OPINION OF ADVOCATE GENERAL LÉGER delivered on 22 November 2005 [1]

Table of contents

1 — Original language: French.

1. The European Parliament has brought before the Court two actions for annulment under Article 230 EC. In Case C-317/04 *Parliament* v *Council*, the action is for annulment of the Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection. [2] In Case C-318/04 *Parliament* v *Commission*, the Parliament seeks annulment of the Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection. [3]

2. In these two cases, the Court is called upon to rule on issues relating to protection of personal data of airline passengers where, in order to justify the transfer and processing of such data in a third country, in this case the United States, [4] requirements pertaining to public security and to the field of criminal law, such as the prevention and combating of terrorism and other serious crimes, are invoked.

3. These two cases have their origin in a series of events which should now be outlined. I shall then set out in detail their legal context.

I — Background to the dispute

4. Soon after the terrorist attacks on 11 September 2001, the United States passed legislation providing that air carriers operating flights to, from or through United States territory must provide the United States customs authorities with electronic access to the data contained in their automatic reservation and departure control systems, known as Passenger Name Records ('PNR'). [5] While acknowledging the legitimacy of the security interests at stake, the Commission of

2 — Decision 2004/496/EC (OJ 2004 L 183, p. 83; 'the Council decision').

3 — Decision 2004/535/EC (OJ 2004 L 235, p. 11; 'the decision on adequacy').

4 — These issues also concern the Community's relations with other third countries. An agreement of the same type as that at issue in Case C-317/04 was signed by the European Community and Canada on 3 October 2005.

5 — See the Aviation and Transportation Security Act (ATSA) of 19 November 2001 (Public Law 107–71, 107th Congress, Title 49, section 44909(c)(3), of the United States Code). That act was followed by implementing regulations adopted by the United States Department of Homeland Security, Bureau of Customs and Border Protection ('CBP'), such as the Passenger and Crew Manifests Required for Passenger Flights in Foreign Air Transportation to the United States, published in the *Federal Register* on 31 December 2001, and the Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States, published in the *Federal Register* on 25 June 2002 (Title 19, section 122.49b, of the Code of Federal Regulations).

the European Communities informed the United States authorities, from June 2002, that those provisions might come into conflict with Community and Member State legislation on the protection of personal data, as well as with certain provisions of the regulation on the use of computerised reservation systems (CRSs). [6] The United States authorities postponed the entry into force of the new provisions but refused to waive the right to impose sanctions on airlines failing to comply with those provisions after 5 March 2003. Since then, several large airlines established in Member States have provided the United States authorities with access to their PNR.

5. The Commission entered into negotiations with the United States authorities, which gave rise to the drawing up of a document containing undertakings on the part of CBP, with a view to the adoption of a Commission decision intended to establish the adequacy of the level of protection of personal data afforded by the United States, on the basis of Article 25(6) of 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. [7]

6. On 13 June 2003, the Article 29 Data Protection Working Party [8] delivered an opinion in which it expressed doubts regarding the level of protection guaranteed by those undertakings for the data processing operations envisaged. [9] It reiterated its doubts in a further opinion of 29 January 2004. [10]

7. On 1 March 2004, the Commission placed the draft decision on adequacy, together with the draft undertakings of CBP, before the Parliament.

6 — Council Regulation (EEC) No 2299/89 of 24 July 1989 on a code of conduct for computerised reservation systems (OJ 1989 L 220, p. 1), as amended by Council Regulation (EC) No 323/1999 of 8 February 1999 (OJ 1999 L 40, p. 1).

7 — OJ 1995 L 281, p. 31, directive as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 adapting to Council Decision 1999/468/EC the provisions relating to committees which assist the Commission in the exercise of its implementing powers laid down in instruments subject to the procedure referred to in Article 251 of the EC Treaty (OJ 2003 L 284, p. 1).

8 — This working party was set up under Article 29 of Directive 95/46. It is an independent advisory body which concerns itself with the protection of individuals with regard to the processing of personal data. Its tasks are defined in Article 30 of that directive and Article 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37).

9 — Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data. See internet site: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm.

10 — Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to be Transferred to the United States Bureau of Customs and Border Protection (US CBP). See internet site: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2004_en.htm.

8. On 17 March 2004, the Commission submitted to the Parliament, with a view to consulting it in accordance with the first subparagraph of Article 300(3) EC, a proposal for a Council decision concerning the conclusion of an agreement between the Community and the United States. By letter of 25 March 2004, the Council, referring to the urgent procedure provided for in Rule 112 of the Rules of Procedure of the Parliament (now Rule 134), requested the opinion of the Parliament on that proposal by 22 April 2004 at the latest. In its letter, the Council stated: 'The fight against terrorism, which justifies the proposed measures, is a key priority of the European Union. Air carriers and passengers are at present in a situation of uncertainty which urgently needs to be remedied. In addition, it is essential to protect the financial interests of the parties concerned.'

9. On 31 March 2004 the Parliament, acting pursuant to Article 8 of the Council Decision of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission, [11] adopted a resolution expressing a number of reservations of a legal nature regarding that approach. In particular, the Parliament considered that the draft decision on adequacy exceeded the powers conferred on the Commission by Article 25 of Directive 95/46. It called for the conclusion of an appropriate international agreement respecting fundamental rights, and asked the Commission to submit a new draft decision to it. It also reserved the right to refer the matter to the Court for review of the legality of the projected international agreement and, in particular, of its compatibility with the protection of the right to respect for private life.

10. On 21 April 2004 the Parliament, at the request of its President, approved a recommendation from the Committee on Legal Affairs and the Internal Market that the Court be requested to give an Opinion on the compatibility of the agreement envisaged with the Treaty, in accordance with Article 300(6) EC, a procedure which was initiated on that day. The Parliament also decided, on the same date, to refer to committee the report on the proposal for a Council decision, thus implicitly rejecting, at that stage, the Council's request for urgent debate made on 25 March 2004.

11. On 28 April 2004 the Council, acting on the basis of the first subparagraph of Article 300(3) EC, sent a letter to the Parliament asking it to give its opinion on the conclusion of the agreement by 5 May 2004. In order to justify the urgency, the Council restated the reasons set out in its letter of 25 March 2004. [12]

11 — Decision 1999/468/EC (OJ 1999 L 184, p. 23).

12 — See point 8 of this Opinion.

12. On 30 April 2004, the Registrar of the Court informed the Parliament that the Court had set 4 June 2004 as the time-limit for the submission of observations by the Member States, the Council and the Commission in the proceedings concerning Opinion 1/04.

13. On 4 May 2004, the Parliament rejected the request for urgent debate which the Council had made to it on 28 April. [13] Two days later, the President of the Parliament contacted the Council and the Commission to ask them not to continue with their intended course of action until the Court had delivered the Opinion requested on 21 April 2004.

14. On 14 May 2004, the Commission adopted the Decision on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to CBP, under Article 25(6) of Directive 95/46.

15. On 17 May 2004, the Council adopted the Decision on the conclusion of an Agreement between the Community and the United States on the processing and transfer of PNR data by Air Carriers to CBP.

16. By letter of 9 July 2004, the Parliament informed the Court of the withdrawal of its request for Opinion 1/04. [14] It then decided to take legal proceedings regarding the matters in dispute between it and the Council and the Commission.

II — Legal context of the two cases

A — *The EU Treaty*

17. Article 6 EU provides:

'1. The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States.

2. The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they

13 — In its applications, the Parliament justifies that rejection on the basis that there was found to be a continuing lack of all the language versions of the proposal for a Council decision.

14 — That request for an Opinion was removed from the register of the Court by order of the President of the Court of 16 December 2004.

result from the constitutional traditions common to the Member States, as general principles of Community law.

...'

B — *The Treaty establishing the European Community*

18. Article 95(1) EC provides:

'By way of derogation from Article 94 and save where otherwise provided in this Treaty, the following provisions shall apply for the achievement of the objectives set out in Article 14. The Council shall, acting in accordance with the procedure referred to in Article 251 and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.'

19. With regard to the procedure for the conclusion of international agreements by the Community, the first subparagraph of Article 300(2) EC provides in its first sentence that '[s]ubject to the powers vested in the Commission in this field, the signing ... and the conclusion of the agreements shall be decided on by the Council, acting by a qualified majority on a proposal from the Commission'.

20. Article 300(3) EC is worded as follows:

'The Council shall conclude agreements after consulting the European Parliament, except for the agreements referred to in Article 133(3), including cases where the agreement covers a field for which the procedure referred to in Article 251 or that referred to in Article 252 is required for the adoption of internal rules. The European Parliament shall deliver its opinion within a time-limit which the Council may lay down according to the urgency of the matter. In the absence of an opinion within that time-limit, the Council may act.

By way of derogation from the previous subparagraph, agreements referred to in Article 310, other agreements establishing a specific institutional framework by organising cooperation procedures, agreements having important budgetary implications for the Community and agreements entailing amendment of an act adopted under the procedure referred to in Article 251 shall be concluded after the assent of the European Parliament has been obtained.

The Council and the European Parliament may, in an urgent situation, agree upon a time-limit for the assent.'

C — *European law on the protection of personal data*

21. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms ('the ECHR') provides:

'1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as 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.'

22. European data protection law first emerged within the framework of the Council of Europe. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was thus opened for signature by the member States of the Council of Europe in Strasbourg on 28 January 1981.[15] Its purpose is to secure in the territory of each contracting Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.

23. So far as the European Union is concerned, in addition to Article 7 which relates to respect for private and family life, Article 8 of the Charter of fundamental rights of the European Union[16] is specifically devoted to the protection of personal data. It is worded as follows:

'1. Everyone has the right to the protection of personal data concerning him or her.

15 — European Treaty Series, No 108 ('Convention No 108'). That convention entered into force on 1 October 1985. Amendments to the convention were adopted by the Committee of Ministers of the Council of Europe on 15 June 1999 in order to allow the accession of the European Communities (those amendments have not, to date, been accepted by all the States party to Convention No 108). See also Additional Protocol to Convention No 108, regarding supervisory authorities and transborder data flows, which was opened for signature on 8 November 2001 and entered into force on 1 July 2004 (European Treaty Series, No 181).

16 — OJ 2000 C 364, p. 1. That charter, which was signed and proclaimed by the presidents of the Parliament, the Council and the Commission at the Nice European Council on 7 December 2000, is set out in Part II of the Treaty establishing a Constitution for Europe, which to date has not entered into force (OJ 2004 C 310, p. 41). As the Court of First Instance has pointed out, 'although [the Charter of fundamental rights of the European Union] does not have legally binding force, it does show the importance of the rights it sets out in the Community legal order'. See the judgment in Joined Cases T-377/00, T-379/00, T-380/00, T-260/01 and T-272/01 *Philip Morris International and Others* v *Commission* [2003] ECR II-1, paragraph 122.

2. Such 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. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.'

24. As regards primary Community law, Article 286(1) EC provides that, '[f]rom 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty'. [17]

25. In secondary Community legislation, the relevant basic enactment is Directive 95/46. [18] Its relationship to the provisions originating from Council of Europe is expressly indicated in the 10th and 11th recitals in its preamble. The 10th recital states that 'the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the [ECHR] and in the general principles of Community law; ... for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community'. In addition, the 11th recital states that 'the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in ... Convention [No 108]'.

26. Adopted on the basis of Article 100a of the EC Treaty (now, after amendment, Article 95 EC), Directive 95/46 has its origin in the idea expressed in the third recital in its preamble, according to which 'the establishment and functioning of an internal market ... require not only that personal data should be able to flow freely from one Member State

17 — Article 286(2) EC is worded as follows:
'Before the date referred to in paragraph 1, the Council, acting in accordance with the procedure referred to in Article 251, shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate.'
Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1) was adopted on the basis of Article 286 EC.

18 — For a detailed account of the general context in which that directive was drawn up and of its provisions, see M.-H. de Boulanger, C. de Terwangne, T. Léonard, S. Louveaux, D. Moreau and Y. Poullet, 'La protection des données à caractère personnel en droit communautaire', JTDE, 1997, Nos 40, 41 and 42. See also Simitis, S., *Data Protection in the European Union — the Quest for Common Rules*, Collected Courses of the Academy of European Law, Volume VIII, Book I, 2001, p. 95. I would also point out that a specific directive, namely Directive 2002/58, is intended to govern the electronic communications sector.

to another, but also that the fundamental rights of individuals should be safeguarded'. More specifically, the Community legislature started from the finding that 'the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State', [19] and this may in particular constitute an obstacle to the pursuit of activities at Community level and distort competition. The Community legislature therefore considered that, 'in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States'. [20] That approach must have the result that, 'given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy'. [21]

27. Article 1 of Directive 95/46, headed 'Object of the directive', applies that approach in these terms:

'1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.'

28. Article 2 of the directive defines inter alia the terms 'personal data', 'processing of personal data' and 'controller'.

29. Thus, under Article 2(a) of Directive 95/46, 'personal data' means 'any information relating to an identified or identifiable natural person ...; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

19 — Seventh recital in the preamble.

20 — Eighth recital in the preamble.

21 — Ninth recital in the preamble.

30. Under Article 2(b) of that directive, 'processing of personal data' covers 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

31. Article 2(d) defines 'controller' as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data ...'.

32. As regards the material scope of Directive 95/46, Article 3(1) provides that the directive 'shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system'.

33. Article 3(2) of the directive indicates one of the limits on the material scope of the directive since it provides:

'This Directive shall not apply to the processing of personal data:

— in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

...'

34. Chapter II of Directive 95/46 is devoted to '[g]eneral rules on the lawfulness of the processing of personal data'. Within that chapter, Section I covers the '[p]rinciples relating to data quality'. Article 6 of the directive lists those principles known as

fairness, lawfulness, purpose, proportionality and accuracy of processing of personal data. It is worded as follows:

'1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes ...;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date ...;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed ...

2. It shall be for the controller to ensure that paragraph 1 is complied with.'

35. Section II of Chapter II of the directive is devoted to the '[c]riteria for making data processing legitimate'. Article 7, which makes up that section, reads as follows:

'Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; ...'

36. With regard to personal data commonly categorised as 'sensitive', Article 8(1) lays down the principle that the processing of such data is prohibited. It provides that 'Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'. There are, however, a number of exceptions to that principle of prohibition; their content and the conditions to which they are subject are set out in detail in the subsequent paragraphs of Article 8.

37. Article 13(1) of Directive 95/46 provides under the heading 'Exemptions and restrictions':

'Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.'

38. The Community legislature also wished that the protective regime thus established should not be impaired when personal data leave Community territory. It became apparent that the international dimension of information flows [22] would render legislation that was effective only in that territory inadequate if not useless. The Community legislature therefore opted for a system requiring, in order for transfers of personal data to a third country to be allowed, that the country concerned ensure an 'adequate level of protection' for such data.

39. The Community legislature thus laid down the rule that 'the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited'. [23]

40. Accordingly, Article 25 of Directive 95/46 sets out the principles to which transfers of personal data to third countries are to be subject:

'1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States

22 — As examples, the data flows relating to personal mobility, electronic commerce and transmissions within a group of companies may be cited.

23 — 57th recital in the preamble to Directive 95/46.

shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.'

41. Finally, it should be mentioned that, within the framework of Title VI of the EU Treaty, which relates to police and judicial cooperation in criminal matters, the protection of personal data is governed by various specific instruments. These include instruments establishing common information systems at European level, such as the Convention implementing the Schengen Agreement, [24] which contains specific provisions on the protection of data under the Schengen Information System (SIS); [25] the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office; [26] the Council decision setting up Eurojust [27] and the Rules of Procedure on the processing and protection of personal data at Eurojust; [28] the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, which contains provisions relating to protection of personal data applicable to the Customs Information System; [29] and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. [30]

42. On 4 October 2005, the Commission submitted a proposal for a Council frame-

24 — Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, signed at Schengen on 19 June 1990 (OJ 2000 L 239, p. 19).

25 — See Articles 102 to 118 of that convention. As regards the second generation Schengen Information System (SIS II), the Commission has submitted proposals with a view to the adoption of a Council decision (COM(2005) 230 final), and of two regulations (COM(2005) 236 final et COM(2005) 237 final).

26 — OJ 1995 C 316, p. 2, 'the Europol Convention'.

27 — Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ 2002 L 63, p. 1; 'the Eurojust Decision'). See Article 14 et seq. of that decision.

