COUNCIL OF
THE EUROPEAN UNION

Brussels, 12 April 2011 (19.04)
(OR. fr)

8850/11

Interinstitutional File:
2011/0023 (COD)

LIMITE

JUR 163
GENVAL 38
AVIATION 92
DATAPROTECT 30
CODEC 618

OPINION OF THE LEGAL SERVICE (*)

Subject: Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (6007/11)

– Compatibility with the right to privacy and the right to the protection of personal data

I. INTRODUCTION

1. In its opinion of 28 March 2011 on the above proposal, the Legal Service indicated its intention to examine in a separate opinion the compatibility of the said proposal (including extending its scope of application to internal flights between Member States of the European Union) with the applicable data protection rules, in particular with regard to the principles of necessity and proportionality (8230/11).

* This document contains legal advice protected under Article 4(2) of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, and not released by the Council of the European Union to the public. The Council reserves all its rights in law as regards any unauthorised publication.

2. During the discussions some delegations raised the question of compatibility with fundamental rights and data protection[1]. Various bodies or agencies of the Union, and the European Parliament, have also raised this question[2].

II. CONTENT OF THE PROPOSAL FOR A DIRECTIVE

3. The transfer in advance and processing of air passenger name record data ("PNR data"), provided for in the proposal for a Directive, are designed to provide a tool for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (transnational in the case of certain processing operations), thus enhancing internal security.

4. The main content of the proposal has already been described in the previous opinion of the Legal Service (points 2 to 5 of 8230/11). The main factors of relevance from the point of view of data protection are as follows:

- processing of PNR data solely for the purpose of preventing, detecting, investigating or prosecuting serious offences, listed exhaustively: terrorist offences referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA[3] , serious offences referred to in Article 2(2) of Framework Decision 2002/584/JHA (list of 32 offences)[4] and, for certain processing operations, serious transnational crime (Articles 1(2) and 2(g) to (i) of the proposal)[5];
- obligation for air carriers to forward automatically, in advance, the PNR data that they collect for their own commercial purposes (up to 19 data items according to the Annex) for flights entering and leaving the Member States and third States (Article 6);[6]

---

1 See also notes from the Austrian delegation (7414/11) and the German delegation (8118/11).

2 See opinion of the European Data Protection Supervisor of 25 March 2011 on the above proposal. See also, on a similar earlier proposal for a framework decision, the opinions of the Article 29 Data Protection Working Party (opinion of 5 December 2007) and the European Agency for Fundamental Rights (see references in the explanatory memorandum of the proposal for a Directive) and the Resolution of the European Parliament of 20 November 2008. For a comparison between the two proposals, see 6361/11.

3 Framework Decision 2002/475/JHA on combating terrorism (OJ L 164, 22.6.2002, p. 3).

4 Framework Decision 2002/584/JHA on the European Arrest Warrant (OJ L 190, 18.7.2002, p. 1), the Member States being able to exclude minor offences for which the processing of PNR data would contravene the principle of proportionality.

5 These are the same offences as those listed in the Framework Decision on the arrest warrant, but transnational in nature within the meaning of the United Nations Convention of December 2000 on Transnational Organised Crime (OJ L 261, 6.8.2004, p. 69) (see definition in Article 2(i) of the proposal).

6 And possibly flights between Member States, if the Union legislator so decides.

- storage of such data in the database of an authority that each Member State must set up or designate for the purpose ("Passenger Information Unit", hereinafter "PIU"), responsible for collecting data, storing them, analysing them and transmitting the result of the analysis to the competent authorities of the Member State (Article 3);[7]
- four types of processing: two a priori processing operations (before arrival or departure of the plane) and two a posteriori processing operations (Article 4(2)(a) to (d)):
  - a priori, by screening the PNR data, firstly against "*pre-determined criteria*", and secondly against databases recording persons or objects sought or under alert for the purpose of "*carrying out an assessment of the passengers* (…) *in order to identify any persons who may be involved in* [one of the offences in question] *and who require further examination by the competent authorities* (…)*, any positive match resulting from* (…) *automated processing* [having to be] *individually reviewed by non-automated means*";
  - a posteriori, either at the duly reasoned request of a competent authority in specific cases (prevention, detection, investigation and prosecution of offences), or to update or define new "*pre-determined criteria*" for risk assessment;[8]
- further processing, by the competent authorities, limited to terrorist offences and serious crime (without the transnational condition) (Article 5(4));
- transfer, on a case-by-case basis, by the PIU to the competent authorities for further examination of the PNR data of the persons identified in the prior screening (Article 4(4));
- transfer of these same data (screening results) by the PIU to the PIUs of other Member States when the PIU considers it necessary for the prevention, detection, investigation or prosecution of terrorist offences or serious crime (without the transnational condition) (Article 7(1));
- retention of the PNR data by the PIU for 30 days in an "active" form, then for 5 years subject to certain restrictions (masking of data elements enabling the passenger to be identified, but without making them anonymous, limits on the number of persons authorised to access it and specific conditions governing access), after which they must be destroyed (Article 9);[9]

