prevent a crime, watch or arrest persons before a crime has been committed or because a crime has been or is being committed. In such cases PNR data may be used for running such data against predetermined assessment criteria in order to identify persons that were previously 'unknown' to law enforcement authorities, or for running the data against various databases. Finally, 'pro-active' use concerns the use of the data for analysis and creation of (new) assessment criteria, which could then be used for a pre-arrival and pre-departure assessment of passengers.

Dealing with the 2007 proposal, stakeholders expressed their concerns with regard to the impact of using PNR data for profiling for the fundamental rights of individuals. These rights include the right to privacy and data protection[14]; non-discrimination rights[15]; and the right to free movement. With regard to the latter, the Meijers Committee notes that one must distinguish between the right to freedom of movement as a human right protected in Article 2 of the 4th Protocol to the European Convention on Human Rights (ECHR) on the one hand, and the freedom of movement as one of the fundamental rights of EU citizens and their family members, based on Article 20 of the Treaty on the Functioning of the European Union and Directive 2004/38.

5.1 Profiling and the right to non-discrimination

In November 2010, the Committee of Ministers of the Council of Europe adopted a recommendation on the use of profiling in the public and private sector, setting important standards which should be taken into account discussing the current proposal on PNR.[16] Profiling can be understood as an automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.[17] This often implies the use of investigative or law enforcing powers based on generalised criteria, such as nationality, country of origin, religion etc.[18] Article 14 ECHR and the12th Protocol to the ECHR, prohibit discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. According to the case-law of the European Court of Human Rights (ECtHR), a difference of treatment is discriminatory, if it 'has no objective and reasonable justification', that is if it does not pursue a 'legitimate aim' or if there is not a 'reasonable relationship of proportionality between the means employed and the aim sought to be realised'.[19] With regard to discrimination based on race, sex, or nationality, very weighty reasons have to be submitted. In *Timishev v. Russia*, the ECtHR found that no difference in treatment based exclusively or to a decisive extent on a person's ethnic origin, is capable of being objectively justified in a contemporary democratic society built on the principles of plurality and respect for different cultures'.[20] In this case the ECtHR found a violation of the right to non-discrimination with regard to the right to liberty of movement as protected in Article 2 of the 4th Protocol to the ECHR.

Profiling on the basis of PNR data may expose passengers to high risks of discrimination, resulting in a differentiated treatment based on pre-selected criteria.[21] Its use should be limited to situations where an objective and reasonable justification exists and when based on sex, race, or ethnic origin only take place on the basis of very weighty reasons.

---

[14] Article 8 ECHR and 7 of the EU Charter on Fundamental Rights; the right to data protection as protected in Article 8 of the EU Charter and in the EC Directive 95/46.

[15] Article 14 ECHR, the Convention on Elimination of Racial Discrimination, Articles 2 and 26 of the International Covenant on Civil and Political Rights, and the Racial Equality Directive 2000/43.

[16] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling. Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies.

[17] Definition used in the aforementioned Recommendation CM/Rec(2010)13 of the Council of Europe.

[18] See the definition of the Open Society Justice Initiative on 'ethnic profiling' in *Ethnic Profiling in the European Union. Pervasive, Ineffective and Discriminatory*, May 2009: "the use by law enforcement of generalizations grounded in ethnicity, race, religion, or national origin—rather than objective evidence or individual behavior—as the basis for making law enforcement and/or investigative decisions about who has been or may be involved in criminal activity."

[19] *Gaygusuz v. Austria*, 16 September 1996, appl.no. 17371/90.

[20] *Timishev c. Russia*, 13 December 2005, appl.no. 55762/00 and 55974/00, para. 58-59.

[21] See the aforementioned recommendation of the Council of Europe, Olivier de Schutter and Julie Ringelheim, Ethnic Profiling: a Rising Challenge for European Human Rights Law, *The Modern Law Review* (2008) 71 93), p. 358-384; András Pap, *Ethnicity and Race-based Profiling in CounterTerrorism, Law Enforcement and Border Control*, Study for the Directorate General Internal Policies of the LIBE Committee of the European Parliament, November 2008; Evelien Brouwer, *The EU Passenger Name Record (PNR) System and Human Rights. Transferring Passenger Data or Passenger Freedom?* CEPS Working Document No. 320, September 2009, www.ceps.eu and the Report of the Special Rapporteur on the protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 29 January 2007.