28 — OJ 2005 C 68, p. 1.

29 — OJ 1995 C 316, p. 34. See, in particular, Articles 13 to 15, 17 and 18 of that convention.

30 — Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union that convention (OJ 2000 C 197, p. 1). See, inter alia, Article 23 of the convention.

work decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. [31]

III — The contested decisions

43. I shall examine the two contested decisions in the chronological order in which they were adopted.

A — *The decision on adequacy*

44. The decision on adequacy was adopted by the Commission on the basis of Article 25(6) of Directive 95/46, which, it should be recalled, confers on the Commission the power to find that a third country ensures an adequate level of protection of personal data. [32] As the second recital in the preamble to the decision states, '[i]n that case, personal data may be transferred from the Member States without additional guarantees being necessary'.

45. In the 11th recital in the preamble to the decision, the Commission states that '[t]he processing by CBP of personal data contained in the PNR of air passengers transferred to it is governed by conditions set out in the undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) of 11 May 2004 ... and in United States domestic legislation to the extent indicated in the undertakings'. The Commission therefore states, in the 14th recital in the preamble to the decision, that '[t]he standards by which CBP will process passengers' PNR data on the basis of United States legislation and the undertakings cover the basic principles necessary for an adequate level of protection for natural persons'.

46. Consequently, Article 1 of the decision on adequacy provides:

'For the purposes of Article 25(2) of Directive 95/46/EC, [CBP] is considered to ensure an adequate level of protection for PNR data transferred from the Community concerning

31 — COM(2005) 475 final. That proposal for a framework decision is based on Articles 30 EU, 31 EU and 34(2)(b) EU. It is one of the measures provided for by the Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union (OJ 2005 C 198, p. 1, paragraph 3.1).

32 — Since it was a measure implementing Directive 95/46, the decision on adequacy was adopted in accordance with the procedure laid down in Article 31(2) of that directive, which itself requires the application of Articles 4, 7 and 8 of Decision 1999/468. Thus, when it adopts a measure implementing the directive, the Commission is assisted by a committee composed of representatives of the Member States and chaired by the Commission's representative. In the present instance, the committee in question is the 'Article 31 Committee'.

flights to or from the United States, in accordance with the undertakings set out in the Annex.'

47. In addition, Article 3 of the decision on adequacy provides that data flows to CBP may be suspended on the initiative of the competent authorities in Member States as follows:

'1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to CBP in order to protect individuals with regard to the processing of their personal data in the following cases:

(a) where a competent United States authority has determined that CBP is in breach of the applicable standards of protection; or

(b) where there is a substantial likelihood that the standards of protection set out in the Annex are being infringed, there are reasonable grounds for believing that CBP is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk of grave harm to data subjects, and the competent authorities in the Member State have made reasonable efforts in the circumstances to provide CBP with notice and an opportunity to respond.

2. Suspension shall cease as soon as the standards of protection are assured and the competent authorities of the Member States concerned are notified thereof.'

48. The Member States are required to inform the Commission when measures are adopted pursuant to Article 3 of the decision on adequacy. Also, the Member States and the Commission must, pursuant to Article 4(2) of that decision, inform each other of any changes in the standards of protection and of cases where those standards appear to be insufficiently complied with. Following those exchanges, Article 4(3) of the decision on adequacy provides that '[i]f the information collected pursuant to Article 3 and pursuant to paragraphs 1 and 2 of this Article provides evidence that the basic principles necessary for an adequate level of protection for natural persons are no longer being complied with, or that any body responsible for ensuring compliance with

the standards of protection by CBP as set out in the Annex is not effectively fulfilling its role, CBP shall be informed and, if necessary, the procedure referred to in Article 31(2) of Directive 95/46/EC shall apply with a view to repealing or suspending this decision'.

49. Moreover, Article 5 of the decision on adequacy lays down the rule that the functioning of the decision is to be monitored and 'any pertinent findings [are to be] reported to the Committee established under Article 31 of Directive 95/46/EC'.

50. In addition, Article 7 of the decision on adequacy states that the latter 'shall expire three years and six months after the date of its notification, unless extended in accordance with the procedure set out in Article 31(2) of Directive 95/46/EC'.

51. Annexed to that decision are the undertakings of CBP, the introduction to which specifically states that they are intended to be '[i]n support of the plan' of the Commission to recognise the existence of an adequate level of protection of data transferred to CBP. As stated in them, those undertakings, which comprise a total of 48 paragraphs, 'do not create or confer any right or benefit on any person or party, private or public'. [33]

52. I shall indicate, in essence, in the course of my arguments, the content of those undertakings which are relevant to the outcome of the proceedings.

53. Finally, the decision on adequacy contains Attachment A which lists the 34 PNR data elements required by CBP from air carriers. [34]

54. That Commission decision is complemented by the Council decision to conclude an international agreement between the European Community and the United States.

33 — See paragraph 47 of the undertakings.

34 — They are the following elements: '1. PNR record locator code; 2. Date of reservation; 3. Date(s) of intended travel; 4. Name; 5. Other names on PNR; 6. Address; 7. All forms of payment information; 8. Billing address; 9. Contact telephone numbers; 10. All travel itinerary for specific PNR; 11. Frequent flyer information (limited to miles flown and address(es)); 12. Travel agency; 13. Travel agent; 14. Code share PNR information; 15. Travel status of passenger; 16. Split/divided PNR information; 17. E-mail address; 18. Ticketing field information; 19. General remarks; 20 Ticket number; 21. Seat number; 22. Date of ticket issuance; 23. No show history; 24. Bag tag numbers; 25. Go show information; 26. OSI information; 27. SSI/SSR information; 28. Received from information; 29. All historical changes to the PNR; 30. Number of travellers on PNR; 31. Seat information; 32. One-way tickets; 33. Any collected APIS (Advanced Passenger Information System) information; 34. ATFQ (Automatic Ticketing Fare Quote) fields'.

B — *The Council decision*

55. The Council decision was adopted on the basis of Article 95 EC, in conjunction with the first sentence of the first subparagraph of Article 300(2) EC.

56. The first recital in the preamble to the decision states that '[o]n 23 February 2004 the Council authorised the Commission to negotiate, on behalf of the Community, an Agreement with the United States of America on the processing and transfer of PNR data by air carriers to [CBP]'. [35] The second recital then states: 'The European Parliament has not given an opinion within the time-limit which, pursuant to the first subparagraph of Article 300(3) of the Treaty, the Council laid down in view of the urgent need to remedy the situation of uncertainty in which airlines and passengers found themselves, as well as to protect the financial interests of those concerned.'

57. By virtue of Article 1 of the Council decision, the agreement is approved on behalf of the Community. In addition, Article 2 of that decision authorises the President of the Council to designate the persons empowered to sign the agreement on behalf of the Community.

58. The text of the agreement is annexed to the Council decision. Article 7 of the agreement provides that it is to enter into force upon signature. In accordance with that article, the agreement, signed in Washington on 28 May 2004, entered into force on that same day. [36]

59. In the preamble to the agreement, the Community and the United States recognise 'the importance of respecting fundamental rights and freedoms, notably privacy, and the importance of respecting these values, while preventing and combating terrorism and related crimes and other serious crimes that are transnational in nature, including organised crime'.

60. The following provisions are cited in the preamble to the agreement: Directive 95/46 and in particular Article 7(c), the undertakings of CBP and the decision on adequacy. [37]

35 — 'The agreement'.

36 — See information concerning the date of entry into force of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004 C 158, p. 1).

37 — It should be noted that the preamble to the agreement gives an incorrect reference for the decision on adequacy. It is actually Decision 2004/535/EC of 14 May 2004, notified under number C(2004) 1914, and not Decision C(2004) 1799 of 17 May 2004. That error was the subject of a corrigendum published in the *Official Journal of the European Union*. See Procès-verbal of rectification to the agreement (OJ 2005 L 255, p. 168).

61. The Contracting Parties also note that 'air carriers with reservation/departure control systems located within the territory of the Member States of the European Community should arrange for transmission of PNR data to CBP as soon as this is technically feasible but that, until then, the US authorities should be allowed to access the data directly, in accordance with the provisions of this Agreement'. [38]

62. Paragraph 1 of the agreement thus provides that 'CBP may electronically access the PNR data from air carriers' reservation/departure control systems ... located within the territory of the Member States of the European Community strictly in accordance with the Decision[[39]] and for so long as the Decision is applicable and only until there is a satisfactory system in place allowing for transmission of such data by the air carriers'.

63. Complementing the power thus conferred on CBP to access PNR data directly, paragraph 2 of the agreement requires air carriers operating passenger flights in foreign air transportation to or from the United States to process PNR data contained in their automated reservation systems 'as required by CBP pursuant to US law and strictly in accordance with the Decision[[40]] and for so long as the Decision is applicable'.

64. According to paragraph 3 of the agreement, CBP 'takes note' of the decision on adequacy and 'states that it is implementing the undertakings annexed thereto'. Furthermore, paragraph 4 of the agreement provides that 'CBP shall process PNR data received and treat data subjects concerned by such processing in accordance with applicable US laws and constitutional requirements, without unlawful discrimination, in particular on the basis of nationality and country of residence'.

65. In addition, CBP and the Community undertake to review implementation of the agreement jointly and regularly. [41] The agreement also provides that '[i]n the event that an airline passenger identification system is implemented in the European Union which requires air carriers to provide authorities with access to PNR data for persons whose current travel itinerary includes a

38 — Transmission of the data by air carriers corresponds to what is commonly known as the 'push' system, whereas direct CBP access to the data corresponds to the 'pull' system.

39 — Namely the decision on adequacy, the only 'decision' referred to in the preamble to the agreement.

40 — Same remark as in the previous footnote.

41 — Paragraph 5 of the agreement.

flight to or from the European Union, DHS [the Department of Homeland Security] shall, in so far as practicable and strictly on the basis of reciprocity, actively promote the cooperation of airlines within its jurisdiction'. [42]

66. Also, in addition to providing that the agreement is to enter into force upon signature, paragraph 7 states that either party may terminate it at any time. In that event, termination is to take effect 90 days from the date of notification of termination to the other party. Paragraph 7 also provides that the agreement may be amended at any time by mutual written agreement.

67. Finally, paragraph 8 of the agreement provides that '[t]his Agreement is not intended to derogate from or amend legislation of the Parties; nor does this Agreement create or confer any right or benefit on any other person or entity, private or public'.

42 — Paragraph 6 of the agreement.

IV — The pleas put forward by the Parliament in the two cases

68. In Case C-317/04, the Parliament puts forward six pleas challenging the Council decision:

— incorrect choice of Article 95 EC as the legal basis;

— infringement of the second subparagraph of Article 300(3) EC, because Directive 95/46 was amended;

— infringement of the right to protection of personal data;

— breach of the principle of proportionality;

— lack of a sufficient statement of reasons for the decision at issue;

— breach of the principle of cooperation in good faith laid down in Article 10 EC.

69. The United Kingdom of Great Britain and Northern Ireland and the Commission were granted leave to intervene in support of the Council. [43] In addition, the European Data Protection Supervisor ('the EDPS') was granted leave to intervene in support of the Parliament. [44]

70. In Case C-318/04, the Parliament puts forward four pleas challenging the decision on adequacy:

— exceeding of the Commission's powers;

— breach of the fundamental principles of Directive 95/46;

— infringement of fundamental rights;

— breach of the principle of proportionality.

71. The United Kingdom was granted leave to intervene in support of the Commission. [45] In addition, the EDPS was granted leave to intervene in support of the Parliament. [46]

72. I shall examine the two actions in the order in which the contested decisions were adopted. I shall therefore consider, first, the action seeking annulment of the decision on adequacy (Case C-318/04) and then, second, that seeking annulment of the Council decision (Case C-317/04).

V — The action seeking annulment of the decision on adequacy (Case C-318/04)

A — *The plea alleging that the Commission exceeded its powers by adopting the decision on adequacy*

1. Arguments of the parties

73. In support of this plea, the Parliament maintains, first, that the decision on ade-

43 — Orders of the President of the Court of 18 January 2005 and 18 November 2004 respectively.

44 — Order of the Court of 17 March 2005.

45 — Order of the President of the Court of 17 December 2004.

46 — Order of the Court of 17 March 2005.

quacy, in so far as it seeks to achieve an objective relating to public security and criminal law, infringes Directive 95/46 since it concerns an area excluded from the scope *ratione materiae* of the directive. That exclusion is expressly provided for in the first indent of Article 3(2) of Directive 95/46 and is not amenable to any interpretation which could reduce its scope. The fact that personal data have been collected in the course of a business activity, namely the sale of an aeroplane ticket providing entitlement to a supply of services, cannot justify the application of that directive, and in particular Article 25, in an area excluded from its scope.

74. Second, the Parliament contends that CBP is not a third country within the meaning of Article 25 of Directive 95/46. Article 25(6) requires that a Commission decision finding an adequate level of protection of personal data relate to a 'third country', that is to say, a State or equivalent entity, and not an administrative unit or component forming part of the executive of a State.

75. Third, the Parliament submits that the Commission exceeded its powers in adopting the decision on adequacy in so far as the undertakings annexed to it expressly permit the transfer by CBP of PNR data to other US, or foreign, government authorities.

76. Fourth, the Parliament submits that the decision on adequacy entails certain restrictions on and exemptions from the principles set out in Directive 95/46, even though Article 13 of that directive reserves the power to adopt such measures solely for the Member States. Thus, by adopting the decision on adequacy, the Commission assumed the role of the Member States and therefore infringed Article 13 of the directive. In adopting a measure implementing Directive 95/46, the Commission appropriated powers strictly reserved for the Member States.

77. Fifth, the Parliament argues that making data available by means of the 'pull' system is not a 'transfer' within the meaning of Article 25 of Directive 95/46, and therefore cannot be allowed.

78. Finally, in view of the interdependence between the decision on adequacy and the agreement, that decision should, in the Parliament's submission, be held to be a measure inappropriate for compelling the transfer of PNR data.

79. Unlike the Parliament, the EDPS submits that providing a person or institution of a third country with access to data may be considered to constitute a transfer and that, consequently, Article 25 of Directive 95/46 is applicable. He considers that restricting the concept to a transfer effected by the sender would make it possible to evade the conditions laid down by Article 25 and thus impair the data protection provided for in that article.

80. The Commission, supported by the United Kingdom, takes the view that the activities of air carriers fall within the scope of Community law and that, consequently, Directive 95/46 remains fully applicable. The regime established in connection with the transfer of PNR data does not concern the activities of a Member State or of public authorities falling outside the scope of Community law.

81. In addition, the Commission points out that the agreement was signed on behalf of the United States and not on behalf of a government department. So far as subsequent transfers of PNR data by CBP are concerned, the Commission submits that the protection of personal data is not incompatible with the authorisation of such transfers, provided that they are subject to appropriate and necessary restrictions.

82. Finally, the Commission observes that Article 13 of Directive 95/46 is not relevant in this case and that 'transfer', within the meaning of Article 25 of that directive, consists, for air carriers, in actively making PNR data available to CBP. The system under consideration does therefore involve a transfer of data within the meaning of Directive 95/46.

2. Assessment

83. By this first plea, the Parliament submits that the decision on adequacy infringes Directive 95/46, and particularly Articles 3(2), 13 and 25. It claims inter alia that that decision could not properly be based on the primary act constituted by that directive.

84. As I have already explained, Directive 95/46 is intended, with a view to the establishment and functioning of the internal market, to remove obstacles to the free flow of personal data by rendering the level of protection of the rights and freedoms of individuals with regard to the processing of such data equivalent in the Member States.

85. The Community legislature also intended that the protective regime thus established should not be jeopardised when personal data leave Community territory. It therefore opted for a system requiring, in order for a transfer of personal data to a third country to be allowed to take place, that the country in question ensure an adequate level of protection for the data. Thus, Directive 95/46 contains the principle that if a third country does not afford an adequate level of protection, the transfer of personal data to that country must be prohibited.

86. Article 25 of that directive imposes a series of obligations on the Member States and the Commission, aimed at controlling transfers of personal data to third countries in the light of the level of protection afforded to such data in each of those countries. It also lays down the method and criteria for assessing whether a third country ensures an adequate level of protection for personal data transferred to it.

