JUDGMENT OF THE COURT (Grand Chamber)

30 May 2006 *

In Joined Cases C-317/04 and C-318/04,

ACTIONS for annulment under Article 230 EC, brought on 27 July 2004,

European Parliament, represented by R. Passos, N. Lorenz, H. Duintjer Tebbens and A. Caiola, acting as Agents, with an address for service in Luxembourg,

applicant,

supported by

European Data Protection Supervisor (EDPS), represented by H. Hijmans and V. Perez Asinari, acting as Agents,

intervener,

* Language of the case: French.

Council of the European Union, represented by M.C. Giorgi Fort and M. Bishop, acting as Agents,

defendant in Case C-317/04,

supported by

Commission of the European Communities, represented by P.J. Kuijper, A. van Solinge and C. Docksey, acting as Agents, with an address for service in Luxembourg,

United Kingdom of Great Britain and Northern Ireland, represented by M. Bethell, C. White and T. Harris, acting as Agents, and by T. Ward, Barrister, with an address for service in Luxembourg,

interveners,

and v

Commission of the European Communities, represented by P.J. Kuijper, A. van Solinge, C. Docksey and F. Benyon, acting as Agents, with an address for service in Luxembourg,

defendant in Case C-318/04,

supported by

United Kingdom of Great Britain and Northern Ireland, represented by M. Bethell, C. White and T. Harris, acting as Agents, and by T. Ward, Barrister, with an address for service in Luxembourg,

intervener,

THE COURT (Grand Chamber),

composed of V. Skouris, President, P. Jann, C.W.A. Timmermans, A. Rosas and J. Malenovský, Presidents of Chambers, N. Colneric (Rapporteur), S. von Bahr, J.N. Cunha Rodrigues, R. Silva de Lapuerta, G. Arestis, A. Borg Barthet, M. Ilešič and J. Klučka, Judges,

Advocate General: P. Léger,
Registrar: M. Ferreira, Principal Administrator,

having regard to the written procedure and further to the hearing on 18 October 2005,

after hearing the Opinion of the Advocate General at the sitting on 22 November 2005,

gives the following

Judgment

1 By its application in Case C-317/04, the European Parliament seeks the annulment of 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 (OJ 2004 L 183, p. 83, and corrigendum at OJ 2005 L 255, p. 168).

2 By its application in Case C-318/04, the Parliament seeks the annulment of 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 (OJ 2004 L 235, p. 11; 'the decision on adequacy').

Legal context

3 Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 ('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.'

4 The second sentence of Article 95(1) EC is worded as follows:

'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.'

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data

and on the free movement of such data (OJ 1995 L 281, p. 31), 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) ('the Directive'), was adopted on the basis of Article 100a of the EC Treaty (now, after amendment, Article 95 EC).

6 The 11th recital in the preamble to the Directive 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 the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data'.

7 The 13th recital in the preamble reads as follows:

'... the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56(2), Article 57 or Article 100a of the Treaty establishing the European Community ...'

8 The 57th recital states:

'... the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited'.

9 Article 2 of the Directive provides:

'For the purposes of this Directive:

(a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); 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;

(b) "processing of personal data" ("processing") shall mean 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;

...'

10 Article 3 of the Directive is worded as follows:

'Scope

1. This 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.

2. 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,

...'

11 Article 6(1) of the Directive states:

'Member States shall provide that personal data must be:

...

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

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

...

(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. ...'

12 Article 7 of the Directive provides:

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

...

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

...

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests [or] fundamental rights and freedoms of the data subject which require protection under Article 1(1).'

13 The first subparagraph of Article 8(5) of the Directive is worded as follows:

'Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.'

14 Article 12 of the Directive provides:

'Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

— confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

— communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

— knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.'

15 Article 13(1) of the Directive is worded as follows:

'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.'

16 Article 22 of the Directive provides:

'Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for 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.'