According to the Commission, the proposed use of PNR data has the advantage that it enables national authorities to perform 'a closer screening only of persons who are most likely, based on objective assessment criteria and previous experience, to pose a threat to security'. This would facilitate the travel of all other passengers and reduce the risk of passengers being subjected 'to screening on the basis of unlawful criteria such as nationality or skin colour which may wrongly be associated with security risks by law enforcement authorities, including customs and border guards.' The Commission addresses an important problem of current border controls and the risk that these controls are lead by discriminatory considerations. However, the Meijers Committee questions whether the aforementioned use of 'pre-determined criteria' will actually result in less discrimination at the borders, or whether it just changes the moment of screening by the PIU's. Both methods will have the same result, namely that a person may be refused entry or subjected to further investigation measures on the basis of 'predetermined criteria', or in other words, the use of profiling.

Article 5 (6) of the current proposal provides that competent authorities may not take any decision that produces an adverse legal effect on a person or significantly affects a person 'on the basis of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life.' Although a general prohibition of discriminatory decision making is to be approved, it does not exclude that the analysis or assessment of PNR data by the PIU is based on one or more of the aforementioned criteria. This means, that indirectly, on the basis of this Directive, decision making by competent authorities based on one of the aforementioned discrimination grounds is still possible. Furthermore, the reference to 'decisions' does not make clear that this prohibition also applies to measures of national authorities, including physical measures such as search measures or preventing persons to enter the territory.

5.2 The right to privacy

In *Marper v. United Kingdom*, the ECtHR referred to the stigmatising effect of long-term, systematic storage of fingerprints and DNA samples of individuals, including minors, who were suspected of having committed criminal offences, but not convicted.[22] In this judgment, the ECtHR found that the applicable UK law violated Article 8 ECHR, particularly on the grounds that these data were stored for indefinite periods and concerned unconvicted persons as disproportional.

The storage and use of PNR may result in a disproportional infringement of the right to privacy, based on the stigmatising effect of being selected repeatedly on the basis of 'pre-determined criteria'.[23] Relevant with regard to the indiscriminate transfer and use of PNR data, is the consideration of the ECtHR in the aforementioned Marper-case, in which it states to be struck by 'the blanket and indiscriminate nature of the power of retention in England and Wales' and the fact that 'the material may be retained irrespective of the nature of gravity of the offence with which the individual was originally suspected or of the age of the suspected offender' (para. 119). The ECtHR concluded there was a violation of Article 8 ECHR also because of limited possibilities for the individual to have the data removed from the nationwide database or to have the materials destroyed and because of the lack of independent review. Furthermore, as the ECtHR has pointed out repeatedly in its judgments, in order to fulfil the requirement that the breach of privacy is in accordance with the law, including the principle of foreseeability, the law must be sufficiently clear in its terms 'to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures'.[24] As we have

[22] *S. and Marper v. United Kingdom*, 4 December 2008, appl.no. 30562/04 and 30566/04, see para. 122.
[23] See the report of the Dutch National Ombudsman on the devastating effects for a Dutch businessman, who as a result of identity theft and incorrect information in the Schengen Information System, has been searched and arrested for more than ten years, including at the Schiphol airport each time he had to fly for business or family reasons.
[24] *Copland v. United Kingdom*, appl.no. 62617/00, 3 April 2007, para 45.

seen above, the current proposal does not offer harmonised criteria and leaves the different Member States wide discretionary powers with regard to the use, retention and further dissemination of passenger data. Therefore, the current proposal does not meet the criterion 'in accordance with the law' of Article 8 (2) ECHR.

5.3 The right to data protection

In November 2010, the European Commission adopted a Communication on 'a comprehensive approach on personal data protection in the European Union', including proposals and approach for the review of the EU legal system on the protection of personal data.[25] In this Communication, the Commission defined general principles and guidelines for the future architecture of EU data protection law. The content of the current PNR proposal is difficult to reconcile with these general principles. In the first place, the Commission advocates further harmonisation of data protection law, which as we have seen, is not provided in the PNR proposal. Secondly, the Commission calls for enhancing control over one's own data, for example by harmonising law on the individual's right of access, correction and deletion of his data, strengthening the principle of data minimisation, and clarifying the so-called 'right to be forgotten', or the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes.