87. The Court has described the regime relating to the transfer of personal data to third countries as a 'special regime, with specific rules, intended to allow the Member States to monitor transfers of personal data to third countries'. It has also made clear that it is 'a complementary regime to the general regime set up by Chapter II of that directive concerning the lawfulness of processing of personal data'. [47]

88. The specific nature of the rules governing the transfer of personal data to third countries can largely be explained by the key role played by the concept of adequate protection. In order to define the scope of that concept, it must be clearly distinguished from the concept of equivalent protection which would require third countries to recognise and actually apply all the principles contained in Directive 95/46.

89. The concept of adequate protection means that the third country must be able to guarantee suitable protection on the basis of a model considered acceptable in terms of the degree of protection of personal data. Such a system based on the adequacy of the protection ensured by a third country allows the Member States and the Commission considerable discretion in their assessment of the safeguards established in the country to which the data is transferred. That assessment is guided by Article 25(2) of Directive 95/46, which lists some of the

47 — Case C-101/01 *Lindqvist* [2003] ECR I-12971, paragraph 63.

factors which may be taken into consideration for the purposes of the assessment.[48] In this connection the rule laid down by the Community legislature is that '[t]he adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations'.

90. As the Court has already stated, Directive 95/46 does not define the concept of 'transfer to a third country'.[49] In particular, it does not specify whether that concept covers only an action by which a controller actively discloses personal data to a third country or whether it extends to cases in which an entity of a third country is authorised to have access to data located in a Member State. The directive is therefore silent as to the method by which a transfer of data to a third country may be carried out.

91. Unlike the Parliament, I am of the opinion that, in this case, the access to PNR data enjoyed by CBP falls within the concept of a 'transfer to a third country'. In my view, the defining characteristic of such a transfer is the flow of data from a Member State to a third country, in this instance the United States.[50] It does not matter in that regard whether the transfer is carried out by the sender or by the recipient. As the EDPS points out, if the scope of Article 25 of Directive 95/46 were limited to transfers carried out by the sender, it would be easy to evade the conditions laid down by that article.

92. That said, attention should nevertheless be drawn to the fact that Chapter IV of the directive, in which Article 25 appears, is not intended to govern *all* transfers of personal data, of whatever nature, to third countries. As Article 25(1) of the directive states, Chapter IV covers only transfers of personal data '*which are undergoing processing* or are intended *for processing* after transfer'.

93. I would point out in that regard that, as stated in Article 2(b) of Directive 95/46, processing of personal data means 'any operation or set of operations which is

48 — Those factors include the nature of the data and the purpose and duration of the proposed processing operation or operations.

49 — Judgment in *Lindqvist*, cited above, paragraph 56. In that case, the Court held that loading personal data onto an internet page does not constitute a 'transfer to a third country' within the meaning of Article 25 of Directive 95/46 merely because it makes them accessible to people in a third country. In reaching that conclusion, the Court took account both of the technical nature of the operations in question and of the purpose and structure of Chapter IV of that directive, in which Article 25 appears.

50 — Even if the data are received by a specific element of the internal administrative structure of the third country in question.

performed upon personal data, ... such as collection, recording, ... consultation, use, disclosure by transmission, dissemination or otherwise making available ...'. [51]

94. Whatever its specific nature, which is largely based, as we have seen, on the concept of adequacy, the regime relating to the transfer of personal data to third countries must comply with the rules relating to the scope of Directive 95/46 of which it forms part. [52]

95. Consequently, in order to be covered by Article 25 of Directive 95/46, a transfer to a third country must concern personal data the processing of which, whether currently carried out in the Community or merely envisaged in the third country, falls within the scope of that directive. Only on that condition may a decision on adequacy properly constitute a measure implementing Directive 95/46.

96. In that regard, I would point out that the directive does not apply, *ratione materiae,* to all personal-data processing which could come within one of the categories of referred to in Article 2(b). The first indent of Article 3(2) of Directive 95/46 provides that the directive does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and *in any case to processing operations concerning public security,* defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and *the activities of the State in areas of criminal law*'. [53]

97. I am of the view that the consultation, the use by CBP and the making available to

51 — It is worth pointing out that the concepts of 'processing' and 'transfer' of personal data overlap to some extent. Thus, disclosure by the transmission, dissemination or making available of such data seems to me to be capable of constituting both the processing and the transfer of data within the meaning of the directive. In the present case, the concepts of transfer and processing overlap to the extent that the regime established is concerned, in particular, with making PNR data available to CBP. That finding is explained, in my opinion, by the very wide definition of processing, which covers an extensive sample group of operations. In the final analysis, in such an instance the transfer of data to a third country is regarded as a specific form of processing. See to that effect the Commission's proposal for a framework decision: Article 15, relating to '[t]ransfer to competent authorities in third countries or to international bodies', forms part of Chapter III, headed 'Specific forms of processing'.

52 — I would observe, by way of example, that Commission Decision 2000/519/EC of 26 July 2000 pursuant to Directive 95/46 on the adequate protection of personal data provided in Hungary (OJ 2000 L 215, p. 4) provides, in Article 1, that, '[f]or the purposes of Article 25(2) of Directive 95/46/EC, *for all the activities falling within the scope of that directive,* Hungary is considered as providing an adequate level of protection of personal data transferred from the Community' (emphasis added).

53 — Emphasis added. In its judgment in *Lindqvist,* the Court observed that '[t]he activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals' (paragraph 43).

the latter of air passenger data from air carriers' reservation systems located within the territory of the Member States constitute personal-data processing operations which concern public security and relate to State activities in areas of criminal law. Those processing operations are, therefore, excluded from the material scope of Directive 95/46.

98. The wording used in the decision on adequacy demonstrates the purpose of the processing operations to which air passengers' personal data are subjected. After stating that the requirements for personal data contained in the PNR of air passengers to be transferred to CBP are based on a statute enacted by the United States in November 2001 and on implementing regulations adopted by CBP under that statute, [54] the Commission makes it clear that one of the purposes of the United States legislation is 'the enhancement of security'. [55] It is also stated that '[t]he Community is fully committed to supporting the United States in the fight against terrorism within the limits imposed by Community law'. [56]

99. Moreover, the 15th recital in the preamble to the decision on adequacy states that 'PNR data will be used strictly for purposes of preventing and combating: terrorism and related crimes; other serious crimes, including organised crime, that are transnational in nature; and flight from warrants or custody for those crimes'.

100. Directive 95/46, and in particular Article 25(6), cannot, in my view, constitute an appropriate basis for the adoption by the Commission of an implementing measure such as a decision on the adequate protection of personal data that are subjected to processing operations expressly excluded from its scope. To authorise transfers of such data on the basis of that directive would amount to extending its scope in an indirect manner.

101. It should be borne in mind that Directive 95/46, which was adopted on the basis of Article 100a of the EC Treaty, lays down protection principles which must apply to processing of personal data by any person whose activities are governed by Community law, but that, precisely because of the legal basis chosen the directive is not capable of governing State activities, such as those which concern public security or

54 — Sixth recital in the preamble.

55 — Seventh recital in the preamble.

56 — Eighth recital in the preamble.

pursue law-enforcement purposes, which do not fall within the scope of Community law. [57]

102. It is true that the processing constituted by the collection and recording of air passenger data by airlines has, in general, a commercial purpose in so far as it is connected with the operation of the flight by the air carrier. Consequently, it is fair to assume that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely the sale of an aeroplane ticket which provides entitlement to a supply of services. However, the data processing which is taken into account in the decision on adequacy is quite different in nature, since it covers a stage subsequent to the initial collection of the data. It covers, as we have seen, the consultation, the use by CBP and the making available to the latter of air passenger data from air carriers' reservation systems located within the territory of the Member States.

103. In actual fact, the decision on adequacy does not concern a data processing operation necessary for a supply of services, but one regarded as necessary to safeguard public security and for law-enforcement purposes. That is certainly the purpose of the transfer and the processing of PNR data. Consequently, the fact that personal data have been collected in the course of a business activity cannot, in my view, justify the application of Directive 95/46, and in particular Article 25 of that directive, in an area excluded from its scope.

104. Those arguments are sufficient, in my view, for it to be held that, as the Parliament believes, the Commission did not have, under Article 25 of Directive 95/46, the power to adopt a decision on the adequate protection of personal data transferred *in the course* and *for the purpose* of a processing operation expressly excluded from the scope of that directive. [58]

57 — See, to that effect, the article by Y. Poullet and M.V. Peres Asinan, 'Données des voyageurs aériens: le débat Europe — États-Unis', JTDE, 2004, No 113, p. 274. According to those authors, 'whatever solution is found to legitimise these cross-border flows of a very particular type must ensure the validity of the transfer of data to foreign public authorities carried out with a view to combating terrorism ..., an activity which is known to go beyond the scope of a first-pillar directive'. They add that '[t]his corresponds, at European level, to a third-pillar matter, which calls into question the Commission's competence to act in that connection ...'. See also O. De Schlutter, 'La Convention européenne des droits de l'homme à l'épreuve de la lutte contre le terrorisme' in *Lutte contre le terrorisme et droits fondamentaux*; E. Bribosia and A. Weyembergh (ed.), Collection droit et justice, Bruylant, Brussels, 2002, p. 112, note No 43: after citing the first indent of Article 3(2) of Directive 95/46, the author remarks that '[t]his restriction on the scope of the directive can be explained by the limited nature of the competence of the European Community, which does not have general legislative competence in the area of human rights, but may act in that area in particular where, and to the extent that, as is the case with [the aforementioned directive], it is a question of facilitating the establishment of an internal market involving inter alia the removal of obstacles to the free movement of goods and freedom to provide services'.

58 — The PNR data undergo processing within the Community, which consists in making them available to CBP. They are also destined for processing after their transfer, by reason of their use by CBP.

105. The decision on adequacy therefore infringes the primary act, namely Directive 95/46, and in particular Article 25 which is not the appropriate basis for it. I am of the opinion that the decision must, for that reason, be annulled.

106. In addition, in so far as I take the view that the decision on adequacy falls outside the scope of Directive 95/46, it does not seem to me to be relevant to examine that decision, as the Parliament requests in its second plea, in the light of the fundamental principles contained in the directive.[59] I therefore do not think that there is any need to consider the second plea.

107. The third and fourth pleas in the action under examination, which I shall consider only in the alternative, cannot, in my opinion, be analysed separately, since investigation of whether any fundamental rights are infringed by the decision on adequacy necessarily includes an assessment of that measure's compliance with the principle of proportionality in the light of the objective pursued by it. I therefore propose that the Court should examine the third and fourth pleas together.

B — *The pleas alleging infringement of fundamental rights and breach of the principle of proportionality*

108. The Parliament maintains that the decision on adequacy fails to respect the right, as guaranteed in Article 8 of the ECHR, to the protection of personal data. More specifically, having regard to the conditions laid down by that article, the Parliament submits that the decision constitutes interference in private life which cannot be regarded as in accordance with the law, since it is a measure which is not accessible and foreseeable. In addition, the Parliament submits that that measure is not proportionate to the objective pursued by it, in view inter alia of the excessive number of PNR data elements required and of the excessive length of time for which the data are kept.

109. In the action which it has brought in Case C-317/04, seeking annulment of the Council decision, the Parliament also puts forward these two pleas and, in support of them, arguments which overlap to a large extent. I take the view that these pleas put forward in the two cases brought before the

59 — This does not mean that a decision on adequacy adopted in a context similar to that of this case would have to be regarded, in the European Union legal order, as exempt from compliance with the fundamental safeguards concerning the protection of personal data, as set out inter alia in Convention No 108. I am, however, of the opinion that, from this point of view, Directive 95/46 is not the appropriate reference standard since, as we have seen, the aim of the decision on adequacy goes beyond the scope of the parent legislation which that directive constitutes. Consequently, in the absence of any secondary legislation applying in the case of processing of personal data for law-enforcement and public-security purposes, it is not possible to undertake an abstract judicial review of those safeguards. In such a case, judicial protection is not lacking, however. Review of compliance with the fundamental safeguards concerning the protection of personal data is, as we shall see, closely linked to examination of the conditions laid down by Article 8(2) of the ECHR.

Court must form the subject of a single examination which, it seems to me, it is apposite to carry out in the course of my discussion of Case C-317/04.

110. It is apparent from the arguments advanced by the parties in their pleadings that it is impossible to understand separately, from the point of view of the right to respect for private life, the components of the regime relating to the processing of PNR data by CBP,[60] consisting of the agreement as approved by the Council decision, the decision on adequacy and the undertakings of CBP which are annexed to that Commission decision. Indeed, the parties refer on many occasions to all of those measures in order to support their case.

111. The interdependence of those three components of the PNR regime is expressly indicated by the very wording of the agreement. Both the undertakings of CBP and the decision on adequacy are referred to in the preamble to the agreement. Secondly, paragraph 1 of the agreement states that CBP may access the PNR data 'strictly in accordance with the decision [on adequacy] and for so long as the decision is applicable ...'. Likewise, although, under paragraph 2 of the agreement, the air carriers referred to therein are to process PNR data 'as required by CBP pursuant to US law', this again is to be 'strictly in accordance with the decision [on adequacy] and for so long as the decision is applicable'. Finally, paragraph 3 of the agreement provides that 'CBP takes note of the decision [on adequacy] and states that it is implementing the undertakings annexed thereto'.

112. It follows that both the right of access to PNR data conferred on CBP and the obligation of the air carriers referred to in that agreement to process those data are subject to strict and genuine application of the decision on adequacy.

113. Both the interdependence of the three components of the PNR regime and the fact that the pleas alleging infringement of fundamental rights and breach of the principle of proportionality are put forward by the Parliament in both the cases which the Court has been asked to decide lead me to construe those pleas as seeking a finding by the Court that the PNR regime is incompatible, in its three components, with the right to respect for private life guaranteed in Article 8 of the ECHR. In my opinion, it would be artificial to examine the decision on adequacy without taking account of the agreement, which imposes certain obligations on airlines and, conversely, to examine the agreement without taking into consideration the other applicable provisions to which that instrument expressly refers.

60 — 'The PNR regime'.

114. In view of the fact that the system comprises a number of inseparable elements, the analysis should therefore not be artificially split up.

115. Seen in that light, the interference in private life is constituted by the body of provisions formed by the agreement as approved by the Council decision, the decision on adequacy and CBP's undertakings. In order to examine whether that interference is in accordance with the law, pursues a legitimate objective and is necessary in a democratic society, it is also necessary to take into account the whole of the 'three-speed' mechanism thus set up, as the Parliament does in its two applications. In order to obtain an overview of the PNR regime, I shall carry out that examination in the context of the action seeking annulment of the Council decision.

VI — The action seeking annulment of the Council decision (Case C-317/04)

A — *The plea alleging that Article 95 EC was incorrectly chosen as the legal basis for the Council decision*

1. Arguments of the parties

116. The European Parliament claims that Article 95 EC is not the appropriate legal basis for the Council decision. The aim and content of the latter are not the establishment and functioning of the internal market. The objective of the Council decision is, rather, to legalise the processing of personal data imposed by US law on airlines established in Community territory. The decision does not specify to what extent that legalisation of transfers of data to a third country contributes to the establishment or functioning of the internal market.

117. Nor, in the Parliament's view, does the content of the Council decision justify the use of Article 95 EC as a legal basis. That decision consists in establishing the right of CBP to access airlines' reservation systems within Community territory, with a view to the operation of flights between the United States and Member States in accordance with US law, in order to prevent and combat terrorism. However, the achievement of those objectives does not fall within the scope of Article 95 EC.

118. Finally, the Parliament adds that Article 95 EC is not capable of justifying Community competence to conclude the agreement concerned since the agreement relates to data processing operations which are carried out for purposes of public security and

therefore excluded from the scope of Directive 95/46, which is based on that article of the Treaty.

119. The Council, on the other hand, contends that its decision was correctly based on Article 95 EC. In its submission, that article can be the basis for measures aimed at ensuring that the conditions of competition are not distorted in the internal market. It maintains that the agreement is intended to eliminate any distortion of competition between the Member States' airlines and between the latter and the airlines of third countries which could arise, as a result of the US requirements, for reasons relating to the protection of individual rights and freedoms. The conditions of competition between Member States' airlines operating international passenger flights to and from the United States could have been distorted if only some of them had granted the US authorities access to their databases.

