RANKED AMONG THE WORLD'S TOP 10 THINK TANKS
CEPS Working Document
Thinking ahead for Europe
CENTRE FOR EUROPEAN POLICY STUDIES

The EU Passenger Name Record (PNR) System and Human Rights:

Transferring Passenger Data or Passenger Freedom?

CEPS Working Document No. 320/September 2009

Evelien Brouwer

Abstract

The European Commission presented the 'EU Passenger Name Record (PNR) system' in 2007 as a tool in the fight against terrorism and organised crime. One of the proposed instruments of this system is the Framework Decision on the use of PNR, which provides for the storage and exchange of passenger data between EU member states and between member states and non-EU countries. Current Council proposals make clear that the passenger data may also be used to investigate other (serious) crimes or to prevent illegal immigration, which raises both practical and legal concerns. This paper describes the legal implications of the EU PNR system, focusing in particular on international human rights standards. It is to be hoped that, when preparing the so-called 'Stockholm programme', including a new multiannual programme for policies in the field of freedom, security and justice, both the EU institutions and member states will take these standards sufficiently into account.

ISBN 978-92-9079-919-1
Available for free downloading from the CEPS website (http://www.ceps.eu)

Contents

THE EU PASSENGER NAME RECORD (PNR) SYSTEM AND HUMAN RIGHTS:
TRANSFERRING PASSENGER DATA OR PASSENGER FREEDOM?

CEPS WORKING DOCUMENT NO. 320/SEPTEMBER 2009

EVELIEN BROUWER*

1. Introduction

Under the Swedish Presidency, EU member states are currently preparing the so-called 'Stockholm programme' including a new multiannual programme for EU policies and legislation. With the aim of preparing the goals of this programme in the field of justice and home affairs, the European Commission published the Communication: *An area of freedom, security and justice serving the citizen*[1] in June 2009. Under the headings: "Promoting citizens' rights – a Europe of rights", this Communication recalls that:

> the area of freedom, security and justice must above all be a single area in which fundamental rights are protected, and in which respect for the human person and human dignity, and for the other rights enshrined in the Charter of Fundamental Rights, is a core value.

According to the Commission, this means, among other things, that:

> the exercise of these freedoms and the citizen's privacy must be preserved beyond national borders, especially by protecting personal data; allowance must be made for the special needs of vulnerable people; and citizens must be able to exercise their specific rights to the full, even outside the Union.

The meaning of this goal as set out by the Commission, and which will hopefully be repeated in the final Stockholm programme, should not be underestimated in light of the current proposals regarding data processing. The principle of safeguarding the right to privacy and freedoms of EU citizens, but also of 'vulnerable people' has never been more important, considering the different legislative measures and proposals dealing with the large-scale processing of personal data of EU citizens and other nationals travelling within, towards and outside the EU territory.

In 2007, the European Commission published a proposal for a Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (COM (2007) 654). The principal purpose of the draft Framework Decision is the establishment of a tool in the fight against terrorism and organised crime. Considering the current discussions within the Council and the relation of the proposed Framework Decision to other instruments in this field, it is to be

---

* Assistant Professor in Constitutional Law, Utrecht University, August 2009. This paper is based on my Briefing Paper *Towards an European PNR System? Questions on the Added Value and the Protection of Fundamental Rights*, written at the request of the LIBE Committee of the European Parliament, January 2009. The author would like to thank Sergio Carrera for his comments on an earlier version of this paper, which falls within the context of the CHALLENGE project (the Changing Landscape of European Liberty and Security) funded by Sixth Framework Programme of DG Research of the European Commission.

[1] Communication of 10 June 2009, COM (2009) 262.

expected that the data to be processed and stored within the so-called 'EU PNR system' will also be used to investigate other crimes and to prevent irregular immigration. It is therefore important to take into account the other instruments recently adopted within the EU that contribute to the large-scale collection and storage of personal information, for example SIS, VIS, and the Commission Border Package.[2] Furthermore, both the EU and different member states signed bilateral agreements with third countries, such as the United States of America, Australia and Canada, on the transfer of passenger data to the authorities of those states.

While confirming that law enforcement authorities should have all the tools they need to adequately carry out their tasks, in its resolution of 20 November 2008, the European Parliament rightfully underlined that the justification of the current proposals need to be convincingly substantiated. Not only because of the considerable impact of these instruments on the personal lives of citizens, but also because of their consequences for air carriers. This paper, taking into account the different comments by the organisations and institutions involved, describes both the practical and legal issues of the proposed EU PNR data system. It will firstly consider the content of the Commission proposal and different questions and issues raised within the EU Council on the basis of this proposal. To assess the practical meaning and consequences of this PNR proposal, it will take into account existing measures closely related to the current proposal, including the aforementioned Directive 2004/82/EC and the use of large-scale information systems within the EU. In the second part, the legal implications of the proposed EU PNR system will be analysed on the basis of the latest available draft of the proposed Framework Decision.[3] Emphasising that the EU and EU member states are bound by the international, EU and national standards on human rights, in section 5 I will focus on the limitations imposed by data protection rights, the right to a private life and the prohibition of discrimination.

Although this paper focuses on the proposed EU PNR system, questions raised about the proportionality, including the questionable 'added value' of data processing, data protection principles, and especially the right of non-discrimination, are important for the whole 'EU information network' field. As pointed out by different key actors, it is important that the EU policy-makers are not too influenced by technical possibilities, neglecting both the actual needs and requirements of 'actors in the field' (border guards, law enforcement authorities and air carriers) and the rights and freedoms of individuals.[4] Otherwise, the new developments will not lead to a 'Europe of Rights' as intended by the European Commission, but to a 'Europe of Lost Freedoms' as a result of new technical and bureaucratic boundaries.

2. The transfer of API data - Directive 2004/82/EC

In April 2004, the Council adopted Directive 2004/82/EC on the obligation of air carriers to transmit passenger data to the border control authorities of the EU member states.[5] This Directive concerns the transfer of API or advanced passenger information data, which is to be

---

[2] See on this Borders Package: Elspeth Guild, Sergio Carrera and Florian Geyer, *The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?*, CEPS Policy Brief No. 154, CEPS, Brussels, March 2008.

[3] Council doc. 5618/1/09, 17 April 2009.

[4] See, for example, the Opinion of the European Data Protection Supervisor of 10 July 2009 on the aforementioned Communication of the Commission of 10 June 2009, stating in point 53: "that the future of the Area of freedom, security and justice should not be 'technology-driven', in the sense that the almost limitless opportunities offered by new technologies should always be checked against relevant data protection principles and used only insofar as they comply with those principles".

[5] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, *OJ* L 261.

differentiated from Passenger Name Records or PNR, to be dealt with below. API concerns data from the machine readable zone of the passport, including name, date of birth, passport number and nationality. PNR data includes the data that are registered by the airline companies or travel agencies when a traveller makes a booking: including the name of the person, seat number, travelling route, booking agent etc. The most important difference between API and PNR is that the information that can be extracted from PNR data mainly depends on the information that the passenger submits him/herself to the reservation system. In terms of passport information therefore, API data offer national officers more objective and permanently valid information, permitting the identification of individuals, whereas PNR data is used more in profiling, offering national officers information on the background of the individuals and their possible relationship to other persons being searched.

Following Directive 2004/82/EC, EU member states must oblige carriers to transmit information concerning the passengers they will carry (Article 3) by the end of check-in at the request of the authorities responsible for borders checks. The fact that the data must only be transmitted in response to a prior request is an important difference with the proposed PNR Framework Decision which, as we will see below, includes the systematic transmission of each flight entering or leaving from the territory of a member state. On the basis of Directive 2004/82/EC, when carriers fail to observe this obligation, by not transmitting the required data or by transmitting incomplete or false data, member states should take the necessary measures to impose sanctions, including a maximum of €5,000 and a minimum of €3,000 (Article 4).

Shortly before the final adoption of the Directive, despite earlier agreements reached within the Council on a strict purpose limitation, two important extensions have been included in the draft text, after pressure from the UK. Firstly, in Article 6 of the Directive an exception has been added to the general rule that data transferred to border authorities must be deleted within 24 hours of their transmission: they may be stored for a longer period if the data are needed "for the purposes of exercising the statutory functions of the authorities responsible for the external border checks in accordance with national law and subject to the data protection provisions under Directive 95/46/EC". Secondly, Article 6 provides that member states may also use the passenger data for law enforcement purposes. This latter amendment to the original proposal extends the purpose of Directive significantly, raising the question as to whether this goal of the Directive could still be based on its current legal basis: Articles 62 (2) (a) and 63 (3) (b) of the EC Treaty. Furthermore, Article 6 and the explicit reference in preamble 12 of this Directive to the purpose limitation principle of Article 6 (1) (b) of the 95/46/EC Directive seem to include a (twofold) contradiction. Either the sole purpose of this Directive 2004/82 is to combat irregular immigration, and then further use for law enforcement purposes will infringe the rule of purpose limitation in Directive 95/46, or the API Directive clearly implies the use for law enforcement purposes, but then this use will fall outside the scope of Directive 95/46, as is provided in Article 3 of this Directive.

The implementation date of this Directive went beyond 5 September 2006. Although the majority of the participating states (except Denmark, Spain, and Poland) adopted implementation measures, in many countries the required data systems would not be operational yet. In April 2008, the European Commission informed the British House of Lords that there was no clear picture on whether the data are useful for the purposes for which they are collected.[6] As we will see in section 3.6, a survey carried out by the Article 29 Data Protection Working Party demonstrated the member states' lack of enthusiasm for implementing this Directive.

---

[6] House of Lords – European Union Committee, *The EU/U.S. Passenger Name record (PNR) Agreement*, London, 5 June 2007.

3. The Draft Framework Decision on the use of PNR for law enforcement purposes

3.1 Commission proposal: COM (2007) 654

In addition to the existing Directive on the transfer of API data, in November 2007 the European Commission published a proposal for a Framework Decision on the use of PNR for law enforcement purposes.[7] Unlike Directive 2004/82/EC, whose sole purpose is the fight against irregular immigration, the central purpose of this proposal is to prevent and combat terrorist offences and organised crime (the current Council proposal refers to "serious crime" instead of "organised crime", see below). According to the Impact Assessment study, PNR data should be useful for law enforcement purposes in five ways:

- running PNR data against alert systems in order to identify known terrorist and criminals;
- identification of (unsuspected) passengers connected to a known terrorist or criminal (for example when they use the same address, credit card number, contact details);
- identifying "high risk passengers" by running PNR data against a combination of "characteristics and behavioural patterns";
- identifying "high-risk passengers" by running PNR data against risk intelligence relevant at a certain time;
- providing intelligence on travel patterns associations after a terrorist offence has been committed.

Whereas the first two goals include the identification of individual persons, namely terrorist or criminals or persons connected to these persons known at the time of the searches, the third and fourth goals include the identification of "high-risk passengers" unknown at the time of running the PNR data by using profiles or intelligence available at that time. The fifth goal does not address the identification or search for individual passengers at all, but only aims at establishing new profiles or providing new information on "travel or behavioural patterns".

The reasons for submitting this proposal, as set out by the Commission in its Explanatory Memorandum, are a little ambiguous. On the one hand, the Commission refers to the fact that only a limited number of member states adopted legislation in this field, meaning "that the potential benefits of an EU-wide scheme in preventing terrorism and organised crime are not fully realised." This seems to indicate that the proposal is an autonomous initiative of the Commission to tackle threats of security in the EU within the general goals of creating a "European area of freedom, security and justice". This view is supported by the fact that at the time of the presentation of the Commission proposal, only the United Kingdom, France and Denmark had already enacted primary legislation for the capture and use of PNR data. On the other hand, the Commission emphasises the necessity of a harmonised approach: "a harmonised approach makes it possible to ensure EU-wide exchange of the relevant information". This goal is recalled by the Commission when explaining the choice of instruments: "As the aim is approximating member states' legislation, other instruments than a Framework Decision are not appropriate."[8]

The Commission proposal provided for the duty of air carriers to transmit the data of their passengers of international flights to the member state on whose territory the flight is entering,

---

[7] COM (2007) 654, see also the Commission's Impact Assessment accompanying this proposal, 6 November 2007, SEC (2007) 14253 and its summary SEC(2007) 1422.

[8] See the Explanatory Memorandum at p. 2 and p. 7.

departing or transiting. According to the proposal, the data must be made available 24 hours before the scheduled flight departure to so-called Passenger Information Units (PIU) to be established in each member state. With the establishment of the PIUs, the Commission proposal envisaged a decentralised collection of PNR data, considering this as a better policy option to protect data and to minimise costs for its setup and operation. The data may be retained for thirteen years: five years after their transfer to the PIU of the first member state on whose territory the international flight is entering, departing or transiting, and upon expiry of this period of five years, another period of eight years. During this second period the data may be accessed, processed and used only with the approval of the competent authority and "only in exceptional circumstances in response to a specific and actual threat or risk related to the prevention or combat of terrorist offences and organised crime."

Article 8 of the Commission proposal provided that passenger data could be transmitted to law enforcement authorities of third countries for the prevention, detention, investigation or prosecution of terrorist events or organised crime. As we will see below, also with regard to the transfer to third countries, the Council proposal changed "organised crime" into "serious crime".

3.2 Discussions within the EU Council

3.2.1 General issues

During the negotiations within the EU Council on the Commission proposal, several issues were raised for further discussion. These issues have been summarised in the *Report on the thematic work carried out from July to November 2008* published by the French Presidency in November 2008.[9] An important question dealt with within the Council is the functional and geographical scope of applicability of this Framework Decision: whether this should be extended to other modes of transport and whether, in addition to the international flights to and from the European Union, all or some intra-Community flights should be covered. A second issue of discussion is the widening of the purpose of the PNR Framework Decision to the integrated border management and, aside from terrorist offences and organised crime, to other serious crime. Further discussion points are the composition and specific tasks of the PIUs, including the applicable rules with regard to the data processing by the PIUs, and the interconnection between the PNR database and the API database and other files on persons or objects sought or under alert with a view to determining the action to be taken (SIS).

In their meeting of 24 October 2008, the Ministers of the JHA Council discussed further characteristics of the future Passenger Name Records system.[10] It was emphasised that the data to be forwarded to the public authorities would serve as input for analysing the terrorist and criminal threat, but also in the context of individual inquiries. With regard to the transfer of PNR data on intracommunity flights, the Council noted that the cost-benefit ratio should be assessed before including these data into the system. Referring to the fact that some member states already collect these data at national discretion, the Council agreed to review this issue once the PNR system had been in operation for a few years. In these conclusions of October 2008, the Council seems to imply the possible extension of PNR data to other means of transport, stating that: "PNR data are related to travel movements, usually flights (author's underlining) and include passport data, name, address, telephone numbers, travel agent, credit card number, history of changes in the flight schedule, seat preferences and other information."

---

[9] Note from the French Presidency to the COREPER/Council, *Report on the thematic work carried out from July to November 2008*, Council doc. 15319/1/08, 20 November 2008.

[10] JHA Council Conclusions, 24 October 2008, Council doc. 14667/08 (Presse 299).

During the Council discussions, the added value of PNR data for law enforcement purposes has been described as follows: "the establishment of a PNR database offers both opportunities to analyze behavioural tendencies in criminal circles, on which basis the criminal risk on particular flights can be assessed, and opportunities to provide information for investigations by intelligence services, customs, police and the criminal justice system. It allows the proactive use of the information contained in it, with the aim of preventing crime and detecting crimes which have been committed or are being planned; also, thanks to the later use of data which have been stored", it may help to clear up unsolved crimes."[11] This clearly indicates the intended use of the PNR data for profiling purposes, in a proactive and repressive responsive to terrorism or security threats. It also indicates that the data may be used for the investigation of general crimes.

In the meeting of 27-28 November 2008, the JHA Council referred to the aforementioned Presidency report on the thematic work, which according to the Council, would have resulted in "an increasingly clear vision of the practical scope and essential features of a possible European PNR system reconciling operational effectiveness with respect for citizens' fundamental rights in general and personal data protection rights in particular".[12] The Council furthermore instructed the preparatory bodies within the Council to examine all outstanding, legal and operational, issues and announced to continue the dialogue with the European Parliament, and in the member states, the national parliaments and economic operators. In the Conclusions of both October 2008 as November 2008, the Council notes that the PNR data to be forwarded prior to boarding is commercial information already collected by airlines for their own commercial purposes. This explicit note is meant to underline that transport organisations will not be required to collect extra information on their passengers.

3.2.2 Council amendments to the Commission proposal

During the negotiations within the Council, different provisions in the original Commission proposal have been amended. The following analysis is based on the draft text of the Framework Decision of June 2009.[13] According to Article 1 of this proposal, its objective is to provide for the transfer or the making available by air carriers of PNR data of passengers of international flights to the member states: "for the purpose of preventing, detecting, investigating, and prosecuting terrorist offences or serious crime", as well as the processing of those data, including their collection, use and retention by the member states and the exchange between them. Article 2 refers for the definition of "terrorist offences" to the offences under national law referred to in Articles 1 to 4 of the *Framework Decision 2002/475 on combating terrorism* as amended by the *Framework Decision 2008/918*. This latter instrument extended the definition of terrorist offences, including offences linked to terrorist activities, by adding activities including public provocation to commit a terrorist offence, recruitment for terrorism and training for terrorism, when committed intentionally. With regard to the definition of "serious crime", the draft Framework Decision refers to Article 2 of the *Framework Decision 2008/841 on the fight against organised crime* as well as the offences under national law referred to in Article 2(2) of the *Framework Decision on the European Arrest Warrant*.

According to Article 4, member states must adopt lists of the competent authorities which shall be entitled to request or receive PNR data or analysis of PNR data. These authorities may only include authorities "responsible for the prevention, detection, investigation, or prosecution of

---

[11] Council doc. 15319/1/08, 20 November 2008, p. 7.

[12] JHA Council Conclusions, 27-28 November 2008, Council doc. 16325/08 (Presse 344).

[13] Council doc. 5618/2/09, 29 June 2009. For an earlier version see Council doc. 5618/1/09, 17 April 2009 and, including data protection provisions, Council doc. 5618/09, 23 January 2009.

terrorist offences or serious crime". This list of competent authorities must be notified to the Commission and the General Secretariat of the Council within 12 months after the Framework Decision enters into force, and these lists will be published by the Commission in the Official Journal of the European Union, which is a very important achievement with regard to the transparency of the use of PNR data. Further processing of PNR data is in principle only allowed with the aim of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, according to Article 4 (4), however Article 4 (5) includes an important derogation from this purpose limitation. According to this paragraph, the aforementioned limitation "shall not affect or interfere with national enforcement or judicial powers in case other offences, or indications thereof, are detected in the course of enforcement action of further to such processing".

Article 5 of this proposal obliges member states to take the necessary measures to ensure that air carriers make available PNR data of passengers of international flights to the national PIUs of the member state on whose territory the international flight is entering, departing or transiting. In April 2009, Article 5 (1a) has been added, allowing for a gradual implementation of this obligation of member states to collect PNR data. In the first period, PNR data from only 30% of all flights should be collected, in the next period from 60%, and in the following period from all flights. With regard to the exchange of information between member states, Article 7 (1) of the latest proposal includes the duty of PIUs to transmit, aside from PNR data, also "the analysis of PNR data" to their relevant competent authorities. Additionally, according to Article 7 (2), national PIUs may ask PIUs of any other member states for this analysis of PNR data as well. Furthermore, a new provision in Article 7 (2a) adds the right of "competent authorities of the member states" to directly request the PIU of any member state to provide it with the PNR data held in its database. PIUs should respond to such requests as a matter of priority. The right of national authorities to request this information directly is limited to "those cases where it is absolutely necessary for the prevention of an immediate and serious threat to public security".

Article 8 of the proposed text allows national PIUs to transmit data to third countries.[14] This includes the transfer of PNR data and the analysis of PNR data for the purpose of preventing, detecting, investigating or prosecuting of terrorist offences or serious crimes. In case the information was obtained from another member state, this state must have given its consent for this transmission. However, Article 8 (2) allows for the further transfer of PNR data to a third country without the prior consent of this member state "if the transfer of the data is essential for the prevention of an immediate and serious threat related to the prevention, detection, investigation or prosecution of terrorist offences or serious crime, and the prior consent cannot be obtained in time. In that case the original member state must be informed without delay. The third state should provide "an adequate level of protection for the intended data processing" and it may not transmit the data to another third state without the express consent of the member state.

3.2.3 Data protection provisions

Article 11 of the draft text obliges member states to ensure that all processing of PNR data pursuant to this proposal takes place in accordance with the provisions of the Framework Decision. The proposal of January 2009 did not refer to other (EC and international) standards of privacy and data protection law, however in June 2009, a reference was included to the Framework Decision on data protection for the third pillar, the Council of Europe Data Protection Convention of 1981 and the Recommendation of 1987 dealing with data processing

[14] The April text of the proposal, Council doc. 5618/1/09, allowed for the transfer of 'information' to third countries instead of 'data'.

in the police sector.[15] Article 11 (3) furthermore permits member states to provide at a national level higher safeguards for the protection of PNR data. It should be noted that this provision only refers to "PNR data" and not to "analysis of PNR data" or "information", which raises the question of whether this information is covered by the safeguards in question.

Article 11a obliges member states to ensure that "any processing, other than the collection or storage" by the PIU of the PNR data "may not be based solely on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual orientation." In January 2009, this prohibition of non-discrimination applied to every form of data processing by the PIU: the exclusion of "collection and storage of data" seems to imply the wish of member states to allow data analysis on the basis of the grounds mentioned above. For the purpose of verification of the lawfulness of data processing, the draft Framework Decision includes a logging mechanism, comparable to the system used for the Schengen Information System.[16] Article 11b however provides for the duty to log or document all transmissions of PNR data and to keep these logs for five years. This retention period is still subject to negotiation.

With regard to the enforcement of the rights of passengers, it is important that Article 11c of the proposal obliges member states to ensure that air carriers inform their passengers about the transmission of PNR data to the PIUs, the purpose of this processing, the period of data retention, and about their rights. In the latest version of June 2009 it was added that passengers should be informed in a 'timely' fashion, which raises questions about the scope of this obligation. Does this mean that member states may inform passengers after their data has been transferred? Article 11 d provides for the right to access of the data subject/passenger, on request at reasonable intervals, to receive without constraint and without excessive delay or expense at least:

- confirmation from the PIU or national supervisory authority as to whether or not PNR data have been transmitted to a competent authority;
- communication of the PNR data undergoing processing;
- where possible, information on this competent authority.

Furthermore, the data subject should be given at least confirmation by the national supervisory authority that all necessary verifications have taken place.

The current draft allows the member states to limit the right to information in their national laws on numerous grounds, provided in Article 11d (2). Amongst others, the access to information can be restricted to avoid obstructing official or legal inquiries, investigations or procedures, for protecting public security or national security, and for the protection of the data subject or of the rights and freedoms of others. According to Article 11d (3) any refusal of restriction of access should be set out in writing to the data subject. A right to rectification and erasure has been included in Article 11e of the proposal.

Importantly, Article 11f includes a right to compensation to a data subject who has suffered damage as result of an unlawful processing operation or of any act incompatible to the national laws adopted to implement this Framework decision. Finally, Article 11g provides the data subject a right to judicial remedies for any breach of the rights guaranteed to him by the national

---

[15] Compare Council doc. 5618/09, 23 January 2009 and 5618/2/09, 29 June 2009.

[16] This provision obliges the PIU to store or document all transmissions of PNR data and all requests by competent authorities or PIUs of other member states for the purpose of verification of the lawfulness of the data-processing, self-monitoring and ensuring proper data integrity, security and accountability of data processing.

provisions adopted pursuant to the Framework decision. This means that the scope of the right to compensation ànd the right to judicial remedies is dependent on the provisions included in the national laws and is therefore left to the scrutiny of the member states.

Article 11i of the proposal refers to the powers of national supervisory authorities. These powers include "effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, and ensuring appropriate publication of such opinions". Furthermore, a supervisory authority may order "the blocking, erasure or destruction of data, imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions". Article 11i further provides that a national supervisory authority may hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data, and that the person shall be informed of the outcome of the claim. The Framework Decision does not include the power for national supervisory authorities to issue binding decisions, or to impose financial sanctions to the data processor or national authority involved. Finally, Articles 11h and 12 of the text of June 2009 include safeguards with regard to the confidentiality and security of data processing.

3.3 Position of the European Parliament

In November 2008, the European Parliament (EP) adopted a critical resolution on the draft Framework Decision of the Commission.[17] With this resolution, the EP decided to reserve its formal opinion on the framework-decision once its concerns have been addressed. The report, prepared by Sophia in 't Veld and adopted by 512 votes in favour, 5 against and 19 abstentions, criticised the lack of evidence that this instrument would be a legally justified and efficient tool in the fight against terrorism. Considering the communitarian principle of subsidiarity, the EP notes that the need for Community action has not been sufficiently demonstrated. Whereas the Commission claims that the aim of the measure is to harmonise national schemes, the EP points to the fact that few member states have a system for the use of PNR data for law enforcement purposes. Therefore, according to the EP rather than harmonising (non-existing) national systems, the Commission proposal merely imposes a duty for member states to set up such a system. Furthermore, the EP points out that the Commission proposal includes a decentralised scheme, meaning that the European added value is even less clear.

In its resolution, the EP expressed serious concerns with regard to the protection of individuals' rights. According to the EP, since the proposed measure has a considerable impact on the personal life of Union citizens, their justification in terms of necessity, proportionality and usefulness in achieving their stated objectives needs to be convincingly substantiated. The EP therefore stressed that effective safeguards for privacy and legal protection must be put in place. More specifically, the EP proposes further clarification of the relationship between the use of PNR and other measures such as the API Directive, the Electronic System for Travel Authorisation, biometrics in passports, SIS, VIS and national border protection schemes. Further, referring to the earlier ECJ judgment on the legal basis of the EU-US PNR agreement,[18] the EP urges the Commission to examine carefully which legal basis is appropriate for the proposals but also for the accompanying measures. Other points of important criticism of the EP concern the lack of precise purpose limitation in the proposal, the use of profiling and further use of sensitive data, the retention periods and transfers of PNR data to third countries. Finally, the EP emphasised the importance of a clear definition of the role and powers of the PIUs "in

[17] Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of PNR for law enforcement purposes, B6-0615/2008.

[18] *European Parliament v Council*, Joined cases C-317/04 and C-318/04, 30 May 2006.

particular in terms of transparency and democratic accountability and in order to lay down appropriate data protection rules".

3.4 Position of the European Data Protection Supervisor

In his opinion of December 2007 on the draft proposal for the Framework Decision of the Commission, Peter Hustinx, the European Data Protection Supervisor, puts this proposal in the context of other measures dealing with the transmission of PNR, including the aforementioned Directive 2004/82/EC but also the EU agreements with third states, including the US, Canada, Australia and South Korea.[19] The EDPS emphasises that the current proposal for the transmission of PNR for law enforcement purposes is a further step towards "a routine collection of data of individuals who are in principle not suspected of any crime". In his comments, the EDPS concentrates on four main issues:

- the legitimacy of the intended proposal, including its purpose, necessity and proportionality assessed against the criteria of Article 8 of the EU Charter of Fundamental Rights;[20]
- the data protection regime applicable to the proposed data processing operations;
- the quality of data recipients at national level: including the quality of the PIUs, intermediaries and competent authorities designated to perform risk-assessment and analysis of passenger data;
- the conditions of transfer of data to third countries.

Concerning the first question of legitimacy, including the criterion of necessity of the proposed measure, the EDPS notes that when referring to other national PNR systems put in place, the Commission fails to give precise facts and figures relating to those systems in the Impact Assessment study. The EDPS criticises the mere reference to the reporting of "numerous arrests" with regard to "various crimes" in the UK system and the fact that no details are given with regard to the US programme, except that "the EU has been able to assess the value of PNR data and to realize its potential for law enforcement purposes". Furthermore, the EDPS points out that not only is there a lack of precise information on concrete results in the proposal itself, but that reports published by other agencies such as the Government Accountability Office in the United States, did not confirm at this stage the efficiency of the measures (point 27-28). Considering the criterion of proportionality, the EDPS recalls other large-scale systems monitoring the movement of individuals within or at the borders of the EU, whether in operation (SIS) or about to be implemented, such as the Visa Information System. According to the EDPS, the way in which they can already contribute to in-depth and comprehensive analysis should in itself be subjected to "in-depth and comprehensive analysis, before deciding to establish a new form of systematic scanning of all persons leaving or entering the EU by plane" (point 34). Therefore, as to the legitimacy of the proposal, the EDPS concludes that clear and undeniable elements of justification are missing and that the necessity and proportionality tests are not fulfilled.

As to the question of the applicable data protection regime, the EDPS questions the fact that a third pillar instrument creates legal obligations on a routine basis for law enforcement purposes upon private or public sector actors falling outside the framework of law enforcement cooperation. With this conclusion, the EDPS seems to derive from the conclusions of the ECJ in

---

[19] European Data Protection Supervisor, Opinion on the draft proposal for a Council Framework Decision on the use of Passenger name Records (PNR) data for law enforcement purposes, Brussels, 20 December 2007.

[20] Published in *OJ* 2007 C 303, 14.12.2007.

the aforementioned judgment in *European Parliament v Council*, however, according to the EDPS the case of this judgment would have been different to the present EU PNR proposal.[21] Furthermore, the EDPS points out that the relationship between the current PNR proposal and the Framework Decision on the protection of personal data for the third pillar remains unclear. This, according to the EDPS, may result in a lack of legal certainty with regard to the applicable data protection regime, for example with regard to which provision on purpose limitation will apply, noting that the data protection Framework Decision allows processing for wider purposes compared to the PNR proposal and the Directive 95/46/EC. Also, according to the EDPS, the different regimes that would apply at national level will have a major impact, primarily on the exercise of the rights by the data subjects, especially with regard to the rights of access and the rectification of data. The data subject risks being confronted not only by different competent entities (the airline companies, the PIUs, the law enforcement authorities) but also by different recipients of data: the data may be transmitted to the PIU of the country of departure or arrival of the flights but possibly also to PIUs of other member states on a case-by-case basis.

Thirdly, the EDPS concludes that the draft PNR Framework Decision does not provide any specification with regard to the quality of the recipients of personal data collected by airlines, nor of the intermediaries and PIUs. As to the latter organisations, the EDPS underlines that while the proposal entrusts PIUs with very sensitive processing of information, it does not give any detail on the quality and conditions with which they must exercise this competence. Furthermore, the EDPS notes that the enforcement of an EU PNR system will be rendered difficult since law enforcement authorities have different competences, depending on the national laws of the member states, including or not intelligence, tax, immigration or police.

Finally, dealing with the conditions of transfer to third countries, the EDPS highlights various gaps – all serious – in the Commission proposal. These include the lack of rules concerning the quality of member states' consent for forwarding data from a third country to another third country; the concurring rules on the transfer of data to third countries in the data protection Framework Decision; the question of reciprocity (the fact that other third countries will ask the EU for PNR data for flights from the EU to their territory) and the impact of the EU PNR proposal on existing agreements with third countries.

Raising other substantial issues and emphasising again the "unprecedented impact of the proposal in terms of fundamental rights", the EDPS finally advises not to adopt this proposal under the present Treaty framework, but await the new legal structure foreseen by the Lisbon Treaty. This would safeguard a co-decision procedure and strengthen the legal grounds for the proposed measures.

3.5 Comments of the Article 29 Data Protection Working Party

In December 2007, the Article 29 Working Party submitted, together with the special Working Party on Police and Justice,[22] a rather critical joint opinion on the Commission's proposal for the Framework decision.[23] In general, in this joint opinion the European data protection authorities considered that this draft proposal is not only disproportionate but may also violate

---

[21] The EDPS notes that the EU-US PNR agreement concerns data transfer to the CBP in a "systematic fashion", whereas the proposed EU PNR system would create "obligations on a routine basis", however without clarifying the precise difference.