The PNR proposal does not include an explicit right of access, correction or deletion of the individual, but only obliges Member States to ensure that the private organisations involved (air carriers, agents or other ticket sellers) will inform passengers at the time of booking a flight and at the time of purchasing a ticket 'in clear and precise manner' about the provision of PNR data to the PIU, purposes of processing, period of data retention, possible further use and exchange of such data, and their data protection rights (Article 11 of the proposal). For this purpose, the Meijers Committee refers to the right to information as formulated in paragraph 4.1 of the Recommendation of the Committee of Ministers of the Council of Europe (the text is attached in the annex to this comment).[26]

Another measure, announced by the Commission in the aforementioned Communication, is to make remedies and sanctions more effective. According to the Commission, the power of data protection authorities and civil society associations, as well as other associations representing data subjects' interests, to bring an action before the national courts should be extended. Furthermore, the Commission proposed to assess whether existing provisions on sanctions can be strengthened, for example by explicitly including criminal sanctions in case of serious data protection violations, in order to make them more effective. It is positive that, different from the 2007 proposal, the current PNR proposal includes a provision obliging Member States to impose 'effective, proportionate and dissuasive penalties' in case of infringements of the provisions adopted pursuant this Directive (Article 11 (7)). However, these sanctions are not further specified and it is not clear against which authorities or organisations they may be imposed. Article 12 of the proposed Directive obliges Member States to ensure national supervisory authorities to be responsible for 'advising and monitoring' the application of this Directive, without supplying these organisations with binding or coercive powers. Furthermore, the proposal does not include any direct reference to individual data protection rights or legal remedies.

5.4 Freedom of movement of EU citizens, family members, and third-country nationals under EU law

Aside from non-discrimination, privacy and data protection rights, it should also be emphasised that the current proposal raises problems from the perspective of the fundamental freedoms of

[25] COM (2010) 609, 4 November 2010. These principles have been further developed by the EU Justice Commissioner Viviane Reding in her speech before the Privacy Platform "The Review of the EU Data Protection Framework", 16 March 2011 SPEECH/11/183.
[26] CM(2010)13.

Union citizens and their family members. Article 27 of the Directive 2004/38 provides that every measure restricting the freedom of movement and residence of EU citizens and their family members must comply with the principle of proportionality and 'be based on their personal conduct representing a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society'. Stop and search measures on EU citizens and their family members at the airport of a Member State which are solely based on an analysis of PNR data of his or her flight cause an unlawful limitation of their freedom of movement. Furthermore, in the case *Heinz Huber v Germany*, the Court of Justice of the European Union (CJEU) made clear that the systematic and strict monitoring of EU citizens may infringe the right of non discrimination of EU citizens in relation to the proportionality principle to be observed on the basis of the Directive 95/46 on the protection of personal data.[27] In this case, the CJEU found that the German central aliens administration (AZR) including data on EU citizens violated their right to non-discrimination on the basis of a strict application of the condition of necessity as laid down in article 7 (e) of the EC Directive 95/46. Amongst others, the German legislator had failed to justify the necessity of the centralised nature of the database, the storage of individualised personal data in the AZR for statistical purposes, and the possible use of the personal data on EU citizens for law enforcement purposes.

Furthermore, search measures based on PNR analysis on the basis of this Directive may also cause infringement of the freedom of movement of third-country nationals whose rights are guaranteed by EU law (for example the EU-Turkey Association Agreements, the Directive 2003/86 on family reunification, and Directive 2003/108 on long term resident third country nationals). Therefore, any measure on the large-scale collection and use of personal data should include a clause taking into account the freedom of movement and rights of EU citizens and third- country nationals. A comparable clause has been included in the Schengen Borders Code and the Returns Directive.[28]