17 Articles 25 and 26 of the Directive constitute Chapter IV, on the transfer of personal data to third countries.

18 Article 25, headed 'Principles', provides:

'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 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.'

19 Article 26(1) of the Directive, under the heading 'Derogations', is worded as follows:

'By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:

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

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.'

20 It was on the basis of the Directive, in particular Article 25(6) thereof, that the Commission of the European Communities adopted the decision on adequacy.

21 The 11th recital in the preamble to that decision states:

'The processing by CBP [the Bureau of Customs and Border Protection] of personal data contained in the PNR [Passenger Name Record] 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 (hereinafter referred to as the Undertakings) and in United States domestic legislation to the extent indicated in the Undertakings.'

22 The 15th recital in the preamble to the decision 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.

23 Articles 1 to 4 of the decision on adequacy provide:

'*Article 1*

For the purposes of Article 25(2) of Directive 95/46/EC, the United States Bureau of Customs and Border Protection (hereinafter referred to as CBP) is considered to

ensure an adequate level of protection for PNR data transferred from the Community concerning flights to or from the United States, in accordance with the Undertakings set out in the Annex.

Article 2

This Decision concerns the adequacy of protection provided by CBP with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and shall not affect other conditions or restrictions implementing other provisions of that Directive that pertain to the processing of personal data within the Member States.

Article 3

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.

Article 4

1. Member States shall inform the Commission without delay when measures are adopted pursuant to Article 3.

2. The Member States and the Commission shall inform each other of any changes in the standards of protection and of cases where the action of bodies responsible for ensuring compliance with the standards of protection by CBP as set out in the Annex fails to secure such compliance.

3. If 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.'

24 The 'Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP)' annexed to the decision on adequacy state:

'In support of the plan of the European Commission (Commission) to exercise the powers conferred on it by Article 25(6) of Directive 95/46/EC ... and to adopt a decision recognising the Department of Homeland Security Bureau of Customs and Border Protection (CBP) as providing adequate protection for the purposes of air carrier transfers of [PNR] data which may fall within the scope of the Directive, CBP undertakes as follows ...'

25 The Undertakings comprise 48 paragraphs, arranged under the following headings: 'Legal authority to obtain PNR'; 'Use of PNR data by CBP'; 'Data requirements'; 'Treatment of "sensitive" data'; 'Method of accessing PNR data'; 'Storage of PNR data'; 'CBP computer system security'; 'CBP treatment and protection of PNR data'; 'Transfer of PNR data to other government authorities'; 'Notice, access and opportunities for redress for PNR data subjects'; 'Compliance issues'; 'Reciprocity'; 'Review and termination of Undertakings'; and 'No private right or precedent created'.

26 The Undertakings include the following:

'1. By legal statute (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the United States must provide CBP (formerly, the US

Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems (reservation systems).

...

3. 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. Use of PNR data for these purposes permits CBP to focus its resources on high-risk concerns, thereby facilitating and safeguarding bona fide travel.

4. Data elements which CBP requires are listed herein at Attachment A. ...

...

27. CBP will take the position in connection with any administrative or judicial proceeding arising out of a FOIA [Freedom of Information Act] request for PNR information accessed from air carriers, that such records are exempt from disclosure under the FOIA.

...

29. CBP, in its discretion, will only provide PNR data to other government authorities, including foreign government authorities, with counter-terrorism or law-enforcement functions, on a case-by-case basis, for purposes of preventing and combating offences identified in paragraph 3 herein. (Authorities with whom CBP may share such data shall hereinafter be referred to as the Designated Authorities).

30. CBP will judiciously exercise its discretion to transfer PNR data for the stated purposes. CBP will first determine if the reason for disclosing the PNR data to another Designated Authority fits within the stated purpose (see paragraph 29 herein). If so, CBP will determine whether that Designated Authority is responsible for preventing, investigating or prosecuting the violations of, or enforcing or implementing, a statute or regulation related to that purpose, where CBP is aware of an indication of a violation or potential violation of law. The merits of disclosure will need to be reviewed in light of all the circumstances presented.