120. Similarly, the Council points out, firstly, that airlines failing to comply with the US requirements could have had fines imposed on them by the US authorities, suffered delays to their flights and lost passengers to other airlines which had entered into arrangements with the United States. Secondly, some Member States could have penalised airlines transferring the personal data in question, whereas other Member States would not necessarily have acted in the same way.

121. In those circumstances, and in the absence of any common rules on access by the US authorities to PNR data, the Council submits that the conditions of competition were liable to be distorted and that serious harm would have been inflicted upon the unity of the internal market. It was therefore, in its view, necessary to establish harmonised conditions governing access by the US authorities to those data, while at the same time safeguarding the Community requirements concerning respect for fundamental rights. In issue are the imposition of harmonised obligations on all the airlines concerned and the external aspect of the establishment and functioning of the internal market.

122. Finally, the Council observes that the agreement was concluded after the decision on adequacy, which was adopted under Article 25(6) of Directive 95/46. In its view, it was therefore natural and proper to found the decision concluding the agreement on the same legal basis as that directive, namely Article 95 EC.

123. In its statement in intervention, the Commission observes that the preamble to the agreement demonstrates that, for the United States, the vital objective is the fight against terrorism, whereas for the Community the main aim is to uphold the principal elements of its legislation on the protection of personal data.

124. It observes that, while criticising the choice of Article 95 EC as the legal basis for the Council decision, the Parliament does not put forward any credible alternatives. In the Commission's view, that article is the 'natural' legal basis for the Council decision in so far as the external dimension of the protection of personal data must be based on the article of the Treaty which is the basis for the internal measure, namely Directive 95/46, especially since that external aspect is expressly provided for in Articles 25 and 26 of the directive. Moreover, in view of the close link and the interdependence between the agreement, the decision on adequacy and the undertakings of CBP, Article 95 EC proves to be the appropriate legal basis. In any event, the Commission contends that the Council had the power to conclude the agreement on the basis of that article since Directive 95/46 would have been affected, within the meaning of the *ERTA* case-law, [61] if the Member States had, separately or jointly, concluded such an agreement outside the Community framework.

61 — Case 22/70 *Commission* v *Council* [1971] ECR 263, '*ERTA*'.

125. Finally, the Commission contends that the initial processing of the data in question by the airlines is carried out for a commercial purpose. Consequently, the use made of them by the US authorities does not exempt them from the effect of Directive 95/46.

2. Assessment

126. By its first plea, the Parliament asks the Court to decide whether Article 95 EC is the appropriate legal basis for the Council decision on the conclusion by the Community of an international agreement such as the one at issue in this case. In order to answer that question, it is necessary to apply the Court's settled case-law according to which the choice of the legal basis for a Community measure must be based on objective factors which are amenable to judicial review, including in particular the aim and content of the measure. [62] Indeed, 'in the context of the organisation of the powers of the Community the choice of the legal basis for a measure may not depend simply

62 — See, inter alia, Case C-300/89 *Commission* v *Council* [1991] ECR I-2867, '*Titanium dioxide*', paragraph 10; Case C-84/94 *United Kingdom* v *Council* [1996] ECR I-5755, paragraph 25; Joined Cases C-164/97 and C-165/97 *Parliament* v *Council* [1999] ECR I-1139, paragraph 12; Case C-269/97 *Commission* v *Council* [2000] ECR I-2257, paragraph 43; Case C-336/00 *Huber* [2002] ECR I-7699, paragraph 30; Case C-338/01 *Commission* v *Council* [2004] ECR I-4829, paragraph 54; and Case C-176/03 *Commission* v *Council* [2005] ECR I-7879, paragraph 45.

on an institution's conviction as to the objective pursued ...'. [63]

127. I would point out that the Court has held that '[t]he choice of the appropriate legal basis has constitutional significance. Since the Community has conferred powers only, it must tie [the international agreement concerned] to a Treaty provision which empowers it to approve such a measure'. According to the Court, '[t]o proceed on an incorrect legal basis is therefore liable to invalidate the act concluding the agreement and so vitiate the Community's consent to be bound by the agreement it has signed'. [64]

128. In accordance with the method of analysis used by the Court, I shall therefore examine whether the aim and content of the agreement authorised the Council to adopt on the basis of Article 95 EC a decision the object of which, as stated in Article 1 thereof, was to approve that agreement on behalf of the Community.

129. As regards the aim of the agreement, it is expressly indicated in the first recital in its preamble that it pursues two objectives, namely, on the one hand, preventing and combating terrorism and related crimes and other serious crimes that are transnational in nature, including organised crime, [65] and, on the other hand, respecting fundamental rights and freedoms, notably privacy.

130. Pursuit of the objective of combating terrorism and other serious crimes is attested to by the reference, in the second recital in the preamble to the agreement, to the US statutes and regulations adopted in the aftermath of the terrorist attacks of 11 September 2001, requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to provide CBP with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems.

131. The objective of respecting fundamental rights, notably privacy, is manifested through the reference to Directive 95/46. It is thus a question of affording the individuals transported the guarantee that their personal data will be protected.

63 — Case 45/86 *Commission* v *Council* [1987] ECR 1493, paragraph 11.

64 — Opinion 2/00 given under Article 300(6) EC [2001] ECR I-9713, paragraph 5.

65 — From now on, I shall use the expression 'combating terrorism and other serious crimes' to refer to that objective.

132. That guarantee is sought both in the undertakings entered into by CBP on 11 May 2004, which, according to the fourth recital in the preamble to the agreement, would be published in the *Federal Register*, and in the decision on adequacy, which is mentioned in the fifth recital.

133. Those two objectives must, in accordance with the first recital in the preamble to the agreement, be pursued simultaneously. The agreement, concluded between the Community and the United States, therefore attempts to reconcile those two objectives, that is to say, it is based on the idea that the fight against terrorism and other serious crimes must be conducted with respect for fundamental rights, notably the right to privacy, and more specifically the right to the protection of personal data.

134. The content of the agreement confirms that analysis. Paragraph 1 provides that CBP may electronically access the PNR data from air carriers' reservation control systems located within the territory of the Member States 'strictly in accordance with' the decision on adequacy 'and for so long as the decision is applicable'. I infer from this that access to air passengers' PNR data as a means of combating terrorism and other serious crimes is authorised by the agreement only in so far as it is recognised that those data are afforded an adequate level of protection in the United States. The content of that provision of the agreement thus reflects the simultaneous pursuit of the objectives of combating terrorism and other serious crimes and protecting personal data.

135. The same finding must be made upon examination of paragraph 2 of the agreement which obliges air carriers operating passenger flights in foreign air transportation to or from the United States to process PNR data contained in their automated reservation systems 'as required by CBP pursuant to US law and strictly in accordance with the decision [on adequacy] and for so long as the decision is applicable'. Here too, the obligation now imposed on air carriers with a view to combating terrorism and other serious crimes is closely linked to adequate protection of airline passengers' personal data.

136. Other provisions of the agreement are intended to reflect the objectives of combat-

ing terrorism and other serious crimes and protecting airline passengers' personal data.

137. Thus, specifically with regard to the objective of protecting those passengers' personal data, paragraph 3 of the agreement indicates that 'CBP takes note of the decision [on adequacy] and states that it is implementing the undertakings annexed thereto'.

138. In addition, paragraph 6 of the agreement contemplates the possibility that the European Union may, in turn, implement an airline passenger identification system requiring air carriers to provide the competent authorities with access to PNR data for persons whose travel itinerary includes a flight to or from the European Union. In the event that the European Union implements such a measure, the agreement provides that the Department of Homeland Security 'shall, in so far as practicable and strictly on the basis of reciprocity, actively promote the cooperation of airlines within its jurisdiction'. That is a provision which, once again, reflects the objective of combating terrorism and other serious crimes.

139. I would point out, in reply to certain arguments put forward by the Commission, that it therefore seems to me to be difficult to claim that the objective of combating terrorism and other serious crimes is being pursued unilaterally and solely by the United States, the Community's sole aim being to protect airline passengers' personal data.[66] In fact, I am of the opinion that, from the point of view of each Contracting Party, the aim and content of the agreement are reconciliation of the objective of combating terrorism and other serious crimes with that of protecting airline passengers' personal data. The agreement thereby establishes cooperation between the Contracting Parties which is specifically intended to achieve that twofold objective in simultaneous fashion.

140. In light of the aim and content of the agreement as described above, I am of the view that Article 95 EC is not an appropriate legal basis for the Council decision.

141. Article 95(1) EC concerns the adoption by the Council of measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

66 — Moreover, terrorism is an international phenomenon which makes light of the erection of spatial barriers.

142. The competence conferred on the Community by that article of the Treaty is horizontal in character, that is to say, it is not restricted to a particular field. The extent of Community competence is therefore defined 'by reference to a criterion of a *functional* nature, extending laterally to all measures designed to ensure attainment of the "internal market"'. [67]

143. In addition, according to the Court's case-law, the measures referred to in Article 95(1) EC are intended to improve the conditions for the establishment and functioning of the internal market and must genuinely have that object, actually contributing to the elimination of obstacles to the free movement of goods or to the freedom to provide services, or to the removal of distortions of competition. [68] It also follows from that case-law that, although recourse to Article 95 EC as a legal basis is possible if the aim is to prevent the emergence of future obstacles to trade resulting from divergent development of national laws, the emergence of such obstacles must be likely and the measure in question must be designed to prevent them. [69]

144. As I have already stated, the Council contends that its decision was validly adopted on the basis of Article 95 EC since, by removing any distortion of competition between the Member States' airlines and between the latter and the airlines of third countries, the agreement with the United States helped to prevent serious harm from being inflicted upon the unity of the internal market.

145. Indeed, it should be noted that the second recital in the preamble to the Council decision refers to 'the urgent need to remedy the situation of uncertainty in which airlines and passengers found themselves, as well as to protect the financial interests of those concerned'. That phrase could be construed as alluding to the sanctions which might be imposed by the competent US authorities on airlines which refuse to provide access to their passengers' PNR data, sanctions which could have financial consequences for those airlines. It is conceivable that, in such a situation, those sanctions with adverse

67 — See point 10 of the Opinion of Advocate General Tesauro in *Titanium dioxide*, cited above.

68 — Case C-376/98 *Germany* v *Parliament and Council* [2000] ECR I-8419, paragraphs 83, 84 and 95, and Case C-491/01 *British American Tobacco (Investments) and Imperial Tobacco* [2002] ECR I-11453, paragraph 60.

69 — See, to that effect, Case C-350/92 *Spain* v *Council* [1995] ECR I-1985, paragraph 35; *Germany* v *Parliament and Council*, cited above, paragraph 86; Case C-377/98 *Netherlands* v *Parliament and Council* [2001] ECR I-7079, paragraph 15; *British American Tobacco (Investments) and Imperial Tobacco*, cited above, paragraph 61; and Case C-434/02 *Arnold André* [2004] ECR I-11825, paragraph 31.

financial implications for certain airlines could give rise to distortions of competition between all the airlines established within the territory of the Member States.

146. Moreover, I can also conceive that different attitudes on the part of the Member States, some prohibiting, on pain of sanctions, the airlines established within their territory from authorising the transfer of their passengers' PNR data, but others not acting in that way, could have an effect, even indirectly, on the functioning of the internal market as a result of the possible distortions of competition which could arise between airlines.

147. However, the fact remains that such an objective of preventing distortions of competition, to the extent that it is actually pursued by the Council, is *incidental in character* to the two main objectives of combating terrorism and other serious crimes and protecting passengers' personal data, which, as we have seen, are expressly mentioned and actually implemented in the provisions of the agreement.

148. The objective of preventing distortions of competition, whether it be, as the Council asserts, between the airlines of the Member States or between them and the airlines of third countries, is not expressly mentioned anywhere in the agreement. It is implicit, and therefore necessarily incidental to the other two.

149. I would point out that, as the Court has already held, 'the mere fact that an act may affect the establishment or functioning of the internal market is not sufficient to justify using that provision as the basis for the act'.[70]

150. Above all, it is apparent from the Court's settled case-law that when examination of a Community measure reveals that it pursues more than one purpose or that it has more than one component, and if one is identifiable as the main or predominant purpose or component, whereas the other is merely incidental, the measure must be founded on a single legal basis, namely that required by the main or predominant purpose or component.[71] Only in exceptional cases, if it is established that the measure simultaneously pursues several objectives which are indissociably linked, without one being secondary and indirect

70 — See, inter alia, Case C-426/93 *Germany* v *Council* [1995] ECR I-3723, paragraph 33.

71 — See, inter alia, Case C-155/91 *Commission* v *Council* [1993] ECR I-939, paragraphs 19 and 21; Case C-42/97 *Parliament* v *Council* [1999] ECR I-869, paragraphs 39 and 40; Case C-36/98 *Spain* v *Council* [2001] ECR I-779, paragraph 59; and Case C-281/01 *Commission* v *Council* [2002] ECR I-12049, paragraph 34.

in relation to the others, will such a measure have to be founded on the relevant different legal bases.[72] That is not, in my view, the case here.

151. Furthermore, even if the three objectives were to be regarded as being pursued indissociably by the agreement, the fact would nevertheless remain that the Council's choice to found its decision on Article 95 EC as its sole legal basis would, according to that case-law, have to be considered inappropriate.

152. In actual fact, it is apparent from the second recital in the preamble to the Council decision, read as a whole, that the main purpose of the reference to an 'urgent need' in that recital is to explain that a time-limit was laid down for the Parliament to deliver its opinion, in accordance with the first subparagraph of Article 300(3) EC which provides, as part of the procedure for the conclusion of agreements, that '[t]he European Parliament shall deliver its opinion within a time-limit which the Council may lay down according to the urgency of the matter'. That article also provides that '[i]n the absence of an opinion within that time-limit, the Council may act'. That was the case in the procedure carried out for the purpose of adopting the Council decision.

153. To put it another way, although 'the urgent need to remedy the situation of uncertainty in which airlines and passengers found themselves, as well as to protect the financial interests of those concerned' may indeed have been taken into consideration in the process for setting up a PNR data regime, it seems to me that such consideration played more of a role in the procedure followed than it did in the definition of the aim and content of the agreement.

154. As regards the argument of the Council and the Commission that a measure relating to the external dimension of the protection of personal data should be founded on a legal basis identical to that of the internal measure, namely Directive 95/46, the Court has already held that the fact that a particular Treaty provision has been chosen as the legal basis for the adoption of internal measures is not sufficient to establish that the same basis must be used when approving an international agreement with similar subject-matter.[73] Moreover, I have shown that the agreement does not have either as its principal aim or its content the improvement of the conditions for the functioning of the internal market, whereas Directive 95/46, adopted on the basis of Article 95 EC, 'is intended to ensure the free movement of personal data between Member States through the harmonisation of national pro-

72 — See, inter alia, *Titanium dioxide*, cited above, paragraphs 13 and 17; Case C-42/97 *Parliament* v *Council*, cited above, paragraphs 38 and 43; *Huber*, cited above, paragraph 31; and Case C-281/01 *Commission* v *Council*, cited above, paragraph 35.

73 — Case C-281/01 *Commission* v *Council*, cited above, paragraph 46.

visions on the protection of individuals with regard to the processing of such data'. [74]

155. In view of the foregoing considerations, I am of the opinion that examination of the aim and content of the agreement demonstrates that Article 95 EC is not the appropriate legal basis for the Council decision.

156. I therefore propose that the Court should hold that the first plea put forward by the Parliament is well founded. It follows that the Council decision must be annulled on account of the incorrect choice of its legal basis.

157. It would, admittedly, be interesting at this stage to consider what the appropriate legal basis of such a decision would be. However, the Court is not required to address that tricky question in this case. I shall therefore confine myself to making a few remarks on this problem and, more generally, on the nature of the PNR regime as negotiated with the United States.

158. First, contrary to a proposition advanced by the Council, the fact that the PNR regime was not set up under the provisions of the EU Treaty is not, in my view, capable of establishing the validity in law of the approach adopted by the Council and the Commission.

159. Secondly, and more generally, I am of the opinion that a measure which provides for consultation and use of personal data by an entity that has the task of ensuring a State's internal security, and the making available of those data to such an entity, may be treated as an act of cooperation between public authorities. [75]

160. Moreover, requiring a legal person to undertake such processing of data and obliging it to transfer those data do not seem to me to be fundamentally different from a direct exchange of data between

74 — Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, paragraph 39. In view of the difference of subject-matter and purpose between the agreement and Directive 95/46, I am also of the view that it is unlikely that, as the Commission contends, that directive would have been affected, in the sense contemplated in the *ERTA* judgment, if the Member States had either separately or jointly concluded an agreement of the type in question outside the Community framework.