6 Conclusion

The Meijers Committee concludes that the Commission does not provide real evidence of the added value of the current PNR proposal for the prevention or prosecution of terrorist offences or serious crime. Before adopting this new measure, existing measures (API Directive, SIS, Prüm) should be evaluated first to establish the existence of any 'security gap'. Without further information on the added value of the dissemination of passenger data of every traveller flying from and into the 27 Member States, one must conclude that this proposal does not meet the general principle of proportionality. This principle of proportionality, as reaffirmed by the CJEU in a case dealing with dissemination of personal information on internet, is one of the general principles of European Union law and 'requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it'.[29] The Meijers Committee notes that earlier criticisms of the European Parliament, the EDPS, and other stakeholders with regard to the necessity and proportionality of the 2007 PNR Directive has not or only partially been taken into account. The new proposal does not offer clear rules with regard to the powers of national authorities to use PNR data or to transfer these data to other countries, nor does it include sufficient safeguards to protect the fundamental rights of individuals. The proposal lacks in particular harmonised rules with regard to the following subjects:

[27] *Heinz Huber v. Germany*, C-524/06, 16 December 2008.
[28] See for example: Article 3 of the Schengen Borders Code: 'This Regulation shall apply to any person crossing the internal or external borders of Member States, without prejudice to: (a) the rights of persons enjoying the Community right of free movement; (b) the rights of refugees and persons requesting international protection, in particular as regards non-refoulement', and;
Article 4 (2) Returns Directive 2008/115: 'This Directive shall be without prejudice to any provision
which may be more favourable for the third-country national, laid down in the Community acquis relating to immigration and asylum.'
[29] C-92/09 *Volker and Markus Schecke v. Land Hessen* & C-93/09 *Eifert v. Land Hessen*, 9 November 2010. para. 74. See also Case C-58/08 *Vodafone and Others* [2010] ECR I-0000, para. 51 and 86.

- purpose limitation;
- data retention;
- transfer of data to third countries;
- individual rights;
- legal remedies;
- powers of supervisory and judicial authorities.

Considering the risks of violation of non-discrimination, privacy and data protection, and the freedom of movement of EU citizens and third-country nationals, together with the failure to address its necessity and added value (and the high costs for the individual Member States and air transport organisations), the Meijers Committee recommends the withdrawal of the proposed PNR Directive. Before submitting new measures, applicable measures on the collection of personal data for law enforcement and migration control purposes should be evaluated and 'security gaps' identified. Any new draft on the transfer of PNR data should include an extended impact assessment with reliable and up-to-date information on the efficiency, financial costs, and consequences with regard to the aforementioned fundamental rights.

If the aforementioned requirements are met, any future proposal on the use of PNR data should include precise criteria limiting the discretionary powers of national authorities, including PIU's with regard to the collection and use of personal data. This proposal should include limitative rules on the grounds for which data may be collected, the authorities 'competent' to receive and use such data, time limits for data retention, and applicable safeguards and sanctions for misuse or incorrect use of data. Furthermore, the rights and legal remedies of individuals with regard to the collection and use of their data should be formulated more precisely, including the right to information and right to financial repair.[30]

[30] With regard to the right to information, the Meijers Committee refers to the provision as included in the Recommendation of the Council of Europe on profiling, as included in the annex to this comment.

Annex : paragraph 4.1 of the Recommendation CM/REC(2010)13 of the Committee of Ministers of the Council of Europe, 23 November 2010:

Where personal data are collected in the context of profiling, the controller should provide the data subjects with the following information:

a. that their data will be used in the context of profiling;
b. the purposes for which the profiling is carried out;
c. the categories of personal data used;
d. the identity of the controller and, if necessary, her or his representative;
e. the existence of appropriate safeguards;
f. all information that is necessary for guaranteeing the fairness of recourse to profiling, such as:

- the categories of persons or bodies to whom or to which the personal data may be communicated, and the purposes for doing so;
- the possibility, where appropriate, for the data subjects to refuse or withdraw consent and the consequences of withdrawal;
- the conditions of exercise of the right of access, objection or correction, as well as the right to bring a complaint before the competent authorities;
- the persons from whom or bodies from which the personal data are or will be collected;
- the compulsory or optional nature of the reply to the questions used for personal data collection and the consequences for the data subjects of not replying;
- the duration of storage;
- the envisaged effects of the attribution of the profile to the data subject.

o-0-o