...

35. No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law. CBP will advise the European Commission regarding the passage of any US legislation which materially affects the statements made in these Undertakings.

...

46. These Undertakings shall apply for a term of three years and six months (3.5 years), beginning on the date upon which an agreement enters into force between the United States and the European Community, authorising the processing of PNR data by air carriers for purposes of transferring such data to CBP, in accordance with the Directive. ...

47. These Undertakings do not create or confer any right or benefit on any person or party, private or public.

...'

27 Attachment A to the Undertakings contains the 'PNR data elements' required by CBP from air carriers. The PNR data elements include the 'PNR record locator code', date of reservation, name, address, all forms of payment information, contact telephone numbers, travel agency, travel status of the passenger, e-mail address, general remarks, seat number, no-show history and any collected APIS (Advanced Passenger Information System) information.

28 The Council adopted Decision 2004/496 on the basis, in particular, of Article 95 EC in conjunction with the first sentence of the first subparagraph of Article 300(2) EC.

29 The three recitals in the preamble to that decision state:

'(1) On 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 the United States Department of Homeland Security, Bureau of Customs and Border Protection.

(2) 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.

(3) This Agreement should be approved.'

30 Article 1 of Decision 2004/496 provides:

'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 is hereby approved on behalf of the Community.

The text of the Agreement is attached to this Decision.'

31 That agreement ('the Agreement') is worded as follows:

'The European Community and the United States of America,

Recognising 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,

Having regard to US statutes and regulations requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to provide the Department of Homeland Security (hereinafter "DHS"), Bureau of Customs and Border Protection (hereinafter "CBP") with electronic access to Passenger Name Record (hereinafter "PNR") data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems,

Having regard to Directive 95/46/EC ..., and in particular Article 7(c) thereof,

Having regard to the Undertakings of CBP issued on 11 May 2004, which will be published in the Federal Register (hereinafter "the Undertakings"),

Having regard to Commission Decision 2004/535/EC adopted on 14 May 2004, pursuant to Article 25(6) of Directive 95/46/EC, whereby CBP is considered as providing an adequate level of protection for PNR data transferred from the

European Community (hereinafter "Community") concerning flights to or from the US in accordance with the Undertakings, which are annexed thereto (hereinafter "the Decision"),

Noting 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,

...

Have agreed as follows:

(1) CBP may electronically access the PNR data from air carriers' reservation/ departure control systems ("reservation systems") located within the territory of the Member States of the European Community strictly in accordance with the Decision 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.

(2) Air carriers operating passenger flights in foreign air transportation to or from the United States shall process PNR data contained in their automated reservation systems as required by CBP pursuant to US law and strictly in accordance with the Decision and for so long as the Decision is applicable.

(3) CBP takes note of the Decision and states that it is implementing the Undertakings annexed thereto.

(4) 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.

...

(7) This Agreement shall enter into force upon signature. Either Party may terminate this Agreement at any time by notification through diplomatic channels. The termination shall take effect ninety (90) days from the date of notification of termination to the other Party. This Agreement may be amended at any time by mutual written agreement.

(8) This 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.'

32 According to Council information concerning the date of its entry into force (OJ 2004 C 158, p. 1), the Agreement, signed in Washington on 28 May 2004 by a representative of the Presidency-in-Office of the Council and the Secretary of the United States Department of Homeland Security, entered into force on the date of its signature, as provided by paragraph 7 of the Agreement.

Background

33 Following the terrorist attacks of 11 September 2001, the United States passed legislation in November 2001 providing that air carriers operating flights to or from the United States or across United States territory had to provide the United States customs authorities with electronic access to the data contained in their automated reservation and departure control systems, referred to as 'Passenger Name Records' ('PNR data'). While acknowledging the legitimacy of the security interests at stake, the Commission informed the United States authorities, in June 2002, that those provisions could come into conflict with Community and Member State legislation on data protection and with certain provisions of 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). The United States authorities postponed the entry into force of the new provisions but, ultimately, refused to waive the right to impose penalties on airlines failing to comply with the legislation on electronic access to PNR data after 5 March 2003. Since then, a number of large airlines in the European Union have granted the United States authorities access to their PNR data.

34 The Commission entered into negotiations with the United States authorities, which gave rise to a document containing undertakings on the part of CBP, with a view to the adoption by the Commission of a decision on adequacy pursuant to Article 25(6) of the Directive.

35 On 13 June 2003 the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, set up by Article 29 of the Directive, delivered an opinion in which it expressed doubts regarding the level of data protection guaranteed by those undertakings for the processing operations envisaged. It reiterated those doubts in an opinion of 29 January 2004.

36 On 1 March 2004 the Commission placed before the Parliament the draft decision on adequacy under Article 25(6) of the Directive, together with the draft undertakings of CBP.

37 On 17 March 2004 the Commission submitted to the Parliament, with a view to its consultation in accordance with the first subparagraph of Article 300(3) EC, a proposal for a Council decision concerning the conclusion of an agreement with the United States. By letter of 25 March 2004, the Council, referring to the urgent procedure, requested the Parliament to deliver an opinion on that proposal by 22 April 2004 at the latest. In that 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.'

38 On 31 March 2004 the Parliament, acting pursuant to Article 8 of Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (OJ 1999 L 184, p. 23), adopted a resolution setting out a number of reservations of a legal nature regarding the proposal which had been submitted to it. In particular, the Parliament considered that the draft decision on adequacy exceeded the powers conferred on the Commission by Article 25 of the Directive. It called for the conclusion of an appropriate international agreement respecting fundamental rights that would cover a number of points set out in detail in the resolution, 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 protection of the right to privacy.

39 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, in accordance with Article 300(6) EC, an Opinion be obtained from the Court on the compatibility of the agreement envisaged with the Treaty. That procedure was initiated on that very day.

40 The Parliament also decided, on the same day, to refer to committee the report on the proposal for a Council decision, thus implicitly rejecting, at that stage, the Council's request of 25 March 2004 for urgent consideration of the proposal.

41 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 deliver its opinion on the proposal for a decision relating to the conclusion of the Agreement by 5 May 2004. To justify the urgency of that request, the Council restated the reasons set out in its letter of 25 March 2004.

42 After taking note of the continuing lack of all the language versions of the proposal for a Council decision, on 4 May 2004 the Parliament rejected the Council's request to it of 28 April for urgent consideration of that proposal.

43 On 14 May 2004 the Commission adopted the decision on adequacy, which is the subject of Case C-318/04. On 17 May 2004 the Council adopted Decision 2004/496, which is the subject of Case C-317/04.

44 By letter of 4 June 2004, the Presidency-in-Office of the Council informed the Parliament that Decision 2004/496 took into account the fight against terrorism — a priority of the Union — but also the need to address the uncertain legal situation of air carriers as well as their financial interests.

45 By letter of 9 July 2004, the Parliament informed the Court of the withdrawal of its request for an Opinion, which had been registered under No 1/04.

46 In Case C-317/04, the Commission and the United Kingdom of Great Britain and Northern Ireland were granted leave to intervene in support of the form of order sought by the Council, by orders of the President of the Court of 18 November 2004 and 18 January 2005.

47 In Case C-318/04, the United Kingdom was granted leave to intervene in support of the form of order sought by the Commission, by order of the President of the Court of 17 December 2004.

48 By orders of the Court of 17 March 2005, the European Data Protection Supervisor was granted leave to intervene in support of the form of order sought by the Parliament in both cases.

49 Given the connection, confirmed at the hearing, between the cases, it is appropriate to join them under Article 43 of the Rules of Procedure for the purposes of the judgment.

The application in Case C-318/04

50 The Parliament advances four pleas for annulment, alleging, respectively, *ultra vires* action, breach of the fundamental principles of the Directive, breach of fundamental rights and breach of the principle of proportionality.