75 — I note that the 'third pillar' dimension of the transfer of airlines' personal data to the United States is sometimes mentioned. Thus, the Article 29 Data Protection Working Party was able, in an opinion adopted on 24 October 2002 (Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States), to express the view that, '[i]n essence, data transfers made to the public authorities of third countries for reasons of public order in [those countries] should be understood in the context of cooperation mechanisms set up under the third pillar (judicial and police cooperation) ... It appears to be important for the cooperation mechanisms laid down in the third pillar not to be circumvented via the first pillar.' See Internet site: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2002_en.htm.

public authorities.[76] It is the compulsory disclosure of data for security and law-enforcement purposes that is important, and not the specific form it takes in any given situation. The present case actually concerns a new set of issues, relating to the use of commercial data for law enforcement purposes.[77]

161. Finally, it should be noted that the Court of First Instance has held that 'the fight against international terrorism ... cannot be made to refer to one of the objects which Articles 2 EC and 3 EC expressly entrust to the Community'.[78]

162. In view of the fact that my analysis of the first plea leads me to propose that the Court should annul the Council decision on account of the incorrect choice of legal basis for it, I shall examine only in the alternative the other pleas put forward by the Parliament in support of the present action.

76 — As regards the direct exchange of information between public authorities, I would mention the Council Decision of 27 March 2000 authorising the Director of Europol to enter into negotiations on agreements with third States and non-EU-related bodies (OJ 2000 C 106, p. 1). On that basis, an agreement between Europol and the United States of America on the exchange of personal data was signed on 20 December 2002.

77 — These issues are at the heart of the current inter-institutional debate concerning the retention of data by providers of telephony and electronic communication services. The opposing views expressed during this debate, between those who advocate dealing with these issues under the first pillar and those who, by contrast, believe that the matter falls under the third pillar, testify to both the novelty and the complexity of the issues surrounding the use of commercial data for law-enforcement purposes. See, in this context, the Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (draft submitted on 28 April 2004 on the initiative of the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom), and the concurrent Commission Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58, submitted on 21 September 2005 (document COM(2005) 438 final).

78 — See, as regards the imposition of economic and financial sanctions, such as the freezing of funds, in respect of individuals and entities suspected of contributing to the funding of terrorism, the judgments of the Court of First Instance in Case T-306/01 *Yusuf and Al Barakaat International Foundation* v *Council and Commission* [2005] ECR II-3533, paragraph 152, and Case T-315/01 *Kadi* v *Council and Commission* [2005] ECR II-3649, paragraph 116. In the particular context of those cases, the Court did however take account of 'the bridge explicitly established at the time of the Maastricht revision between Community actions imposing economic sanctions under Articles 60 EC and 301 EC and the objectives of the Treaty on European Union in the sphere of external relations' (paragraph 159 of the judgment in Case T-306/01 and paragraph 123 of the judgment in Case T-315/01). More generally, it also held that 'the fight against international terrorism and its funding is unarguably one of the Union's objectives under the CFSP, as they are defined in Article 11 EU ...' (paragraph 167 of the judgment in Case T-306/01 and paragraph 131 of the judgment in Case T-315/01). I would add that Article 2 EU provides that '[t]he Union shall set itself the following objectives: ... to maintain and develop the Union as an area of freedom, security and justice, in which the free movement of persons is assured in conjunction with *appropriate measures with respect to* external border controls, asylum, immigration and *the prevention and combating of crime* ...' (emphasis added). Moreover, under the second paragraph of Article 29 EU, the objective of the Union of providing citizens with a high level of safety within an area of freedom, security and justice 'shall be achieved by *preventing and combating crime, organised or otherwise, in particular terrorism* ...' (emphasis added). On the external dimension of the European criminal-law area, see G. de Kerchove and A. Weyembergh, *Sécurité et justice: enjeu de la politique extérieure de l'Union européenne*, Éditions de l'Université de Bruxelles, 2003.

B — *The plea alleging that the second subparagraph of Article 300(3) EC was infringed because Directive 95/46 was amended*

1. Arguments of the parties

163. By this second plea, the Parliament contends that the agreement between the Community and the United States could be approved on behalf of the Community only by complying with the procedure laid down in the second subparagraph of Article 300(3) EC. That article provides that '... agreements entailing amendment of an act adopted under the procedure referred to in Article 251 shall be concluded after the assent of the European Parliament has been obtained'. In the view of that institution, the agreement in question entails amendment of Directive 95/46, which was adopted under the procedure referred to in Article 251 EC.

164. In the Parliament's opinion, the undertakings which the US authorities agreed to implement under the agreement fall short of the conditions for processing data laid down by Directive 95/46. The agreement therefore has the effect of derogating from certain fundamental principles in that directive and of rendering processing operations which are not authorised by it lawful. In that sense, the agreement amends Directive 95/46. In particular, the Parliament identifies the following amendments.

165. First, the agreement is aimed at preventing and combating terrorism and other serious crimes, whereas the first indent of Article 3(2) of Directive 95/46 excludes from the scope of the directive the transfer of data to public authorities of a third State for reasons connected with the public security of that State. The Parliament notes that Member States have laid down specific provisions for that purpose in the Europol Convention and it can therefore be considered that there is complementarity in that field between the two instruments, which are founded on different legal bases.

166. Second, allowing the competent US authorities to access directly personal data within the territory of the Community (the 'pull' system) also amounts to an amendment of Directive 95/46. Articles 25 and 26 of the latter contain no provision permitting a third country to be entitled to access such data directly.

167. Third, the agreement, by referring to the undertakings, authorises CBP, at its discretion and on a case-by-case basis, to transmit PNR data to government law-

enforcement or counter-terrorism authorities other than those of the United States. That discretion conferred on the US authorities infringes Directive 95/46, and in particular Article 25(1), under which 'the transfer to a third country of personal data ... may take place only if ... the third country in question ensures an adequate level of protection'. The Parliament submits that the system of protection drawn up in the directive would be reduced to nothing if the third country covered by a positive decision on adequacy were then free to transfer the personal data to other countries which had not been the subject of any assessment by the Commission.

168. Fourth, the agreement contains an amendment to Directive 95/46 in so far as CBP, even if it decided not to use 'sensitive' personal data, is legally authorised to collect them, which itself constitutes processing within the meaning of Article 2(b) of that directive.

169. Fifth, the Parliament submits that the agreement amends Directive 95/46 since the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question, as provided for in Article 22 of the directive, is not sufficiently ensured. In particular, a data subject whose PNR data are transferred does not have any right to a judicial remedy, for example, in the case of incorrect data concerning him, of use of sensitive data or of transmission of the data to another authority.

170. Sixth and last, the Parliament stresses the excessive length of time for which PNR data transferred to CBP are kept, which constitutes an amendment of Directive 95/46, and more specifically Article 6(1)(e), which provides that data must be kept 'for no longer than is necessary for the purposes for which the data were collected or for which they are further processed'.

171. The EDPS supports the claims of the Parliament in that, in his view, the agreement affects Directive 95/46. He is of the opinion that the agreement could be concluded only under the democratic supervision of the Parliament since it affects the level of harmonisation of national laws as provided for by that directive, and even respect for fundamental rights. In his submission, the impairment of the level of protection of personal data which is provided for by that directive results inter alia from the fact that, under both the 'pull' system and the 'push' system, air carriers are obliged to act in breach of the directive, in particular Article 6(1)(b) and (c). Inasmuch as that impairment of the level of data protection entails

amendment of Directive 95/46, the EDPS submits that the procedural safeguards provided for in the second subparagraph of Article 300(3) EC have not been complied with. He is also of the view that the 'substantive safeguards' have likewise not been complied with, in particular because the undertakings of CBP are non-binding.

172. By contrast, the Council, supported by the Commission, submits that the agreement does not entail amendment of Directive 95/46. In support of that view, it cites paragraph 8 of the agreement, according to which the latter 'is not intended to derogate from or amend legislation of the Parties'. It also contends that the directive gives the Commission a wide discretion in assessing whether the protection ensured by a third country is adequate. In the Council's view, the question whether the Commission exceeded the limits of its discretion is rather the subject-matter of the action for annulment of the decision on adequacy in Case C-318/04.

173. The Council also observes that, in its view, the reasons (security, fight against terrorism or other reasons) which led CBP to require the transmission of PNR data do not constitute, from the point of view of the Community, either the aim or the content of the agreement. Furthermore, within the context of the internal market, Directive 95/46 allows personal data to be used for legitimate purposes such as protection of the security of a State.

174. In any event, in the Council's view, even if the Community did not have competence to conclude the agreement, it does not therefore follow that the Parliament should have given its assent, on the alleged ground that the agreement amends Directive 95/46. The Parliament's assent may on no account have the effect of widening the Community's sphere of competence.

175. As regards the provision made for CBP to access PNR data directly (the 'pull' system currently applicable, pending the setting up of a 'push' system), while the Council acknowledges that Directive 95/46 does not expressly mention any such possibility, it does not prohibit it either. From the Community's point of view, it is the conditions governing access to the data that matter.

176. The Commission adds to those arguments the point that, regardless of the purpose for which the personal data are used by CBP, the fact remains that the data are and remain, for air carriers in the Community, commercial data falling within the scope of Directive 95/46 which must, therefore, be protected and processed in accordance with that directive.

2. Assessment

177. When international agreements are concluded by the Community, consultation of the Parliament appears to be the generally applicable procedure outside the sphere of the common commercial policy. Under the first subparagraph of Article 300(3) EC, such consultation of the Parliament must take place including in cases where the agreement covers a field for which the codecision procedure under Article 251 EC is required for the adoption of internal rules.

178. By way of derogation from that generally applicable procedure, the second subparagraph of Article 300(3) EC requires the assent of the Parliament in four circumstances, including, so far as is of interest in this case, where the agreement entails 'amendment of an act adopted under the procedure referred to in Article 251'. It is a question of guaranteeing the Parliament's ability, as co-legislator, to exercise control over any amendment by an international agreement of an act adopted by it.

179. Directive 95/46 was adopted under the codecision procedure. The Parliament therefore submits that, since the agreement entails amendment of that directive, the Council decision approving the agreement on behalf of the Community required its assent in order to be adopted in compliance with the rules laid down by the Treaty.

180. In assessing the merits of this plea, I would point out first and foremost that little importance attaches, in my view, to the fact that the agreement states, in paragraph 8, that it 'is not intended to derogate from or amend legislation of the Parties'. What is important for the purpose of giving effect to the second subparagraph of Article 300(3) EC is to ascertain whether the international agreement *entails* amendment of the internal Community act, that is to say, whether it has *the effect* of amending that act, irrespective of the fact that that is not its aim.

181. That said, it seems that the Court has not yet ruled on the meaning to be given to the relatively vague expression 'amendment of an act adopted under the procedure referred to in Article 251'.[79] Some authors have raised the question here whether the term 'amendment' means an 'amendment conflicting with the provisions' of the internal act or whether 'any amendment, even one consistent with the provisions' of the internal act is sufficient to require compliance with the assent procedure.[80]

79 — The Court has, however, already ruled on another situation in which the Parliament's assent is required, namely that concerning 'agreements having important budgetary implications for the Community' (Case C-189/97 *Parliament* v *Council* [1999] ECR I-4741).

80 — See C. Schmitter, 'Article 228', in V. Constantinesco, R. Kovar and D. Simon, *Traité sur l'Union européenne, commentaire article par article*, Economica, 1995, p. 725, especially paragraph 43.

182. The expression used in the second subparagraph of Article 300(3) EC also invites the question whether, in order for assent to be required, the field of application of the proposed agreement must overlap, at least in part, with that of the internal act adopted or whether the mere fact that an internal act has been adopted on the legal basis used for the conclusion of that agreement is sufficient. [81]

183. Generally speaking, I am of the opinion that, in order for there to be 'amendment' by an international agreement of an internal Community act adopted under the codecision procedure, one of the conditions is that the field of application of the agreement overlap with that of the internal act. In that case, the internal act may be amended by the international agreement, either if the agreement contains a provision which conflicts with one of those of the internal act or because the agreement adds to the content of the internal act, even when there is no direct conflict.

184. In the present case, I take the view that the agreement was not capable of amending the content of Directive 95/46.

185. My view is based, first, on the fact that, as is apparent from my analysis of the first plea, the agreement's primary objective is to combat terrorism and other serious crimes while at the same time guaranteeing protection for airline passengers' personal data. By contrast, Directive 95/46 seeks to ensure the free flow of personal data between Member States through the harmonisation of national provisions protecting individuals with regard to the processing of such data. The two acts therefore have two clearly separate objectives, even though they both concern the field of protection of personal data. [82]

186. Secondly, and consistent with the finding that their objectives are distinct, it is clear that the agreement and Directive 95/46 have different fields of application. Whereas the agreement applies to the processing of personal data in the course of activities relating to the internal security of the United States and, at the same time and more specifically, to activities relating to the fight against terrorism and other serious crimes, the first indent of Article 3(2) of the directive expressly excludes from its field of application the processing of personal data 'in the course of an activity which falls outside the scope of Community law, such as those

81 — See, to that effect, C. Schmitter, op. cit.

82 — I would point out that the approach adopted in the Treaty establishing a Constitution for Europe is broader and more favourable to consent by the Parliament: Article III-325 of that Treaty, which concerns the procedure for concluding international agreements, provides, in paragraph 6(a)(v), that the Council is to adopt the decision concluding the agreement after obtaining the consent of the Parliament inter alia in the case of 'agreements covering *fields* to which either the ordinary legislative procedure applies, or the special legislative procedure where consent by the European Parliament is required' (emphasis added).

provided for by Titles V and VI of the [EU] Treaty ... and *in any case ... processing operations concerning public security*, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and *the activities of the State in areas of criminal law*'. [83]

187. In view of the fact that, in this case, the two acts have different objectives and fields of application, I do not see how the content of one could amend that of the other. Indeed, the agreement concerns personal-data processing which the Community legislature has clearly excluded from coverage by the system of protection established by Directive 95/46. That approach adopted by the Community legislature is, moreover, consistent with the choice of legal basis for that directive, namely Article 95 EC.

188. That analysis cannot, it seems to me, be rebutted by the Commission's argument according to which, irrespective of the purpose for which the personal data are used by CBP, the fact remains that they are and continue to be, for air carriers in the Community, commercial data falling within the scope of Directive 95/46 which must be protected and processed in accordance with the latter.

189. Although it is true that the processing consisting of the collection and recording of air passenger data by the airlines has, in general, a commercial purpose in so far as it is directly linked to the operation of the flight by the air carrier, the processing of the data which is governed by the agreement is quite different in nature, since it both covers a stage subsequent to the collection of the data and pursues a security-related objective.

190. Having regard to all those considerations, I am of the opinion that the second plea put forward by the Parliament is unfounded and must therefore be dismissed.

191. For the same reasons as those mentioned when considering Case C-318/04, [84] I shall now examine together the third and fourth pleas put forward by the Parliament, namely infringement of the right to protection of personal data and breach of the principle of proportionality.

83 — Emphasis added.

84 — Point 107 of this Opinion.

192. I also reiterate the point that, in view of the interdependence of the agreement as approved by the Council decision, the decision on adequacy and the undertakings of CBP annexed to that Commission decision, it is necessary, in my view, to examine the PNR regime as a whole in the light of those pleas. [85]

C — *The pleas alleging infringement of the right to protection of personal data and breach of the principle of proportionality*

1. Arguments of the parties

193. The Parliament contends that the PNR regime infringes the right, as recognised in particular by Article 8 of the ECHR, to protection of personal data.

194. In its submission, by providing that CBP may electronically access PNR data from air carriers' reservation systems located within the territory of the Member States, and by stipulating that those carriers, where they operate passenger flights in foreign air transportation to or from the United States, are to process the PNR data in question as required by CBP pursuant to US law, the agreement relates to a form of processing of personal data which constitutes an interference in private life for the purposes of Article 8 of the ECHR. Similarly, the decision on adequacy does not comply with that article.