---

7 Art. 5(2): "*Competent authorities shall consist of authorities competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime*", the list of authorities having to be established by each Member State, forwarded to the Commission and published in the Official Journal.

8 These assessment criteria must be defined by the PIU in cooperation with the competent authorities referred to in Article 5. The criteria cannot be based on "sensitive" data (race, ethnic origin, religious or philosophical belief, political opinion, trade union membership, health, sexual life) (Article 4(3)).

9 A positive result from prior screening is retained only for the time necessary to inform the competent authorities of this result. When the check results in the match being declared negative, it is stored for 3 years in order to avoid future "false" positive matches (Article 9(4)).

- in certain specific circumstances (for example, specific case, immediate and serious threat or specific and actual threat, or in exceptional circumstances) and on request, transfer to another Member State of some or all of the PNR data, or of the result of the processing (Article 7(2 to (5), without the transnational condition);
- transfer of PNR data, and of the results of the processing, to a third country under certain conditions (compliance with Article 13 of Framework Decision 2008/977/JHA,[10] same purpose as the Directive and limits on transmission to another country) (Article 8);
- application by analogy of various rules concerning data protection, by reference to Articles 17 to 22 and to Article 25 of Framework Decision 2008/977/JHA, plus: prohibition on taking an adverse decision solely on the basis of automated processing (Article 5(6)); prohibition on processing sensitive data; logging of processing operations; information of passengers about the processing to be carried out; and prohibition on the transfer of data to private parties (Articles 11 and 12).

5. According to the explanatory memorandum and recital 7, one of the innovative features of the proposal is the risk analysis tool provided for in Article 4(2) (a) and (d), which would enable the law enforcement authorities to detect "*persons who were previously "unknown", i.e. persons previously unsuspected of involvement in serious crime and terrorism, but whom an analysis of the data suggests may be involved* (…) *and who should therefore be subject to further examination by the competent authorities*".

   The use of this analysis tool (definition and update of "*pre-determined criteria*" for risk analysis and automatic screening of all passenger data against these criteria), in view of the fact that it concerns "*data of innocent and unsuspected persons*" (recital 7), is limited solely to terrorist offences and serious transnational crime.

[10] Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).

6. Finally, according to the impact analysis and the explanatory memorandum, it would be necessary to oblige the Member States to collect PNR data in order to prevent different and potentially contradictory national systems from developing. The United Kingdom appears to be the only Member State to have a PNR system, covering all flights (and other modes of transport), for the purpose of combating terrorism, crime and illegal immigration, with a data retention period of 10 years (5 years in active form and 5 years archived[11]. Other Member States (France, Denmark, Belgium, Sweden and the Netherlands) are planning or have adopted legislation in this area, but with a more limited scope (purpose, data retention period), or are using PNR data on an experimental basis.

7. The proposal for a Directive will stand alongside several existing or planned Union instruments governing the collection, storage and cross-border exchange of personal data for the purpose of law enforcement or migration management, an overview of which is provided in a Commission communication of July 2010[12]. Two instruments in particular have certain points in common with the proposal for a Directive:

   - Directive 2004/82/EC ("API"), which also provides for the transfer in advance of certain air passenger data, but with the aim of improving border controls and combating irregular immigration[13]. The transfer only concerns flights entering the EU from outside, is made only at the request of the competent authorities and involves 9 data items, which are deleted within 24 hours of entry of the passengers, unless "*the data are needed later for the purposes of exercising the statutory functions of the authorities* [checking persons] and may be used "*for law enforcement purposes*" subject to compliance with the provisions of Directive 95/46/EC[14];

---

[11] According to an information document distributed by the United Kingdom delegation to the working party ("*EU PNR Directive: information from the UK*"), since 2005 the analysis of the PNR data of more than 279 million passengers has led to 8 100 arrests (55 for murder, 165 for rape or sex offences and 857 for violence).

[12] Communication from the Commission of July 2010 "Overview of information management in the area of freedom, security and justice" (COM(2010)385 final).

[13] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ L 261, 6.8.2004, p. 24).

[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

- Directive 2006/24/EC,[15] which provides for the obligation for telecommunications operators to retain certain (listed) telecommunications data for a period of 6 months to 2 years, in order to "*ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime*". The Directive leaves it to Member States to define the retention period, the concept of serious crime, which authorities have access to the data and the conditions governing such access and the use of the data. The Directive stipulates that the data may be "*provided only to the competent authorities in specific cases*". The transposition of this Directive has, in certain Member States, given rise to quite serious constitutional problems[16].

III. LEGAL ANALYSIS

8. Since the entry into force of the Lisbon Treaty, the Charter of Fundamental Rights of the European Union ("the Charter") has the value of primary law.[17] The Charter is addressed, in particular, to the institutions of the Union, and therefore to the Council when it legislates, and to the Member States "*only when they are implementing Union law*"[18]. Consequently, the Union legislator's failure to observe the Charter may lead to the annulment by the Court of Justice of the act concerned.

---

15 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54).

16 In response to an appeal lodged by 34 000 citizens, the German Constitutional Court on 2 March 2010 acknowledged the principle of data retention for 6 months, stressing that the fact that the data were held by the operators themselves individually and not in a database directly accessible to the State, was a positive element of the protection of individuals. However, it annulled the German transposition law as being contrary to the principle of proportionality since it did not offer sufficient safety nets to protect the (very large number) of non-suspects whose data would be stored as a precautionary measure. Since the planned data retention constituted serious interference ("*schwerwiegender Eingriff*") with private life, the Court demanded that the security standards applicable to retention should be very high, that the purpose of the processing should be limited to the specific cases of the most serious crimes, to be listed, that the transparency measures should be enhanced to compensate for the general impression of being under surveillance that citizens might have and that the protection of the courts and the penalties for violation of the data protection rules should be strengthened. The Court added that the right of citizens to exercise their freedom without their every act being recorded was at the heart of Germany's constitutional identity ("*verfassungsrechtlichen Identität*") which the Constitutional Court in accordance with its case law, in particular on the Lisbon Treaty, has a responsibility to protect, including with regard to EU acts. The Court states that the scale of such preventive retention of telecommunications data reduces accordingly the possibility of adopting, including at European level, other preventive retention measures on that scale (see Judgment of 2 March 2010, *Data retention*,1 BvR 256/08, paragraphs 213 to 218, and Judgment of 30 June 2009, *Lisbon Treaty*, 2 BvE 2/08, paragraph 240).
The Bulgarian Supreme Administrative Court delivered a similar judgment on 11 December 2008 with regard to the Bulgarian transposition law (Judgment No 13627) and the Romanian Constitutional Court on 8 October 2009 declared as contrary to Article 8 ECHR the retention of such a volume of data on unsuspected persons (Judgment No 1258).

17 See Article 6(1) of the Treaty on European Union (TEU) which confers on the Charter "*the same legal value as the Treaties*".

18 Article 51(1) of the Charter.

9. Article 8(1) of the Charter provides that "*everyone has the right to the protection of personal data concerning him or her*"[19]. According to the Court of Justice, "*that fundamental right is closely connected with the right to respect of private life expressed in Article 7*"[20] of the Charter, according to which "*everyone has the right to respect for his or her private and family life, home and communications*".

10. The right to respect for private life is taken from Article 8(1) of the European Convention on Human Rights (ECHR) and therefore, in accordance with Article 52(3) of the Charter, has the same meaning and scope as those laid down by the CEDH[21].

11. Personal data[22] may undergo processing[23] only where there is respect for certain common principles in this area, the principles of fairness, purpose, legitimacy, transparency and control by independent authorities, which the Charter expresses as follows: the data "*must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*". Furthermore, "*everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*" and "*compliance with these rules shall be subject to control by an independent authority*" (Article 8(2) and (3) of the Charter).[24]

---

19 This right is repeated in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) among the provisions having general application.

20 Paragraph 47 of the Judgment of 9 November 2010, Volker, C-92/09 and C-93/09 (not yet published).

21 For a description of the conditions of application of Article 8 of the ECHR, and in particular the conditions under which interference with the right to respect for private life may be justified, see opinion of the Legal Service of 20 June 2001 (10146/01).

22 "Personal data" mean "*any information relating to an identified or identifiable natural person*" (Article 2(a) of Framework Decision 2008/977/JHA, which reproduces Article 2(a) of Directive 95/46/EC on data protection. Data are "*made anonymous*" where the person concerned is no longer identifiable (see recital 26 of Directive 95/46/EC and Article 2(k) of Framework Decision 2008/977/JHA).

23 "Processing" means "*any operation or set of operations* (…)*, such as collection, recording, organisation, storage* (…) *retrieval, consultation, use, disclosure* (…)*, alignment or combination, blocking, erasure or destruction*" (Article 2(b) of Framework Decision 2008/977/JHA, taken from Article 2(b) of Directive 95/46/EC.

24 This corresponds inter alia to the principles of lawfulness, proportionality and purpose provided for in Article 3 of Framework Decision 2008/977/JHA and to the principles relating to quality (fairness, lawfulness, purpose) and to legitimacy provided for in Articles 6 and 7 of Directive 95/46/EC. Framework Decision 2008/977/JHA applies only to the data exchanged between Member States, without covering the data processed within a Member State (see recital 7 and Article 1(2) of the Framework Decision). It therefore covers only partially the processing referred to in the proposal for a Directive, and for this reason it is intended to make some of these provisions applicable to the processing operations provided for in the Framework Decision. As for Directive 95/46/EC, it does not apply to the processing operations covered by the proposal for a Directive since it does not apply to processing operations concerning public security, State security and the activities of the State in areas of criminal law (see Article 3(2) of Directive 95/46/EC; on the non-application of this Directive to the Agreement on the transfer of PNR data to the United States of America, see Judgment of 30 May 2006, Parliament v. Council, C-317/04 and C-318/04, [2006] ECR I-4721).

12. Limitations on the right to privacy and data protection may be applied only when certain conditions are met. Article 8(2) of the European Convention on Human Rights accepts interference only where it is "*in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*".

Article 52(1) of the Charter accepts limitations only where they are "*provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*".

13. These are the provisions that serve as a frame of reference for the Court of Justice, which follows the lead of the European Court of Human Rights (Court of Human Rights) on this matter, when examining the compatibility of a data-processing measure with the rights in question[25].

Once an interference or infringement of the rights has been established, then, in application of the Court of Human Rights criterion that "*[t]he mere storing of data relating to the private life of an individual amounts to an interference*",[26] the grounds for that interference must be examined, which involves the examination of three cumulative conditions[27]:

(1) the interference or infringement must be in accordance with the law (which must have certain qualities of accessibility and foreseeability, and in particular an adequate framework for the processing operation);
(2) it must meet a general-interest objective recognised by the Union (legitimate aim); and
(3) it must be necessary and respond effectively to a general-interest objective (which presupposes a review of proportionality).

---

[25] See the aforementioned Volker judgment. See also the judgment of 20 May 2003 (Österreichischer Rundfunk) in Joined Cases C-465/00, C-138/01 and C-139/01 (ECR 2003, p. I-4989).

[26] Judgment of the Court of Human Rights, Marper, dated 4 December 2008, 30562/04 and 30566/04, paragraph 67.

[27] See paragraph 62 of the aforementioned Volker judgment and paragraph 76 of the aforementioned Österreichischer Rundfunk judgment. On the case-law of the Court of Human Rights, see also the aforementioned opinion of the Legal Service 10146/01.

As they constitute exceptions to the fundamental rights guaranteed by the Charter and the European Convention on Human Rights, grounds for interference are "*to be interpreted narrowly*"[28]. The Court of Justice follows the same line: "*derogations and limitations […] must apply only in so far as is strictly necessary*"[29].

14. The measures put forward under the proposal for a directive must, in the light of those criteria, be regarded as an infringement of or interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter and in Article 8 of the European Convention on Human Rights. It should therefore be examined whether the conditions justifying such an infringement are met.

Accordance with the law

15. For the Court of Justice, as for the Court of Human Rights, the expression "*in accordance with the law*" in the meaning of Article 52(1) of the Charter and Article 8(2) of the European Convention on Human Rights "*not only requires that the […] measure should have some basis in domestic law, but also refers to the quality of the law in question, [which] should be accessible to the person concerned and foreseeable as to its effects*"[30]. The proposal for a directive will constitute the legal basis for the measures and will be accessible by virtue of its publication in the Official Journal. Those two conditions are therefore met.

The condition of forseeability requires that the measure be drawn up "*with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct*"[31]. There must be "*a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by [the European Convention on Human Rights]. Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident*"[32]. There must therefore be provision for a framework that includes the following aspects, laid down by the Court of Human Rights: it is "*essential […] to have clear, detailed rules governing the scope and application of measures, as well as*

---

28 Judgment of the Court of Human Rights, Rotaru, dated 4 May 2000, 2841/95, paragraph 47.
29 See paragraph 77 of the aforementioned Volker judgment.
30 See paragraph 52 of the aforementioned Rotaru judgment.
31 See paragraph 95 of the aforementioned Marper judgment. See also paragraph 77 of the aforementioned judgment of the Court of Justice on Österreichischer Rundfunk.
32 Paragraph 55 of the aforementioned Rotaru judgment, quoting paragraph 67 of the Malone judgment of the Court of Human Rights of 2 August 1984, 8691/79.

minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness"[33].

The Court of Human Rights places particular emphasis on the importance of this framework when personal data are processed for the purposes of intelligence operations or when they are subject to automatic processing for police purposes, as is the case under the proposal for a directive, particularly as regards a priori processing of PNR data (Article 4(2)(a) and (b) of the proposal).

16. The proposal for a directive contains several provisions intended to meet the framework-related conditions set out by the Court of Human Rights. This is the case in particular for the purpose of processing (limited to a list of serious crimes that are transnational in nature for the identification of "*unknown*" persons and the definition of "*pre-determined criteria*"), conditions for data transfer, retention period, implementation of the provisions of Framework Decision 2008/977/JHA (right of access, right to rectification, erasure or blocking, right to compensation, right to judicial remedy, confidentiality and security of processing and supervisory authorities), the logging of processing operations as well as the ban on processing sensitive data and on taking decisions on the basis of automated processing.

17. However, the proposal for a directive is marked in this respect by the scope and volume of the data of a very large number of unsuspected persons[34] who will be subject to systematic processing by means of checking against a wanted persons' database and screening on the basis of "*pre-determined criteria*" to allow law-enforcement agencies to detect "*persons who were previously 'unknown'*" to them.

---

[33] See paragraph 99 of the aforementioned Marper judgment.

[34] According to the impact assessment, approximately 500 million air passengers entered and left the EU in 2006 (3.3 million flights). There were 4.5 million flights in 2010. Including all intra-EU flights would mean a threefold increase in passenger numbers (i.e. approx. 1 500 million passengers a year).

According to the case law of the Court of Human Rights,[35] "*as concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field*". However, it stresses that "*this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance".* It adds that "*whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse".*[36] It assesses, in particular, whether the limitative conditions specified by the legislation in question are sufficient for "*exploratory or general surveillance (...) not* to be *permitted".*[37]

18. To avoid a measure that can be regarded as authorising "*so-called exploratory or general surveillance"*, the framework provided for in the Directive should be strengthened and its provisions adjusted. However, this issue is related to the issue of proportionality which should be considered before suggesting changes to the text (see points 20 to 24 below).

---

[35] Judgment of the Court of Human Rights, Klass, dated 6 September 1978, No 5029/71, paragraphs 49 and 50. In this Judgment, regarding legislation authorising surveillance measures by secret services, the Court states that "*being aware of the danger that such a law poses of undermining or even destroying democracy on the ground of defending it,* [the Court] *affirms* [that the States] *may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate*" (paragraph 49, repeated in paragraph 59 in the aforementioned Rotaru Judgment).
See also the Judgment dated 4 April 2006 of the German Constitutional Court (BvR 518/02) which overturned a decision authorising searches by electronic profiling, through cross-checking data in a number of databases, without there being a sufficiently clear danger justifying the protection of the major interests concerned. For such a decision to be taken, there would need to have been a sufficient likelihood of the interests in question being endangered in the near future, i.e. sufficiently clear and established facts are required.

[36] According to the Court of Human Rights "*the need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes."* The legislation should "*ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored*" (aforementioned Marper Judgment, paragraph 103).

[37] See paragraph 51 of the aforementioned Klaas Judgment.

Legitimacy of the aim pursued

19. Article 52(1) of the Charter requires that the restrictions imposed on the exercise of the rights in question "*genuinely meet objectives of general interest recognised by the Union*"[38]. Article 8(2) of the ECHR lists the various legitimate goals, including "*national security,* (…) *public safety* [and] (…) *the prevention of crime*".

The aim of the proposal for a Directive as set out in recital 4 and in Article 1(2), namely preventing and detecting terrorist offences and serious transnational crime and improving internal security, is clearly "*a legitimate aim"* within the meaning of Article 8(2) of the ECHR. It is also an "*objective of general interest recognised by the European Union*" within the meaning of Article 52(1) of the Charter. The "*prevention and combating of crime*" are among the aims of the European Union listed in Article 3(2) of the TEU. Article 67(3) of the TFEU gives the European Union the mandate to endeavour "*to ensure a high level of security through measures to prevent and combat crime*".

Necessity and proportionality

20. According to the Court of Justice, so as to justify a limitation imposed on the rights in question, is justified only if it is "*proportionate to the legitimate aim pursued*".[39] The Court of Human Rights requires that such a limitation be *"necessary in a democratic society"* to attain a legitimate aim, which implies that it "[answers] *a pressing social need and, in particular,* [that it is] *proportionate to the legitimate aim pursued and* [that] *the reasons adduced by the (...) authorities to justify it are relevant and sufficient"*.[40] The authorities "*enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved*".[41]

---

38 See paragraph 67 of the aforementioned Volker Judgment (C-92/09 and C-93/09).
39 See paragraph 71, Volker judgment.
40 See paragraph 101 of the aforementioned Marper Judgment. See also paragraph 83 of the Österreichischer Rundfunk Judgment.
41 See paragraph 83 of the aforementioned Österreichischer Rundfunk judgment.

21. According to settled case-law of the Court of Justice "the principle of proportionality, which is one of the general principles of European Union law, requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it".[42] In this case, the measures provided for by the proposal for a Directive are certainly "*appropriate for attaining the objective pursued*" which is that of improving security.

However, the necessity of the measures proposed to attain this objective and, as a consequence, their proportionality, cannot be determined without a more thorough examination.

The objective pursued must in effect be reconciled with the fundamental rights set forth in Articles 7 and 8 of the Charter.[43] It is thus necessary to balance on the one hand "*the European Union's interest*" in improving security through the prevention and combating of crime and, on the other hand, "*the interference with the right of* [airline passengers] *to respect for their private life in general and to the protection of their personal data in particular*".[44]

It is therefore necessary to examine whether the proposed measure does not "*go beyond what* [is] *necessary for achieving the legitimate aims pursued, having regard in particular to the interference with the rights guaranteed by Articles 7 and 8 of the Charter*".[45]

---

42 See paragraph 74 of the aforementioned Volker Judgment (C-92/09 and C-93/09).
43 See paragraph 76 of the aforementioned Volker Judgment.
44 See paragraph 77 of the aforementioned Volker Judgment.
45 See paragraph 79 of the aforementioned Volker Judgment. See also point 86, 88 and 90 of the Österreichischer Rundfunk Judgment.

22. It is apparent from the case-law of the Court of Human Rights that a measure authorising "*so-called exploratory or general surveillance*" would contravene Article 8 of the ECHR[46]. Similarly, "*the blanket and indiscriminate nature of the power of retention*" of data (fingerprints, biological samples and DNA profiles) "*of persons suspected but not convicted of offences*", *which are* "*retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender*" and without restriction of time, "*overstep[s] any acceptable margin of appreciation in this regard [and] constitutes a disproportionate interference with the [...] right to respect for private life*"[47].

23. The PNR data to be processed automatically under the proposal for a directive would be the data of all air passengers entering or leaving via an external border of the Union, which, according to the impact assessment, equates to approximately 500 million people a year (or 1 500 million if the measures are extended to internal flights). They would be kept for 30 days in an "active" form, and then for five years in a form allowing searches to be carried out, although the subjects' identity would be concealed (in the event of a positive result, their identity could be retrieved).

As is the case for data stored under Directive 2006/24/EC on telecommunications (for a period of between six months and two years) and for data of air passengers under the API Directive obtained at the request of the authorities (stored for 24 hours), the directive would apply to persons "*innocent and unsuspected*" of a crime (Recital 7). However, in contrast to those instruments, all PNR data would be processed a priori regardless of the level of suspicion the persons concerned are under and in the absence of any specific risk situation.

---

[46] See paragraph 17 above and the penultimate subparagraph of paragraph 5 of the opinion of the Legal Service 10146/01. See also the strict conditions laid down by the German Constitutional Court concerning the preventive storage of information on a large number of people not suspected of any offence (footnote 17 above).

[47] Marper judgment, paragraphs 119 and 125.

Systematic and automatic a priori processing as provided for in Article 4(2)(a) and (b) of the proposal raises a serious question of proportionality in view of the relevant case-law. In the Legal Service's view, it would mean that the directive (if adopted in its current form, and even more so if internal flights were added) would be exposed to real risks in the event of proceedings not only before the Court of Justice but also before national constitutional or supreme courts,[48] particularly taking into account the insufficiently precise nature of the explanation for the necessity of such measures.

24. In order to remedy the problem of proportionality that it raises, the proposal would need to be adapted in at least four areas:

(1) By providing proof (currently lacking) of the need for the collection and storage of PNR data on a national database in each Member State to be added to existing personal data collection systems and mechanisms that are already available to or accessible by public authorities in the Member States, such as:

- the Schengen Information System (SIS);
- the Visa Information System (VIS);
- the system set up by the API Directive;
- data retained by telecommunications operators under Directive 2006/24/EC;
- the Europol information system.

To demonstrate this need it would have to be established that extending the remit of API data collection or law-enforcement authorities' access to all the data included in the SIS would not be enough to attain the intended objective adequately.

[48] The experience of measures implementing Directive 2006/24/EC on telecommunications being reversed by national supreme courts shows that the Union legislator must also take into account the risks of certain acts that it adopts being challenged before national constitutional courts. The Legal Service draws the Council's attention in particular to the warnings that certain courts, including the German Constitutional Court, have given the Union legislator concerning compliance with certain rights that they view as affecting (to quote Article 4(2) TEU) "*their national identities, inherent in their fundamental structures, political and constitutional*". Were such a court to challenge a legal act of the Union, this would harm the principles on which the Union is based, such as primacy (see footnote 17 above). Given its scope, the PNR Directive would, if adopted, constitute a preventive data retention measure, in addition to the existing European measures (which are set out in the Commission's communication of July 2010), and would thereby contribute to an accumulation of laws, an issue that the German Constitutional Court has indicated it intends to monitor closely.

(2) Show that the aims pursued could not be achieved by a system that, on the one hand, limited the storage of PNR data by competent national authorities solely to data concerning flights thought by the authorities to be "at risk"- with the data only being transferred at the request of the authorities on a case-by-case basis (as happens with API data) - and that, on the other hand, left the responsibility for retaining other PNR data to economic operators (carriers or reservation systems) while allowing access by the law enforcement authorities on a case-by-case basis (as with telecommunications data).

(3) Limit the period during which data held by economic operators and national authorities is retained to that which has been determined to be strictly necessary and laid down as such. The API Directive provides for a period of 24 hours and Directive 2006/24/EC (telecommunications) provides for a choice of a period of between six months and two years. If a longer data retention period is chosen, it should be done in order to meet specific and demonstrable requirements. A balanced approach might involve, for example, limiting to 30 days the data retention period for "at risk" flights, whose data is sent directly to the competent national authorities, and limiting the retention period of other PNR data by economic operators to no more than six months.

(4) Specify the categories of offence against which such a PNR system (or expanded API) could be used, and restrict their number as much as possible. They could, among others, include offences against State security, offences against the life or physical integrity of persons or offences that constitute a collective danger, such as terrorism. Indeed, the greater the number of offences covered by the proposal for a Directive, the more serious is the risk that the measures may be considered disproportionate.

IV. CONCLUSION

25. In conclusion, the opinion of the Legal Service is that the limitations which the directive, as proposed, places on the right to respect for private life and the right to protection of personal data mean that it would be exposed to a real risk of litigation with regard to the requirements of necessity and proportionality under Articles 7, 8 and 52 of the Charter and the general principles of EU law, particularly if the rationale for these restrictions is not reinforced.