[22] The Working Party on Police and Justice (WPPJ) was set up by the Conference of the European Data Protection Authorities in June 2007 to monitor data protection developments in the third pillar and to forward proposals and solutions in this field to the legislator.

[23] Joint opinion on the proposal for a Council Framework Decision on the use of PNR for law enforcement purposes, WP 145.

fundamental principles of recognised data protection standards, as included in Article 8 ECHR (see below) and the Data Protection Convention no. 108 of the Council of Europe. The data protection authorities express their concern that the EU PNR regime will lead to general surveillance of all travellers.

- the proposal did not justify a pressing need for the collection of data other than API data;
- the amount of personal data to be transferred by air carriers is excessive;
- the filtering of sensitive data should be done by the air controller;
- the 'push' method should apply to all air carriers;
- the data retention period is disproportionate;
- the data protection regime is completely unsatisfactory: the rights of data subjects and the obligations of the controllers is nowhere specified;
- the great deal of discretion left to member states might result in varying interpretations of the Framework decision;
- the data protection regime of onward transfers to third countries is unclear.

In December 2008, the Article 29 Data Protection Working Party sent a letter to Mr. Barrot, Vice-President of the Commission concerning the transposition of Directive 2004/82/EC, or the aforementioned API Directive. According to the Working Party, this survey (a questionnaire sent to all participating countries) confirmed the fears as expressed in an earlier opinion (WP 127) that the huge discretion left to the participating countries would lead to widely diverging interpretations and that the implementation would not always be consistent across Europe. One significant finding was that only a minority of respondents was aware of any experience the receiving agencies had and whether they considered the data useful or could confirm the relevance of the data. Also, the supervising data protection authorities would, according to the survey, have very little experience concerning the processing of API data by the implementing authorities, as no authority has carried out an investigation and no statistics as to the use of API data are available. The main conclusion of the Working Party is that the answers to the survey do not amount to a pressing need for other legal instruments, let alone the collection of additional passenger name record data or biometric data.

3.6 Opinion of the EU Fundamental Rights Agency

Rather unexpectedly, the EU Agency for Fundamental Rights (FRA) was invited by the French Presidency in September 2008 to give its opinion on the proposed Framework Decision. In response to this invitation, the FRA published an extensive and critical opinion in October 2008.[24] Where the FRA is focusing on three fundamental rights: the right to private life; the right to data protection; and the prohibition of non discrimination, the general conclusions of the FRA with regard to the legitimacy and proportionality of the proposed EU PNR system are comparable to those of the EDPS. In its opinion, the FRA gives an extensive analysis of the jurisprudence of the European Court for Human Rights (ECtHR) dealing with Article 8 ECHR, protecting the right to private life, and data processing by national authorities. Based on this jurisprudence, the FRA concludes that precisely defined data processing operations to be undertaken by authorities constitute an essential guarantee against arbitrariness in the imposition of restrictive measures. Such protection is even more important as regards secret surveillance

[24] European Data Protection Supervisor, *Opinion on the draft proposal for a Council Framework Decision on the use of Passenger Name Records (PNR) data for law enforcement purposes*, Brussels, 20 December 2007.

measures, due to the heightened risk of arbitrariness in such circumstances.[25] In its conclusions, the FRA finds that the proposal lacks these essential guarantees, containing open-ended and imprecise formulations, fails to give sufficient evidence 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.

Before adopting the new EU PNR system, the FRA recommends the evaluation of already existing measures, including VIS, SIS and the API Directive, with a view to determining why these measures are not able to provide the additional intelligence required. The FRA is concerned about the consequences of the EU PNR system in particular, and its use for profiling, for the right to non-discrimination as protected in the different instrument by which EU member states are bound, including Article 21 of the EU Charter of Fundamental Rights. With regard to the practice of profiling based on passenger data, the FRA stressed that reports published on earlier measures of profiling in Germany and the United Kingdom, for example, do not confirm the efficiency of profiling based on or associated with ethnicity, national origin or religion. Rather, the FRA points to the fact that available evidence suggests that these profiling practices are an unsuitable and ineffective, and therefore disproportional, means of countering terrorism and organised crime.

The FRA therefore concludes that profiling based on stereotypical generalisations about ethnic, national or religious groups should be explicitly banned. The FRA also recommends monitoring closely, if the proposal is adopted, who in fact is targeted by the proposed risk assessment, to ensure compatibility with the prohibition of discrimination.

3.7 Comments of the Association of European Airlines

Air transport operators carefully followed the negotiations with regard to the Framework Decision, being aware that its implementation involves extra costs and efforts for their organisations.[26] In the first place therefore, airline companies advocated the greatest possible harmonisation of the obligations imposed on them in order to limit the cost and the burden of legal responsibilities. Also, the Association of European Airlines (AEA) underlined repeatedly that airlines or private entities should not be systematically required to collect passenger data on behalf of governments for non-aviation purposes.[27] As the AEA stated in its position paper of December 2007, "security of citizens cannot be the responsibility of airlines: this should remain the exclusive task of national Authorities". In its comments of 2007, the AEA also questioned the level of harmonisation in the Commission proposal, considering that a Framework Decision would not be the appropriate legal instrument to guarantee the goals as pursued by the Commission. According to the AEA this did not seem to be the intention of the Commission, when referring to the Explanatory Memorandum it stated that this instrument: "leaves as much scope as possible to the national decision-makers". The AEA underlined the preference of airlines for a central collection/filtering system at EU level.[28] The AEA regrets the choice of the European Commission for a decentralised system, whereby airlines would have to transmit data to national PIUs. According to the AEA, this could imply multiple transmission requirements

---

[25] *Klass and others v. Germany*, 6 September 1978, *Rotaru v. Romania*, 4 May 2000, appl.no. 28341/95, *Segerstedt-Wiberg and others v. Sweden*, 6 June 2006, appl.no. 62332/00.

[26] Council doc. 15319/1/08, 20 November 2008, p. 3.

[27] AEA Comments on the European Commission Proposal to the Council of the European Union for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5 December 2007 and Policy Paper on transfer of airline passenger data to governments, April 2008, www.aea.be

[28] See also the AEA *Policy Paper on transfer of airline passenger data to governments*, April 2008.

and extra costs for air carriers. The AEA also expressed its concern about the possible impact of the EU requirements on international relations. The AEA referred to the growing number of third countries asking for reciprocity and requested clarification on the management of relations with these third countries, advocating that these relations would be dealt with at the EU level.

Dealing with the provision on sanctions against airlines not transmitting data or transmitting incomplete or erroneous data, AEA emphasises that PNR only contains data "that are actually provided by the passenger", and that therefore PNR will almost always be incomplete even in terms of APIS data. According to AEA, airlines have no possibility of checking the accuracy of data provided by the passenger voluntarily and therefore cannot be held liable for incorrect data.

4. Relationship with the development of other EU information systems

Within the EU, many instruments have recently been developed on the use of large-scale databases and the exchange of personal data.[29] The use of these instruments will be closely related to the use of passenger PNR data. The proposals of the European Commission for a *European Border Management Strategy* are important, for example.[30] The Commission's 'Border Package' of February 2008, including the proposal of an entry/exit system, allows the electronic recording of the dates of entry and exit of third country nationals into and out of the Schengen area. This entry/exit system would enable national authorities to identify overstayers and to "take the appropriate measures".[31] Another Commission proposal includes the introduction of automated gates for "Bona Fide or Registered Travellers" enabling "the automated verification of travellers' identity without the intervention of border guards". A machine will read the biometric data contained in the travel documents or stored in a system or database and compare them against the biometrics of the traveller, "accelerating border checks by creating automated separate lanes replacing the traditional control booths". Persons will be granted "Registered Traveller" status after appropriate screening on the basis of common vetting criteria, including a reliable travel history (no previous overstays; data to this effect can be retrieved from the entry/exit system), proof of sufficient means of subsistence, and holding a biometric passport.

As mentioned above, in the discussions on the EU PNR data system, different options are to be discussed with regard to the interconnection with 'SIS-type files'. Article 3 (3) of the draft Framework Decision of April 2009 provided that the PIUs may process PNR-data against pre-determined risk criteria and "against relevant international, European, or national files on persons or objects sought or under alert".[32] In a note of April 2009, the Terrorism Working Party of the Council referred to the importance of using PNR data alongside other databases/systems "establishing a clearer picture of the movement of known and suspected terrorists and allowing for appropriate interventions to be made."[33] According to this Working Party also the combined use of API data alongside PNR data would be necessary for a better detection of terrorist movements. The usefulness of PNR data would be maximised when combined with API data, as API data are validated data necessary to identify travellers. This

---

[29] For an overview see Florian Geyer, *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CHALLENGE Research Paper No. 9, CEPS, Brussels, May 2008.

[30] See the Commission's *Communication on Examining the creation of a European Border Surveillance System (EUROSUR)* and the *Communication on Preparing the next steps in border management in the European Union* COM (2008) 68 resp. COM (2008) 69, 13.2.2008.

[31] COM (2008) 69, pp. 5-6.

[32] Council doc. 5618/01/09, 17 April 2009.

[33] Council doc. 8667/09, 14 April 2009.

possibility of linking PNR data with other databases was slightly amended in the draft of June 2009. Article 3 (3) of this draft now provides that PIUs may process PNR data against pre-determined risk criteria, and against "relevant databases, including international or national files or national mirrors of European files, on persons or objects sought or under alert". With "national mirrors of European files", the authors of this draft seem to refer to the national databases connected to SIS and VIS.

At the moment, the Schengen Information System or SIS is one of the most important databases used for border control and law enforcement purposes in the EU.[34] In January 2009, the SIS included nearly 28 million records on objects and persons, of which approximately 1 million alerts concerned persons.[35] Since its launch in 1995, the majority of personal data held in the SIS concerns third-country nationals to be refused entry on the basis of Article 96 SC.[36] The decision to report a third-country national in the SIS is based primarily on a national decision that this person is considered a threat to public order, public security or national security. Secondly, the decision can be based on immigration law decisions regarding the deportation, refusal of entry or removal of this person. The consequence of this decision to report an individual in the SIS is that the person in principle will be refused entry to every other Schengen State (which meanwhile entails more than 27 Schengen States, including non-EU member states Norway, Iceland and Switzerland). On the basis of an SIS alert, a third-country national can also be denied a visa or a residence permit, or even be expelled or detained.

In a Presidency note of October 2008 on the PNR Framework Decision, the following options are proposed: to interconnect SIS type files with PNR data on all passengers on the flights selected; only passengers deemed positive upon profiling; interconnection is to be assigned to PIUs; or interconnection is to be assigned to competent authorities.[37] The use of databases such as the SIS, and the future SIS II,[38] including its use by consular staff in third countries for the issuing of visas, raises important issues with regard to the responsibility and accountability of member states when running passenger data against this database. The SIS is based on the principle of mutual trust and the mutual enforcement of national administrative decisions. This means that Schengen states can invoke another state's decision in order to legitimise their own acts on the basis of SIS information, including refusal at the borders, the rejection of visa applications, or even expulsions. In this regard, it is important to recall the proposal to include so-called 'troublemakers' into the SIS.[39] The purpose of this proposal is to share information on persons "whom certain facts give reason to believe that they will commit significant criminal offences". The proposal gives no definition of "significant criminal crime" other than that this should fall within a category higher than that of petty crime that is likely to disturb public peace

---

[34] For more details on the SIS and the development of SIS II, see Evelien Brouwer, *Digital Borders and Real Rights. Effective remedies for third-country nationals in the Schengen Information System*, Leiden/Boston: Martinus Nijhoff Publishers, 2008.

[35] In January 2008, SIS included 23 million pieces of data, so the amount of data increased by 5 million alerts within one year. SIS Database Statistics, Council document 5764/09, 28 January 2009.

[36] On 1 January 2009, from the 927,318 records on persons held in the SIS, 746,994 (80.5%) were third-country nationals reported for the purpose of refusal of entry.

[37] Note of 21 October 2008 from the French Presidency, Council doc. 14592/08.

[38] On the basis of Regulation 1987/2006 on the establishment, operation and use of the second generation Schengen Information System, *OJ* L 381/4, 28.12.2006 and with regard to its use for police and judicial cooperation in criminal matters: Council Decision 2007/533/JHA of 12 June 2007 *OJ* L 205, 7.8.2007.

[39] See, for earlier discussions on this proposal the JHA Council of 5/6 June 2003, Council doc. 9808/03. It was set on the agenda again in 2008, Council doc. 7544/08, 14 March 2008 and 17608/08, 23 December 2008.

and have a considerable effect on the public's sense of security. With shared information, persons, including EU citizens, could be barred from certain events by refusing them entry to the territory of the EU member state in question.

5. The protection of human rights

It is clear that the different measures dealing with the use of passenger data affect both the right to privacy and the right to data protection. In February 2009, the European Court of Human Rights (ECtHR) affirmed again, in the case of *Nolan and K. v. Russia*, the close relationship between the effects of border control and targeting persons as "inadmissible persons" on the one hand and the protection of fundamental rights of individuals on the other.[40] Except for the detailed comments of the Fundamental Rights Agency (dealt with above), the consequences of the use of passenger data, and in particular the use of profiling for the right to non-discrimination, has so far received less attention. Therefore, the following sections will focus on the relation of the EU PNR system and the right to non-discrimination as well as the right to privacy. As this has been dealt with at some length by other organisations such as the EDPS, only certain issues of data protection law will be considered here.

5.1 The right to privacy – Article 8 ECHR

As has been underlined several times by the ECtHR, the systematic collection and storage of personal information, including administrative data, fall within the scope of the right to a private life as protected by Article 8 ECHR.[41] One very important decision is the judgment of 16 February 2000 in *Amann v. Switzerland*, applying Article 8 to the storage of information relating to an individual's private life by a public authority, regardless of the sensitivity of the data and regardless of the use that is effectively being made by third parties.[42] In *Rotaru v. Romania*, the ECtHR referred more explicitly to the criterion of systematic collection and storage.[43] This case concerned the complaint by Mr. Rotaru about the information stored on him since 1948 by the Romanian Intelligence Services. According to the ECtHR, even public information may fall within the scope of private life when it is "systematically collected and stored in files held by the authorities". This would be all the more true if such information concerned a person's distant past.

5.1.1 Proportionality and procedural guarantees necessary in a democratic society

Dealing with the question of whether any interference with the right to a private life meets the criterion, "necessary in a democratic society", the ECtHR generally leaves a wider margin of appreciation to the national authorities when it comes to national security or the prevention of disorder or crime than it would in regular cases. However, even when national governments invoke internal security objectives, the ECtHR requires evidence of a substantiated balance of the different interests at stake. Also, the ECtHR requires the availability of procedural guarantees with regard to the scope and time of the specific measures being used, but also to

---

[40] Judgment of 12 February 2009, appl. no. 2512/04.

[41] This jurisprudence has also been dealt with by the European Agency for Fundamental Rights in the *Opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, 28 October 2008.

[42] *Amann v. Switzerland* of 16 February 2000, no. 27798/95, *ECHR* 2000-II, § 68-70.

[43] *Rotaru v. Romania*, 4 May 2000, no. 28341/95 *ECHR* 2000-V, §§ 43-44. See further section 6.4.2 below.

allow independent courts or authorities to assess the necessity and proportionality of the security measures.

The proposed EU PNR data system concerns the systematic data processing on large groups of persons. These passengers, EU and non-EU citizens, are (generally) not suspected of any crime, nor are they the subject of a criminal investigation or security measures. The only reason their data are submitted to either the government of third countries, or the law enforcement and immigration authorities of the member states, is the fact that they have booked a flight. As the ECtHR in the aforementioned *Amann* judgment made clear, the fact that the information is only stored or transferred and not always subsequently used in practice, is irrelevant for the application of Article 8 ECHR. The ECtHR developed criteria for the necessary balance of powers between the data-collecting authorities on the one hand and the protection of the interests and rights of the individual on the other. This includes: limitations on the exercise of powers to store and use the information; the duty to inform the person concerned in advance with regard to the storage of his or her information; clear definition of the kind of information that may be recorded, of the categories of people against whom surveillance measures may be taken and the purposes for which the information can be used. With regard to the latter criterion, in the case of *Segerstedt-Wiberg v. Sweden*, the ECtHR assessed in particular whether the powers of the Swedish Security Service to store information in Secret Police registers for "special reasons", as provided under the Swedish Police Data Act, included unfettered powers for these authorities.[44] In this case, the ECtHR concluded that the scope of discretion conferred upon the competent authorities and the manner of its exercise were indicated with "sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference". This criterion is closely related to the data protection principle of purpose limitation, dealt with in section 5.2.1 below.

What I would like to emphasise at this point is that, aside from these requirements to guarantee a fair balance between the rights of the individuals and the goals of public authorities, it remains important that these latter goals are always clearly established. This means that when considering new measures dealing with the use or exchange of personal data and (potentially) affecting privacy rights of individuals, the (national ànd EU) legislator must always provide convincing information on the added value or efficiency of these measures. One cannot consider the proportionality of a proposal without establishing its efficiency first. Therefore, also in the light of Article 8 ECHR, when assessing the use of new databases or data exchange, it is necessary to evaluate existing measures in this field.[45] What are the lessons of SIS, Eurodac and the current agreements on the use of passenger data, as for example the aforementioned API Directive? As long as there is no information on the added value of these measures, the introduction of new databases or the extension of existing information flows cannot be considered.

5.1.2 In accordance with the law

The criteria as developed by the ECtHR on the basis of Article 8 (2) ECHR should also be taken into account when assessing the current proposals on the EU PNR system. The criteria are important in terms of the "accessibility and foreseeability" of the law. In the *Huvig and Kruslin* case-law, the ECtHR defined a set of criteria for lawful telephone tapping that should have been provided for in French law. These criteria included the categories of persons liable to have their

---

[44] *Segerstedt-Wiberg and Others v. Sweden*, 6 June 2006, no. 62332/00, § 79.

[45] See for example on the implementation of the EU-Canada PNR Agreement: Peter Hobbing, *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, CEPS Special Report, September 2008, revised version 17.11.2008.

telephones tapped by judicial order and the nature of the offences that may give rise to such an order; the lack of an obligation to set a limit on the duration of telephone tapping; the circumstances under which recordings may or must be erased or the tapes destroyed, in particular when an accused party has been discharged by an investigating judge or acquitted by a court.[46] Interestingly, a comparable list of criteria is given in *Rotaru v. Romania* with regard to the law regulating the collection, recording and archiving of information in secret files. After assessing the 'quality' of the Romanian law involved, the ECtHR concluded that this law did not include any limits on the exercise of the powers on the storage and use of the information by the Romanian Intelligence Services. Furthermore, Romanian law did not specify which information could be collected or stored and against which categories of people or under which circumstances these surveillance measures were allowed. The ECtHR also denounced the absence of limits on the length of time for which the information could be stored.[47] In the view of the ECtHR, the criteria of "in accordance with the law" and "quality of law" of Article 8 (2) require supervision procedures and adequate and effective safeguards against abuse of the rule of law.[48] Since the Romanian system did not provide such safeguards or a supervisory mechanism, the ECtHR ruled that in this case the storage and use of information by the intelligence service was not "in accordance with the law".

Considering this criterion "accessibility of law', one has to note that the whole process of PNR data transmission on the basis of the draft Framework decision shall be covered by at least four legal regimes: the EC Directive 95/46 for the data collection by the air carriers; the draft PNR Framework Decision will apply to the data transfers by the airline companies to the Passenger Information Units; thirdly, the Framework Decision on data protection for the data transfers to third countries and finally the data transfers between PIU and national law enforcement authorities will be covered by national data protection law. The legal rules dealing with the collection and use of passenger data, the competences of the PIUs, the powers of national authorities ànd authorities of third countries, the rights of data subjects and data protection authorities are still insufficiently clear and precise. This, as we saw, has also been emphasised by the FRA, the EDPS and the European Parliament.

5.1.3 Limitations within the national constitutional laws

When dealing with the current EU measures of information processing, national authorities should not only take into account the EU and international standards of human rights, but also their own constitutional laws. In this regard, recent judgments of the German Constitutional Court established some clear and strict limitations for the storage and use of personal data. For example, on 27 February 2008, the Constitutional Court annulled the new law of North Rhine Westphalia allowing secret spying of personal computers and the use of internet (1), because these laws were in breach of the constitutional right to privacy.[49] For the same reason, on 11 March 2008 the Court annulled a new provision in the police laws of Hessen and Schleswig-Holstein on the automatic identification and storage of vehicle registration plates of private cars.[50] These laws provided for the registration of these plates by video cameras without prior suspicion in order to compare these data with information in the existing police files. Also on 11 March 2008, the Constitutional Court, (partially) suspended, (on the basis of a so-called "Eilantrag" or interim appeal of 30,000 citizens) the German implementation act of the EC

[46] *Kruslin* § 35, *Huvig* § 34.

[47] *Rotaru v. Romania*,§ 41.

[48] *Rotaru v. Romania*, § 43.

[49] BvR 370/07.

[50] 1 BvR 2074/05.

Directive on Data Retention.[51] Generally, criteria used by the German Constitutional Court to conclude that the refuted measures were in breach of the constitutional right to privacy were: the lack of legal certainty or transparency; the absence of a clear purpose limitation; the disproportionality of the data-processing measures and the absence of concrete justification for the collection of data. This case law of the Constitutional Court in Germany, and especially the latter judgment dealing with the Data Retention Directive, are a signal that because of the structural shortcomings in the EU instruments itself, the implementing measures at the national level risk annulment by national courts or supervisory authorities.

5.2 The right to data protection

An important step for the meaning of the right to data protection in practice has been its inclusion as a fundamental right in the Charter of Fundamental Rights of the EU. Although this inclusion affirmed the separate and autonomous meaning of data protection, its relation with the right to a private life remains clear.[52] Considering the current developments with regard to the use of passenger data, the following central data protection principles need careful examination:

- purpose limitation principle;
- prohibition of automated decision-making;
- quality of data;
- time limits;
- individual access and correction rights;
- supervision of national and European data protection supervisors;
- adequate level of data protection in third countries;
- security of data.

5.2.1 Purpose limitation

The principle of *purpose limitation*, at risk of being undermined by the inclusion of vague and open criteria in the current proposals merits special attention. According to Article 6.1 (b) of EC Directive 95/46, personal data must be collected for specified, explicit and legitimate purposes and must not be further processed in a way that is incompatible with those purposes. This principle includes different layers of protection. Firstly, it prohibits the collection of personal data for unknown or unspecified purposes. Secondly, it prohibits the use or disclosure of personal information for purposes other than the specific purpose for which the data have been collected. Thirdly, the principle of purpose limitation provides that data should not be retained any longer than is necessary for the specified purpose. Purpose limitation is closely linked to the principle of purpose specification, which implies that data-holders should specify and make transparent the purposes of the relevant data processing. Both the purpose limitation and the purpose specification principle reflect the idea that data processing should be foreseeable for the

[51] 1 BvR 256/08.

[52] This has been confirmed in the aforementioned case of *Österreichischer Rundfunk* (C-465/00), where the ECJ ruled that if national courts were to conclude that national legislation with regard to the processing of personal data is incompatible with Article 8 ECHR, legislation would also be "incapable of satisfying the requirement of proportionality in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46".

data subject and should not go beyond the reasonable expectations of the person concerned.[53] As we have seen above, in its jurisprudence on the protection of the right to private life, the ECtHR explicitly emphasised the importance of "foreseeability" with regard to the processing of personal data by governmental authorities.[54]

In principle, the use of PNR data in the proposed Framework Decision is limited to member states' activities against terrorist offences or serious crime. The text of the proposal, however, leaves different possibilities to extend the goals of processing PNR data. In the first place, throughout the text, the use of PNR data is allowed for "the prevention, investigation, detection or prosecution" of terrorist offences or serious crime, which extends the activities of national authorities during which PNR data may be gathered or used meaningfully. Secondly, as we have seen above, Article 4 (5) allows the further use of PNR data for other offences, when these offences or "indications thereof" are detected during the enforcement action with regard to terrorist offences or serious crime. Thirdly, although the definitions of "terrorist offences" and "serious crime" refer to the definitions as adopted in earlier Framework Decisions on combating terrorism, organised crime, and on the European Arrest Warrant, it seems unclear at this moment whether these latter instruments have actually led to a more harmonised approach in this field.

Finally, the draft Framework Decision allows the transmission of PNR and PNR data analysis to law enforcement authorities of third countries for the prevention, detention, investigation or prosecution of terrorist events or serious crime. As we saw above, the Council envisaged allowing the use of PNR data not only for the fight against terrorism and organised crime, but also for integrated border management and the investigation of other serious crimes. The proposed interconnection with other databases, including SIS, and the currently open issues with regard to which authorities and third countries will obtain access to the passenger data, are also important for the question of whether the standards of the purpose limitation principle are met. The member states should be absolutely clear about the envisaged use of PNR data and its possible links with other systems, before adopting the current PNR Framework Decision.

5.2.2 Data retention

The Commission proposal included the possibility to retain data for thirteen years: five years after their transfer to the PIU of the first member state on whose territory the international flight enters, departs or transits, and, upon expiry of this period of five years, another period of eight years. During this second period the data may be accessed, processed and used only with the approval of the competent authority and "only in exceptional circumstances in response to a specific and actual threat or risk related to the prevention or combat of terrorist offences and serious crime." The latest draft of the Framework Decision (June 2009) proposes a data retention period of initially three years after the first transfer of the PNR data to the PIU of the first member state on whose territory the international flight is landing or departing, and a subsequent period of seven years for archiving these data.[55] With regard to the data retention period to be observed by third countries receiving PNR data and the analysis of PNR data, the draft Framework Decision does not include any binding rules.

---

[53] See D. Elgesem, "The structure of rights in Directive 95/46 on the protection of individuals with regard to the processing of personal data and the free movement of such data", *Ethics and Information Technology* 1: 283-293, 1999.

[54] Judgment *Peck vs. United Kingdom*, 28 January 2003, appl. no. 44647/98.

[55] Article 9 of the draft text. As is noted by the Presidency, the member states have not reached any consensus about this additional retention period, see Council doc. 5618/2/09, 29 June 2009.

5.2.3 Prohibition of automated decision-making

Another subject to be dealt with further is the principle on the *prohibition of automated decision-making*. Article 15 of EC Directive 95/46 provides that every person has the right "not to be subject to a decision which produces legal effects concerning him or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." In the light of current EU developments, where measures on border and immigration control tend to be based increasingly on automated data processing, the banning of "automated decision-making" becomes even more important. Data stored within a database or the outcome of group profiling should never be the sole basis for an individual decision.

Preamble 20 and Article 3 (5) of the Commission proposal of November 2007 provides that no enforcement action shall be taken by the PIUs and the competent authorities of the member states solely on the basis of the automated processing of PNR data. A new text has been proposed within the Council, stating "the PIUs shall not take any decision which produces an adverse legal effect concerning a person or significantly affects him based solely on the automated processing of a passenger's PNR data.[56] A comparable provision has been included with regard to the tasks of the competent authorities in Article 4 (6). This proposed provision is to be welcomed, however it should be taken into account that for individuals it is difficult to assess on which grounds, other than PNR data, he or she will be submitted for more specific checks or refused entry. For that reason the prohibition of automated decision-making is closely related to the right of a person to be informed on the reasons of the decision-making.

5.3 Profiling and the right to non-discrimination

As has been made clear in the Impact Assessment accompanying the proposal for the Framework decision and in the discussions of the EU Council, profiling will be an important tool with regard to the implementation of the EU PNR data system. Its meaning will be twofold. In the first place, PNR data transmitted by air carriers to national authorities of the EU member states will be assessed on the basis of current profiles – resulting in possible identification of high-risk passengers. Secondly, the transmitted PNR data will be used by the PIUs or by the national authorities of the receiving states, for the establishment of new profiles to be used for current or subsequent investigations.

Despite the sovereignty of governments to control their borders and to differentiate between their own citizens and foreigners, among other things by using intelligence tools to safeguard internal security, it is clear that the powers of border guards are restrained by the right of non-discrimination, as protected by the Convention on the Elimination of All Forms of Racial Discrimination (CERD), EC law and Article 14 ECHR.

5.3.1 Article 14 and 12th Protocol to the ECHR

Article 14 ECHR obliges member states to secure the enjoyment of the rights and freedoms as protected in the ECHR without 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. Aside from Article 14 ECHR, Protocol no. 12

[56] See Council doc. 7656/3/08, 19 June 2008.

to the ECHR includes a separate right protecting the "enjoyment of any right set forth by law" without discrimination on the aforementioned grounds.[57]

The relevance of the right of non-discrimination in the field of border controls has been underlined by the ECtHR in the case *Timishev v. Russia*.[58] This case concerned the complaint of a Russian national of Chechen ethnicity, who was refused by the Russian authorities to pass administrative borders within Russia. The ECtHR ruled that there was a violation of Article 14 ECHR in combination with Article 2 of the 4th Protocol (dealing with the freedom of movement). According to the ECtHR "no difference in treatment which is 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 pluralism and respect for different cultures." The ECtHR also emphasised that racial discrimination is "a particularly invidious kind of discrimination and, in view of its perilous consequences, requires from the authorities special vigilance and a vigorous reaction" (para. 58). It should be emphasised that the right to liberty of movement and freedom to choose his residence within the territory of a state as protected by the 4th Protocol applies to everyone lawfully within that state. This includes third-country nationals. The considerations in the *Timishev* case and the prohibition of a different treatment which is solely based on ethnic origin have been repeated in *Nachova v. Bulgaria* and *D.H. and others v. Czech Republic*.[59]

In this regard it is important to note that the underlying proposals will affect third-country nationals residing or seeking access to the territory of the EU member states as much or even more than EU nationals. As has been emphasised earlier by the Commissioner of Human Rights of the Council of Europe, this latter group of persons are especially vulnerable to wrongful actions or decision-making based on the use of incorrect or incomplete data: "While biometric identity documents, which operate between countries, are important security measures, the effect of mistakes on migrants will be much greater than on citizens where a computer malfunctions, and misidentifies an individual, or fails to record a legal entry, and so nullifies lawful entry; appeals should be a part of immigration law."[60]

5.3.2 UN Convention on the Elimination of Racial Discrimination

The *International Convention on the Elimination of all forms of Racial Discrimination* or CERD has been ratified by all EU member states and must therefore be observed when implementing the PNR instruments at stake.[61] Article 1(1) CERD defines racial discrimination as any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin that has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life. Article 2 of the CERD obliges the state parties to engage in no act or practice of racial discrimination against persons, groups of persons or institutions and to ensure that all public authorities and public institutions, national and local, shall act in conformity with this obligation (Article 2 (1) a). Also, on the basis of Article 2.1 c, state parties must take effective measures to review governmental,

---

[57] *CETS* no. 177, this protocol entered into force on 1 April 2005.

[58] EHRM *Timishev v. Russia*, 13 December 2005, no. 55762/00 and 55974/00, see paras. 58-59.

[59] *Nachova and Others v. Bulgaria* [GC], nos. 43577/98 and 43579/98, ECHR 2005-, and *D.H. v. Czech Republic*, 13 November 2007, EHRC 2008/5.

[60] Commissioner of Human Rights, Council of Europe, *The Human Rights of Irregular Migrants in Europe*, Strasbourg: CommDH/IssuePaper (2007)1, 17 December 2007.

[61] Adopted by the UN General Assembly resolution 2106, 21 December 1965, entry into force 4 January 1969.

national and local policies, and to amend, rescind or nullify any laws and regulations that have the effect of creating or perpetuating racial discrimination wherever it exists. Considering the definition of racial discrimination, Article 2(1)(a) therefore does not allow any justification for a different treatment on the basis of ethnicity or origin by governmental authorities. The Committee tasked with the supervision of the CERD in its General Comment no. 14 of 1993 with regard to the meaning of Article 1(1) only accepted the adoption of positive actions for certain groups as legitimate: "The Committee observes that a differentiation of treatment will not constitute discrimination if the criteria for such differentiation, judged against the objectives and purposes of the Convention, are legitimate or fall within the scope of Article 1, paragraph 4, of the Convention." Article 1 (4) only includes differentiating measures taken for the sole purpose of securing adequate advancement of certain racial or ethnic groups or individuals requiring such protection as may be necessary in order to ensure such groups or individuals equal enjoyment or exercise of human rights and fundamental freedoms.

Even if the CERD does not prohibit distinctions, exclusions, restrictions or preferences made by a State Party to this Convention between citizens and non-citizens, Article 1 (3) of the Convention makes clear that national legal provisions concerning nationality, citizenship or naturalisation are only legitimate as far they do not discriminate against any particular nationality. This means that when particular measures are directed against persons of certain national or ethnic origin, it may be in breach of the CERD. With regard to border control measures, this meaning of the CERD has been emphasised in the conclusions of the British House of Lords in 2004 in the case *Immigration Office at Prague Airport.*[62] This case concerned the so-called 'pre-flight checks' by British officials at the airport in Prague to prevent irregular immigration to the United Kingdom. Based on special instructions published by the Ministry of Home Affairs, these officials specifically checked Czech nationals of Roma origin. In her conclusions, supported by the majority of the House of Lords, Baroness Hale concluded that these pre-flight checks entailed an infringement of Article 1(2) CERD.

5.3.3 Article 8 ECHR and the stigmatising effect of data profiling

In the aforementioned opinion on the draft PNR Framework Decision, the FRA underlined the adverse effects of profiling, alienating and victimising certain ethnic and religious groups, which engender a deep mistrust of the police. An important signal to the EU legislator when further developing the EU PNR system should be the judgment of the German Constitutional Court on the practice of 'Rasterfahndung' or data profiling by the German police in their fight against terrorism.[63] In this judgment of 2006, concerning the complaint of a Moroccan student, the Court declared the German practice of data profiling unlawful, because it would include a disproportional breach of the constitutional right to privacy. For this conclusion, the German Court explicitly referred to the extended scope of the collection of information; the use of many different data bases; the increased risk for the person concerned of becoming a target of criminal investigation; and the possibility of stigmatisation of a group of persons in public life. The Constitutional Court also referred to the possibility of stigmatising a group of persons in public life, especially when it concerns, as in the refuted practice of data profiling, persons from specific countries who are also Muslim. In this judgment, the German Constitutional Court

---

[62] House of Lords 9 December 2004, R v. Immigration Office at Prague Airport and another (Respondents) ex parte European Roma Rights Centre and others (Appellants) [2004] UKHL 55 par. 101.

[63] Judgment of the Bundesverfassungsgericht, 4 April 2006, 1 BvR 518/02 published on 23. May 2006. I have dealt with this judgment previously in "The use of biometrics in EU data bases and Identity documents. Keeping track of foreigner's movements and rights", in Juliet Lodge (ed.) *Are you who you say you are? The EU and Biometric Borders*, Nijmegen: Wolf Legal Publishers, 2007, pp. 45-66.

explicitly emphasised the higher risk of certain groups of being affected by data profiling measures, I quote:

> For those persons whose constitutional rights it affects, data profiling means a higher risk of becoming the target of further official investigative measures. This has been demonstrated to a certain extent by the outcome of the data profiling implemented since 11 September 2001. (…) Furthermore, the very fact of police data profiling having been carried out according to certain criteria – if it becomes known – can have a stigmatising effect on those who meet these criteria. (…) It is relevant, with regard to the intensity of the effects of the data profiling carried out since 11 September 2001, that it is targeted at foreigners of certain origins and Muslim beliefs, which always involves the risk of spreading prejudice and stigmatising these population groups in the public perception.[64]

According to the Constitutional Court, such a measure could only be justified on the basis of a concrete danger of a terrorist attack that would cause great harm, the risk of which could be based on concrete facts. The Court considered that the general situation of threat that has existed since 9/11 or a tense situation based on foreign policy matters, are not sufficient reasons to justify the practice of data profiling:

More recently, in *S. & Marper v. the United Kingdom*, the ECtHR also warned against the risk of 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.[65] In this judgment, the ECtHR found that the applicable UK law violated Article 8 ECHR, particular on the grounds that these data were stored for indefinite periods and also concerned unconvicted persons as disproportional. Also important in this regard is the consideration in para. 119, where the ECtHR declared that they were 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". The ECtHR also based its conclusion that there was a violation of Article 8 ECHR on the grounds that there were only limited possibilities for the individual to have the data removed from the nationwide database or to have the materials destroyed (paragraph 35 of the judgment). Furthermore, there was no provision for an independent review of the justification for the retention according to the defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.

5.3.4 Inclusion of non-discrimination clauses in the PNR proposal

In the original Commission proposal, the preamble 20 and Article 3 (3) provided that no enforcement action should be taken by the PIU and the competent authorities of the member states based only on a person's race or ethnic origin, religious or philosophical belief, political

---

[64] Paras. 110-112: "Die Rasterfahndung begründet für die Personen, in deren Grundrechte sie eingreift, ein erhöhtes Risiko, Ziel weiterer behördlicher Ermittlungsmaßnahmen zu werden. Dies hat etwa der Verlauf der nach dem 11. September 2001 durchgeführten Rasterfahndung gezeigt. (...) Ferner kann die Tatsache einer nach bestimmten Kriterien durchgeführten polizeilichen Rasterfahndung als solche - wenn sie bekannt wird - eine stigmatisierende Wirkung für diejenigen haben, die diese Kriterien erfüllen. (...) So fällt etwa für die Rasterfahndungen, die nach dem 11. September 2001 durchgeführt wurden, im Hinblick auf deren Eingriffsintensität ins Gewicht, dass sie sich gegen Ausländer bestimmter Herkunft und muslimischen Glaubens richten, womit stets auch das Risiko verbunden ist, Vorurteile zu reproduzieren und diese Bevölkerungsgruppen in der öffentlichen Wahrnehmung zu stigmatisieren."

[65] *S. and Marper v. United Kingdom*, 4 December 2008, appl. no. 30562/04 and 30566/04, see para. 122.

opinion or sexual orientation. This provision was repeated in Articles 3 (3) and 4 (6) in the Council version of the draft Framework Decision of June 2008, however by adding "trade union membership" and "health" as sensitive data.[66] Article 3 (3) of this Council text provided that "no risk assessment criterion shall be based on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual orientation." This has been slightly changed in the text of April 2009, providing in Article 3 (4) that the risk criteria to be set up by the PIU and/or national authorities shall "in no circumstances be based on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual orientation."[67] With regard to the decision-making of the competent authorities of the member states, Article 4 (6) of the proposal (April and June 2009 version) prohibits them to "take any decision which produces an adverse legal effect on a person or significantly affects him only by reason of an automated processing of PNR data or only on the basis of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual orientation."

At this place, it is also important to refer to the non-discrimination clause in the Schengen Borders Code obliging border guards while carrying out border checks not to discriminate on grounds of sex, racial or ethnical origin, religion or belief, disability, age or sexual orientation.[68]

The inclusion of non-discrimination clauses could mean an important safeguard against the discriminatory treatment of passengers. However, it should be taken into account that profiling as such is always based on the mechanism to differentiate between different groups of persons on the basis of specific criteria. Even if these criteria are not the (prohibited) grounds mentioned above, certain features, such as food preferences, use of medicines, names, can always include information on someone's religion, health or ethnic origin. Before adopting new profiling measures, current instruments used within the EU member states should be systematically evaluated to investigate their possible discriminatory effects. An important study in this regard is the recent report of the Open Society Justice Initiative, *Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory*, underlining the necessity of a EU-wide prohibition on ethnic profiling and the need to provide for safeguards against profiling and clear oversight mechanisms.[69]

6. General conclusions

6.1 Assessing the necessity and proportionality of the EU PNR system

Tools have been developed within the EU without supporting evidence that these measures actually assist in the prevention or detection of terrorism or serious crimes. In this regard, the survey of the Article 29 Data Protection Working Party on the transposition of Directive 2004/82/EC (API Directive) is meaningful, concluding "that there is no overwhelming enthusiasm for the collection of passenger data at EU level". The failure to justify the necessity or proportionality, but also the efficiency or added value of the EU PNR system is unlikely to be solved by sunset or review clauses, allowing the legislator to adopt amendments or improvements to the instruments involved at a later stage. Nor can the intrusive effects of data systems be taken away by a general reference to applicable data protection rules, or by granting the data subject limited rights such as the right to apply for access or correction. The exercise of

---

[66] Council doc. 7656/3/08, 19 June 2008.

[67] This is maintained in the June 2009 version.

[68] Regulation 562/2006, *OJ* L/105, 13.4.2006. See Articles 6 lid 1 and 4 (2).

[69] An important study in this regard is the recent report of the Open Society Justice Initiative, *Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory*, New York, May 2009.

these rights will not, or only marginally, prevent the risk of wrongful use or misuse of data, nor prevent the general loss of privacy or data protection caused by the use of surveillance systems. The "analysis of PNR data" on the basis of the Framework Decision and its implied use of profiling is a matter of great concern, especially when considering its impact on the right to non-discrimination and the risk of stigmatisation of certain groups of passengers.

6.2 Harmonisation of national practices and definitions

A considerable problem in the current proposals is the lack of harmonisation in the underlying definitions used for the implementation of the measures in question. As has also been pointed out by the Fundamental Rights Agency, the PNR proposal contains open-ended and imprecise formulations with regard to the possible use of PNR data and the authorities acquiring access to these data. This amounts to a major deficit in the purpose limitation principle as described above, concerning for example the use of 'terrorism' or 'serious crime' to describe the purpose of the draft PNR Framework Decision. Even if these definitions are linked to the definitions used in third pillar instruments dealing with the fight against terrorism, organised crime, and the European Arrest Warrant, it is doubtful whether this prevents PNR data from being used on the basis of the policy and priorities of the 27 member states and of third countries gaining access to these data, considering the current provision in Article 4 (5) of the proposal and the uncontrollable use of PNR data by third countries. This raises doubts about the efficiency of these measures to address joint problems in a coherent way. The problem is not unique to the PNR proposal. It also applies to the inclusion of data in EU databases, for example the registration of "inadmissible aliens" into the Schengen Information System or SIS (and the proposal to report "violent troublemakers" in the SIS). The fact that the different instruments are meant to be connected for different purposes and by different national authorities will only increase the problems of assessing the usefulness and reliability of the data. As we saw above, the problem of the use of different definitions also applies to the general cooperation between the US and EU authorities on information-sharing.

6.3 Data subject rights: financial redress or compensation

An important issue with regard to the future use of EU databases, including PNR data, is the possibility of lodging a claim for damages caused by the use of information or data processing by governmental organisations in breach of Article 8 ECHR or other human rights.[70] This applicability of Article 6 ECHR with regard to damage caused by government information files is recognised by the ECtHR in the aforementioned judgment in *Rotaru v. Romania*.[71] The ECtHR considered the applicant's claim for compensation for non-pecuniary damage and costs as a civil claim within the meaning of Article 6 (1) ECHR. The failure of the national courts to consider the claim violated the applicant's right to a fair hearing in this case within the meaning of Article 6 (1) ECHR.

A positive achievement in the current draft of the PNR Framework Decision is the inclusion of the obligation for member states to ensure that passengers are informed of the use of PNR data; the current text leaves unclear the question of at what moment this information should be communicated, however. The draft Framework Decision includes the 'usual data protection rights' such as the right of access, rectification, and erasure. Unfortunately, these provisions do not include strict deadlines within which these requests must be met or fulfilled. Furthermore,

---

[70] For example, in the aforementioned *Nolan and K. v. Russia* case, the ECtHR found that the refusal of entry of Mr. Moon by the Russian authorities, established a violation of his right to freedom of religion, as protected in Article 9 ECHR. Judgment of 12 February 2009, appl. no. 2512/04.

[71] *Rotaru v. Romania*, §§ 74-79.

the current draft permits the member states to introduce or maintain an indirect system through which the individual should first apply through the intermediary of the national data protection authority. Practice with regard to the use of the Schengen Information System has shown that such intermediary procedures often cause long delays for individuals.[72] According to the current text, member states may restrict the right to access on numerous grounds, as long as this is necessary and proportional: this implies an individual assessment of all requests for access. It is also important that the data subject has the right to appeal against any refusal or restriction of access to the national supervisory authority, judicial authority or a court.[73]

As we have seen above, the current proposal provides in Article 11f for a right to compensation to a data subject who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national laws adopted to implement this Framework Decision. Also, it gives the data subject a right to judicial remedies for any breach of the rights guaranteed to him by the national provisions adopted pursuant to the Framework Decision. However, the scope of these rights is left to the scrutiny of the national legislators in the Framework Decision. It should be underlined that the national laws should provide for effective remedies, respecting the criteria and conditions as formulated by the ECtHR on the basis of Articles 6 and 13 ECHR and incorporated in Article 47 of the EU Charter of Fundamental Rights. To ensure that the rights of individuals are respected with regard to the storage and use of their personal data, the current legal proposals should include strict rules on the liability of the different authorities involved. Only this will allow the competent judicial or administrative authorities to impose sanctions when necessary.

Finally, the provision included on the transfer of information, including PNR data and analysis of PNR data to third countries, may undermine the protection of individual rights as protected by EU law. These transfers of data establish the risk of further storage and use of passenger data by authorities or agencies of foreign states, with no means for individuals or European courts or data protection authorities to control the lawfulness of these practices.

6.4 Effective control by national data protection authorities

The current draft of the Framework Decision (Article 11i) includes the duty of member states to empower national supervisory authorities with investigative powers and effective powers of intervention, without giving clear and uniform standards as to the scope of these powers, however. The only binding powers of the supervisory authority referred to in the draft proposal are those to order the blocking, erasure or destruction of the data. The draft Framework Decision does not include a power of the supervisory or data protection authority to issue binding decisions on the lawfulness of the data processing or data retention, or to give binding advice to the national legislator regarding new proposals on the use of PNR data.

Before expanding the existing 'EU information network', research must be developed on the practical effects and meaning of the role of data protection authorities. Until now, the scope of

---

[72] See my research on the French implementation of SIS, in *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden/Boston: Martinus Nijhoff Publishers, 2008, p. 329 ff. and p. 379.

[73] On the importance of effective remedies with regard to the use of PNR data see also Elspeth Guild and Evelien Brouwer, *The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief No. 109, CEPS, Brussels, July 2006 and Didier Bigo, Sergio Carrera, Elspeth Guild and R.B.J. Walker, *The Changing Landscape of European Liberty and Security: Mid-Term Report on the Results of the CHALLENGE Project*, CHALLENGE Research Paper No. 4, February 2007, available for free downloading from the CEPS website (http://www.ceps.be) and the Challenge website (www.libertysecurity.org).

review by data protection authorities is restricted and the independence and efficiency is threatened by their lack of power and financial resources. It is important that these data protection authorities perform further investigations with regard to the accuracy and reliability of information being stored, not least because of the irregularities already found in existing databases such as the SIS.[74] General inquiries or audits make national authorities aware of their obligations regarding the lawfulness and quality of data held in their systems. It also emphasises the 'watchdog' role of national and European data protection authorities.

As a final general remark: one has to reconsider the meaning and weight of the advice of data protection authorities and other advisory organisations concerning the development of the "European information model and data protection".[75] Despite the overwhelmingly critical reactions towards the PNR system, it is remarkable, to say the least, that the EU institutions and member states are going ahead with this initiative. More general, critical reactions to such proposals may have led to text amendments improving the legal position of data subjects; however (to my knowledge) a proposal has never been withdrawn as a result of negative advice concerning its very goal or scope. For the legal and political accountability of EU measures involving the use of personal information of millions and millions of EU citizens and foreigners, it is very important that politicians listen carefully to the actors involved. At the same time, the Stockholm process could be used to rephrase clear goals and limitations of the 'European information model', taking into account the EU's basic values: freedom of movement and the protection of fundamental rights and freedoms.

[74] The reports of national data protection authorities indicating a lack of accuracy and legitimacy of national SIS reports has been described in: Evelien Brouwer, *Digital Borders and Real Rights. Effective remedies for third-country nationals in the Schengen Information System*, Leiden/Boston: Martinus Nijhoff Publishers, 2008.

[75] As referred to by the European Data Protection Supervisor (EDPS) in his *Opinion on the Communication of the Commission on an Area of freedom, security and justice serving the citizen*, 10 July 2009, point 53.

References

Legislation – Europe

Association of European Airlines, *Comments on the European Commission Proposal to the Council of the European Union for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, 5 December 2007

Association of European Airlines, *Policy Paper on transfer of airline passenger data to governments*, April 2008

Association of European Airlines, *Position Paper: Background Information on Passenger Data Transfer*, 22 August 2006

Council of the European Union, *Report on the thematic work carried out from July to November 2008* Council doc. 15319/1/08, 20 November 2008

European Agency for Fundamental Rights, *Opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, 28 October 2008

European Commission *Communication on Examining the creation of a European Border Surveillance System (EUROSUR)* COM (2008) 68, 13.2.2008.

European Commission *Communication on Preparing the next steps in border management in the European Union* COM (2008) 69, 13.2.2008.

European Data Protection Supervisor, *Opinion on the draft proposal for a Council Framework Decision on the use of Passenger name Records (PNR) data for law enforcement purposes*, Brussels: 20 December 2007.

European Data Protection Supervisor EDPS *Opinion on transatlantic information sharing for law enforcement purposes: progress is welcomed, but additional work is needed*, Brussels: 11 November 2008.

European Data Protection Supervisor EDPS *Opinion on the Communication of the Commission on an Area of freedom, security and justice serving the citizen*, Brussels: 10 July 2009.

European Parliament Recommendation of 22 October 2008 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service

European Parliament Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of PNR for law enforcement purposes, B6-0615/2008

House of Lords – European Union Committee, *The EU/US Passenger Name record (PNR) Agreement*, London, 5 June 2007

Bibliography

Bigo, Didier, Sergio Carrera, Elspeth Guild and R.B.J. Walker (2008), *The Changing Landscape of European Liberty and Security: Mid-Term Report on the Results of the CHALLENGE Project*, CHALLENGE Research Paper No. 4, CEPS, Brussels, February, available for free downloading from the CEPS website (http://www.ceps.be) and the Challenge website (www.libertysecurity.org).

Brouwer, Evelien (2008), *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden/Boston: Martinus Nijhoff Publishers.

de Hert, Paul and Rocco Bellanova (2008), *Data Protection from a Transatlantic Perspective: The EU and U.S. move towards an International Data Protection Agreement?*, Study for CEPS on behalf of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, September.

Geyer, Florian (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CHALLENGE Research Paper No. 9, CEPS, Brussels.

Guild, Elspeth and Evelien Brouwer (2006), *The Political Life of Data. The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief No. 109, CEPS, Brussels, July.

Guild, Elspeth, Sergio Carrera and Florian Geyer (2008), *The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?*, CEPS Policy Brief No. 154, CEPS, Brussels, March.

Hobbing, Peter (2008), *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, CEPS Special Report, CEPS, Brussels, September, revised version 17.11.2008.

Lodge, Juliet (ed.) (2007), *Are you who you say you are? The EU and Biometric Borders*, Nijmegen: Wolf Legal Publishers.

Open Society Justice Initiative (2009), *Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory*, New York, May.

About CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is among the most experienced and authoritative think tanks operating in the European Union today. CEPS serves as a leading forum for debate on EU affairs, but its most distinguishing feature lies in its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

Goals

- To carry out state-of-the-art policy research leading to solutions to the challenges facing Europe today.
- To achieve high standards of academic excellence and maintain unqualified independence.
- To provide a forum for discussion among all stakeholders in the European policy process.
- To build collaborative networks of researchers, policy-makers and business representatives across the whole of Europe.
- To disseminate our findings and views through a regular flow of publications and public events.

Assets

- Complete independence to set its own research priorities and freedom from any outside influence.
- Formation of nine different research networks, comprising research institutes from throughout Europe and beyond, to complement and consolidate CEPS research expertise and to greatly extend its outreach.
- An extensive membership base of some 120 Corporate Members and 130 Institutional Members, which provide expertise and practical experience and act as a sounding board for the utility and feasability of CEPS policy proposals.

Programme Structure

CEPS carries out its research via its own in-house research programmes and through collaborative research networks involving the active participation of other highly reputable institutes and specialists.

Research Programmes

Economic & Social Welfare Policies
Energy, Climate Change & Sustainable Development
EU Neighbourhood, Foreign & Security Policy
Financial Markets & Taxation
Justice & Home Affairs
Politics & European Institutions
Regulatory Affairs
Trade, Development & Agricultural Policy

Research Networks/Joint Initiatives

Changing Landscape of Security & Liberty (CHALLENGE)
European Capital Markets Institute (ECMI)
European Climate Platform (ECP)
European Credit Research Institute (ECRI)
European Network of Agricultural & Rural Policy Research Institutes (ENARPRI)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)
European Security Forum (ESF)

CEPS also organises a variety of activities and special events, involving its members and other stakeholders in the European policy debate, national and EU-level policy-makers, academics, corporate executives, NGOs and the media. CEPS' funding is obtained from a variety of sources, including membership fees, project research, foundation grants, conferences fees, publication sales and an annual grant from the European Commission.

E-mail: info@ceps.be
Website: http://www.ceps.be
Bookshop: http://shop.ceps.be

CENTRE FOR EUROPEAN POLICY STUDIES

Place du Congrès 1 • B-1000 Brussels
Tel: 32(0)2.229.39.11 • Fax: 32(0)2.219.41.51