195. The Parliament points out that, in order not to infringe Article 8 of the ECHR, such interference must be in accordance with the law, pursue a legitimate objective and be necessary in a democratic society in order to achieve that objective. It submits that the agreement and the decision on adequacy do not fulfil those conditions.

196. As regards, first, the condition that the interference must be in accordance with the law, the Parliament states that both the agreement and the decision on adequacy fail to satisfy the requirements of accessibility and foreseeability of the law which are laid down by the case-law of the European Court of Human Rights. First, as to the requirement of accessibility of the law, the Parliament submits that, by referring in a general and imprecise manner to the applicable US law, the agreement and the decision on adequacy do not themselves contain the rights and obligations which fall upon passengers and European airlines. The requirement of legal certainty means that a Community act which creates legal obliga-

85 — See point 109 et seq. of this Opinion.

tions must enable those concerned to know precisely the extent of the obligations which it imposes on them. [86] In addition, contrary to the requirement of accessibility of the law, the applicable United States legislation is not available in all the official languages of the Community. The Parliament also notes the incorrect reference and date of adoption for the decision on adequacy in the preamble to the agreement. Second, the requirement of foreseeability of the law is not met since the agreement and the decision on adequacy do not set out sufficiently precisely the rights and obligations of airlines and citizens established in the Community. Moreover, passengers receive only general information, which is contrary to the obligation to provide information, as laid down in Articles 10 and 11 of Directive 95/46 and Article 8(a) of Convention No 108. Finally, the agreement and the undertakings of CBP include a number of instances of a lack of precision incompatible with Article 8 of the ECHR.

197. Secondly, the Parliament accepts that the condition under Article 8(2) of the ECHR requiring interference with the right to respect for private life to pursue a legitimate aim is satisfied. It draws attention in that regard to the support which it has expressed on many occasions to the Council in the fight against terrorism.

198. As regards, thirdly, the condition that the interference must be 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, the Parliament submits that this condition is not satisfied for the following reasons:

— it is apparent from paragraph 3 of the undertakings of CBP that the processing of the data is not solely for the purpose of combating terrorism, but also for the purpose of preventing and combating other serious crimes, including organised crime, and flight from warrants or custody for the crimes referred to above. In so far as processing of the data goes beyond the sole purpose of combating terrorism, it is not necessary for the achievement of the legitimate aim pursued;

— the agreement provides for the transfer of an excessive number of data elements (34), thereby failing to comply with the principle of proportionality. From the point of view of observance of an adequate level of protection of personal data, 19 of those 34 data elements appear acceptable. The Parliament submits that there is a 'considerable discrepancy' between the amount of data prescribed by comparable legal instruments applicable at European Union

86 — The Parliament cites in this connection Case C-108/01 *Consorzio del Prosciutto di Parma and Salumificio S. Rita* [2003] ECR I-5121, paragraph 89.

level and that required under the agreement.[87] Moreover, some of the PNR data elements required could include sensitive data;

— the data are stored for too long by the US authorities having regard to the aim pursued. The effect of the undertakings of CBP is that, following online access to the data for authorised CBP personnel, which is available for seven days, all the data are kept for a period of three years and six months, and then data which have been manually accessed during that period are transferred by CBP to a deleted record file as raw data, where they remain for a period of eight years before they are destroyed. Comparison with the information systems established, for example, under the Convention implementing the Schengen Agreement, the Europol Convention and the Eurojust Decision, which provide for a period of storage of one to three years, demonstrates the excessive length of the period mentioned in the undertakings;

— the agreement makes no provision for judicial review with regard to the processing of the data by the US authorities. Moreover, in so far as the agreement and the undertakings do not create any rights for persons whose personal data are processed, the Parliament does not see how those persons can rely on such rights before the US courts;

— the agreement permits the transfer of data to other public authorities; it thus goes beyond what is necessary to combat terrorism.

199. The EDPS takes the view that the processing of six categories of data manifestly constitutes an infringement of the right to private life.[88] Its infringement also results from the possibility of drawing up personal profiles from those data. The EDPS supports the Parliament's arguments seeking to demonstrate that the interference is not justified under Article 8(2) of the ECHR. He further submits that the level of protection afforded by CBP is not adequate within the meaning of Article 25 of Directive 95/46,

87 — The Parliament cites inter alia in this connection the Europol Convention which provides, in Article 8(2), for processing of five pieces of data, and Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ 2004 L 261, p. 24). That directive, which has as its legal basis Articles 62(2)(a) EC and 63(3)(b) EC, provides, in Article 3, for an obligation for air carriers to transmit, at the request of the authorities responsible for carrying out checks on persons at external borders, a total of nine pieces of personal data.

88 — Those are, in his view, data elements Nos 11 'Frequent flyer information (limited to miles flown and address(es))', 19 'General remarks', 26 'OSI information [Other Service Information]', 27 'SSI/SSR [Special Service Request] information', 30 'Number of travellers on PNR' and 33 'Any collected APIS (Advanced Passenger Information System) information'.

in particular because Article 8 of the ECHR is not complied with.

200. By contrast, the Council and the Commission submit that the PNR regime complies with the conditions laid down in Article 8(2) of the ECHR, as interpreted by the European Court of Human Rights.

201. As regards, firstly, the condition that the interference must be in accordance with the law, the Council submits that it is not necessary, in order to satisfy the requirement of accessibility of the law, that the text of the agreement itself contain all the provisions which may affect the persons concerned. It is not unlawful to include in the agreement a reference to the decision on adequacy and to the undertakings of CBP which are set out in the Annex to that decision, since all those acts were published in the *Official Journal of the European Union*. In addition, the latter does not have the task of publishing legislation of third countries. The Council states with regard to the incorrect reference to the decision on adequacy which appears in the preamble to the agreement that it will make the necessary arrangements for a corrigendum to be published in the Official Journal, but submits that those errors of a technical nature do not affect the accessibility of the acts in question for the purposes of the case-law of the European Court of Human Rights. As for the condition requiring foreseeability of the law, the Council submits that the fact that the undertakings of CBP and the applicable US legislation and constitutional requirements were not reproduced in full in the agreement itself does not constitute an infringement of that requirement. Furthermore, the undertakings of CBP, which are formulated with sufficient precision, enable the persons concerned to regulate their conduct accordingly.

202. As regards, secondly, the condition that the interference must pursue a legitimate aim, the Council points out that combating serious crimes other than terrorism falls within several of the categories of legitimate interests mentioned in Article 8(2) of the ECHR (notably public safety and the prevention of disorder and crime). Consequently, the agreement and the undertakings of CBP also pursue a legitimate aim in so far as they relate to those other serious crimes.

203. The Council submits, thirdly, that the interference is proportionate to the aim pursued. More specifically, it contends that the categories of PNR data required by CBP are useful for the purpose of preventing terrorist acts and organised crime, as well as for throwing light on the investigations which follow attacks and other crimes, in that they facilitate the task of identifying those associated with terrorist groups or organised crime. As for the number of PNR data elements to be transferred, the comparison with the information systems established within the European Union is irrelevant since, apart from the fact that those systems have a different aim and content from those of the PNR regime, the need to profile potential terrorists requires access to a greater number of pieces of data. As

regards the three PNR data elements which could, according to the Parliament, include sensitive data, [89] the Council observes that CBP's access to those three elements is strictly limited under paragraph 5 of the undertakings given by CBP. [90] Moreover, according to paragraphs 9, 10 and 11 of the undertakings, any use of sensitive data by CBP is in any case precluded. [91] As for the length of time during which PNR data are kept, the Council submits that, in view of the fact that investigations following attacks and other crimes sometimes take several years, a normal period of storage fixed at three years and six months, except in specific cases where that period may be longer, constitutes a balanced solution. Furthermore, there is no basis for the view that a system of independent review is lacking. Finally, the transfer of data to other public authorities is subject to sufficient safeguards: in particular, CBP may transfer data to other public authorities only on a case-by-case basis, and only for the purpose of preventing or combating terrorism or other serious crimes.

204. In the Commission's view, there is no doubt that the body of provisions formed by the agreement, the decision on adequacy and the undertakings of CBP allows some interference in private life to take place, of varying seriousness depending on the data transferred. That interference is in accordance with the law, that is to say, the aforementioned body of provisions pursues a legitimate aim, namely resolving a conflict between US security legislation and the Community rules on the protection of personal data, and is necessary in a democratic society in order to achieve that aim.

205. The United Kingdom submits that, in assessing a possible infringement of the right to protection of personal data, the Council decision, the agreement, the decision on adequacy and the undertakings of CBP must be considered together, since they are closely related legal instruments. It also submits that it is the accessibility and foreseeability of the applicable Community legislation that must be considered, not those of the laws which apply within the territory of the United States. If the agreement, the decision on adequacy and the undertakings of CBP are considered together, Community law contains, in the opinion of the United Kingdom,

89 — Those are elements Nos 19, 26 and 27 (see previous footnote).

90 — Paragraph 5 of the undertakings provides:
'With respect to the data elements identified as "OSI" and "SSI/SSR" (commonly referred to as general remarks and open fields), CBP's automated system will search those fields for any of the other data elements identified [in the list of PNR data elements required]. CBP personnel will not be authorised to manually review the full OSI and SSI/SSR fields unless the individual that is the subject of a PNR has been identified by CBP as high-risk in relation to any of the purposes identified in paragraph 3 hereof.'

91 — Paragraph 9 of the undertakings provides:
'CBP will not use "sensitive" data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual) from the PNR, as described below.'
Paragraph 10 of the undertakings provides:
'CBP will implement, with the least possible delay, an automated system which filters and deletes certain "sensitive" PNR codes and terms which CBP has identified in consultation with the ... Commission.'
Paragraph 11 of the undertakings is worded as follows:
'Until such automated filters can be implemented CBP represents that it does not and will not use "sensitive" PNR data and will undertake to delete "sensitive" data from any discretionary disclosure of PNR under paragraphs 28 to 34.'
Paragraphs 28 to 34 of the undertakings relate to the transfer of PNR data to other government authorities.

a clear and thorough statement of the legal position of all affected parties. Moreover, the United Kingdom does not accept that the undertakings of CBP are unilateral in character and may be varied or retracted by the US authorities with impunity.

206. On the necessity of the interference, the United Kingdom first points out that the struggle against other serious crimes is clearly announced as an objective of the agreement and represents a goal of public policy which is quite as legitimate as the fight against terrorism. The United Kingdom then submits that the range of data elements which may be transferred, the length of time for which those elements may be held, and the possibility of their transfer to other authorities correspond to and are proportionate to those objectives, particularly given the numerous safeguards that are included in the undertakings and the decision on adequacy to reduce the risk posed to passengers' privacy. Finally, it states that, in its view, the proportionality criterion must be applied, under the case-law of both the Court of Justice and the European Court of Human Rights, in the light of the nature and importance of the objectives at issue.

2. Assessment

207. By these pleas, the Parliament contends that both the Council decision and the decision on adequacy infringe the right as guaranteed in particular in Article 8 of the ECHR to protection of personal data.

208. It is settled case-law that fundamental rights form an integral part of the general principles of law whose observance the Court ensures. [92] For that purpose the Court draws inspiration from the constitutional traditions common to the Member States and from the guidelines supplied by international treaties for the protection of human rights on which the Member States have collaborated or of which they are signatories. It views the ECHR as having 'special significance' in that respect. [93] Measures which are incompatible with respect for the human rights thus recognised and guaranteed cannot find acceptance in the Community. [94] These principles have been repeated in Article 6(2) EU.

209. In the course of laying down that case-law, the Court has found it necessary to

92 — See, inter alia, Case 29/69 *Stauder* [1969] ECR 419, paragraph 7; Case 11/70 *Internationale Handelsgesellschaft* [1970] ECR 1125, paragraph 4; and Case 4/73 *Nold* v *Commission* [1974] ECR 491, paragraph 13.

93 — See, inter alia, Case C-260/89 *ERT* [1991] ECR I-2925, paragraph 41; Case C-299/95 *Kremzow* [1997] ECR I-2629, paragraph 14; and Case C-274/99 P *Connolly* v *Commission* [2001] ECR I-1611, paragraph 37.

94 — Case 5/88 *Wachauf* [1989] ECR 2609, paragraph 19.

incorporate the right to respect for private life into Community law.[95] The right to protection of personal data constitutes one of the aspects of the right to respect for private life and is therefore protected by Article 8 of the ECHR, including in the Community legal order, through the prism of the general principles of law.

210. I shall examine whether the PNR regime constitutes an infringement of the right to respect for private life by following the analytical pattern which stems from the wording of Article 8 of the ECHR. Thus, after establishing whether that regime constitutes interference in the private life of airline passengers, I shall determine whether that interference is duly justified.

(a) Existence of interference in private life

211. The existence of interference in private life brought about by the body of provisions formed by the Council decision approving the agreement, the decision on adequacy and the undertakings of CBP is hardly in doubt, in my opinion. It seems clear to me that the consultation, the use by CBP and the making available to the latter of airline passengers' data from air carriers' reservation systems located within the territory of the Member States constitute interference by public authorities in the private life of those passengers.

212. Also, the interference in the private life of airline passengers appears to me to be established even though certain PNR data elements, considered in isolation, could be regarded as not individually infringing the privacy of the passengers concerned. It seems to me necessary to view as a whole the list of PNR data elements required by CBP, since cross-checking those data may enable personal profiles to be built up.

213. Interference in private life infringes the right to respect for private life unless it is duly justified.

(b) Justification for the interference in private life

214. In order to be permissible, interference in private life must be found to satisfy three

95 — Case 136/79 *National Panasonic* v *Commission* [1980] ECR 2033, paragraphs 18 and 19. That right includes inter alia the right to the protection of medical confidentiality (see Case C-62/90 *Commission* v *Germany* [1992] ECR I-2575 and Case C-404/92 P *X* v *Commission* [1994] ECR I-4737). As for the right to the protection of personal data, I refer again to the judgments in *Österreichischer Rundfunk and Others* and *Lindqvist*, cited above.

conditions. it must be in accordance with the law, pursue a legitimate aim and be necessary in a democratic society.

(i) Is the interference in accordance with the law?

215. According to the consistent case-law of the European Court of Human Rights, this condition requires that the impugned measure should have a basis in law, but also refers to the quality of the law in question. [96] Examination of the quality of the law means that the latter should be accessible to citizens, precise and foreseeable in its consequences. This requires that it define with sufficient precision the conditions and detailed rules for the limitation of the right guaranteed, in order to enable the citizen to regulate his conduct and have adequate protection against arbitrary interference. [97]

216. The Parliament submits that the measure which provides for the interference is neither accessible nor foreseeable in its consequences. I do not share that opinion.

217. On the contrary, I take the view that, by reading the Council decision and the agreement annexed to it, together with the decision on adequacy, which contains in its annex the undertakings of CBP, the persons concerned, namely airlines and airline passengers, can be informed with sufficient precision for the purpose of regulating their conduct.

218. I would draw attention, in this regard, to the relatively extensive nature of the 48 paragraphs of the undertakings of CBP, which provide details of the applicable legal framework. Moreover, the decision on adequacy sets out in its preamble the references for the relevant US statute and the implementing regulations adopted by CBP under that statute. [98] It would therefore seem to me to be unreasonable to require the relevant provisions of US statute and secondary legislation to be published in full in the *Official Journal of the European Union*. Apart from the fact that the latter, as the Council points out, does not have the task of publishing laws of third countries, I consider the undertakings of CBP, which were published in the Official Journal, to contain the essential information on the procedure for the use of data by CBP and on the safeguards to which that procedure is subject.

96 — See Eur. Court H.R., *Kruslin v. France*, judgment of 24 April 1990, Series A no. 176-A, § 27.

97 — See Eur. Court H.R., *Olsson v. Sweden*, judgment of 24 March 1988, Series A no. 130, § 61 and 62. The restrictions must be laid down in legal provisions worded with sufficient precision to enable the citizen to regulate his conduct by taking, if need be, appropriate advice (Eur. Court H.R., *Sunday Times v. the United Kingdom*, judgment of 26 April 1979, Series A no. 30, § 49).

98 — See the sixth recital in the preamble to the decision on adequacy and footnotes 2 and 3 to that decision.