The first limb of the first plea: breach of the first indent of Article 3(2) of the Directive

Arguments of the parties

51 The Parliament contends that adoption of the Commission decision was *ultra vires* because the provisions laid down in the Directive were not complied with; in particular, the first indent of Article 3(2) of the Directive, relating to the exclusion of activities which fall outside the scope of Community law, was infringed.

52 In the Parliament's submission, there is no doubt that the processing of PNR data after transfer to the United States authority covered by the decision on adequacy is, and will be, carried out in the course of activities of the State as referred to in paragraph 43 of the judgment in Case C-101/01 *Lindqvist* [2003] ECR I-12971.

53 The Commission, supported by the United Kingdom, considers that the air carriers' activities clearly fall within the scope of Community law. It submits that those private operators process the PNR data within the Community and arrange for their transfer to a third country. Activities of private parties are therefore involved, and

not activities of the Member State in which the carriers concerned operate, or of its public authorities, as defined by the Court in paragraph 43 of *Lindqvist*. The aim pursued by the air carriers in processing PNR data is simply to comply with the requirements of Community law, including the obligation laid down in paragraph 2 of the Agreement. Article 3(2) of the Directive refers to activities of public authorities which fall outside the scope of Community law.

Findings of the Court

54 The first indent of Article 3(2) of the Directive excludes from the Directive's scope the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities provided for by Titles V and VI of the Treaty on European Union, and in any case processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.

55 The decision on adequacy concerns only PNR data transferred to CBP. It is apparent from the sixth recital in the preamble to the decision that the requirements for that transfer are based on a statute enacted by the United States in November 2001 and on implementing regulations adopted by CBP under that statute. According to the seventh recital in the preamble, the United States legislation in question concerns the enhancement of security and the conditions under which persons may enter and leave the country. The eighth recital states that the Community is fully committed to supporting the United States in the fight against terrorism within the limits imposed by Community law. The 15th recital 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.

56 It follows that the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law.

57 While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account in the decision on adequacy is, however, quite different in nature. As pointed out in paragraph 55 of the present judgment, that decision concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes.

58 The Court held in paragraph 43 of *Lindqvist*, which was relied upon by the Commission in its defence, that the activities mentioned by way of example in the first indent of Article 3(2) of the Directive are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals. However, this does not mean that, because the PNR data have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country, the transfer in question is not covered by that provision. The transfer falls within a framework established by the public authorities that relates to public security.

59 It follows from the foregoing considerations that the decision on adequacy concerns processing of personal data as referred to in the first indent of Article 3(2) of the Directive. That decision therefore does not fall within the scope of the Directive.

60 Accordingly, the first limb of the first plea, alleging that the first indent of Article 3(2) of the Directive was infringed, is well founded.

61 The decision on adequacy must consequently be annulled and it is not necessary to consider the other limbs of the first plea or the other pleas relied upon by the Parliament.

The application in Case C-317/04

62 The Parliament advances six pleas for annulment, concerning the incorrect choice of Article 95 EC as legal basis for Decision 2004/496 and breach of, respectively, the second subparagraph of Article 300(3) EC, Article 8 of the ECHR, the principle of proportionality, the requirement to state reasons and the principle of cooperation in good faith.

The first plea: incorrect choice of Article 95 EC as legal basis for Decision 2004/496

Arguments of the parties

63 The Parliament submits that Article 95 EC does not constitute an appropriate legal basis for Decision 2004/496. The decision does not have as its objective and subject-matter the establishment and functioning of the internal market by contributing to the removal of obstacles to the freedom to provide services and it does not contain provisions designed to achieve such an objective. Its purpose is to make lawful the

processing of personal data that is required by United States legislation. Nor can Article 95 EC justify Community competence to conclude the Agreement, because the Agreement relates to data processing operations which are excluded from the scope of the Directive.

64 The Council contends that the Directive, validly adopted on the basis of Article 100a of the Treaty, contains in Article 25 provisions enabling personal data to be transferred to a third country which ensures an adequate level of protection, including the possibility of entering, if need be, into negotiations leading to the conclusion by the Community of an agreement with that country. The Agreement concerns the free movement of PNR data between the Community and the United States under conditions which respect the fundamental freedoms and rights of individuals, in particular privacy. It is intended to eliminate any distortion of competition, between the Member States' airlines and between the latter and the airlines of third countries, which may result from the requirements imposed by the United States, 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 because only some of them granted the United States authorities access to their databases. The Agreement is designed to impose harmonised obligations on all the airlines concerned.

65 The Commission observes that there is a 'conflict of laws', within the meaning of public international law, between the United States legislation and the Community rules and that it is necessary to reconcile them. It complains that the Parliament, which disputes that Article 95 EC can constitute the legal basis for Decision 2004/496, has not suggested an appropriate legal basis. According to the Commission, that article is 'the natural legal basis' for the decision because the Agreement concerns the external dimension of the protection of personal data when

transferred within the Community. Articles 25 and 26 of the Directive justify exclusive Community external competence.

66 In addition, the Commission submits that the initial processing of the data by the airlines is carried out for commercial purposes. The use which the United States authorities make of the data does not remove them from the effect of the Directive.

Findings of the Court

67 Article 95 EC, read in conjunction with Article 25 of the Directive, cannot justify Community competence to conclude the Agreement.

68 The Agreement relates to the same transfer of data as the decision on adequacy and therefore to data processing operations which, as has been stated above, are excluded from the scope of the Directive.

69 Consequently, Decision 2004/496 cannot have been validly adopted on the basis of Article 95 EC.

70 That decision must therefore be annulled and it is not necessary to consider the other pleas relied upon by the Parliament.

Limitation of the effects of the judgment

71 Under paragraph 7 of the Agreement, either party may terminate the Agreement at any time and the termination takes effect 90 days from the date of notification of termination to the other party.

72 However, in accordance with paragraphs 1 and 2 of the Agreement, CBP's right of access to PNR data and the obligation imposed on air carriers to process them as required by CBP exist only for so long as the decision on adequacy is applicable. In paragraph 3 of the Agreement, CBP stated that it was implementing the Undertakings annexed to that decision.

73 Given, first, the fact that the Community cannot rely on its own law as justification for not fulfilling the Agreement which remains applicable during the period of 90 days from termination thereof and, second, the close link that exists between the Agreement and the decision on adequacy, it appears justified, for reasons of legal certainty and in order to protect the persons concerned, to preserve the effect of the decision on adequacy during that same period. In addition, account should be taken of the period needed for the adoption of the measures necessary to comply with this judgment.

74 It is therefore appropriate to preserve the effect of the decision on adequacy until 30 September 2006, but its effect shall not be preserved beyond the date upon which the Agreement comes to an end.

Costs

75 Under Article 69(2) of the Rules of Procedure, the unsuccessful party is to be ordered to pay the costs if they have been applied for in the successful party's pleadings. Since the Parliament has applied for costs and the Council and the Commission have been unsuccessful, the Council and the Commission must be ordered to pay the costs. Pursuant to the first subparagraph of Article 69(4), the interveners in the present cases must bear their own costs.

On those grounds, the Court (Grand Chamber) hereby:

1. **Annuls 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, and 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;**

2. **Preserves the effect of Decision 2004/535 until 30 September 2006, but not beyond the date upon which that Agreement comes to an end;**

3. **Orders the Council of the European Union to pay the costs in Case C-317/04;**

4. **Orders the Commission of the European Communities to pay the costs in Case C-318/04;**

5. **Orders the Commission of the European Communities to bear its own costs in Case C-317/04;**

6. **Orders the United Kingdom of Great Britain and Northern Ireland and the European Data Protection Supervisor to bear their own costs.**

[Signatures]