219. In accordance with the requirement of legal certainty, the airlines covered by the PNR regime are informed of the obligations imposed on them under the agreement, and airline passengers are informed of their rights, in particular as regards access to and rectification of data. [99]

220. Admittedly, in view of the interdependence of the component parts of the PNR regime, it is to be regretted that the preamble to the agreement contains errors in respect of the reference and date of the decision on adequacy. Those errors add to the complexity of the steps to be taken by a Community citizen wishing to obtain information about the content of the regime negotiated with the United States. However, they do not, in my view, make such research excessively difficult, since the decision on adequacy was published in the Official Journal and research tools, in particular those which are computer-based, make it easy to find. Furthermore, the Council undertook to arrange for a corrigendum to be published in the Official Journal, which it indeed did. [100]

221. In the light of those considerations, I take the view that the interference in the private life of the airline passengers concerned must be regarded as 'in accordance with the law' within the meaning of Article 8(2) of the ECHR.

99 — See paragraphs 36 to 42 of the undertakings.

100 — See the Procès-verbal of rectification to the agreement which, it should be recalled, was published in OJ 2005 L 255, p. 168.

(ii) Does the interference pursue a legitimate aim?

222. In the light of the various objectives mentioned in Article 8(2) of the ECHR, I am of the view that the interference in private life which is at issue in this case pursues a legitimate aim. That is, in particular, the case with regard to combating terrorism.

223. Like the Council, I believe that combating serious crimes other than terrorism [101] also falls within several of the categories of legitimate interests mentioned in Article 8(2) of the ECHR, such as national security, public safety or the prevention of disorder or crime. Consequently, I am of the view that the PNR regime also pursues a legitimate aim in so far as it relates to those other serious crimes.

224. It is now necessary to determine whether the interference is proportionate by enquiring whether it is necessary in a democratic society for the purpose of preventing and combating terrorism and other serious crimes.

101 — I would reiterate that the preamble to the agreement talks about preventing and combating terrorism 'and related crimes and other serious crimes that are transnational in nature, including organised crime'. Moreover, paragraph 3 of the undertakings provides that 'PNR data are used by CBP strictly for purposes of preventing and combating: 1. terrorism and related crimes; 2. other serious crimes, including organised crime, that are transnational in nature; and 3. flight from warrants or custody for the crimes described above'. See also the 15th recital in the preamble to the decision on adequacy, in which the same wording is used.

(iii) Is the interference necessary in a democratic society for the purpose of achieving such an aim?

225. Before investigating specifically whether that condition of proportionality is satisfied, I shall make a few preliminary observations regarding the scope of the review to be carried out by the Court.

226. According to the European Court of Human Rights, the adjective 'necessary' within the meaning of Article 8(2) of the ECHR implies that 'a pressing social need' should be involved and that the measure adopted should be 'proportionate to the legitimate aim pursued'. [102] In addition, 'the national 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'. [103]

227. In reviewing the margin of appreciation enjoyed by States, the European Court of Human Rights traditionally determines whether the reasons invoked in support of the interference are relevant and sufficient, then whether the interference is proportionate to the legitimate aim pursued, and then satisfies itself that a balance has been struck between the general interest and the interests of the individual. [104] Drawing conclusions from that case-law, it has thus been possible to observe that '[t]he principle of proportionality, which reflects a requirement that there be an appropriate relationship between a legitimate objective and the means used to achieve it, is therefore at the heart of the review of the national margin of appreciation'. [105]

228. The review of proportionality by the European Court of Human Rights varies according to parameters such as the nature of the right and activities at issue, the aim of the interference and the possible presence of a common denominator in the States' legal systems.

229. As regards the nature of the right and activities at issue, where the right is one which intimately affects the individual's private sphere, such as the right to confidentiality of health-related personal data, [106] the European Court of Human

102 — See, inter alia, Eur. Court H.R., *Gillow v. the United Kingdom*, judgment of 24 November 1986, Series A no. 109, § 55.

103 — Eur. Court H.R., *Leander v. Sweden*, judgment of 26 March 1987, Series A no. 116, § 59.

104 — See, for example, Eur. Court H.R., *Klass and Others v. Germany*, judgment of 6 September 1978, Series A no. 28, § 59, concerning the secret surveillance of citizens' correspondence and telecommunications for the purpose of combating terrorism. In that judgment, the Court of Human Rights held that 'some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention'.

105 — F. Sudre, *Droit européen et international des droits de l'homme*, 7th edition, revised, PUF, 2005, p. 219. The author also observes that,'[d]epending on how strictly it formulates the condition of proportionality — strict, proper or reasonable proportion — the European Court of Human Rights varies the intensity of its review and, therefore, causes the extent of the State's margin of appreciation to vary ...'.

106 — See Eur. Court HR, *Z. v. Finland*, judgment of 25 February 1997, *Reports of Judgments and Decisions* 1997-I.

Rights seems to take the view that the State's margin of appreciation is more limited and that its own judicial review must be stricter. [107]

230. However, where the aim of the interference is to maintain national security [108] or to combat terrorism, [109] the European Court of Human Rights tends to allow States a wide margin of appreciation.

231. In the light of the nature and importance of the objective of combating terrorism, which seems predominant in the PNR regime, and having regard to the politically sensitive context in which the negotiations between the Community and the United States were conducted, I am of the opinion that, in this case, the Court should hold that the Council and the Commission had a wide margin of appreciation in negotiating, with the US authorities, the content of the PNR regime. It follows that, in order to respect that wide margin of appreciation, the Court's review of the necessity of the interference should, in my view, be limited to determining whether there was any manifest error of assessment on the part of those two institutions. [110] By carrying out a restricted review of that kind, the Court would thus avoid the pitfall of substituting its own assessment for that of the Community political authorities as to the nature of the most appropriate and

107 — See, to that effect, F. Sudre, op. cit., p. 219. See also P. Wachsmann, 'Le droit au secret de la vie privée', in *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, S. Sudre (ed.), Bruylant, 2005, p. 141: with regard to the *Z. v. Finland*, judgment, cited above, the author notes that '[t]he review of the necessity of the interference is in this case exercised strictly, which is explained by the extreme sensitivity of the question of disclosure to third parties of a person's HIV-positive status.

108 — *Leander* judgment, cited above. Mr Leander had become a security guard at a naval museum in Sweden and had lost his job following a personnel control which gathered secret information about him, resulting in the conclusion that he could not work in a museum of which several warehouses were located in a restricted military zone. That case enabled the European Court of Human Rights to affirm clearly the principle that both the storing and the release of personal data, coupled with a refusal to allow an opportunity to refute the data, amount to an interference with the right to respect for private life. In examining the justification for such an interference, the European Court of Human Rights held that '[t]here can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power, firstly, to collect and store in registers not accessible to the public information on persons and, secondly, to use this information when assessing the suitability of candidates for employment in posts of importance for national security' (§ 59). In view of the safeguards contained in the Swedish personnel control system and of the wide margin of appreciation available to the State, the Court held that 'the respondent State was entitled to consider that in the present case the interests of national security prevailed over the individual interests of the applicant'. The interference to which Mr Leander was subjected was therefore not disproportionate in the light of the legitimate aim pursued (§ 67).

109 — See Eur. Court HR, *Murray v. the United Kingdom*, judgment of 28 October 1994, Series A, no. 300-A, § 47 and 90. In that case, the objective of combating terrorism provided justification for the recording by the armed forces of personal details concerning the first applicant. The Court of Human Rights pointed out that it is not for it 'to substitute for the assessment of the national authorities its own assessment of what might be the best policy in the field of investigation of terrorist crime' (§ 90). See also *Klass* judgment, cited above, § 49.

110 — According to D. Ritleng, as with the synonymous concept of 'patent disregard', there is manifest error of assessment 'when there is infringement of the statutory provisions so serious as to be obvious. However discretionary it may be, assessment of the facts cannot lead the Community institutions to decide just anything; by checking for manifest errors of assessment, the Court prevents any seriously mistaken use of the freedom of assessment'. See 'Le contrôle de le légalité des actes communautaires par la Cour de justice et le Tribunal de première instance des Communautés européennes', thesis defended on 24 January 1998 at the Université Robert Schuman de Strasbourg, p. 538, paragraph 628.

expedient means of combating terrorism and other serious crimes.

232. In order to determine the scope of the review which it intends to carry out, the Court could, in addition to the case-law of the European Court of Human Rights cited above, rely on its own case-law, in which it has held that, where a Community institution has a wide discretion in a particular sphere, '... the legality of a measure adopted in that sphere can be affected only if the measure is manifestly inappropriate having regard to the objective which the competent institution is seeking to pursue'. [111] The review of proportionality 'must be limited in that way in particular if ... the Council has to reconcile divergent interests and thus select options within the context of the policy choices which are its own responsibility'. [112] Limitation of the review may also be justified where, in a given sphere of action, a Community institution is obliged to carry out complex assessments. [113]

233. It seems to me that that case-law and the reasons underlying it must be applied in this case inasmuch as, when developing the PNR regime, the Council and the Commission were faced with policy choices between different interests which were difficult to reconcile and with complex assessments. [114] That would be in keeping with the principle of the separation of powers which requires the Court to respect the policy responsibilities which belong to the Community legislative and administrative organs and, consequently, to refrain from assuming their role in the policy choices which they find it necessary to make.

234. It must now be determined precisely whether, in adopting the various components of the PNR regime, the Council and the Commission manifestly exceeded the limits

111 — See, in regard to the common agricultural policy, Case C-331/88 *Fedesa and Others* [1990] ECR I-4023, paragraph 14. See also, in regard to anti-dumping duties, Case T-162/94 *NMB France and Others* v *Commission* [1996] ECR II-427, paragraph 70.

112 — See, in regard to the common agricultural policy, Case C-280/93 *Germany* v *Council* [1994] ECR I-4973, paragraph 91. That case-law extends to other fields, such as that of social policy, for example, where the Court was able to allow the Council 'a wide discretion in an area which ... involves the legislature in making social policy choices and requires it to carry out complex assessments' (*United Kingdom* v *Council*, cited above, paragraph 58). I would also point out that, with regard to public access to documents of the Community institutions and the scope of judicial review of the legality of a decision refusing access, the Court of First Instance has allowed the Council a wide discretion in the context of a decision refusing access founded on the protection of the public interest concerning international relations or on the protection of the public interest as regards public security: see, inter alia, in regard to the fight against terrorism, Joined Cases T-110/03, T-150/03 and T-405/03 *Sison* v *Council* [2005] ECR II-1429, paragraphs 46 and 71 to 82.

113 — In addition to the judgment in *United Kingdom* v *Council*, cited above, there are numerous examples of the Community judicature recognising the complex nature of assessments which the Community institutions are required to make; see, inter alia, in regard to freedom of establishment, Case C-233/94 *Germany* v *Parliament and Council* [1997] ECR I-2405, paragraph 55. For an example of recognition by the Court of First Instance of 'complex assessments of an economic and social nature', see Joined Cases T-244/93 and T-486/93 *TWD* v *Commission* [1995] ECR II-2265, paragraph 82.

114 — Thus, for example, the Commission had, in my view, a wide discretion in determining whether, in the particular context of the transfer of PNR data, the United States was able to ensure an adequate level of protection of those personal data.

to which their margin of appreciation was subject in the light of the right to respect for private life, and in particular of the right of airline passengers to the protection of their personal data, having regard to the legitimate aim pursued.

235. In the context of that examination, the content of the undertakings of CBP assumes particular importance inasmuch as they contain the detail of the safeguards to which the PNR regime is subject. In that regard, it would be a mistake to consider that those undertakings are in no way binding and contain commitments which can be freely amended or retracted by the US authorities.

236. The undertakings, which, it will be recalled, are annexed to the decision on adequacy, constitute one of the components of the PNR regime and, as such, failure to comply with them would lead to paralysis of the entire regime. I would point out that paragraphs 1 and 2 of the agreement make the air carriers' obligation to process PNR data conditional upon strict application of the decision on adequacy, that obligation applying only 'for so long as the decision is applicable'. Also, under paragraph 3 of the agreement, CBP 'states that it is implementing the undertakings annexed [to the decision on adequacy]'. Finally, Articles 3, 4 and 5 of the decision on adequacy lay down the measures to be taken in the event of breach of the standards of protection contained in the undertakings. Among those measures, it is provided that the competent authorities in Member States may suspend data flows to CBP and that, in the event of non-compliance with the basic principles necessary for an adequate level of protection of data subjects, the decision on adequacy may be suspended or repealed, which would have the effect of rendering paragraphs 1 and 2 of the agreement inapplicable.

237. For the purpose of obtaining a declaration by the Court that the interference in the private life of air passengers fails to comply with the principle of proportionality, the Parliament pleads, first, that the amount of data required by CBP from the airlines is excessive. In addition, it submits that some of the PNR data elements required may include sensitive data.

238. I am of the opinion that, in adopting the list of 34 personal-data elements as attached to the decision on adequacy, the Commission did not agree to a manifestly inappropriate measure for the purpose of achieving the objective of combating terrorism and other serious crimes. First, the importance of intelligence activity in counter-terrorism should be stressed, since obtaining sufficient information may enable a State's security services to prevent a possible terrorist attack. From that point of view, the need to profile potential terrorists

may require access to a large number of pieces of data. Second, the fact that other instruments relating to the exchange of information adopted within the European Union provide for disclosure of less data is not sufficient to demonstrate that the amount of data required in the specific counter-terrorism instrument constituted by the PNR regime is excessive. [115]

239. Furthermore, although it is correct, as the Parliament observes, that three of the data elements required may include sensitive data, [116] I would point out (i) that CBP's access to those three elements has been strictly limited under paragraph 5 of the undertakings, (ii) that, under paragraphs 9 to 11 of the undertakings, CBP is precluded from using sensitive data and (iii) that a system for filtering those data has been set up by CBP, in accordance with the undertaking given by it. [117]

240. Secondly, the Parliament submits that airline passengers' PNR data are kept for too long by the US authorities, having regard to the aim pursued.

241. The period of storage of those data is mentioned in paragraph 15 of the undertakings, which provides, in essence, for online access to PNR data by authorised CBP users for an initial period of seven days. After that period, access to the PNR data by a limited number of authorised officers is possible for a period of three years and six months. Finally, after that second period, data that have not been manually accessed during that time are destroyed, whereas data that have been manually accessed during the period of three years and six months are transferred by CBP to a deleted record file, where they remain for a period of eight years before they are destroyed. [118]

242. The effect of that provision is that the normal length of time for which data from PNR are kept is three years and six months, except for data which have been accessed manually during that period. I take the view that that period is not manifestly excessive bearing in mind in particular the fact that, as the Council points out, investigations which may be conducted following terrorist attacks or other serious crimes sometimes last

115 — According to the Commission, 'the PNR regime establishes a specific solution to a specific problem ... The Community and the United States negotiated a closed system of data protection specific to CBP, distinct from the US system and subject to the additional administrative safeguards of US review and European administrative and legal scrutiny' (point 13 of its observations on the statement in intervention of the EDPS in Case C-318/04).

116 — It will be recalled that the elements in question are Nos 19 'General remarks', 26 'OSI information [Other Service Information]', and 27 'SSI/SSR [Special Service Request] information'.

117 — See points 20 and 21 of the Commission's observations on the statement in intervention of the EDPS in Case C-318/04.

118 — It is also made clear, in footnote 7 to the undertakings, that when the PNR record is transferred to a deleted record file, it is stored as raw data, which is not a readily searchable form and, therefore, of no use for 'traditional' law-enforcement investigations.

several years. Consequently, although it is in principle desirable that personal data should be kept for a short period, it is necessary, in this case, to consider the period of storage of data from PNR in light of their usefulness, not only for purposes of preventing terrorism but, more widely, for law-enforcement purposes.

243. Having regard to those considerations, the data storage regime, as laid down in paragraph 15 of the undertakings, does not seem to me to constitute a patent infringement of the right to respect for private life.

244. Thirdly, the Parliament complains that the PNR regime does not provide for any judicial review of the processing of personal data by the US authorities.

245. I note that both Convention No 108 and Directive 95/46 provide for a judicial remedy in the event of infringement of the provisions of national law implementing the rules contained in those two legal instruments. [119]

119 — See Articles 8(d) and 10 of Convention No 108 and Article 22 of Directive 95/46.

246. In the light of Article 8(2) of the ECHR, I am of the opinion that the rules set out in paragraph 36 et seq. of the undertakings, which provide for a series of safeguards in terms of information, access to data and remedies for the airline passengers concerned, make it possible to avoid any abuses. That body of safeguards leads me to consider that, having regard to the wide discretion which the Council and the Commission must, in my view, be allowed in this case, the interference in the private life of airline passengers is proportionate to the legitimate aim pursued by the PNR regime.

247. More specifically, it should be noted that, in addition to the general information which CBP has undertaken to provide to airline passengers, [120] paragraph 37 of the undertakings provides that data subjects may, under the Freedom of Information Act, [121] receive a copy of PNR

120 — See paragraph 36 of the undertakings, which states: 'CBP will provide information to the travelling public regarding the PNR requirement and the issues associated with its use (i.e. general information regarding the authority under which the data are collected, the purpose for the collection, protection of the data, data-sharing, the identity of the responsible official, procedures available for redress and contact information for persons with questions or concerns, etc., for posting on CBP's website, in travel pamphlets, etc.)'.

121 — Title 5, section 552, of the United States Code, 'the FOIA'. So far as documents held by CBP are concerned, those provisions of the FOIA should be read in conjunction with Title 19, section 103.0 et seq., of the Code of Federal Regulations.

data regarding them contained in CBP databases. [122]

248. It is true that paragraph 38 of the undertakings provides that, '[i]n certain exceptional circumstances', CBP may deny or postpone disclosure of all or part of the PNR record, for example, if such disclosure 'could ... interfere with enforcement proceedings' or 'would disclose techniques and procedures for law enforcement investigations'. However, apart from the fact that that power which may be exercised by CBP is set within the statutory framework, it is important to note that, as the same paragraph of the undertakings states, under the FOIA 'any requester has the authority to *administratively and judicially challenge* CBP's decision to withhold information'. [123]

249. Furthermore, as regards requests for rectification of PNR data contained in the CBP database and complaints by individuals about CBP's handling of their PNR data, paragraph 40 of the undertakings states that such requests and complaints must be made to CBP's Assistant Commissioner. [124]

250. If a complaint cannot be resolved by CBP, it must be directed to the Chief Privacy Officer at the Department of Homeland Security. [125]

251. Moreover, paragraph 42 of the undertakings provides that 'the DHS Privacy Office will address on an expedited basis complaints referred to it by DPAs [data protection authorities] in the European Union (EU) Member States on behalf of an EU resident to the extent such resident has authorised the DPA to act on his or her behalf and believes that his or her data-protection complaint regarding PNR has not been satisfactorily dealt with by CBP (as set out in paragraphs 37 to 41 of these undertakings) or the DHS Privacy Office'.

122 — The FOIA establishes the presumption that any federal government document must be made available to anyone. However, the government body concerned may be freed from that presumption of disclosure if it proves that the information sought falls within a category of information which is exempted from the disclosure requirement. In that regard, it should be observed that, as provided in paragraph 37 of the undertakings, '[i]n the case of a first-party request, the fact that CBP otherwise considers PNR data to be confidential personal information of the data subject and confidential commercial information of the air carrier will not be used by CBP as a basis under FOIA for withholding PNR data from the data subject'.

123 — Emphasis added. Paragraph 38 of the undertakings refers in that regard to Title 5, section 552(a)(4)(B), of the United States Code and to Title 19, section 103.7 to 103.9, of the Code of Federal Regulations. It is apparent from those provisions that an application for judicial review of the rejection by CBP of a request for disclosure must be preceded by an administrative appeal before the FOIA Appeals Officer (Title 19, section 103.7, of the Code of Federal Regulations). If disclosure is still refused after that administrative appeal, the requester may then bring an application for judicial review before a federal district court, which has jurisdiction to order the disclosure of any information improperly withheld by a government body.

124 — The address of the Assistant Commissioner is given in the same paragraph.

125 — Her address is given in paragraph 41 of the undertakings.

252. Paragraph 42 also provides, first, that the DHS Privacy Office 'will report its conclusions and advise the DPA or DPAs concerned regarding actions taken, if any' and, secondly, that the Chief Privacy Officer 'will include in her report to Congress issues regarding the number, the substance and the resolution of complaints regarding the handling of personal data, such as PNR'. [126]

253. The Parliament correctly points out that the Chief Privacy Officer is not a judicial authority. However, I would observe that the Officer is an administrative authority with some degree of independence from the Department of Homeland Security and that her decisions are binding. [127]

254. Consequently, the provision thus made for airline passengers to lodge a complaint with the Chief Privacy Officer and the availability to them of a judicial remedy under the FOIA constitute significant safeguards with regard to their right to respect for their private life. Because of those safeguards, I take the view that the Council and the Commission did not exceed the limits placed on their margin of appreciation when adopting the PNR regime.

255. Finally, the Parliament submits that the PNR regime goes beyond what is necessary to combat terrorism and other serious crimes since it allows the transfer of airline passengers' data to other public authorities. In its view, CBP has a discretion to transfer data from PNR to other public authorities, including foreign government authorities, and this is incompatible with Article 8(2) of the ECHR.

256. I do not share that view. Here again, the safeguards surrounding the transfer of PNR data to other government authorities make it possible, in my view, to consider that the interference in the private life of airline passengers is proportionate for the purpose of achieving the aim pursued by the PNR regime.

257. Even though the undertakings allow CBP a significant degree of latitude, that

126 — See, to that effect, section 222(5) of the US Homeland Security Act of 2002 — Public Law, 107-296, of 25 November 2002, which provides that the Chief Privacy Officer must prepare a report to Congress on an annual basis on activities of the Department of Homeland Security that affect the protection of privacy, including complaints of privacy violations.

127 — See footnote 11 to the undertakings, which states that the Chief Privacy Officer 'is independent of any directorate within the Department of Homeland Security. She is statutorily obligated to ensure that personal information is used in a manner that complies with relevant laws ... The determinations of the Chief Privacy Officer shall be binding on the Department and may not be overturned on political grounds'. I would further point out that the requirement concerning provision for the submission of an appeal to an independent authority with power of decision is to be found inter alia in the judgment of the European Court of Human Rights of 7 July 1989 in *Gaskin v. the United Kingdom* (Series A, no. 160, § 49). I also note that Article 8(3) of the Charter of fundamental rights of the European Union provides that compliance with the rules laid down by Article 8 'shall be subject to control by an independent authority'.

discretion is set within a framework. Thus, under paragraph 29 of the undertakings, the transfer of PNR data to other government authorities 'with counter-terrorism or law-enforcement functions', 'including foreign government authorities', may be carried out only 'on a case-by-case basis' and only, in principle, 'for purposes of preventing and combating offences identified in paragraph 3 herein'. Under paragraph 30 of the undertakings, CBP must determine if the reason for disclosing the data to another authority fits within those purposes.

258. It is true that paragraphs 34 and 35 of the undertakings widen those purposes in so far as they have the effect of permitting respectively, first, the use or disclosure of PNR data to relevant government authorities 'where such disclosure is necessary for the protection of the vital interests of the data subject or of other persons, in particular as regards significant health risks' and, second, the use or disclosure of PNR data 'in any criminal judicial proceedings or as otherwise required by law'.

259. However, apart from the fact that those purposes are largely linked to the legitimate aim pursued by the PNR regime, I note that the undertakings contain a certain number of safeguards. Thus, for example, paragraph 31 provides that, '[f]or purposes of regulating the dissemination of PNR data which may be shared with other designated authorities, CBP is considered the "owner" of the data and such designated authorities are obligated by the express terms of disclosure' to comply with a number of requirements Those requirements imposed on the authorities receiving the data include the obligation to 'ensure the orderly disposal of PNR information that has been received, consistent with the designated authority's record retention procedures', and the obligation 'to obtain CBP's express authorisation for any further dissemination'.

260. In addition, paragraph 32 of the undertakings makes it clear that '[e]ach disclosure of PNR data by CBP will be conditioned upon the receiving agency's treatment of this data as confidential commercial information and law enforcement sensitive, confidential personal information of the data subject ... which should be treated as exempt from disclosure under the Freedom of Information Act ...'. Moreover, the same paragraph states that 'the recipient agency will be advised that further disclosure of such information is not permitted without the express prior approval of CBP', which will not authorise 'any further transfer of PNR data for purposes other than those identified in paragraphs 29, 34 or 35 herein'. Finally, paragraph 33 of the undertakings provides that '[p]ersons employed by such designated authorities who without appropriate authorisation disclose PNR data, may be liable for criminal sanctions'.

261. When all those safeguards are taken into account, the Council and the Commission cannot be considered to have exceeded the limits of the wide discretion which they must, in my view, be allowed for the purpose of combating terrorism and other serious crimes.

262. It follows that the pleas alleging infringement of the right to protection of personal data and breach of the principle of proportionality are unfounded and must therefore be dismissed.

D — *The plea alleging that the statement of reasons for the Council decision is inadequate*

263. The Parliament submits that the Council decision does not comply with the requirement to state reasons as laid down in Article 253 EC. In particular, it complains that the decision does not contain any reasons explaining whether, and to what extent, it concerns the functioning of the internal market.

264. By contrast, the Council, supported by the United Kingdom and the Commission, contends that the statement of reasons for its decision is in compliance with the requirements laid down by the Court.

265. I take the view that, even though brief, the statement of reasons for the Council decision is adequate.

266. As the Court has consistently held, the statement of reasons required by Article 253 EC 'must be appropriate to the measure at issue and must disclose in a clear and unequivocal fashion the reasoning followed by the institution which adopted the measure in question in such a way as to enable the persons concerned to ascertain the reasons for the measure and to enable the Court to carry out its review'. It is also clear from that case-law that 'it is not necessary for the reasoning to go into all the relevant facts and points of law, since the question whether the statement of reasons meets the requirements of [Article 253 EC] must be assessed with regard not only to its wording but also to its context and to all the legal rules governing the matter in question'. [128]

267. The measure at issue is a decision intended primarily to approve on behalf of the Community the agreement between it and the United States. The decision contains in that regard the necessary details of the procedure followed, namely adoption by the Council in accordance with the procedure laid down in the first subparagraph of Article 300(2) EC, and a statement that the Parliament did not give an opinion within the

128 — See, for example, Case C-56/93 *Belgium* v *Commission* [1996] ECR I-723, paragraph 86.

time-limit laid down by the Council pursuant to the first subparagraph of Article 300(3) EC. In addition, I note that the citations in the preamble to the Council decision mention Article 95 EC.

268. Moreover, in view of the particular nature of that decision, which it is difficult to isolate completely from the international agreement to which it relates, review of the adequacy of the statement of reasons must also, in my opinion, encompass the preamble to the agreement itself. On reading the Council decision in conjunction with the preamble to the agreement the Court can, as the examination of the previous pleas demonstrates, carry out its review, in particular as regards the appropriateness of the legal basis chosen.

269. Accordingly, I am of the opinion that the plea alleging that the Council decision does not include an adequate statement of reasons is unfounded and must therefore be dismissed.

E — *The plea alleging breach of the principle of cooperation in good faith laid down in Article 10 EC*

270. By this plea, the Parliament submits that, even though the first subparagraph of Article 300(3) EC allows the Council to set it, according to the urgency of the matter, a time-limit within which to deliver its opinion, and although the procedure for requesting an Opinion on an envisaged agreement from the Court, laid down in Article 300(6) EC, does not have suspensory effect, the Council acted, in the procedure for adopting the agreement, in breach of the duty to cooperate in good faith imposed on it by Article 10 EC.

271. The Council, supported by the Commission and the United Kingdom, contends that it did not infringe the principle of cooperation in good faith by concluding the agreement even though the Parliament had requested the Court for an Opinion pursuant to Article 300(6) EC.

272. Article 10 EC places the Member States under a duty to cooperate in good faith with the Community institutions, but does not expressly lay down the principle of cooperation in good faith between those institutions. However, the Court has held that 'inter-institutional dialogue, on which the consultation procedure in particular is based, is subject to the same mutual duties of sincere cooperation as those which govern relations between Member States and the Community institutions'. [129]

129 — Case 204/86 *Greece* v *Council* [1988] ECR 5323, paragraph 16, and Case C-65/93 *Parliament* v *Council* [1995] ECR I-643, paragraph 23.

273. It is apparent from the facts of this case that on 17 March 2004 the Commission submitted the proposal for a Council decision to the Parliament and that, by letter of 25 March 2004, the Council asked the Parliament to deliver its opinion on that proposal by 22 April 2004 at the latest. In its letter, the Council stressed that '[t]he fight against terrorism, which justifies the proposed measures, is a key priority of the European Union. Air carriers and passengers are at present in a situation of uncertainty which urgently needs to be remedied. In addition, it is essential to protect the financial interests of the parties concerned'.

274. On 21 April 2004, the Parliament decided, in accordance with Article 300(6) EC, to obtain the Opinion of the Court as to whether the agreement envisaged was compatible with the provisions of the Treaty.

275. On 28 April 2004, the Council, acting on the basis of the first subparagraph of Article 300(3) EC, sent a letter to the Parliament asking it to give its opinion on the conclusion of the agreement by 5 May 2004. To justify the urgency, the Council restated the reasons set out in its letter of 25 March 2004.

276. That request for urgency was rejected by the Parliament, whose President also called on the Council and the Commission not to continue with their intended course of action until the Court had delivered the Opinion requested on 21 April 2004. The Council nevertheless adopted the contested decision on 17 May 2004.

277. I do not think that the Council acted in breach of its duty to cooperate in good faith with the Parliament by adopting that decision to approve the agreement on behalf of the Community before the procedure concerning the Parliament's request pursuant to Article 300(6) EC for an Opinion from the Court was completed.

278. As the Parliament itself acknowledges, the initiation of such a procedure for requesting an Opinion from the Court does not have suspensory effect. It therefore does not prevent the Council from taking the decision to approve the agreement while that procedure is still in progress, even where the interval between bringing the request for an Opinion before the Court and the decision approving the agreement is, as in this case, relatively short.

279. The fact that a request to the Court for an Opinion, made pursuant to Article 300(6) EC, lacks suspensory effect may be inferred both from the wording of that article, which does not expressly provide for such suspensory effect, and from the Court's case-law.

The Court held in Opinion 3/94 [130] that such a request for an Opinion becomes devoid of purpose, and that there is no need for the Court to reply to it, when the agreement to which it relates, which was an agreement envisaged at the time when the matter was brought before the Court, has in the meantime been concluded. The Court also pointed out, first, that the procedure under Article 300(6) EC 'aims, first, ... to forestall difficulties arising from the incompatibility with the Treaty of international agreements binding the Community and *not to protect the interests and rights of the Member State or Community institution which has requested the Opinion*' [131] and that, '[i]n any event, the State or Community institution which has requested the Opinion may bring an action for annulment of the Council's decision to conclude the agreement ...'. [132]

280. Moreover, it is apparent both from the documents in the file and from the second recital in the preamble to the Council decision that the Council stated adequate reasons for the urgency invoked by it in order to obtain the opinion of the Parliament, in accordance with the first subparagraph of Article 300(3) EC, within a short time-limit. I note, finally, that that article expressly provides that, '[i]n the absence of an opinion within that time-limit, the Council may act'.

130 — [1995] ECR I-4577, an Opinion delivered at the request of the Federal Republic of Germany regarding the compatibility with the Treaty of the Framework Agreement on Bananas between the European Community and Colombia, Costa Rica, Nicaragua and Venezuela.

131 — Paragraph 21 of the Opinion (emphasis added).

132 — Paragraph 22 of the Opinion.

281. In the light of all those considerations, I am of the opinion that the plea alleging breach by the Council of its duty to cooperate in good faith is unfounded and must therefore be dismissed.

VII — Costs

282. In Case C-318/04, the conclusion that the action brought by the Parliament is well founded means that the Commission should be ordered to pay the costs, in accordance with Article 69(2) of the Rules of Procedure of the Court. In addition, pursuant to Article 69(4) of those rules, the interveners, namely the United Kingdom and the EDPS, must bear their own costs.

283. In Case C-317/04, the conclusion that the action brought by the Parliament is well founded means that the Council should be ordered to pay the costs, in accordance with Article 69(2) of the Rules of Procedure. In addition, pursuant to Article 69(4) of those rules, the interveners, namely the United Kingdom, the Commission and the EDPS, must bear their own costs.

VIII — Conclusion

284. In the light of all the foregoing considerations, I propose that the Court should:

— in Case C-318/04, annul Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection;

— in Case C-317/04, annul Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection.