JEAN MONNET CENTRE OF EXCELLENCE
EU CONSTITUTIONAL VALUES OBSERVATORY

Collections of Case law
Volume 3
PERSONAL DATA PROTECTION

Co-funded by the
Erasmus+ Programme
of the European Union

LIST OF CASES

C-28/08 P

C-92/09 and C-93/09

T-82/09

C-70/10

C-468/10 and C-469/10

C-360/10

C-362/14

F-57/14

T-343/13

C-203/15 and C-698/15

C-291/12

C-293/12 and C-594/12

C-131/12

C-141/12 and C-372/12

The information were retrieved in

https://curia.europa.eu/common/recdoc/repertoire_jurisp/bull_1/tab_index_1_04_03.htm

JUDGMENT OF THE COURT (Grand Chamber)

29 June 2010 *

In Case C-28/08 P,

APPEAL under Article 56 of the Statute of the Court of Justice, brought on 23 January 2008,

European Commission, represented by C. Docksey and P. Aalto, acting as Agents, with an address for service in Luxembourg,

applicant,

supported by:

United Kingdom of Great Britain and Northern Ireland, represented by E. Jenkinson and V. Jackson, acting as Agents, assisted by J. Coppel, Barrister,

* Language of the case: English.

Council of the European Union, represented by B. Driessen and C. Fekete, acting as Agents,

interveners in the appeal,

the other parties to the proceedings being:

The Bavarian Lager Co. Ltd, established in Clitheroe (United Kingdom), represented by J. Webber and M. Readings, Solicitors,

applicant at first instance,

supported by:

Kingdom of Denmark, represented by B. Weis Fogh, acting as Agent,

Republic of Finland, represented by J. Heliskoski, acting as Agent,

Kingdom of Sweden, represented by K. Petkovska, acting as Agent,

interveners in the appeal,

European Data Protection Supervisor, represented by H. Hijmans, A. Scirocco and H. Kranenborg, acting as Agents,

intervener at first instance,

THE COURT (Grand Chamber),

composed of V. Skouris, President, A. Tizzano, J.N. Cunha Rodrigues, K. Lenaerts, R. Silva de Lapuerta and C. Toader, Presidents of Chambers, A. Rosas, K. Schiemann, E. Juhász (Rapporteur), G. Arestis and T. von Danwitz, Judges,

Advocate General: E. Sharpston,
Registrar: H. von Holstein, Deputy Registrar,

having regard to the written procedure and further to the hearing on 16 June 2009,

after hearing the Opinion of the Advocate General at the sitting on 15 October 2009,

gives the following

Judgment

1 By its appeal, the Commission of the European Communities seeks the annulment of the judgment of the Court of First Instance of the European Communities (now 'the General Court') of 8 November 2007 in Case T-194/04 *Bavarian Lager* v *Commission* [2007] ECR II-4523; 'the judgment under appeal'), in so far as that judgment annulled the Commission's decision of 18 March 2004 ('the contested decision'), rejecting the request by The Bavarian Lager Co. Ltd ('Bavarian Lager') for access to the full minutes of a meeting of 11 October 1996, held in the context of a procedure for failure to fulfil obligations ('the meeting of 11 October 1996').

Legal context

2 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) requires Member States to ensure the protection of the fundamental rights and freedoms of natural persons, and in particular their privacy in relation to the handling of personal data, in order to ensure the free movement of personal data in the European Community.

3 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.

4 Recitals 1, 2, 5, 7, 8, 12, 14 and 15 of Regulation No 45/2001, or certain parts thereof, read as follows:

'(1) Article 286 [EC] requires the application to the Community institutions and bodies of the Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data.

(2) A fully-fledged system of protection of personal data not only requires the establishment of rights for data subjects and obligations for those who process personal data, but also appropriate sanctions for offenders and monitoring by an independent supervisory body.

...

(5) A Regulation is necessary to provide the individual with legally enforceable rights ...

...

(7) The persons to be protected are those whose personal data are processed by Community institutions or bodies in any context whatsoever …

(8) The principles of data protection should apply to any information concerning an identified or identifiable person. …

…

(12) Consistent and homogeneous application of the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data should be ensured throughout the Community.

…

(14) To this end measures should be adopted which are binding on the Community institutions and bodies. These measures should apply to all processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

(15) Where such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation, in particular those laid down in Titles V and VI of the [EU Treaty, in its version prior to the Treaty of Lisbon], the protection of individuals' fundamental rights and freedoms shall be ensured with due regard to Article 6 of [that EU Treaty]. Access to documents, including conditions for access to documents containing personal data, is governed by the rules adopted on the basis of Article 255 … EC the scope of which includes Titles V and VI of [the said EU Treaty].'

5 Article 1 of Regulation No 45/2001 provides:

‘1. In accordance with this Regulation, the institutions and bodies set up by, or on the basis of, the Treaties establishing the European Communities, hereinafter referred to as “Community institutions or bodies”, 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 and shall neither restrict nor prohibit the free flow of personal data between themselves or to recipients subject to the national law of the Member States implementing Directive 95/46 …

2. The independent supervisory authority established by this Regulation, hereinafter referred to as the European Data Protection Supervisor, shall monitor the application of the provisions of this Regulation to all processing operations carried out by a Community institution or body.’

6 Article 2 of that regulation provides:

‘For the purposes of this Regulation:

(a) “personal data” shall mean any information relating to an identified or identifiable natural person hereinafter referred to as “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 or her physical, physiological, mental, economic, cultural or social identity;

(b) "processing of personal data" … 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;

…'

7 Article 3 of the said regulation provides:

'1. This Regulation shall apply to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

2. This Regulation 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.'

8 According to Article 4 of the same regulation:

‘1. 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 …

…’

9 Article 5 of Regulation No 45/2001 provides:

‘Personal data may be processed only if:

(a) processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed, or

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

…

(c) the data subject has unambiguously given his or her consent ...

...'

10 Article 8 of that regulation, headed 'Transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46 ...', provides:

'Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46:

(a) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or

(b) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.'

11 Article 18 of the said regulation, headed 'The data subject's right to object', states:

'The data subject shall have the right:

(a) to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her, except in the cases covered by Article 5(b), (c) and (d). Where there is a justified objection, the processing in question may no longer involve those data;

(b) to be informed before personal data are disclosed for the first time to third parties or before they are used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosure or use.'

12 Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ 2001 L 145, p. 43), defines the principles, conditions and limits for the right of access to documents of those institutions laid down by Article 255 EC. That regulation has applied since 3 December 2001.

13 According to recital 1 of Regulation No 1049/2001:

'The second subparagraph of Article 1 of the [EU Treaty in its version prior to the Lisbon Treaty] enshrines the concept of openness, stating that the Treaty marks a

new stage in the process of creating an ever closer union among the peoples of Europe, in which decisions are taken as openly as possible and as closely as possible to the citizen.'

14 According to recital 2 of Regulation No 1049/2001:

'Openness enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system. Openness contributes to strengthening the principles of democracy and respect for fundamental rights as laid down in Article 6 of the EU Treaty [in its version prior to the Treaty of Lisbon] and in the Charter of Fundamental Rights of the European Union ["the Charter"].'

15 Recitals 4 and 11 of Regulation No 1049/2010 state:

'(4) The purpose of this Regulation is to give the fullest possible effect to the right of public access to documents and to lay down the general principles and limits on such access in accordance with Article 255(2) … EC.

...

(11) In principle, all documents of the institutions should be accessible to the public. However, certain public and private interests should be protected by way of exceptions. The institutions should be entitled to protect their internal consultations and deliberations where necessary to safeguard their ability to carry out their tasks. In assessing the exceptions, the institutions should take account of the principles in Community legislation concerning the protection of personal data, in all areas of Union activities.'

16 According to Article 2 of Regulation No 1049/2001, headed 'Beneficiaries and scope':

'1. Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, has a right of access to documents of the institutions, subject to the principles, conditions and limits defined in this Regulation.

2. The institutions may, subject to the same principles, conditions and limits, grant access to documents to any natural or legal person not residing or not having its registered office in a Member State.

3. This Regulation shall apply to all documents held by an institution, that is to say, documents drawn up or received by it and in its possession, in all areas of activity of the European Union.

4. Without prejudice to Articles 4 and 9, documents shall be made accessible to the public either following a written application or directly in electronic form or through a register. In particular, documents drawn up or received in the course of a legislative procedure shall be made directly accessible in accordance with Article 12.

5. Sensitive documents as defined in Article 9(1) shall be subject to special treatment in accordance with that Article.

…'

17 According to Article 4 of Regulation No 1049/2001, concerning exceptions to the right of access:

'The institutions shall refuse access to a document where disclosure would undermine the protection of:

…

(b) privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data.

2. The institutions shall refuse access to a document where disclosure would undermine the protection of:

…

— the purpose of inspections, investigations and audits,

unless there is an overriding public interest in disclosure.

...'

18 Article 6(1) of Regulation No 1049/2001 provides that '[t]he applicant is not obliged to state reasons for the application.'

Factual background to the dispute

19 The facts behind the present dispute are set out in paragraphs 15 to 28 and 34 to 37 of the judgment under appeal as follows:

'15 [Bavarian Lager] was established on 28 May 1992 for the importation of German beer for public houses and bars in the United Kingdom, situated primarily in the North of England.

16 However, Bavarian Lager was not able to sell its product, since a large number of publicans in the United Kingdom were tied by exclusive purchasing contracts obliging them to obtain their supplies of beer from certain breweries.

17 Under the Supply of Beer (Tied Estate) Order 1989 SI 1989/2390, British breweries holding rights in more than 2 000 pubs are required to allow the managers of those establishments the possibility of buying a beer from another brewery, on condition, according to Article 7(2)(a) of the order, that it is conditioned in a cask and has an alcohol content exceeding 1.2% by volume. That provision is commonly known as the "Guest Beer Provision" ("the GBP").

18 However, most beers produced outside the United Kingdom cannot be regarded as "cask-conditioned beers", within the meaning of the GBP, and thus do not fall within its scope.

19 Considering that the GBP constituted a measure having equivalent effect to a quantitative restriction on imports, and was thus incompatible with Article 30 of the EC Treaty (now, after amendment, Article 28 EC), [Bavarian Lager] lodged a complaint with the Commission by letter of 3 April 1993, registered under reference P/93/4490/UK.

20 Following its investigation, the Commission decided, on 12 April 1995, to institute proceedings against the United Kingdom of Great Britain and Northern Ireland under Article 169 of the EC Treaty (now Article 226 EC). It notified the applicant on 28 September 1995 of that investigation and of the fact that it had sent a letter of formal notice to the United Kingdom on 15 September 1995. On 26 June 1996, the Commission decided to send a reasoned opinion to the United Kingdom and, on 5 August 1996, issued a press release announcing that decision.

21 On 11 October 1996, … [the meeting of 11 October 1996 was held] which was attended by officers of the Directorate-General (DG) for the Internal Market and Financial Services, officials of the United Kingdom Government Department of Trade and Industry and representatives of the Confederation des Brasseurs du Marche Commun ("CBMC"). [Bavarian Lager] had requested the right to attend

the meeting [of 11 October 1996] in a letter dated 27 August 1996, but the Commission refused to grant permission to attend.

22 On 15 March 1997 the Department of Trade and Industry in the United Kingdom announced a proposal to amend the GBP under which a bottle-conditioned beer could be sold as a guest beer, as well as cask-conditioned beer. After the Commission had, on two occasions, namely 19 March 1997 and 26 June 1997, suspended its decision to issue a reasoned opinion to the United Kingdom, the head of Unit 2 "Application of Articles 30 to 36 of the EC Treaty (notification, complaints, infringements etc.) and removal of trade barriers" of Directorate B "Free movement of goods and public procurement" of DG "Internal Market and Financial Services", in a letter of 21 April 1997, informed [Bavarian Lager] that, in view of the proposed amendment of the GBP, the Article 169 procedure had been suspended and the reasoned opinion had not been served on the United Kingdom Government. He indicated that the procedure would be discontinued entirely as soon as the amended GBP came into force. The new version of the GBP became applicable on 22 August 1997. Consequently, the reasoned opinion was never sent to the United Kingdom and the Commission finally decided on 10 December 1997 to take no further action in the infringement procedure.

23 By fax of 21 March 1997, [Bavarian Lager] asked the Director-General of DG "Internal Market and Financial Services" for a copy of the "reasoned opinion", in accordance with the Code of Conduct [concerning public access to Council and Commission documents (OJ 1993 L 340, p. 41)]. That request, despite being repeated, was refused.

24 By [decision] of 18 September 1997 …, the Secretary-General of the Commission confirmed the refusal of the application sent to DG "Internal Market and Financial Services".

25 [Bavarian Lager] brought an action, registered as Case T-309/97, before the [General Court] against the decision of 18 September 1997. In its judgment of 14 October 1999 in Case T-309/97 *Bavarian Lager* v *Commission* [1999] ECR II-3217, the [General Court] dismissed the action, stating that the preservation of the aim in question, namely allowing a Member State to comply voluntarily with the requirements of the Treaty, or, where necessary, to give it the opportunity to justify its position, justified, for the protection of the public interest, the refusal of access to a preparatory document relating to the investigation stage of the procedure under Article 169 of the Treaty …

26 On 4 May 1998, [Bavarian Lager] addressed a request to the Commission under the Code of Conduct for access to all of the submissions made under file reference P/93/4490/UK by 11 named companies and organisations and by three defined categories of person or company. The Commission refused the initial application on the ground that the [said] Code of Conduct applies only to documents of which the Commission is the author. The confirmatory application was rejected on the grounds that the Commission was not the author of the document in question and that any application had to be sent to the author.

27 On 8 July 1998, [Bavarian Lager] complained to the European Ombudsman under reference 713/98/IJH, stating, by letter dated 2 February 1999, that it wished to obtain the names of the delegates of the CBMC who had attended the meeting on 11 October 1996 and the names of the companies and any persons who fell into one of the 14 categories identified in the original request for access to documents containing the communications to the Commission under file reference P/93/4490/UK.

28 Following an exchange of letters between the Ombudsman and the Commission, the latter indicated to the Ombudsman in October and November 1999 that, of the 45 letters that it had written to the persons concerned requesting approval

to disclose their identities to [Bavarian Lager], 20 replies had been received, of which 14 were positive and 6 were negative. The Commission supplied the names and addresses of those that had responded positively. [Bavarian Lager] stated to the Ombudsman that the information provided by the Commission was still incomplete.

…

34 By e-mail of 5 December 2003, [Bavarian Lager] sent a request to the Commission for access to the documents referred to in paragraph 26 above, based on Regulation No 1049/2001.

35 The Commission replied to that request by letter of 27 January 2004 stating that certain documents relating to the meeting [of 11 October 1996] could be disclosed, but drawing [Bavarian Lager's] attention to the fact that five names had been blanked out from the minutes of the meeting of 11 October 1996, following two express refusals by persons to consent to the disclosure of their identity and the Commission's failure to contact the remaining three attendees.

36 By e-mail of 9 February 2004, [Bavarian Lager] made a confirmatory application within the meaning of Article 7(2) of Regulation No 1049/2001, in which it requested the full minutes of the meeting of 11 October 1996, including all of the names.

37 By [the contested decision], the Commission rejected the confirmatory application of [Bavarian Lager]. It confirmed that Regulation No 45/2001 applied to the request for disclosure of the names of the other participants. As [Bavarian Lager] had not established an express and legitimate purpose or need for such a disclosure, the conditions set out by Article 8 of that regulation had not been met and the exception provided for in Article 4(1)(b) of Regulation No 1049/2001 applied. It added that, even if the rules on the protection of personal data did not apply, it would nevertheless have had to refuse to disclose the other names under Article 4(2), third indent, of Regulation No 1049/2001 so as not to compromise its ability to conduct inquiries.'

Procedure before the General Court and the judgment under appeal

20 By the judgment under appeal, the General Court annulled the contested decision.

21 Regarding access to the full minutes of the meeting of 11 October 1996, the General Court took the view, in paragraphs 90 to 95 of the judgment under appeal, that Bavarian Lager's request was based on Regulation No 1049/2001. Whilst pointing out that, according to Article 6(1) of Regulation No 1049/2001, a person requesting access is not required to justify his request and therefore does not have to demonstrate any interest in having access to the documents requested, the Court examined the exception to communication laid down in Article 4(1)(b) of that regulation, where disclosure of such a document might undermine the protection of privacy and the integrity of the individual.

22 In paragraphs 96 to 119 of the judgment under appeal, the General Court examined the relationship between Regulations Nos 45/2001 and 1049/2001. While stating that recital 15 of Regulation No 45/2001 indicates that access to documents, including those containing personal data, is governed by Article 255 EC, the Court emphasised that, according to recital 11 of Regulation No 1049/2001, in assessing the need for an exception, the institutions should take account of the principles in Community legislation concerning the protection of personal data in all areas of activity of the Union, thus including principles laid down in Regulation No 45/2001.

23 Referring to the definitions of 'personal data' and 'processing of personal data' mentioned in Article 2(a) and (b) of Regulation No 45/2001, in paragraph 105 of the judgment under appeal, the General Court concluded that communication of data, by transmission, dissemination or otherwise making available, falls within the definition of 'processing', and thus Regulation No 45/2001 itself provides, independently of Regulation No 1049/2001, for the possibility of making certain personal data public.

24 In paragraph 106 of the judgment under appeal, the General Court stated that the processing of personal data must be lawful under Article 5(a) or (b) of Regulation No 45/2001, according to which the processing must be necessary for the performance of a task carried out in the public interest or for compliance with a legal obligation to which the controller is subject. The Court then pointed out that the right of access to documents of the institutions recognised to citizens of the European Union and to any natural or legal person residing in or having its registered office in a Member State, laid down by Article 2 of Regulation No 1049/2001, constitutes a legal obligation for the purposes of Article 5(b) of Regulation No 45/2001. Therefore, if Regulation No 1049/2001 requires the communication of data, which constitutes 'processing' within the meaning of Article 2(b) of Regulation No 45/2001, Article 5 of that same regulation makes such communication lawful in that respect.

25 Ruling on the question of the obligation to prove the need to transfer, laid down by Article 8(b) of Regulation No 45/2001, and of the data subject's right to object pursuant to Article 18 of that regulation, the General Court held, in particular, in paragraphs 107 to 109 of the judgment under appeal, as follows:

'107 As regards the obligation to prove the need to transfer, laid down by Article 8(b) of Regulation No 45/2001, it should be remembered that access to documents containing personal data falls within the application of Regulation No 1049/2001, and that, according to Article 6(1) of the latter, a person requesting access is not required to justify his request and therefore does not have to demonstrate any interest in having access to the documents requested … Therefore, where personal data are transferred in order to give effect to Article 2 of Regulation No 1049/2001, laying down the right of access to documents for all citizens of the Union, the situation falls within the application of that regulation and, therefore, the applicant does not need to prove the necessity of disclosure for the purposes of Article 8(b) of Regulation No 45/2001. If one were to require the applicant to demonstrate the necessity of having the data transferred, as an additional condition imposed in Regulation No 45/2001, that requirement would be contrary to the objective of Regulation No 1049/2001, namely the widest possible public access to documents held by the institutions.

108 Moreover, given that access to a document will be refused under Article 4(1)(b) of Regulation No 1049/2001 where disclosure would undermine protection of the privacy and the integrity of the individual, a transfer that does not fall under that exception cannot, in principle, prejudice the legitimate interests of the person concerned within the meaning of Article 8(b) of Regulation No 45/2001.

109 As regards the data subject's right to object, Article 18 of Regulation No 45/2001 provides that that person has the right to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her, except in cases covered by, in particular, Article 5(b) of that regulation. Therefore, given that the processing envisaged by Regulation No 1049/2001 constitutes a legal obligation for the purposes of Article 5(b) of Regulation No 45/2001, the data subject does not, in principle, have a right to object. However, since Article 4(1)(b) of Regulation No 1049/2001 lays down an exception to that legal obligation, it is necessary to take into account, on that basis, the impact of the disclosure of data concerning the data subject.'

26 Finally, the General Court held that the exception under Article 4(1)(b) of Regulation No 1049/2001 had to be interpreted restrictively and concerned only personal data that were capable of actually and specifically undermining the protection of privacy and the integrity of the individual. Examination as to whether a person's private life might be undermined had to be carried out in the light of Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 ('the ECHR') and the case-law based thereon.

27 The Court concluded generally in paragraph 133, and specifically in paragraph 139 of the judgment under appeal, that the Commission had erred in law by holding that Bavarian Lager had not established either an express and legitimate purpose or any need to obtain the names of the five persons who participated in the meeting of 11 October 1996 and who, after that meeting, objected to communication of their identity to Bavarian Lager.

28 As regards the exception concerning protection of the purpose of inspections, investigations and audits laid down in Article 4(2), third indent, of Regulation No 1049/2001, the General Court found in general that that provision could not be applied to the

present case, and, in particular, it held that confidential treatment could not be granted to persons other than the complainant and that that protection was justified only if the procedure in question was still in progress.

Procedure before the Court and forms of order sought

29 By order of the President of the Court of Justice of 13 June 2008, the United Kingdom of Great Britain and Northern Ireland and the Council of the European Union were granted leave to intervene in support of the Commission. The Republic of Finland and the Kingdom of Sweden were granted leave to intervene in support of Bavarian Lager, and the Kingdom of Denmark was granted leave to intervene in support of Bavarian Lager and the European Data Protection Supervisor.

30 The Commission claims that the Court should:

— set aside the judgment under appeal, in so far as it annuls the contested decision;

— give a final ruling on the questions which form the subject-matter of the present appeal; and

— order Bavarian Lager to pay the costs incurred by it at first instance and in the current appeal, or, should it be unsuccessful, order it to pay half the costs incurred by Bavarian Lager at first instance.

31 The Council contends that the Court should:

— set aside the judgment under appeal, and

— order Bavarian Lager to pay the costs.

32 The United Kingdom contends that the Court should:

— uphold the appeal by the Commission and grant the forms of order sought by the latter.

33 Bavarian Lager contends that the Court should:

— dismiss the Commission's appeal in its entirety, and

— order the Commission to pay the costs incurred by Bavarian Lager at first instance and in the present appeal, or, should the appeal be upheld, order each of the parties to bear its own costs.

34 The Kingdom of Denmark, the Republic of Finland, the Kingdom of Sweden and the European Data Protection Supervisor contend that the Court should:

— dismiss the appeal in its entirety.

The application for reopening of the oral procedure

35 By letters of 11 and 13 November 2009, the Commission and the European Data Protection Supervisor applied for the reopening of the oral procedure.

36 The Court may of its own motion, or on a proposal from the Advocate General, or at the request of the parties, order the reopening of the oral procedure in accordance with Article 61 of the Rules of Procedure if it considers that it lacks sufficient information, or that the case must be dealt with on the basis of an argument which has not been debated between the parties (Case C-42/07 *Liga Portuguesa de Futebol Profissional and Bwin International* [2009] ECR I-7633, paragraph 31 and case-law cited).

37 In their applications, the Commission and the European Data Protection Supervisor restrict themselves to claiming that the Advocate General's Opinion was based on arguments that were not debated either before the General Court or before the Court of Justice.

38 The Court considers that it has all the material necessary for it to decide the dispute before it and that the case does not have to be examined in the light of an argument that has not been the subject of discussion before it.

39 Therefore, there is no need to reopen the oral procedure.

The appeal

40 In support of its appeal, the Commission puts forward three grounds, namely:

— the General Court, by declaring that Article 8(b) of Regulation No 45/2001 was not applicable to this case, misinterpreted and misapplied Article 4(1)(b) of Regulation No 1049/2001;

— by interpreting restrictively the condition in Article 4(1)(b) of Regulation No 1049/2001, the General Court erred in law by excluding from its scope the Community legislation on protection of personal data contained in a document; and

— as regards the interpretation of Article 4(2), third indent, of Regulation No 1049/2001, the General Court wrongly limited the protection of confidentiality of investigations to complainants only, and, for that confidentiality to be maintained, required that the investigation be still current.

Findings of the Court

41 Since the first two pleas largely overlap, it will be convenient to examine them together.

42 The Commission, supported by the United Kingdom and the Council, argues in essence that the General Court made errors of law in its findings concerning the application of the exemption in Article 4(1)(b) of Regulation No 1049/2001 and thereby rendered certain provisions of Regulation No 45/2001 ineffective.

43 The Commission considers that the General Court ruled without reference to the second part of the sentence in Article 4(1)(b) of Regulation No 1049/2001, which provides that institutions are to refuse access to a document where disclosure would undermine the protection of privacy and the integrity of the individual, 'in particular in accordance with Community legislation regarding the protection of personal data'. The General Court interpreted the exception laid down in Article 4(1)(b) of Regulation No 1049/2001 only in the light of Article 8 of the ECHR and the case-law based thereon.

44 That erroneous interpretation of the exception laid down by the said Article 4(1)(b) had the consequence of rendering ineffective several provisions of Regulation No 45/2001, and in particular Articles 8(b) and 18(a) of that regulation.

45 It is precisely, the Commission argues, by giving precedence to Article 6(1) of Regulation No 1049/2001, which provides that, in the context of requests from the public for access to documents, the applicant is not obliged to state reasons for the application, that the General Court renders ineffective Article 8(b) of Regulation No 45/2001, which requires the recipient of a transfer of personal data to demonstrate the need for their disclosure.

46 The obligation on a recipient of a transfer of personal data to demonstrate that a legitimate purpose is being pursued, contained in Article 8(b) of Regulation 45/2001 is, the Commission submits, one of the key provisions of the whole of the Union legislation concerning data protection. Thus, communication of personal data appearing in a document held by an institution constitutes not only public access to a document under Regulation No 1049/2001, but also a processing of personal data under Regulation No 45/2001, which the General Court did not take into account.

47 The Commission adds that the General Court, in holding that any request for personal data must comply with the legal obligation arising from the right of public access, within the meaning of Article 5(b) of Regulation No 45/2001, renders devoid of purpose Article 18(a) of that regulation, which confers on the data subject the right to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her.

48 It should be noted that the General Court devotes a significant part of its reasoning, and in particular paragraphs 96 to 119 of the judgment under appeal, to the relationship between Regulations Nos 45/2001 and 1049/2001 and then applies, in paragraphs 121 to 139 of that judgment, the criteria which it inferred therefrom to this case.

49 As the General Court rightly states in paragraph 98 of the judgment under appeal, when examining the relationship between Regulations Nos 1049/2001 and 45/2001 for the purpose of applying the exception under Article 4(1)(b) of Regulation No 1049/2001 to the case in point, it must be borne in mind that those regulations have different objectives. The first is designed to ensure the greatest possible transparency of the decision-making process of the public authorities and the information on which they base their decisions. It is thus designed to facilitate as far as possible the exercise of the right of access to documents, and to promote good administrative practices. The second is designed to ensure the protection of the freedoms and fundamental rights of individuals, particularly their private life, in the handling of personal data.

50 As stated in recital 2 of Regulation No 45/2001, the Union legislature intended to establish a 'fully-fledged system' of protection of personal data, and considered it necessary, in the words of recital 12 thereof, to ensure throughout the Community 'consistent and homogeneous application of the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data'.

51 According to that same recital 12, the rights conferred on data subjects for their protection with regard to the processing of personal data constitute rules for the protection of fundamental rights and freedoms. In the mind of the Union legislature, the Union legislation on the processing of personal data serves to protect fundamental rights and freedoms.

52 According to recitals 7 and 14 of Regulation No 45/2001, the measures in question are 'binding measures' which apply to 'all processing of personal data by all Community institutions and bodies' and 'in any context whatsoever'.

53 As indicated in recital 1 thereof, Regulation No 1049/2001 forms part of the intention expressed in the second paragraph of Article 1 EU to mark a new stage in the process of creating an ever closer union among the peoples of Europe, in which decisions are taken as openly as possible and as closely as possible to the citizen.

54 According to recital 2 of that regulation, openness enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system.

55 Regulation No 1049/2001 lays down as a general rule that the public may have access to the documents of the institutions, but provides for exceptions by reason of certain public and private interests. In particular, recital 11 of that regulation states that, '[i]n assessing the exceptions, the institutions should take account of the principles in Community legislation concerning the protection of personal data, in all areas of Union activities'.

56 Regulations Nos 45/2001 and 1049/2001 were adopted on dates very close to each other. They do not contain any provisions granting one regulation primacy over the other. In principle, their full application should be ensured.

57 The only express link between those two regulations is established in Article 4(1)(b) of Regulation No 1049/2001, which provides for an exception to access to a document where disclosure would undermine the protection of privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data.

58 In this case, in paragraphs 111 to 120 of the judgment under appeal, the General Court limits the application of the exception under Article 4(1)(b) of that regulation to situations in which privacy or the integrity of the individual would be infringed for the purposes of Article 8 of the ECHR and the case-law of the European Court of Human Rights, without taking into account the legislation of the Union concerning the protection of personal data, particularly Regulation No 45/2001.

59 It should be observed that, in acting in that way, the General Court disregards the wording of Article 4(1)(b) of Regulation No 1049/2001, which is an indivisible provision and requires that any undermining of privacy and the integrity of the individual must always be examined and assessed in conformity with the legislation of the Union concerning the protection of personal data, and in particular with Regulation No 45/2001.

60 Article 4(1)(b) of Regulation No 1049/2001 establishes a specific and reinforced system of protection of a person whose personal data could, in certain cases, be communicated to the public.

61 According to Article 1(1) of Regulation No 45/2001, the purpose of that regulation is to 'protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'. That provision does not allow cases of processing of personal data to be separated into two categories, namely a category in which that treatment is examined solely on the basis of Article 8 of the ECHR and the case-law of the European Court of Human Rights relating to that article and another category in which that processing is subject to the provisions of Regulation No 45/2001.

62 It is clear from the first sentence of recital 15 of Regulation No 45/2001 that the Union legislature has pointed to the need to apply Article 6 EU and, by that means, Article 8 of the ECHR, '[w]here such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation, in particular those laid down in Titles V and VI of the [EU Treaty in its version prior to the Treaty of Lisbon]'. By contrast, such a reference was not found necessary for processing carried out in the exercise of activities within the scope of that regulation, given that, in such cases, it is clearly Regulation No 45/2001 itself which applies.

63 It follows that, where a request based on Regulation No 1049/2001 seeks to obtain access to documents including personal data, the provisions of Regulation No 45/2001 become applicable in their entirety, including Articles 8 and 18 thereof.

64 By not taking account of the reference in Article 4(1)(b) of Regulation No 1049/2001 to the legislation of the Union concerning the protection of personal data and thus to Regulation No 45/2001, the General Court dismissed at the outset, in paragraph 107 of the judgment under appeal, the application of Article 8(b) of Regulation No 45/2001, and, in paragraph 109 of the judgment under appeal, the application of Article 18 of Regulation No 45/2001. And yet those articles constitute essential provisions of the system of protection established by Regulation No 45/2001.

65 Consequently, the particular and restrictive interpretation which the General Court gave to Article 4(1)(b) of Regulation No 1049/2001 does not correspond to the equilibrium which the Union legislature intended to establish between the two regulations in question.

66 In this case, it is apparent from the information on the file, and in particular from the contested decision, that, following the requests by Bavarian Lager of 4 May 1998, 5 December 2003 and 9 February 2004, the Commission sent the latter a document containing the minutes of the meeting of 11 October 1996, with five names removed. Of those five names, three persons could not be contacted by the Commission in order to give their consent, and two others expressly objected to the disclosure of their identity.

67 In refusing full access to that document, the Commission based its reasoning on Article 4(1)(b) of Regulation No 1049/2001 and Article 8 of Regulation No 45/2001.

68 It should be noted that, in paragraph 104 of the judgment under appeal, the General Court, in examining Article 2(a) of Regulation No 45/2001, that is to say the definition of the concept of 'personal data', correctly held that surnames and forenames may be regarded as personal data.

69 It also correctly established, in paragraph 105 of that judgment, in examining Article 2(b) of that regulation, that is to say the definition of the concept of 'processing of personal data', that the communication of such data falls within the definition of 'processing', for the purposes of that regulation.

70 The General Court was right to conclude, in paragraph 122 of the judgment under appeal, that the list of participants in the meeting of 11 October 1996 appearing in the minutes of that meeting thus contains personal data for the purposes of Article 2(a) of Regulation No 45/2001, since the persons who participated in that meeting can be identified.

71 Therefore, the decisive question is whether the Commission could grant access to the document including the five names of the participants in the meeting of 11 October 1996, in compliance with Article 4(1)(b) of Regulation No 1049/2001 and Regulation No 45/2001.

72 First of all, it should be noted that Bavarian Lager was able to have access to all the information concerning the meeting of 11 October 1996, including the opinions which those contributing expressed in their professional capacity.

73 The Commission, at the time of the first request by Bavarian Lager dated 4 May 1998, sought the agreement of the participants at the meeting of 11 October 1996 to the disclosure of their names. As the Commission indicates in the decision of 18 March 2003, that procedure was in compliance with the requirements of Directive 95/46, in force at that time.

74 Following a new request by Bavarian Lager to the Commission, dated 5 December 2003, seeking communication of the full minutes of the meeting of 11 October 1996, the Commission informed Bavarian Lager on 27 January 2004 that, having regard to the entry into force of Regulations Nos 45/2001 and 1049/2001, it was henceforward obliged to treat that request under the specific regime of those regulations, particularly Article 8(b) of Regulation No 45/2001.

75 Whether under the former system of Directive 95/46 or under the system of Regulations Nos 45/2001 and 1049/2001, the Commission was right to verify whether the data subjects had given their consent to the disclosure of personal data concerning them.

76 This Court finds that, by releasing the expurgated version of the minutes of the meeting of 11 October 1996 with the names of five participants removed therefrom, the Commission did not infringe the provisions of Regulation No 1049/2001 and sufficiently complied with its duty of openness.

77 By requiring that, in respect of the five persons who had not given their express consent, Bavarian Lager establish the necessity for those personal data to be transferred, the Commission complied with the provisions of Article 8(b) of Regulation No 45/2001.

78 As Bavarian Lager has not provided any express and legitimate justification or any convincing argument in order to demonstrate the necessity for those personal data to be transferred, the Commission has not been able to weigh up the various interests of the parties concerned. Nor was it able to verify whether there was any reason to assume that the data subjects' legitimate interests might be prejudiced, as required by Article 8(b) of Regulation No 45/2001.

79 It follows from the above that the Commission was right to reject the application for access to the full minutes of the meeting of 11 October 1996.

80 Therefore, the General Court erred in law in concluding, in paragraphs 133 and 139 of the judgment under appeal, that in this case the Commission had wrongly applied Article 4(1)(b) of Regulation No 1049/2001 and held that Bavarian Lager had not established either an express and legitimate purpose in obtaining, or any need to obtain, the document at issue in its entirety.

81 In the light of those considerations as a whole, it is appropriate, without there being any need to examine the other arguments and pleas of the parties, to set aside the judgment under appeal in so far as it annuls the contested decision.

The consequences of the judgment under appeal being set aside

82 In accordance with the first paragraph of Article 61 of the Statute of the Court of Justice, if the Court quashes the decision of the General Court, it may itself give final judgment in the matter, where the state of the proceedings so permits.

83 That is the case here.

84 As the Court has found in paragraphs 69 and 73 of this judgment, the contested decision did not infringe the provisions of Regulations Nos 45/2001 and 1049/2001.

85 The action for annulment by Bavarian Lager against that decision must therefore be dismissed.

Costs

86 Pursuant to the first paragraph of Article 122 of the Rules of Procedure, where the appeal is well founded and the Court of Justice itself gives final judgment in the case, the Court is to make a decision as to costs. Under Article 69(2) of those rules, which applies to appeal proceedings by virtue of Article 118 thereof, the unsuccessful party is to be ordered to pay the costs, if they have been applied for in the successful party's pleadings. Under Article 69(4) of those rules, which applies to appeal proceedings by virtue of Article 118 thereof, Member States and institutions which intervene in the proceedings are to bear their own costs. The Court may order an intervener to bear its own costs.

87 Since the Commission has applied for costs and Bavarian Lager has been unsuccessful in the appeal, Bavarian Lager must be ordered to pay the costs relating to the appeal.

88 Since the Commission has also applied for an order that Bavarian Lager pay the costs of the procedure before the General Court and the action before that Court has been dismissed, Bavarian Lager must be ordered to pay the costs relating to the procedure at first instance.

89 The Kingdom of Denmark, the Republic of Finland, the Kingdom of Sweden, the United Kingdom, the Council and the European Data Protection Supervisor must be ordered to bear their own costs.

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

1. **Sets aside the judgment of the Court of First Instance of the European Communities of 8 November 2007 in Case T-194/04 *Bavarian Lager* v *Commission*, in so far as it annuls the Commission's decision of 18 March 2004, rejecting an application for access to the full minutes of the meeting of 11 October 1996, including all the names, and in so far as it orders the European Commission to pay the costs of The Bavarian Lager Co. Ltd;**

2. **Dismisses the action of The Bavarian Lager Co. Ltd against the Commission's decision of 18 March 2004, rejecting an application for access to the full minutes of the meeting of 11 October 1996, including all the names;**

3. **Orders The Bavarian Lager Co. Ltd to pay the costs incurred by the European Commission both in the context of the present appeal proceedings and before the Court of First Instance;**

4. **Orders the Kingdom of Denmark, the Republic of Finland, the Kingdom of Sweden, the United Kingdom of Great Britain and Northern Ireland, the Council of the European Union and the European Data Protection Supervisor to bear their own costs.**

[Signatures]

JUDGMENT OF THE COURT (Grand Chamber)

9 November 2010 *

In Joined Cases C-92/09 and C-93/09,

REFERENCES for preliminary rulings under Article 234 EC from the Verwaltungsgericht Wiesbaden (Germany), made by decisions of 27 February 2009, received at the Court on 6 March 2009, in the proceedings

Volker und Markus Schecke GbR (C-92/09),

Hartmut Eifert (C-93/09)

v

Land Hessen,

joined party:

Bundesanstalt für Landwirtschaft und Ernährung,

* Language of the cases: German.

THE COURT (Grand Chamber),

composed of V. Skouris, President, A. Tizzano, J.N. Cunha Rodrigues, K. Lenaerts (Rapporteur), J.-C. Bonichot, K. Schiemann, A. Arabadjiev and J.-J. Kasel, Presidents of Chambers, E. Juhász, C. Toader and M. Safjan, Judges,

Advocate General: E. Sharpston,
Registrar: B. Fülöp, Administrator,

having regard to the written procedure and further to the hearing on 2 February 2010,

after considering the observations submitted on behalf of:

— Volker und Markus Schecke GbR, by R. Seimetz and P. Breyer, Rechtsanwälte, and by Mr Schecke,

— Mr Eifert, by R. Seimetz and P. Breyer, Rechtsanwälte,

— Land Hessen, by H.-G. Kamann, Rechtsanwalt,

— the Greek Government, by V. Kontolaimos, I. Chalkias, K. Marinou and V. Karra, acting as Agents,

— the Netherlands Government, by C. Wissels and Y. de Vries, acting as Agents,

— the Swedish Government, by A. Falk and C. Meyer-Seitz, acting as Agents,

— the Council of the European Union, by E. Sitbon and Z. Kupčová, acting as Agents,

— the European Commission, by B. Smulders, F. Erlbacher and P. Costa de Oliveira, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 17 June 2010,

gives the following

Judgment

1 These references for preliminary rulings concern the validity, first, of Articles 42(8b) and 44a of Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy (OJ 2005 L 209, p. 1), as amended by Council Regulation (EC) No 1437/2007 of 26 November 2007 (OJ 2007 L 322, p. 1) ('Regulation No 1290/2005'), and, second, of Commission Regulation (EC) No 259/2008 of 18 March 2008 laying down detailed rules for the application of Regulation No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD) (OJ 2008 L 76, p. 28) and Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54). Should the Court find that the European Union legislation referred to above is not invalid, the references for preliminary rulings also concern the interpretation of Article 7, the second indent of Article 18(2) and Article 20 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 (OJ 1995 L 281, p. 31).

2 Those questions have been raised in the course of proceedings between Volker und Markus Schecke GbR and Mr Eifert ('the applicants in the main proceedings') and Land Hessen (the *Land* of Hesse) concerning the publication on the internet site of the Bundesanstalt für Landwirtschaft und Ernährung (Federal Office for Agriculture and Food; 'the Bundesanstalt') of personal data relating to them as recipients of funds from the EAGF or the EAFRD.

I — Legal context

A — *European Convention for the Protection of Human Rights and Fundamental Freedoms*

3 Under the heading 'Right to respect for private and family life', Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950, ('the Convention') 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.'

B — *European Union law*

1. Directive 95/46

4 In accordance with Article 1(1) of Directive 95/46, the aim of the directive is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Under Article 2(a) of the directive, 'personal data' means 'any information relating to an identified or identifiable natural person'.

5 Under Article 7 of that directive, 'Member States shall provide that personal data may be processed only if:

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

or

…

(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; …

…'

6 Under Article 18(1) of the directive, 'Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation'.

7 Under the second indent of Article 18(2) of the directive, Member States may provide for the simplification of or exemption from notification inter alia in the following case:

'where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

— for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive;

— for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21(2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.'

8 Article 19(1) of Directive 95/46 provides:

'Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

…'

9 Article 20 of the directive, 'Prior checking', provides in paragraphs 1 and 2:

'1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.'

10 In accordance with the first and second subparagraphs of Article 21(2) of Directive 95/46, 'Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority', and '[t]he register shall contain at least the information listed in Article 19(1)(a) to (e)'.

11 Under Article 28 of the directive, each Member State is to designate one or more public authorities ('supervisory authority') to be responsible for monitoring, acting with complete independence, the application within that State's territory of the national provisions adopted pursuant to that directive.

2. Regulation (EC) No 45/2001

12 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) provides in Article 27(1) and (2):

'1. Processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes shall be subject to prior checking by the European Data Protection Supervisor.

2. The following processing operations are likely to present such risks:

(a) processing of data relating to health and to suspected offences, offences, criminal convictions or security measures;

(b) processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct;

(c) processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes;

(d) processing operations for the purpose of excluding individuals from a right, benefit or contract.'

3. Directive 2006/24

13 Directive 2006/24 requires the Member States to retain for a certain time data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

4. Regulation No 1290/2005

14 Regulation No 1290/2005 sets the specific requirements and rules on the financing of expenditure falling under the common agricultural policy ('the CAP').

15 Article 42 of Regulation No 1290/2005 provides that the detailed rules for the application of that regulation are to be adopted by the European Commission. Under Article 42(8b) of the regulation, the Commission is to determine inter alia:

'the detailed rules on the publication of information concerning beneficiaries referred to in Article 44a and on the practical aspects related to the protection of individuals with regard to the processing of their personal data in accordance with the principles laid down in Community legislation on data protection. These rules shall ensure, in particular, that the beneficiaries of funds are informed that these data may be made public and may be processed by auditing and investigating bodies for the purpose of safeguarding the financial interests of the Communities, including the time that this information shall take place.'

16 Article 44a of Regulation No 1290/2005, 'Publication of the beneficiaries', states:

'… Member States shall ensure annual *ex-post* publication of the beneficiaries of the EAGF and the EAFRD and the amounts received per beneficiary under each of these Funds.

The publication shall contain at least:

(a) for the EAGF, the amount subdivided in direct payments within the meaning of Article 2(d) of Regulation (EC) No 1782/2003 and other expenditure;

(b) for the EAFRD, the total amount of public funding per beneficiary.'

17 Recitals 13 and 14 in the preamble to Regulation No 1437/2007 amending Regulation No 1290/2005 read as follows:

'(13) In the context of the revision of Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities [OJ 2002 L 248, p. 1], the provisions on the annual *ex-post* publication of beneficiaries of funds deriving from the budget were inserted into that Regulation in order to implement the European Transparency Initiative. Sector-specific Regulations are to provide the means for such a publication. Both the EAGF and the EAFRD form part of the general budget of the European Communities and finance expenditure in a context of shared management between the Member States and the Community. Rules should therefore be laid down for the publication of information on the beneficiaries of these Funds. To that end, Member States should ensure annual *ex-post* publication of the beneficiaries and the amounts received per beneficiary under each of these Funds.

(14) Making this information accessible to the public enhances transparency regarding the use of Community funds in the [CAP] and improves the sound financial management of these funds, in particular by reinforcing public control of the money used. Given the overriding weight of the objectives pursued, it is justified with regard to the principle of proportionality and the requirement of the protection of personal data to provide for the general publication of the relevant information as it does not go beyond what is necessary in a

democratic society and for the prevention of irregularities. Taking into account the opinion of the European Data Protection Supervisor of 10 April 2007 [OJ 2007 C 134, p. 1], it is appropriate to make provision for the beneficiaries of funds to be informed that those data may be made public and that they may be processed by auditing and investigating bodies.'

5. Regulation No 259/2008

18 On the basis of Article 42(8b) of Regulation No 1290/2005, the Commission adopted Regulation No 259/2008.

19 Recital 6 in the preamble to Regulation No 259/2008 reads as follows:

'(6) Making … information [concerning beneficiaries of funds from the EAGF and EAFRD] accessible to the public enhances transparency regarding the use of Community funds in the [CAP] and improves the sound financial management of these funds, in particular by reinforcing public control of the money used. Given the overriding weight of the objectives pursued, it is justified with regard to the principle of proportionality and the requirement of the protection of personal data to provide for the general publication of the relevant information as it does not go beyond what is necessary in a democratic society and for the prevention of irregularities.'

20 Recital 7 in the preamble states that '[t]o comply with the data protection requirements beneficiaries of the Funds should be informed of the publication of their data before the publication takes place'.

21 Article 1(1) of Regulation No 259/2008 specifies the content of the publication referred to in Article 44a of Regulation No 1290/2005 and provides that it is to include the following information:

'(a) the first name and the surname where the beneficiaries are natural persons;

(b) the full legal name as registered where the beneficiaries are legal persons;

(c) the full name of the association as registered or otherwise officially recognised where the beneficiaries are associations of natural or legal persons without an own legal personality;

(d) the municipality where the beneficiary resides or is registered and, where available, the postal code or the part thereof identifying the municipality;

(e) for the … EAGF, the amount of direct payments within the meaning of Article 2(d) of Regulation (EC) No 1782/2003 received by each beneficiary in the financial year concerned;

(f) for the EAGF, the amount of payments other than those referred to in point (e) received by each beneficiary in the financial year concerned;

(g) for the … EAFRD, the total amount of public funding received by each beneficiary in the financial year concerned, which includes both the Community and the national contribution;

(h) the sum of the amounts referred to in points (e), (f) and (g) received by each beneficiary in the financial year concerned;

(i) the currency of these amounts.'

22 In accordance with Article 2 of Regulation No 259/2008, '[the] information referred to in Article 1 shall be made available on a single website per Member State through a search tool allowing the users to search for beneficiaries by name, municipality, amounts received as referred to in (e), (f), (g) and (h) of Article 1 or a combination thereof and to extract all the corresponding information as a single set of data.'

23 Article 3(3) of that regulation provides that '[t]he information shall remain available on the website for two years from the date of [its] initial publication.'

24 Article 4 of Regulation No 259/2008 provides:

'1. Member States shall inform the beneficiaries that their data will be made public in accordance with Regulation … No 1290/2005 and this Regulation and that they may be processed by auditing and investigating bodies of the Communities and the Member States for the purpose of safeguarding the Communities' financial interests.

2. In case of personal data, the information referred to in paragraph 1 shall be provided in accordance with the requirements of Directive 95/46 … and the beneficiaries shall be informed of their rights as data subjects under this Directive and of the procedures applicable for exercising these rights.

3. The information referred to in paragraphs 1 and 2 shall be provided to the beneficiaries by including it in the application forms for receiving funds deriving from the EAGF and EAFRD, or otherwise at the time when the data are collected.

…'

II — The actions in the main proceedings and the questions referred for preliminary rulings

25 The applicants in the main proceedings, one established and the other resident in the *Land* of Hesse, are an agricultural undertaking in the legal form of a partnership (Case C-92/09) and a full-time farmer (Case C-93/09). For the financial year 2008 they made applications to the competent local authorities for funds from the EAGF or the EAFRD, which were approved by decisions of 5 December 2008 (Case C-93/09) and 31 December 2008 (Case C-92/09).

26 In each case the application form contained the following statement:

'I am aware that Article 44a of Regulation … No 1290/2005 requires publication of information on the beneficiaries of [funds from] the EAGF and the EAFRD and the amounts received per beneficiary. The publication relates to all measures applied for in connection with the Common Application, which constitutes the single application for the purposes of Article 11 of Regulation (EC) No 796/2004, and is effected annually at the latest by 31 March of the following year.'

27 The referring court explains that the Bundesanstalt's website makes available to the public the names of beneficiaries of aid from the EAGF and the EAFRD, the place in

which they are established or reside and the postcode of that place, and the annual amounts received. The site is provided with a search tool.

28 On 26 September 2008 (Case C-92/09) and 18 December 2008 (Case C-93/09) the applicants in the main proceedings brought proceedings to prevent publication of the data relating to them. In their view, publication of the amounts received from the EAGF or the EAFRD is not justified by overriding public interests. Moreover, the rules governing the European Social Fund do not provide for beneficiaries to be identified by name. In their applications, they ask for the *Land* of Hesse to be ordered to refrain from, or to be prohibited from, transmitting or publishing those data for the purposes of the general publication of information on the financial amounts granted to them from the EAGF and the EAFRD.

29 The *Land* of Hesse, which takes the view that the obligation to publish data relating to the applicants in the main proceedings follows from Regulations No 1290/2005 and No 259/2008, nevertheless undertook not to publish the amounts received by them as beneficiaries of aid from the EAGF and the EAFRD pending final decisions in the main proceedings.

30 The referring court believes that the obligation to publish under Article 44a of Regulation No 1290/2005 constitutes an unjustified interference with the fundamental right to the protection of personal data. It considers that that provision, which pursues the aim of increasing the transparency of the use of European funds, does not improve the prevention of irregularities, since extensive control mechanisms exist at present for that purpose. On the basis of the judgment in Joined Cases C-465/00, C-138/01

and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, it takes the view that, in any event, that obligation to publish is not proportionate to the aim pursued. Moreover, in its view, Article 42(8b) of Regulation No 1290/2005 gives the Commission too broad a discretion with respect to determining both the data to be published and the means of publication and is therefore incompatible with the third indent of Article 202 EC and with the fourth indent of Article 211 EC.

31 Regardless of the validity of Articles 42(8b) and 44a of Regulation No 1290/2005, the referring court considers that Regulation No 259/2008, which prescribes that the information relating to the beneficiaries of aid from the EAGF and the EAFRD is to be published exclusively on the internet, breaches the fundamental right to the protection of personal data. It points out that the latter regulation does not limit access to the internet site concerned to 'internet protocol' (IP) addresses situated in the European Union. Furthermore, it is not possible to withdraw the data from the internet after the expiry of the two-year period laid down in Article 3(3) of Regulation No 259/2008. It its view, publication of the data exclusively on the internet also has a deterrent effect. First, citizens wishing to obtain information must have access to the internet. Second, those citizens run the risk of having their data stored under Directive 2006/24. It is paradoxical to strengthen the supervision of telecommunications on the one hand and to provide on the other hand that information which is intended to enable citizens to participate in public affairs is available only electronically.

32 In case the Court should find that the provisions referred to in paragraphs 30 and 31 above are not invalid, the referring court further seeks an interpretation of a number of provisions of Directive 95/46. It considers that the publication of personal data may take place only if the measures provided for in the second indent of Article 18(2) of that directive have been taken. According to the information provided by the referring court, the German legislature, in particular that of the *Land* of Hesse, has made use of the possibility under that provision. However, according to that court,

the notification by the Ministry of the Environment, Rural Affairs and Consumer Protection of the *Land* of Hesse to the personal data protection official was incomplete. Some information was not communicated to that official, such as the fact that the data are processed by the Bundesanstalt on behalf of the *Land*, in some cases with the assistance of a private third party, specific details of the deletion period and the access provider, and information on the registration of IP addresses.

33 Moreover, according to the national court, the publication of the data relating to the beneficiaries of agricultural aid ought to have been preceded by a prior check as provided for in Article 20 of Directive 95/46. In the present case, however, a prior check was carried out, not by a central supervisory authority, but by the data protection official of the undertaking or office responsible, on the basis of incomplete notifications.

34 Finally, the referring court is uncertain as to the lawfulness, from the point of view of Article 7(e) of Directive 95/46, of the registration of the IP addresses of users who consult the information relating to beneficiaries of aid from the EAGF and the EAFRD on the Bundesanstalt's website.

35 In those circumstances, the Verwaltungsgericht (Administrative Court) Wiesbaden decided to stay the proceedings and to refer the following questions, which are worded identically in Case C-92/09 and Case C-93/09, to the Court for preliminary rulings:

'1. Are Article [42](8b) and Article 44a of … Regulation … No 1290/2005 …, inserted by … Regulation … No 1437/2007 …, invalid?

2. Is … Regulation … No 259/2008 …

   (a) invalid, or

   (b) valid by reason only of the fact that Directive 2006/24 … is invalid?

If the provisions mentioned in the first and second questions are valid:

3. Must the second indent of Article 18(2) of Directive 95/46 … be interpreted as meaning that publication in accordance with … Regulation … No 259/2008 … may be effected only following implementation of the procedure — in lieu of notification to a supervisory authority — established by that article?

4. Must Article 20 of Directive 95/46 … be interpreted as meaning that publication in accordance with … Regulation … No 259/2008 … may be effected only following exercise of the prior check required by national law in that case?

5. If the fourth question is answered in the affirmative: Must Article 20 of Directive 95/46 … be interpreted as meaning that no effective prior check has been performed, if it was effected on the basis of a register established in accordance with the second indent of Article 18(2) of that directive which lacks an item of information prescribed?

6. Must Article 7 — and in this case, in particular, subparagraph (e) — of Directive 95/46 … be interpreted as precluding a practice of storing the IP addresses of the users of a homepage without their express consent?'

36 By order of the President of the Court of 4 May 2009, Cases C-92/09 and C-93/09 were joined for the purposes of the written and oral procedure and the judgment.

III — Consideration of the questions referred

37 The decisions for reference contain questions on the validity of Regulations No 1290/2005 and No 259/2008 (Questions 1 and 2) and questions on the interpretation of Directive 95/46 (Questions 3 to 6). Before examining the substance of the case, the admissibility of the second part of Question 2 and of Question 6 should be considered.

A — *Admissibility*

38 By the second part of Question 2 and by Question 6 respectively, the referring court asks the Court to rule on the validity of Directive 2006/24 and on the interpretation of Article 7(e) of Directive 95/46, so as to enable it to assess whether the retention of certain data relating to the users of the internet sites, laid down by European Union and German legislation, is lawful.

39 It should be recalled at the outset that although, in view of the division of responsibilities in the preliminary-ruling procedure, it is for the referring court alone to determine the subject-matter of the questions which it proposes to refer to the Court, the Court has held that, in exceptional circumstances, it will examine the conditions in which the case was referred to it by the national court, in order to assess whether it has jurisdiction (Case C-567/07 *Woningstichting Sint Servatius* [2009] ECR I-9021, paragraph 42).

40 That is the case in particular where the problem referred to the Court is purely hypothetical or where the interpretation or consideration of the validity of a rule of European Union law which is sought by the national court has no relation to the actual facts of the main action or to its purpose (see, to that effect, Case C-415/93 *Bosman* [1995] ECR I-4921, paragraph 61; Case C-466/04 *Acereda Herrera* [2006] ECR I-5341, paragraph 48; Case C-380/05 *Centro Europa 7* [2008] ECR I-349, paragraph 53; and *Woningstichting Sint Servatius*, paragraph 43).

41 According to the decisions for reference, the applicants in the main proceedings each brought proceedings before the referring court against the publication under Regulations No 1290/2005 and No 259/2008 of data relating to them. Their applications seek for the *Land* of Hesse to refrain from transmitting or publishing, or to refuse to transmit or publish, the information concerning the aid which they have received from the EAGF and the EAFRD.

42 The second part of Question 2 and Question 6 have no relation to the subject-matter of the disputes in the main proceedings. They relate, not to the publication of data relating to the beneficiaries of aid under those Funds, such as the applicants in the main proceedings, but to the retention of data relating to persons consulting websites. Since consideration of the second part of Question 2 and Question 6 is therefore of no relevance for the outcome of the main proceedings, there is no need to answer them.

B — *Substance*

1. Question 1 and the first part of Question 2

(a) Preliminary observations

43 By Question 1 and the first part of Question 2, the national court asks the Court to examine the validity, first, of Article 44a of Regulation No 1290/2005 and of

Regulation No 259/2008 containing the detailed rules for the application of the publication obligation laid down by Article 44a and, second, of Article 42(8b) of Regulation No 1290/2005, the provision which is the legal basis of Regulation No 259/2008.

44 The referring court considers that the obligation to publish data relating to the beneficiaries of aid from the EAGF and the EAFRD, which follows from the provisions cited in the previous paragraph, constitutes an unjustified interference with the fundamental right to the protection of personal data. It refers essentially to Article 8 of the Convention.

45 In accordance with Article 6(1) TEU, the European Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union ('the Charter'), 'which shall have the same legal value as the Treaties'.

46 In those circumstances, the validity of Articles 42(8b) and 44a of Regulation No 1290/2005 and of Regulation No 259/2008 must be assessed in the light of the provisions of the Charter.

47 In this regard, Article 8(1) of the Charter states that '[e]veryone has the right to the protection of personal data concerning him or her'. That fundamental right is closely connected with the right to respect of private life expressed in Article 7 of the Charter.

48 The right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society (see, to that effect, Case C-112/00 *Schmidberger* [2003] ECR I-5659, paragraph 80 and the case-law cited).

49 Article 8(2) of the Charter thus authorises the processing of personal data if certain conditions are satisfied. It provides that personal 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'.

50 Moreover, Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

51 Finally, according to Article 52(3) of the Charter, in so far as it contains rights which correspond to rights guaranteed by the Convention, the meaning and scope of those rights are to be the same as those laid down by the Convention. Article 53 of the Charter further states that nothing in the Charter is to be interpreted as restricting or adversely affecting the rights recognised inter alia by the Convention.

52 In those circumstances, it must be considered that the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual (see, in particular, European Court of Human Rights, *Amann v. Switzerland* [GC], no. 27798/95, § 65, ECHR 2000-II, and *Rotaru v. Romania* [GC], no. 28341/95, § 43, ECHR 2000-V) and the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention.

(b) The validity of Article 44a of Regulation No 1290/2005 and of Regulation No 259/2008

53 It must be recalled, in the first place, that the publication required by Article 44a of Regulation No 1290/2005 and Regulation No 259/2008 implementing that article identifies by name all beneficiaries of aid from the EAGF and the EAFRD, among whom are both natural and legal persons. Having regard to the observations in paragraph 52 above, legal persons can claim the protection of Articles 7 and 8 of the Charter in relation to such identification only in so far as the official title of the legal person identifies one or more natural persons.

54 That is the case with the applicant in the main proceedings in Case C-92/09. The official title of the partnership in question directly identifies natural persons who are its partners.

55 In the second place, it must be ascertained whether Article 44a of Regulation No 1290/2005 and Regulation No 259/2008 interfere with the rights guaranteed by Articles 7 and 8 of the Charter to beneficiaries of aid from the EAGF or the EAFRD who are identified or identifiable natural persons ('the beneficiaries concerned'), and, if so, whether such an interference is justified having regard to Article 52 of the Charter.

(i) Existence of an interference with the rights recognised by Articles 7 and 8 of the Charter

56 Article 44a of Regulation No 1290/2005 requires the Member States to ensure the annual *ex-post* publication of the names of the beneficiaries of aid from the EAGF and the EAFRD and the amounts received by each beneficiary from each of those Funds. It follows from recital 14 in the preamble to Regulation No 1437/2007 amending Regulation No 1290/2005 that that information must be the subject of 'general publication'.

57 Article 1(1)(d) of Regulation No 259/2008 lays down the content of the publication and prescribes that, in addition to the matters mentioned in the preceding paragraph and other information regarding the aid received, 'the municipality where the beneficiary resides or is registered and, where available, the postal code or the part thereof identifying the municipality' must be published. Article 2 of that regulation prescribes that the information is to be made available on a single website per Member State and may be consulted by means of a search tool.

58 It is not disputed that the amounts which the beneficiaries concerned receive from the EAGF and the EAFRD represent part of their income, often a considerable part. Because the information becomes available to third parties, publication on a website of data naming those beneficiaries and indicating the precise amounts received by them thus constitutes an interference with their private life within the meaning of Article 7 of the Charter (see, to that effect, *Österreichischer Rundfunk and Others*, paragraphs 73 and 74).

59 It is of no relevance in this respect that the data published concerns activities of a professional nature (see *Österreichischer Rundfunk and Others*, paragraphs 73 and 74). The European Court of Human Rights has held on this point, with reference to the interpretation of Article 8 of the Convention, that the term 'private life' must not be interpreted restrictively and that 'there is no reason of principle to justify excluding activities of a professional … nature from the notion of"private life"' (see, inter alia, *Amann v. Switzerland*, § 65, and *Rotaru v. Romania*, § 43).

60 Moreover, the publication required by Article 44a of Regulation No 1290/2005 and Regulation No 259/2008 constitutes the processing of personal data falling under Article 8(2) of the Charter.

61 The *Land* of Hesse casts doubt, however, on the very existence of an interference with the private life of the applicants in the main proceedings, as they were informed in the aid application form of the mandatory publication of the data relating to them and, in accordance with Article 8(2) of the Charter, gave their consent to that publication by submitting their applications.

62 On this point, it should be noted that Article 42(8b) of Regulation No 1290/2005 provides only that 'the beneficiaries of funds are informed that these data [concerning

them, namely their names and the amounts received from each of the Funds] may be made public'. Article 4(1) of Regulation No 259/2008 contains a similar provision, stating that 'Member States shall inform the beneficiaries that their data will be made public'.

63 The European Union legislation in question, which merely provides that beneficiaries of aid are to be informed in advance that the data concerning them will be published, thus does not seek to base the personal data processing for which it provides on the consent of the beneficiaries concerned. Furthermore, it must be noted that in the main proceedings, in their aid application forms, the applicants stated only that they were 'aware that Article 44a of Regulation … No 1290/2005 requires publication of information on the beneficiaries of [funds from] the EAGF and the EAFRD'.

64 Since the publication of data by name relating to the beneficiaries concerned and the precise amounts received by them from the EAGF and the EAFRD constitutes an interference, as regards those beneficiaries, with the rights recognised by Articles 7 and 8 of the Charter, and since such processing of personal data is not based on the consent of those beneficiaries, it is necessary to examine whether the interference is justified having regard to Article 52(1) of the Charter.

ii) Justification of the interference with the rights recognised by Articles 7 and 8 of the Charter

65 Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms, and,

subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

66 First, it is common ground that the interference arising from the publication on a website of data by name relating to the beneficiaries concerned must be regarded as 'provided for by law' within the meaning of Article 52(1) of the Charter. Articles 1(1) and 2 of Regulation No 259/2008 expressly provide for such publication.

67 Second, on the question whether that interference meets an objective of general interest recognised by the European Union within the meaning of Article 52(1) of the Charter, it follows from recital 14 in the preamble to Regulation No 1437/2007 amending Regulation No 1290/2005 and from recital 6 in the preamble to Regulation No 259/2008 that publication of the names of the beneficiaries of aid from the EAGF and the EAFRD and of the amounts which they receive from those Funds is intended to '[enhance] transparency regarding the use of Community funds in the [CAP] and [improve] the sound financial management of these funds, in particular by reinforcing public control of the money used'.

68 The principle of transparency is stated in Articles 1 TEU and 10 TEU and in Article 15 TFEU. It enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system (see Case C-41/00 P *Interporc* v *Commission* [2003] ECR I-2125, paragraph 39, and Case C-28/08 P *Commission* v *Bavarian Lager* [2010] ECR I-6055, paragraph 54).

69 By reinforcing public control of the use of the money from the EAGF and the EAFRD, the publication required by the provisions whose validity is contested contributes to the appropriate use of public funds by the administration (see, to that effect, *Österreichischer Rundfunk and Others*, paragraph 81).

70 Moreover, that publication relating to the use of money paid out by the agricultural Funds will enable citizens to participate more closely in the public debate surrounding decisions on the direction to be taken by the CAP.

71 Consequently, by aiming to increase the transparency of the use of funds in the context of the CAP, Article 44a of Regulation No 1290/2005 and Regulation No 259/2008 pursue an objective of general interest recognised by the European Union.

72 Third, it is also necessary to ascertain whether the limitation imposed on the rights conferred by Articles 7 and 8 of the Charter is proportionate to the legitimate aim pursued (see, inter alia, European Court of Human Rights, *Gillow v. United Kingdom*, 24 November 1986, § 55, Series A no. 109, and *Österreichischer Rundfunk and Others*, paragraph 83).

73 The applicants in the main proceedings observe that the data whose publication is provided for in Article 44a of Regulation No 1290/2005 and in Regulation No 259/2008 allows third parties to draw conclusions as to their income. They explain that the aid represents between 30 % and 70 % of the total income of the beneficiaries concerned. The legitimate interests of the public would, they argue, be satisfied by the publication of anonymous statistics.

74 It is settled case-law that the principle of proportionality, which is one of the general principles of European Union law, requires that measures implemented by acts of

the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it (Case C-58/08 *Vodafone and Others* [2010] ECR I-4999, paragraph 51 and the case-law cited).

75 It is not disputed that the publication on the internet of data by name relating to the beneficiaries concerned and the precise amounts received by them from the EAGF and the EAFRD is liable to increase transparency with respect to the use of the agricultural aid concerned. Such information made available to citizens reinforces public control of the use to which that money is put and contributes to the best use of public funds.

76 As to whether the measure is necessary, it must be recalled that the objective of the publication at issue may not be pursued without having regard to the fact that that objective must be reconciled with the fundamental rights set forth in Articles 7 and 8 of the Charter (see, to that effect, Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-9831, paragraph 53).

77 It is thus necessary to determine whether the Council of the European Union and the Commission balanced the European Union's interest in guaranteeing the transparency of its acts and ensuring the best use of public funds against the interference with the right of the beneficiaries concerned to respect for their private life in general and to the protection of their personal data in particular. The Court has held in this respect that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (*Satakunnan Markkinapörssi and Satamedia*, paragraph 56).

78 The Member States which have submitted written observations to the Court, the Council and the Commission argue that the objective pursued by the publication required by Article 44a of Regulation No 1290/2005 and by Regulation No 259/2008 could not be achieved by measures which interfere less with the right of the

beneficiaries concerned to respect for their private life in general and the protection of their personal data in particular. Information limited to those of the beneficiaries concerned who receive aid exceeding a certain threshold would, it is submitted, not give taxpayers an accurate image of the CAP. Taxpayers would have the impression that there were only 'big' beneficiaries of aid from the agricultural Funds, whereas there are numerous 'little' ones. Limiting publication to legal persons only would not be satisfactory either. The Commission submits in this connection that the largest beneficiaries of agricultural aid include natural persons.

79 While it is true that in a democratic society taxpayers have a right to be kept informed of the use of public funds (*Österreichischer Rundfunk and Others*, paragraph 85), the fact remains that striking a proper balance between the various interests involved made it necessary for the institutions, before adopting the provisions whose validity is contested, to ascertain whether publication via a single freely consultable website in each Member State of data by name relating to all the beneficiaries concerned and the precise amounts received by each of them from the EAGF and the EAFRD — with no distinction being drawn according to the duration, frequency or nature and amount of the aid received — did not go beyond what was necessary for achieving the legitimate aims pursued, having regard in particular to the interference with the rights guaranteed by Articles 7 and 8 of the Charter resulting from such publication.

80 As far as natural persons benefiting from aid under the EAGF and the EAFRD are concerned, however, it does not appear that the Council and the Commission sought to strike such a balance between the European Union's interest in guaranteeing the transparency of its acts and ensuring the best use of public funds, on the one hand, and the fundamental rights enshrined in Articles 7 and 8 of the Charter, on the other.

81 There is nothing to show that, when adopting Article 44a of Regulation No 1290/2005 and Regulation No 259/2008, the Council and the Commission took into consideration methods of publishing information on the beneficiaries concerned which would be consistent with the objective of such publication while at the same time causing

less interference with those beneficiaries' right to respect for their private life in general and to protection of their personal data in particular, such as limiting the publication of data by name relating to those beneficiaries according to the periods for which they received aid, or the frequency or nature and amount of aid received.

82 Such limited publication by name might be accompanied, if appropriate, by relevant information about other natural persons benefiting from aid under the EAGF and the EAFRD and the amounts received by them.

83 The institutions ought thus to have examined, in the course of striking a proper balance between the various interests involved, whether publication by name limited in the manner indicated in paragraph 81 above would have been sufficient to achieve the objectives of the European Union legislation at issue in the main proceedings. In particular, it does not appear that such a limitation, which would protect some of the beneficiaries concerned from interference with their private lives, would not provide citizens with a sufficiently accurate image of the aid granted by the EAGF and the EAFRD to achieve the objectives of that legislation.

84 The Member States which submitted written observations to the Court and the Council and the Commission refer also to the significant role of the CAP in the European Union budget in order to justify the need for publication laid down by Article 44a of Regulation No 1290/2005 and by Regulation No 259/2008.

85 That argument must be rejected. It is necessary to bear in mind that the institutions are obliged to balance, before disclosing information relating to a natural person, the European Union's interest in guaranteeing the transparency of its actions and the

infringement of the rights recognised by Articles 7 and 8 of the Charter. No automatic priority can be conferred on the objective of transparency over the right to protection of personal data (see, to that effect, *Commission* v *Bavarian Lager*, paragraphs 75 to 79), even if important economic interests are at stake.

86 It follows from the foregoing that it does not appear that the institutions properly balanced, on the one hand, the objectives of Article 44a of Regulation No 1290/2005 and of Regulation No 259/2008 against, on the other, the rights which natural persons are recognised as having under Articles 7 and 8 of the Charter. Regard being had to the fact that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (*Satakunnan Markkinapörssi and Satamedia*, paragraph 56) and that it is possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives of the European Union rules in question, it must be held that, by requiring the publication of the names of all natural persons who were beneficiaries of EAGF and EAFRD aid and of the exact amounts received by those persons, the Council and the Commission exceeded the limits which compliance with the principle of proportionality imposes.

87 Finally, with regard to the legal persons which received EAGF and EAFRD aid, and in so far as they may invoke the rights conferred by Articles 7 and 8 of the Charter (see paragraph 53 of the present judgment), the view must be taken that the obligation to publish which follows from the provisions of the European Union rules the validity of which has here been brought into question does not go beyond the limits imposed by compliance with the principle of proportionality. The seriousness of the breach of the right to protection of personal data manifests itself in different ways for, on the one hand, legal persons and, on the other, natural persons. It is necessary to point out in this regard that legal persons are already subject to a more onerous obligation in respect of the publication of data relating to them. Furthermore, the obligation on the competent national authorities to examine, before the data in question are published and for each legal person which is a beneficiary of EAGF or EAFRD aid, whether the name of that person identifies natural persons would impose on those authorities an unreasonable administrative burden (see, to that effect, judgment of the European Court of Human Rights, *K.U. v. Finland*, 2 March 2009, application no 2872/02, § 48, not yet published).

88 In those circumstances, it must be held that the provisions of European Union law, the validity of which is questioned by the referring court, observe, in so far as they concern the publication of data relating to legal persons, a fair balance in the consideration taken of the respective interests in issue.

89 On the basis of all of the foregoing, Article 44a of Regulation No 1290/2005 and Regulation No 259/2008 must be declared invalid to the extent to which, with regard to natural persons who are beneficiaries of EAGF and EAFRD aid, those provisions impose an obligation to publish personal data relating to each beneficiary without drawing a distinction based on relevant criteria such as the periods during which those persons have received such aid, the frequency of such aid or the nature and amount thereof.

(c) The validity of Article 42(8b) of Regulation No 1290/2005

90 Article 42(8b) of Regulation No 1290/2005 authorises the Commission to adopt the detailed rules for the implementation solely of Article 44a of that regulation.

91 However, as Article 44a of Regulation No 1290/2005 has to be declared invalid for the reasons indicated above, Article 42(8b) of that regulation must be declared invalid in like manner.

92 The answer to the first question and to the first part of the second question is therefore that Articles 42(8b) and 44a of Regulation No 1290/2005, and Regulation No 259/2008, are invalid in so far as, with regard to natural persons who are beneficiaries of EAGF

and EAFRD aid, those provisions impose an obligation to publish personal data relating to each beneficiary without drawing a distinction based on relevant criteria such as the periods during which those persons have received such aid, the frequency of such aid or the nature and amount thereof.

(d) The effects in time of the invalidity which has been established

93 Where it is justified by overriding considerations of legal certainty, the second paragraph of Article 264 TFEU, which is also applicable by analogy to a reference under Article 267 TFEU for a preliminary ruling on the validity of acts of the European Union, confers on the Court a discretion to decide, in each particular case, which specific effects of the act in question must be regarded as definitive (see, to that effect, Case C-333/07 *Regie Networks* [2008] ECR I-10807, paragraph 121 and the case-law cited).

94 In view of the large number of publications which have taken place in the Member States on the basis of rules which were regarded as being valid, it must be held that the invalidity of the provisions mentioned in paragraph 92 of the present judgment does not allow any action to be brought to challenge the effects of the publication of the lists of beneficiaries of EAGF and EAFRD aid carried out by the national authorities on the basis of those provisions during the period prior to the date on which the present judgment is delivered.

2. The third question

95 By its third question, the referring court seeks, essentially, to ascertain whether the second indent of Article 18(2) of Directive 95/46 is to be interpreted as meaning that the publication of the information resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008 may be effected only if the personal data protection official has, prior to such publication, kept a full register within the terms of the second indent of Article 18(2).

96 It must, in this regard, be borne in mind that Article 18(1) of Directive 95/46 establishes the principle that the supervisory authority must be notified before any wholly or partly automatic operation for the processing of personal data, or any set of such operations intended to serve a single purpose or several related purposes, is carried out. As recital 48 in the preamble to Directive 95/46 explains, 'the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive'.

97 The second indent of Article 18(2) of Directive 95/46, however, provides that Member States may provide for the simplification of or exemption from that obligation in the case where, inter alia, the controller appoints a personal data protection official. It appears from the decisions for reference that such an appointment was made in the *Land* of Hesse so far as concerns the publication of data resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008.

98 According to the second indent of Article 18(2) of Directive 95/46, a personal data protection official has a number of tasks which are designed to ensure that processing

operations are unlikely to have an adverse effect on the rights and freedoms of the persons concerned. The official is thus responsible for, among other things, 'keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21(2) [of Directive 95/46]'. The latter provision refers to Article 19(1)(a) to (e) of Directive 95/46.

99 However, contrary to the view expressed by the referring court, the second indent of Article 18(2) of Directive 95/46 does not require any provision to be adopted which imposes an obligation on the personal data protection official to maintain a register containing the information referred to in Article 21(2) of that directive, read in conjunction with Article 19(1)(a) to (e) thereof, before the processing of the data concerned is undertaken. The register referred to in the second indent of Article 18(2) of Directive 95/46 need contain only 'processing operations carried out'.

100 In those circumstances, the absence, established by the referring court, of a full register prior to the data processing cannot affect the legality of a publication such as that resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008.

101 The answer to the third question is therefore that the second indent of Article 18(2) of Directive 95/46 must be interpreted as not placing the personal data protection official under an obligation to keep the register provided for by that provision before an operation for the processing of personal data, such as that resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008, is carried out.

3. The fourth question

102 By its fourth question, the referring court seeks, essentially, to ascertain whether Article 20 of Directive 95/46 is to be interpreted as making the publication of the information resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008 subject to the prior checks for which that Article 20 provides.

103 It must first be pointed out that Article 20(1) of Directive 95/46 provides that 'Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof'.

104 It follows that Directive 95/46 does not make the processing of personal data subject, in general, to a prior check. As is clear from recital 52 in the preamble to Directive 95/46, the European Union legislature took the view that '*ex post facto* verification by the competent authorities must in general be considered a sufficient measure'.

105 With regard to processing operations which are subject to prior checks, that is to say, processing operations which are likely to pose specific risks to the rights and freedoms of data subjects, recital 53 in the preamble to Directive 95/46 states that processing operations are likely to pose such risks 'by virtue of their nature, their scope or their purposes'. Even though Member States have the option of specifying in greater detail in their legislation the processing operations which may pose specific risks to the rights and freedoms of data subjects, Directive 95/46 provides, as is evident from recital 54 in its preamble, that the number of such operations 'should be very limited'.

106 It must further be pointed out that, under Article 27(1) of Regulation No 45/2001, processing operations which are likely to present specific risks to the rights and freedoms of data subjects are also subject to prior checking when carried out by institutions and bodies of the European Union. Article 27(2) of that regulation specifies the operations which are likely to present such risks. In view of the parallel relationship between the provisions of Directive 95/46 and those of Regulation No 45/2001 which relate to prior checks, the listing in Article 27(2) of Regulation No 45/2001 of the processing operations which are likely to present specific risks to the rights and freedoms of data subjects must be considered relevant for the purpose of interpreting Article 20 of Directive 95/46.

107 However, it does not appear that the publication of the data imposed by Articles 42(8b) and 44a of Regulation No 1290/2005 and by Regulation No 259/2008 comes within any of the categories of processing operations covered by Article 27(2) of Regulation No 45/2001.

108 In those circumstances, the answer to the fourth question is that Article 20 of Directive 95/46 must be interpreted as not imposing an obligation on the Member States to make the publication of information resulting from Articles 42(8b) and 44a of Regulation No 1290/2005 and from Regulation No 259/2008 subject to the prior checks for which that Article 20 provides.

109 In view of the answer to the fourth question, there is no longer any need to answer the fifth question.

IV — Costs

110 Since these proceedings are, for the parties to the main proceedings, a step in the actions pending before the national court, the decisions on costs are a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

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

1. **Articles 42(8b) and 44a of Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, as amended by Council Regulation (EC) No 1437/2007 of 26 November 2007, and Commission Regulation (EC) No 259/2008 of 18 March 2008 laying down detailed rules for the application of Regulation No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD) are invalid in so far as, with regard to natural persons who are beneficiaries of EAGF and EAFRD aid, those provisions impose an obligation to publish personal data relating to each beneficiary without drawing a distinction based on relevant criteria such as the periods during which those persons have received such aid, the frequency of such aid or the nature and amount thereof.**

2. **The invalidity of the provisions of European Union law mentioned in paragraph 1 of this operative part does not allow any action to be brought to challenge the effects of the publication of the lists of beneficiaries of EAGF and EAFRD aid carried out by the national authorities on the basis of those**

provisions during the period prior to the date on which the present judgment is delivered.

3. The second indent of Article 18(2) 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 must be interpreted as not placing the personal data protection official under an obligation to keep the register provided for by that provision before an operation for the processing of personal data, such as that resulting from Articles 42(8b) and 44a of Regulation No 1290/2005, as amended by Regulation No 1437/2007, and from Regulation No 259/2008, is carried out.

4. Article 20 of Directive 95/46 must be interpreted as not imposing an obligation on the Member States to make the publication of information resulting from Articles 42(8b) and 44a of Regulation No 1290/2005, as amended by Regulation No 1437/2007, and from Regulation No 259/2008 subject to the prior checks for which that Article 20 provides.

[Signatures]

Reports of Cases

JUDGMENT OF THE GENERAL COURT (Fifth Chamber)

15 July 2015*

(Access to documents — Regulation (EC) No 1049/2001 — Documents relating to the affiliation of certain Members of the European Parliament to the additional pension scheme — Refusal to grant access — Exception relating to the protection of privacy and the integrity of the individual — Article 8(b) of Regulation (EC) No 45/2001 — Transfer of personal data — Conditions concerning the necessity of having the data transferred and the risk that the data subject's legitimate interests might be prejudiced)

In Case T-115/13,

Gert-Jan Dennekamp, residing in Giethoorn (Netherlands), represented by O. Brouwer, T. Oeyen and E. Raedts, lawyers,

applicant,

supported by

Republic of Finland, represented by H. Leppo, acting as Agent,

by

Kingdom of Sweden, represented initially by A. Falk, C. Meyer-Seitz, S. Johannesson and U. Persson, and subsequently by A. Falk, C. Meyer-Seitz, U. Persson, E. Karlsson, L. Swedenborg, C. Hagerman and F. Sjövall, acting as Agents,

and by

European Data Protection Supervisor (EDPS), represented by A. Buchta and U. Kallenberger, acting as Agents,

interveners,

v

European Parliament, represented by N. Lorenz and N. Görlitz, acting as Agents,

defendant,

APPLICATION for annulment of Decision A(2012) 13180 of the European Parliament of 11 December 2012 refusing to grant the applicant access to certain documents relating to the affiliation of certain Members of the European Parliament to the additional pension scheme,

* Language of the case: English.

THE GENERAL COURT (Fifth Chamber),

composed of A. Dittrich, President, J. Schwarcz (Rapporteur) and V. Tomljenović, Judges,

Registrar: L. Grzegorczyk, Administrator,

having regard to the written part of the procedure and further to the hearing on 19 November 2014,

gives the following

Judgment

Background to the dispute

1 The applicant, Mr Gert-Jan Dennekamp, is a journalist employed by the Nederlandse Omroep Stichting (Netherlands Broadcasting Association).

2 On 25 November 2005, the applicant submitted an application to the European Parliament, on the basis of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ 2001 L 145, p. 43), for access to 'all documents' relating to the additional pension scheme for Members of the European Parliament ('the additional pension scheme'). He was granted access to: (i) a note from the Secretary-General to the Bureau of the European Parliament ('the Bureau'); (ii) 'Annual Reports and Accounts' spanning several years; and (iii) the minutes of a Bureau meeting. Subsequently, the complaint lodged by the applicant with the European Ombudsman against the refusal to grant him access to the list of Members of the European Parliament ('MEPs') who were members of the additional pension scheme was closed.

3 By letter of 20 October 2008, the applicant submitted an application for access to all the documents indicating which MEPs were then members of the additional pension scheme, to the list of MEPs who were members of the scheme on 1 September 2005 and to the list of members of the scheme as at the date of the application for access for whom the European Parliament paid a monthly contribution. By decision of 17 December 2008, the Parliament rejected the confirmatory application for access to the abovementioned documents.

4 The General Court dismissed the action for annulment of the decision of 17 December 2008 by its judgment of 23 November 2011 in *Dennekamp* v *Parliament* (T-82/09, EU:T:2011:688). In essence, the Court ruled that the applicant had failed to take account, in his application for access to the documents, of the principle laid down in the judgment of 29 June 2010 in *Commission* v *Bavarian Lager* (C-28/08 P, ECR, EU:C:2010:378, paragraph 63), that it is necessary, where an application for access relates to personal data, to apply in full 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). More specifically, the Court found that the applicant had failed to demonstrate the necessity for the personal data to be transferred, as was required by the provisions of Article 8(b) of Regulation No 45/2001 (judgment in *Dennekamp* v *Parliament*, EU:T:2011:688, paragraphs 31 to 35).

5 By letter of 10 September 2012, the applicant asked the President of the European Parliament to grant him access to four categories of documents: all documents showing which current MEPs were also members of the additional pension scheme; a list of names of MEPs who were members of the

scheme after September 2005; a list of names of the members of the scheme for whom the Parliament paid a monthly contribution; all documents related to the financial position of the scheme since 2009 ('the initial application').

6 In the initial application, the applicant submitted that there was an objective necessity within the meaning of Article 8(b) of Regulation No 45/2001 for the personal data to be transferred and, moreover, that there was no risk that the data subjects' legitimate interests would be prejudiced by disclosure of the data concerned.

7 As regards the necessity of having the personal data transferred, the applicant, relying on the existence of a broad public interest in transparency, recognised by Regulation No 1049/2001, highlighted the need for the public to have a better understanding of how decisions were being taken and the fact that, to that end, a debate could be generated through press reporting. In the present case, he stressed that it was of the utmost importance for European citizens to know which MEPs had a personal interest in the additional pension scheme, having regard, principally, to the fact that the European Parliament paid two thirds of the contributions of the MEPs participating in the scheme, that it had, on several occasions, made up shortfalls in the scheme and that it had committed itself to compensating any losses suffered by the scheme, thus ensuring the preservation of the acquired pension rights of MEPs participating in the scheme, which, in the applicant's view, translated into considerable use of public funds.

8 As to there being no prejudice to the legitimate interests of the MEPs, the applicant took the view that it was difficult to see what harm could come from disclosing the names of the MEPs participating in the additional pension scheme, as those MEPs could continue to participate in it and to benefit from it, and that this would not lead to disclosure of their private investments. Should the view be taken that disclosure of the names of the MEPs participating in the scheme would affect their private interests, the applicant's arguments that these are not legitimate private interests since, given that the scheme was established and was influenced by elected representatives for elected representatives and pays benefits funded from public money, such private interests ought not to be treated in the same manner as those relating to private contributions into a normal pension scheme. In the applicant's view, a negative public reaction to the membership of certain MEPs in the scheme cannot be regarded as undermining the right to privacy, which Regulation No 1049/2001 seeks to avoid.

9 Lastly, in the initial application, having referred to the Charter of Fundamental Rights of the European Union and to the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950 ('the ECHR'), the applicant claimed that, by his application, he was not seeking to interfere with the MEPs' home or family lives, but to foster a public debate regarding the exercise of public functions, in which European citizens should be allowed to participate.

10 By letter of 17 October 2012, the Secretary-General of the European Parliament refused access to the first three categories of documents on the ground that they were documents containing personal data in respect of which Article 8(b) of Regulation No 45/2001 required the applicant to establish the necessity of having the data transferred and that there was no reason to assume that the data subjects' legitimate interests might be prejudiced. In the Secretary-General's view, the applicant had failed to demonstrate the necessity for the data at issue to be transferred by referring exclusively to the public interest in transparency. Accordingly, he took the view that it was not necessary to examine whether there was a risk that the MEPs' legitimate interests might be prejudiced. Lastly, as regards the fourth category of documents requested by the applicant, the Secretary-General identified the documents relating to the financial position of the additional pension scheme since 2009 and provided the references under which those documents could be found on the Parliament's website.

11 By letter of 8 November 2012, the applicant submitted, pursuant to Article 7(2) of Regulation No 1049/2001, a confirmatory application for access to the first three categories of documents referred to in paragraph 5 above ('the confirmatory application'). The applicant drew particular attention to the reasons why he considered it necessary to have the personal data at issue transferred, relying on the right of access to information and the right to freedom of expression. He noted the European Parliament's failure to weigh the necessity for that data to be transferred against the right to privacy of the MEPs concerned, and the lack of any explanation as to how the requested access could specifically and actually have undermined the privacy of those MEPs. Next, the applicant explained in detail, on the one hand, why it was necessary for the documents requested to be disclosed, namely, in order for him to be able to report on the manner in which public money was being spent, the possible impact of private interests on the voting behaviour of the MEPs and on the functioning of control mechanisms, and, on the other hand, why any private interests of the MEPs concerned by the requested documents could not prevail over the freedom of expression and the public's interest in being informed of how public funds were spent and political decisions taken.

12 By Decision A(2012) 13180 of 11 December 2012, the European Parliament rejected the confirmatory application ('the contested decision').

13 In the contested decision, the European Parliament based the refusal to grant access to the documents requested on the exception relating to a risk of privacy and the integrity of the individual being undermined, as provided for in Article 4(1)(b) of Regulation No 1049/2001, on the grounds that those documents contained personal data within the meaning of Article 2(a) of Regulation No 45/2001, disclosure of which would be contrary to that regulation, which must be applied in its entirety where the documents requested contain such data.

14 As regards the requirement relating to necessity laid down in Article 8(b) of Regulation No 45/2001, in the contested decision the European Parliament first considered that it had to be interpreted restrictively like any other exception to a fundamental right. Secondly, it agreed that the applicant had been very specific about his intentions concerning the personal data at issue, but stated that his arguments failed to establish the necessity of having the data transferred. The Parliament took the view that to accept as a valid argument, in the context of Article 8(b) of Regulation No 45/2001, the assertion of an interest of the public and of the media in exercising control over public expenditure would be to allow the disclosure of personal data beyond any reasonable limit and would infringe the rules on the protection of such data. More specifically, the Parliament noted that the applicant had not established a link between his intentions and the specific data to which he had requested access. It was neither necessary nor proportionate to request the names of all MEPs participating in the additional pension scheme, since decisions relating to that scheme were adopted by the Bureau. Thirdly, the Parliament observed that the risk of a conflict of interest was typical of the situation of a parliament, for a parliament always decided on the remuneration of its members, a fact which could not justify per se the disclosure of personal data. Fourthly, the Parliament considered that Article 8(b) of Regulation No 45/2001 had to be interpreted in such a way as to safeguard the rationale and effectiveness of that regulation and that it could not be applied in such a way as to render the regulation completely devoid of substance, which would be the case if, as in the present case, the sole purpose of the transfer of personal data was the immediate disclosure of the data to the public. However, because the application of Article 8(b) of Regulation No 45/2001 requires the person requesting the transfer to demonstrate the necessity for the personal data to be transferred, the aim pursued by the applicant would enable persons who had not demonstrated any such necessity to have access to those data, contrary to the rule laid down in the judgment in *Commission* v *Bavarian Lager*, cited in paragraph 4 above (EU:C:2010:378, paragraph 63).

15 As regards the weighing up of the necessity of transferring the personal data at issue against the legitimate interests of the data subjects, the European Parliament considered, in the light of Regulation No 45/2001, that those legitimate interests prevailed, on the ground that it would not be proportionate to allow such a transfer. First, the Parliament accepted that MEPs' legitimate interests were less

far-reaching than those of a private person without any public commitment and that, therefore, the degree of protection of their data was lower. Secondly, the Parliament nevertheless pointed out that the public funding of the additional pension scheme did not mean that the MEPs' personal data should not be afforded any protection or that those MEPs would have no legitimate interests in arguing against disclosure of such data. In that context, the Parliament explained that it was necessary to draw a distinction between data falling into the public sphere, subject to a lower degree of protection, and data falling into the private sphere, protected by the concept of legitimate interests. In the Parliament's view, the personal data at issue fell into the MEPs' private sphere, the information those data contained constituting a legitimate interest that was required to be protected. The data related to the personal financial situation of the MEPs concerned, namely contributions into a pension scheme and pension rights under that scheme, which were private concerns. The Parliament noted that while the existence of a parliamentary mandate was the *sine qua non* for gaining access to the scheme, the pension was paid only after the end of the mandate and that the personal contributions were significant. Thirdly, the Parliament argued that, if public funding were sufficient to deny the personal character of the data, then the same would also have to apply to any member of staff of a public authority. Fourthly, the Parliament concluded in the weighing up of the interests that, given, in particular, the general nature of the interest of the media and the general public in the personal situation of MEPs, it was not proportionate to disclose the data requested, unless it were to be accepted that it should be possible to gain access to all personal data of MEPs or of any public officials involving public expenditure. In the Parliament's view, such an approach would render Article 16 TFEU entirely meaningless, when, in order to achieve his goals, the applicant could have merely requested the aggregated figures concerning the financial situation of the scheme. Fifthly, the Parliament noted that there were more appropriate measures for achieving the goals pursued by the applicant, which ensured sufficient control of public expenditure and informed the public.

Procedure and forms of order sought

16 The applicant brought the present action by application lodged at the Court Registry on 22 February 2013.

17 By documents lodged on 29 and 30 May and 11 June 2013 respectively, the European Data Protection Supervisor (EDPS), the Kingdom of Sweden and the Republic of Finland applied for leave to intervene in support of the form of order sought by the applicant.

18 By orders of the President of the Second Chamber of the General Court of 11 September 2013, the EDPS, on the one hand, and the Republic of Finland and the Kingdom of Sweden, on the other, were granted leave to intervene.

19 The composition of the Chambers of the Court having been altered, the Judge-Rapporteur was assigned to the Fifth Chamber, to which this case was therefore allocated.

20 The applicant claims that the Court should:

— annul the contested decision;

— order the European Parliament to pay the costs, including those incurred by the interveners.

21 The Republic of Finland, the Kingdom of Sweden and the EDPS claim that the Court should grant the form of order sought by the applicant and accordingly annul the contested decision.

22 The European Parliament contends that the Court should:

— dismiss the action as unfounded;

— order the applicant to pay the costs.

23 By way of a measure of organisation of procedure, the Court put a question to the main parties. The parties replied by letters lodged on 16 October 2014, in the case of the European Parliament, and on 17 October 2014, in the case of the applicant.

24 After the end of the hearing, a number of questions were sent to the European Parliament in writing, the reply to which was received at the Court Registry on 7 January 2015. The applicant submitted its observations on the Parliament's reply. The oral part of the procedure was closed on 2 February 2015.

Law

1. *Scope of the action*

25 In its response to the measure of organisation of procedure, the applicant stated that 64 MEPs who were members of the additional pension scheme had objected to the amendments to the scheme made by the Bureau in its meetings on 9 March and 1 April 2009 and had brought an action before the General Court in that respect, which was dismissed by order of 15 December 2010 in *Albertini and Others and Donnelly* v *Parliament* (T-219/09 and T-326/09, ECR, EU:T:2010:519).

26 In addition, another MEP who was a member of the additional pension scheme also brought an action before the General Court against the decision of the European Parliament refusing to grant him his voluntary additional pension in the form of a lump sum (judgment of 18 October 2011 in *Purvis* v *Parliament*, T-439/09, ECR, EU:T:2011:600).

27 It must therefore be noted that the names of 65 MEPs who were members of the additional pension scheme had been made public when the Court gave its ruling in the three cases mentioned in paragraphs 25 and 26 above, that is to say, before the present action was brought.

28 To that extent, the present action is devoid of purpose (see, to that effect, order of 11 December 2006 in *Weber* v *Commission*, T-290/05, EU:T:2006:381, paragraph 42).

29 Consequently, there is no need to adjudicate on that aspect of the dispute.

2. *Substance of the action*

30 In challenging the contested decision, the applicant raises two pleas in law. The first plea alleges infringement of Articles 11 and 42 of the Charter of Fundamental Rights and an error of law in the application of Article 4(1)(b) of Regulation No 1049/2001, read in conjunction with Article 8(b) of Regulation No 45/2001. The second alleges failure to state reasons.

First plea in law, alleging infringement of Articles 11 and 42 of the Charter of Fundamental Rights and an error of law in the application of Article 4(1)(b) of Regulation No 1049/2001, read in conjunction with Article 8(b) of Regulation No 45/2001

31 In the first part of the plea, the applicant maintains that, in the confirmatory application, he provided express and legitimate reasons for the necessity of having the personal data contained in the requested documents transferred, in accordance with Article 8(b) of Regulation No 45/2001, acting on the basis of European citizens' right to information. In the second part, the applicant submits that, in the weighing up of interests, MEPs do not have a legitimate interest in the protection of their privacy for the purposes of Article 8(b) of Regulation No 45/2001.

32 The first part of the plea is divided into four claims, by which the applicant submits (i) that he has established the necessity of having the personal data transferred, the test laid down by Article 8(b) of Regulation No 45/2001 and interpreted in the light of the judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above (EU:C:2010:378, paragraph 63), and *Dennekamp* v *Parliament*, cited in paragraph 4 above (EU:T:2011:688, paragraphs 31 to 35); (ii) that the test of necessity must not be interpreted narrowly; (iii) that he has made an express link between the aim pursued by his application for access and the necessity of disclosing all the names requested, the most appropriate means of achieving that aim; and (iv) that the contested decision fails to take sufficient account of the structure and purpose of Regulation No 1049/2001.

33 The second part of the plea is divided into three claims. First, the applicant maintains that MEPs have no legitimate interest in the protection of their privacy for the purposes of Article 8(b) of Regulation No 45/2001, as they open their conduct to a significant degree of public scrutiny. Secondly, the applicant takes the view that the European Parliament failed to establish in the contested decision that the MEPs' legitimate interests would be prejudiced by disclosure of the requested documents. By his third claim, he asserts that even if the Parliament had rightly considered that the requested information fell within the MEPs' private sphere, that would not be sufficient to protect it as a legitimate interest within the meaning of Article 8(b) of Regulation No 45/2001, which requires a weighing up of the interests engaged.

34 It is appropriate, first of all, to examine the conditions under which the transfer of personal data is permitted by Article 8(b) of Regulation No 45/2001, responding in particular to the second and fourth claims in the first part of the plea, which seek to challenge the way in which the European Parliament applied Regulations No 1049/2001 and No 45/2001 in conjunction with each other. Next, the Court must determine whether the Parliament correctly assessed the justification given by the applicant regarding the necessity of having the personal data transferred, responding to the first and third claims in the first part of the plea. Lastly, it is appropriate to examine whether the Parliament correctly weighed up the MEPs' legitimate interests in the protection of their privacy and the interest in having the personal data transferred, responding to all three claims in the second part of the plea, which largely overlap.

The combined application of Regulations No 1049/2001 and No 45/2001 and interpretation of the conditions for the application of Article 8(b) of Regulation No 45/2001

35 It should be recalled, at the outset, that Article 15(3) TFEU provides that any citizen of the European Union, and any natural or legal person residing or having its registered office in a Member State, is to have a right of access to the documents of the institutions of the European Union, subject to the principles and the conditions defined in accordance with the procedure laid down in Article 294 TFEU (see judgment of 27 February 2014 in *Commission* v *EnBW*, C-365/12 P, ECR, EU:C:2014:112, paragraph 61 and the case-law cited). In accordance with recital 1 in the preamble to Regulation No 1049/2001, that regulation reflects the intention expressed in the second paragraph of Article 1 TEU — inserted by the Treaty of Amsterdam — of marking a new stage in the process of creating an ever closer union among the peoples of Europe, in which decisions are taken as openly as possible and as closely as possible to the citizen. As is stated in recital 2 in the preamble to Regulation No 1049/2001, the right of public access to documents of the institutions is related to the democratic nature of those institutions (judgments of 1 July 2008 in *Sweden and Turco* v *Council*, C-39/05 P and C-52/05 P, ECR, EU:C:2008:374, paragraph 34, and 21 July 2011 in *Sweden* v *MyTravel and Commission*, C-506/08 P, ECR, EU:C:2011:496, paragraph 72).

36 To that end, Regulation No 1049/2001 is intended, as is apparent from recital 4 in the preamble thereto and from Article 1, to give the fullest possible effect to the right of public access to documents of the institutions (judgments in *Sweden and Turco* v *Council*, cited in paragraph 35 above, EU:C:2008:374, paragraph 33, and *Sweden* v *MyTravel and Commission*, cited in paragraph 35 above, EU:C:2011:496, paragraph 73).

37 However, that right is none the less subject to certain limitations based on grounds of public or private interest. More specifically, and in reflection of recital 11 in the preamble thereto, Article 4 of Regulation No 1049/2001 provides that the institutions are to refuse access to a document where its disclosure would undermine the protection of one of the interests protected by that provision (judgment in *Sweden* v *MyTravel and Commission*, cited in paragraph 35 above, EU:C:2011:496, paragraph 74).

38 However, since they derogate from the principle of the widest possible public access to documents, those exceptions must be interpreted and applied strictly (judgments in *Sweden and Turco* v *Council*, cited in paragraph 35 above, EU:C:2008:374, paragraph 36, and *Sweden* v *MyTravel and Commission*, cited in paragraph 35 above, EU:C:2011:496, paragraph 75).

39 Thus, if the institution concerned decides to refuse access to a document which it has been asked to disclose, it must, in principle, explain how disclosure of that document could specifically and actually undermine the interest protected by the exception — among those provided for in Article 4 of Regulation No 1049/2001 — that is relied upon by that institution (judgment in *Sweden* v *MyTravel and Commission*, cited in paragraph 35 above, EU:C:2011:496, paragraph 76). Moreover, the risk of that undermining must be reasonably foreseeable and not purely hypothetical (judgments in *Sweden and Turco* v *Council*, cited in paragraph 35 above, EU:C:2008:374, paragraph 43, and *Sweden* v *MyTravel and Commission*, cited in paragraph 35 above, EU:C:2011:496, paragraph 76).

40 It must also be noted that it follows from the case-law that, when examining the relationship between Regulations No 1049/2001 and No 45/2001 for the purposes of applying the exception provided for under Article 4(1)(b) of Regulation No 1049/2001 — namely, the protection of privacy and the integrity of the individual — it must be borne in mind that those regulations have different objectives. Regulation No 1049/2001 is designed to ensure the greatest possible transparency of the decision-making process of the public authorities and the information on which they base their decisions. It is thus designed to facilitate as far as possible the exercise of the right of access to documents and to promote good administrative practices. Regulation No 45/2001 is designed to ensure the protection of the freedoms and fundamental rights of individuals, particularly their private life, in the handling of personal data (judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 49, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 23).

41 As Regulations No 45/2001 and No 1049/2001 do not contain any provisions granting one primacy over the other, the full application of both regulations should, in principle, be ensured (judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 56, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 24).

42 Article 4(1)(b) of Regulation No 1049/2001, on which the European Parliament based its refusal to grant access to the requested documents in the contested decision, provides that '[t]he institutions shall refuse access to a document where disclosure would undermine the protection of … privacy and the integrity of the individual, in particular in accordance with [EU] legislation regarding the protection of personal data'. It is apparent from the case-law that that is an indivisible provision which requires that any undermining of privacy and the integrity of the individual must always be examined and assessed in conformity with the legislation of the European Union concerning the protection of personal data, in particular with Regulation No 45/2001. That provision thus establishes a specific and reinforced system of protection for a person whose personal data could, in certain cases, be

communicated to the public (judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraphs 59 and 60, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 25).

43 Where a request based on Regulation No 1049/2001 seeks access to documents including personal data, Regulation No 45/2001 becomes applicable in its entirety, including Article 8 thereof (judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 63, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 26).

44 It is in the light of those considerations that the Court must examine the arguments of the applicant, who is supported in that respect by the Republic of Finland, the Kingdom of Sweden and the EDPS.

45 The applicant submits that the contested decision fails to take sufficient account of the structure and purpose of Regulation No 1049/2001, namely to increase the accountability and legitimacy of public decision-making by bringing it closer to the citizen through transparency. In accordance with the judgment in *Commission* v *Bavarian Lager*, cited in paragraph 4 above (EU:C:2010:378), Regulation No 1049/2001 cannot be rendered devoid of purpose by an interpretation of the relevant provisions that would mean that legitimate disclosure could never pursue the aim of full disclosure to the public. In addition, such a result would not take into consideration the conditions under which the European Court of Human Rights considers that the public interest in receiving information prevails over the right of a public figure to privacy, namely that the reporting should relate facts capable of contributing to a debate in a democratic society concerning those public figures in the exercise of their official functions. According to the applicant the European Parliament is infringing Article 11 of the Charter of Fundamental Rights, read in the light of Article 10 of the ECHR, when it is claimed in the contested decision that it would be contrary to the objective of Article 8(b) of Regulation No 45/2001 for the public disclosure of data to be a legitimate aim.

46 In his reply, the applicant submits that the test of necessity in Article 8(b) of Regulation No 45/2001 must not be interpreted restrictively; that would lead to a broad interpretation of an exception to the fundamental right of access to documents, an unlawful restriction of that right and inconsistency with the case-law of the European Union.

47 The applicant's argument is based on the notion that the combined application of Regulations No 1049/2001 and No 45/2001, in accordance with the judgment in *Commission* v *Bavarian Lager*, cited in paragraph 4 above (EU:C:2010:378), must not result in the provisions of Regulation No 1049/2001 and, therefore, the fundamental right of access to documents of the EU institutions enjoyed by all European citizens, being neutralised altogether. Furthermore, in its statement in intervention, the Republic of Finland states that the core content and fundamental principles of both regulations must be applied so that each is applied in a manner compatible and consistent with the other. As regards those principles, it is necessary, in its view, to take account in particular of the rule laid down by Regulation No 1049/2001 concerning the lack of justification for applications for access to documents. In that context, the concept of the necessity of having personal data transferred, as provided for in Article 8(b) of Regulation No 45/2001, cannot be interpreted strictly, as that would restrict or remove altogether any possibility of access to documents where the application is based on a public interest such as the right to information.

48 In order to respond to those arguments, which seek to strike a balance between the right of access to documents held by the institutions, under Regulation No 1049/2001, and the obligations under Regulation No 45/2001 in respect of the transfer of personal data by those institutions, it is necessary to clarify the relationship between the rules laid down by those two regulations.

49 In the first place, it must be noted that, in the context of an application for access to documents, Regulation No 45/2001 is applied only when the institution in receipt of the application refuses to grant access to documents by applying vis-à-vis the applicant the exception provided for in

Article 4(1)(b) of Regulation No 1049/2001. That provision requires that any undermining of privacy and the integrity of the individual must be examined and assessed in conformity with the legislation of the European Union concerning the protection of personal data, in particular with Regulation No 45/2001 (see, to that effect, judgment in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 59).

50 If the documents requested contain personal data within the meaning of Article 2(a) of Regulation No 45/2001, the institution must, in principle, ensure the full application of both regulations to the application for access (judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 56, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 24). However, it must be noted that Regulation No 45/2001 establishes a specific and reinforced system of protection for a person whose personal data could be communicated to the public, and that when the application for access is being examined, the provisions of Regulation No 45/2001 become applicable in their entirety, including Article 8 thereof (judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraphs 60 and 63, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraphs 25 and 26). Moreover, recitals 7 and 14 in the preamble to Regulation No 45/2001, read together, indicate that the provisions of that regulation are binding and apply to all processing of personal data by the institutions of the European Union in any context whatsoever.

51 Consequently, if an application for access to documents may, if granted, result in the disclosure of personal data, the institution in receipt of the application must apply all the provisions of Regulation No 45/2001, and the full scope of the protection afforded to those data may not be limited as a result of the various rules and principles in Regulation No 1049/2001. That principle guiding the action of the institutions is, according to recital 12 in the preamble to Regulation No 45/2001, attributable to the importance attached to the rights granted to data subjects for their protection with regard to the processing of such data.

52 In this general context, it is admittedly true, as both the applicant and the Republic of Finland have emphasised, that the right of access to documents is not, in accordance with Article 6(1) of Regulation No 1049/2001, conditional upon an applicant justifying an interest in the disclosure of those documents. That is a concrete expression of the principles of openness and transparency which must drive the action taken by the institutions of the European Union, and of the democratic nature of those institutions.

53 However, it should be noted that, by requiring the institutions to examine the risk that the protection of privacy and of the integrity of the individual may be undermined through Regulation No 45/2001 and the restrictions and limitations thereby imposed on the processing of personal data, notably by means of Article 8(b) thereof, Article 4(1)(b) of Regulation No 1049/2001 indirectly requires an applicant for access to establish, through the provision of one or more express and legitimate reasons, the necessity of the transfer of the personal data contained in the documents to which he has requested access (see, to that effect, judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 78, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 30).

54 Thus, Article 8(b) of Regulation No 45/2001 requires the institution in receipt of an application for access initially to make an assessment of the necessity, and thus proportionality, of the transfer of personal data in the light of the applicant's objective (see, to that effect, judgment in *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 34). That same Article 8(b) of Regulation No 45/2001 requires that institution then to examine whether the legitimate interests of the data subjects might be prejudiced by the transfer of personal data, and to determine in that examination whether the applicant's objective is likely to have that effect (see, to that effect, judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 78,

and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 30). In so doing, the institution will be required to assess the applicant's justification for the transfer of personal data and thus for access to the documents.

55 Accordingly, to apply the condition as to the necessity of the transfer of personal data set out in Article 8(b) of Regulation No 45/2001 is to recognise the existence of an exception to the rule laid down by Article 6(1) of Regulation No 1049/2001. That consequence is justified by the *effet utile* that must be conferred on the provisions of Regulation No 45/2001, since any solution other than that of having the necessity of the transfer of personal data examined in the light of the objective of the applicant for access to documents would necessarily result in Article 8(b) of that regulation being disapplied.

56 In the second place, it is necessary to take into particular consideration the essential characteristics of the system of protection which Regulation No 45/2001 provides to natural persons with respect to the processing of their personal data, since the application of the exception to the right of access provided for in Article 4(1)(b) of Regulation No 1049/2001 means that Regulation No 45/2001 must be fully applied, Article 1 thereof making clear that the object of the regulation is, notably, to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy.

57 In Chapter II, Section 2 of Regulation No 45/2001, Article 5 of Regulation No 45/2001 specifies the grounds on which the processing of personal data is regarded as lawful. Articles 7, 8 and 9 of Regulation No 45/2001 lay down the conditions for making a transfer of personal data within or between EU institutions or bodies; to recipients, other than EU institutions and bodies, subject to 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); and to recipients, other than EU institutions and bodies, which are not subject to Directive 95/46.

58 While neither Article 7, Article 8 nor Article 9 of Regulation No 45/2001 establishes a principle coupled with exceptions, each article precisely limits the possibility of transferring personal data so as to make it subject to strict conditions which, if not fulfilled, prohibit any transfer. Those conditions always include the necessity of the transfer in the light of various aims.

59 According to recital 5 in the preamble to Regulation No 45/2001, the regulation seeks to provide individuals which it defines as data subjects with legally enforceable rights, and to define the data processing obligations of controllers within the EU institutions and bodies. In order to achieve that objective, the conditions subject to which an EU institution or body may transfer personal data must be interpreted strictly, so as not to jeopardise the rights of those persons, which are recognised by Regulation No 45/2001 as being fundamental rights, according to recital 12 in the preamble thereto. Thus, if the condition of necessity is to be fulfilled, it must be established that the transfer of personal data is the most appropriate of the possible measures for attaining the applicant's objective, and that it is proportionate to that objective, which means that the applicant must submit express and legitimate reasons to that effect (see, to that effect, judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 78, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraphs 30 and 34).

60 Contrary to what is argued by the applicant, the condition of necessity provided for in Article 8(b) of Regulation No 45/2001, thus interpreted, cannot be regarded as a broad interpretation of an exception to the fundamental right of access to documents which would result in an unlawful restriction of that right, contrary to EU case-law. Such an interpretation does not have the effect of creating a categorical exception for personal data to the principle of access to documents, but of reconciling two fundamental yet opposing rights where an application for access to documents relates to personal data, protected by Regulation No 45/2001, as is evident from paragraphs 56 to 59 above. In the relationship between the provisions protecting those opposing rights, the right of access to documents

is also preserved, since the mandatory application, as in this case, of Article 8(b) of Regulation No 45/2001 merely results, first, in the applicant being required to establish the necessity of obtaining the transfer of personal data, that is to say, to prove that the measure concerned is proportionate and the most appropriate means of attaining the aim pursued (see, to that effect, judgment in *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 34), and, secondly, in the institution being required to examine whether the legitimate interests of the data subjects might be prejudiced by the transfer of personal data in the light of the applicant's aim (see, to that effect, judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 78, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 30). The strict interpretation of the conditions imposed by Article 8(b) of Regulation No 45/2001 does not in any way therefore result in an exception being established that would generally prevent any access to documents containing personal data.

61 None the less, the strict interpretation of the condition of necessity laid down by Article 8(b) of Regulation No 45/2001 does not mean that a general justification for the transfer of personal data, like the public's right to information concerning the conduct of MEPs in the exercise of their duties, cannot be taken into consideration. In fact, as is already evident from paragraph 54 above, the general nature of the justification for the transfer has no direct effect on whether the transfer is necessary for the purposes of attaining the applicant's aim.

62 It is true that, as the European Parliament notes, the provisions of Article 4(1)(b) of Regulation No 1049/2001 do not provide for the public interest in privacy and the integrity of the individual to be weighed against an overriding public interest. However, with the exception of Article 4(1)(b) of Regulation No 45/2001, which requires that personal data should not be processed in a way incompatible with the purposes for which they were collected, there is nothing in that regulation to limit the scope of the justification for the transfer sought that may be given by the applicant. Nothing prevents the applicant from relying on a general justification such as that relied on in the present case: in essence, the public's right to information.

63 Although the exception to the right of access to documents provided for by Article 4(1)(b) of Regulation No 1049/2001 requires the institutions to examine the risk that the protection of privacy and the integrity of the individual may be undermined — through Regulation No 45/2001 and more specifically through Article 8(b) thereof — it must be applied in such a way as to render effective the other provisions of Regulation No 1049/2001. That would not be the case if the institution in receipt of the application for access to documents containing personal data could, on the basis of Article 4(1)(b) of Regulation No 1049/2001, prohibit the applicant from justifying the transfer of data sought on the basis of a general objective such as, in the present case, the public's right to information.

64 Consequently, it cannot be maintained that the general justification given by the applicant for the transfer of personal data to sustain the condition of necessity laid down by Article 8(b) of Regulation No 45/2001 would effectively reintroduce an overriding public interest test within the meaning of Regulation No 1049/2001.

65 In the third place, notwithstanding what is stated in paragraph 51 above, the Court must reject the European Parliament's arguments that a strict interpretation of the condition of necessity imposed by Article 8(b) of Regulation No 45/2001 would be particularly necessary as, in this instance, the applicant's explicit and exclusive aim is the imminent communication to the public of the personal data that would be transferred to him, which would constitute maximum interference with the right to protection of those data. According to the Parliament, Regulation No 45/2001 is not designed to enable disclosure of personal data *erga omnes*.

66 The applicant has expressed his intention to communicate to the public the personal data whose transfer he has requested. However, it is necessary to bear in mind the legal context in which Article 8(b) of Regulation No 45/2001 is applied. As explained in paragraphs 49 and 50 above, the provisions of Regulation No 45/2001 have become applicable in full because an application for access to documents held by the European Parliament was submitted under Regulation No 1049/2001, and the exception under Article 4(1)(b) of that regulation was applied.

67 Even in that context, the purpose of an application for access and its effect, if successful, is to disclose the documents requested, which means, in accordance with Article 2(4) of Regulation No 1049/2001, that the institution or body in receipt of the application makes those documents available to the public. There can be no question of interpreting the conditions to which the transfer of personal data is subject under Regulation No 45/2001, particularly those laid down by Article 8(b), as meaning that one of those conditions would, as a matter of principle, have the effect of access to the documents containing those data being granted only to the applicant and being denied to the public, and thus of it being impossible for Regulation No 1049/2001 to be applied. Where the person requesting access to the documents containing the personal data has established the necessity of having them transferred, and the institution in question has taken the view that there is no reason to assume that the data subjects' legitimate interests might be prejudiced, the data may be transferred and, provided that none of the exceptions provided for by Regulation No 1049/2001 applies, other than that relating to the undermining of the protection of privacy and the integrity of the individual, the document(s) containing the data are to be disclosed and, therefore, made available to the public.

68 It follows from paragraphs 49 to 67 above that the test of necessity laid down in Article 8(b) of Regulation No 45/2001 must be strictly interpreted; that the condition of the necessity of having the personal data transferred entails an examination of necessity by the relevant institution or body in the light of the objective pursued by the applicant for access to the documents, which restricts the scope of the rule on the absence of justification for an application for access; that the justification for the necessity of having those data transferred, invoked by the applicant, may be of a general nature; and that Regulation No 1049/2001 must not be rendered devoid of purpose by an interpretation of the relevant provisions that would mean that legitimate disclosure could never have the aim of full disclosure to the public.

Assessment of the justification given for the necessity of the transfer of the personal data

69 In essence, the applicant takes the view that he has established the necessity of having the personal data transferred, the test laid down by Article 8(b) of Regulation No 45/2001, as interpreted in the light of the judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above (EU:C:2010:378, paragraph 63), and *Dennekamp* v *Parliament*, cited in paragraph 4 above (EU:T:2011:688, paragraphs 31 to 35), and has made an express link between the aim pursued by his application for access and the necessity of disclosing all the names requested.

70 For the purpose of responding to the applicant's claims, it is appropriate to set out, first of all, the justification for the necessity of having the personal data at issue transferred that was provided during the administrative procedure, and the European Parliament's assessment in that regard in the contested decision, before giving the Court's assessment in the light of the arguments exchanged before it.

– The European Parliament's assessment in the contested decision of the necessity of the transfer of the personal data

71 It should be noted that, as regards the necessity of having the personal data transferred, the initial application highlighted the need for the public to have a better understanding of how decisions were taken and the fact that, to that end, a debate could be generated through press reporting. In this case,

it was said to be of the utmost importance for European citizens to know which MEPs had a personal interest in the additional pension scheme when called upon to take decisions regarding its management.

72 In the confirmatory application, the applicant took the view that the transfer of personal data was necessary, relying on the right to information and the right to freedom of expression. He explained that it was necessary for the documents requested to be disclosed so that he could report on the manner in which public money was being spent, on the possible impact of private interests on the voting behaviour of the MEPs and on the functioning of control mechanisms. With that aim in mind, he indicated that it was essential for the purpose of his report to know the names of the MEPs concerned, in order to exercise his freedom of expression and to communicate that information to the public which, as citizens and taxpayers, had an interest in it. According to him, the disclosure of the names of the MEPs participating in the additional pension scheme would ensure that they could not use their votes to influence the scheme so as to benefit from it in a manner that would not accord with the wishes of their voters. According to the applicant, there is no other way for the public to find out how MEPs have exercised their public powers with regard to the scheme.

73 In the contested decision, the European Parliament found, principally, that the applicant had not established the necessity of having the personal data transferred, relying on two separate grounds in order to reject the reasons put forward. First, the Parliament identified the interest of the public and the media in the expenditure of public money, which includes the financial benefits enjoyed by MEPs, as constituting one justification for the application in the context of the freedom of information and the freedom of expression. On that point, it took the view that the public interest asserted was abstract and very general, and that if this argument were a valid argument in the context of Article 8(b) of Regulation No 45/2001, it would allow for the disclosure of personal data beyond any reasonable limit, and would result in a situation that would not be in line with EU rules on data protection. Secondly, the Parliament stated that the applicant had failed to provide a link between his aims and the specific personal data he had requested to be transferred, the reasons why the transfer was necessary being unclear. It went on to note that, in order to exercise public control, it was neither necessary nor proportionate to request the names of all members of the additional pension scheme as decisions on that scheme were adopted by the Bureau, and pointed out that the applicant should have identified a particular and specific risk of conflict of interest in order to prove the necessity of the data transfer.

– Arguments of the parties

74 By his first claim, the applicant submits that his justification for the necessity of having the personal data transferred was that this was information of public interest which, as a journalist, he could present to European citizens so that they would know how public money was spent, how their elected representatives conducted themselves and whether the voting behaviour of those representatives with regard to the additional pension scheme had been influenced by their financial interest. By his second claim, the applicant states that he expressly established a link between the aim of his application and the necessity of disclosing all the names requested, which is the only way for the public to hold its representatives accountable for their actions in relation to the scheme. He was not obliged to be more precise in his application regarding those MEPs who were members of the Bureau.

75 In the view of the Republic of Finland, the Kingdom of Sweden and the EDPS, the disclosure of the requested information is justified by the general public interest in transparency, which must make it possible to provide the public with a meaningful assessment of the facts relating to the additional pension scheme, such as the voting behaviour of MEPs, and to offer the opportunity of interviewing or hearing those MEPs; by the fact that the threshold for establishing whether the transfer of personal data is necessary must be low when the exception to the right of access provided for in Article 4(1)(b)

of Regulation No 1049/2001 is to be interpreted; and by the fact that necessity for the purposes of that article may be based on reasons relating to the public interest, as the applicant precisely and specifically argued in his application for access.

76 The European Parliament's principal contention is that the applicant does not satisfy the requirements of proportionality stemming from EU case-law in order to establish the necessity of having the personal data in question transferred. It observes that that interpretation of 'necessity' is consistent with Article 15 TEU and with Regulation No 1049/2001. This is, *a fortiori*, the case when, as in this instance, the purpose of the application for the transfer of personal data is the disclosure of the data to the public, which constitutes maximum interference with the right to protection of the data. In the Parliament's view, Regulation No 45/2001 is not designed to enable disclosure *erga omnes*, but to allow the exclusive transfer of personal data to specific recipients. Furthermore, it notes that the applicant did not, prior to the adoption of the contested decision, provide any argument objectively substantiating the alleged public interest, in particular as to the existence, currently, of a public debate on the additional pension scheme or the questionable behaviour of an MEP, as envisaged by the judgment in *Dennekamp* v *Parliament*, cited in paragraph 4 above (EU:T:2011:688).

– Findings of the Court

77 As noted in paragraph 59 above, if the condition of necessity laid down by Article 8(b) of Regulation No 45/2001, which is to be interpreted strictly, is to be fulfilled, it must be established that the transfer of personal data is the most appropriate of the possible measures for attaining the applicant's objective, and that it is proportionate to that objective. In the present case, it is appropriate to answer together the two claims that the transfer of data in question is the most appropriate measure for attaining the objectives pursued.

78 So far as concerns the objectives in the light of which the applicant maintained in his confirmatory application that it was necessary for the European Parliament to transfer the personal data at issue, a distinction must be made between, on the one hand, public control over the way in which public funds are spent, through the exercise of the right to information, and, on the other hand, the possible influence of MEPs' interests on their voting behaviour in respect of the additional pension scheme, that is to say, the identification of potential conflicts of interest of MEPs.

79 In the first place, the applicant states his intention to present information on the additional pension scheme through articles in the press and television reporting, to allow the public to participate in a legitimate debate about the scheme, emphasising particularly his role as a journalist in a democratic society.

80 To that end, the applicant argued at the hearing that the necessity of the transfer of personal data had to be assessed in the light of Article 9 of Directive 95/46, which laid down specific rules where the processing of such data was being carried out for journalistic purposes, because Article 4(1)(b) of Regulation No 1049/2001 referred to EU legislation regarding the protection of personal data without giving further details. However, it is apparent from the provisions of Article 76(d), in conjunction with Article 84(1), of the Rules of Procedure of the General Court that the application initiating proceedings must state the subject-matter of the proceedings and contain a summary of the pleas in law relied on, and that no new plea in law or argument may be introduced in the course of proceedings unless it is based on matters of law or of fact which come to light in the course of the procedure (judgment of 21 October 2010 in *Umbach* v *Commission*, T-474/08, EU:T:2010:443, paragraph 60) or it is a plea or an argument that amplifies a plea put forward previously, whether directly or by implication, in the original application, and which is closely connected therewith (see judgment of 29 November 2012 in *Thesing and Bloomberg Finance* v *ECB*, T-590/10, EU:T:2012:635, paragraph 24 and the case-law cited). That is not the case in this instance, and that argument, belatedly put forward, must be rejected as inadmissible.

81 In so far as the applicant relied in his confirmatory application on the right to information and on the right to freedom of expression in order to justify the necessity of having the personal data at issue transferred, it must be held that that is not sufficient to establish that the transfer of the names of the MEPs participating in the additional pension scheme is the most appropriate of the possible measures for attaining his objective or that it is proportionate to that objective.

82 It is true that, by his arguments, the applicant clearly specified his aims and the reasons why he regarded the transfer of the data as being necessary: in essence, to produce a report on the additional pension scheme in order to make the European public aware of how the scheme operates and to exercise oversight over the MEPs who represent it. In so doing, he did not, however, make clear in what respect transferring the names of the MEPs participating in the scheme was the most appropriate measure for attaining the objective he had set himself, contrary to the requirement under Article 8(b) of Regulation No 45/2001, as interpreted by the judgment in *Dennekamp* v *Parliament*, cited in paragraph 4 above (EU:T:2011:688, paragraphs 30 and 34).

83 The applicant merely asserted in the confirmatory application that the measures designed to provide public control over public expenditure in the context of the additional pension scheme, like the discharge procedure, did not protect the fundamental rights he had invoked, namely the right to information and to communicate to the public the information gathered, and that those measures could not, therefore, justify the non-disclosure of the data at issue. It must be noted that it cannot be determined from those points in what respect the transfer of the names of MEPs participating in the scheme is the most appropriate measure for attaining the applicant's objective, or how it is proportionate to that objective. The mere assertion that that transfer would best ensure the protection of fundamental rights cannot be considered to have been the result of even a limited analysis of the effects and implications of the various measures that might be adopted in order to meet the applicant's objectives.

84 As regards the applicant's argument that there is already a debate about the additional pension scheme, given the controversy about its creation and funding, or that, even without such a debate, it would be necessary to have the MEPs' names in order to encourage a debate to arise, the applicant is merely relying on arguments that relate to the purpose of his application for access to documents. Those arguments do not establish that it is necessary for him to have the data at issue transferred, no link to the appropriateness or proportionality of the measure requested being apparent, as required by EU case-law (see, to that effect, judgment in *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 34). In addition, the existence of a debate about the scheme, or, more specifically, about the advantageous nature of the scheme for MEPs at the expense of public funds tend, like the various matters of fact alluded to by the applicant, to show that he already has precise information on the rules and operation of the scheme that may enable him to encourage or develop the public debate he seeks to initiate with regard to the sound management of the scheme and to the financial risks to the EU budget. In addition to the absence of proof of the necessity of the transfer of the personal data at issue, it must be noted that those various matters put forward by the applicant himself do not militate in favour of the proposition that it would be necessary to know the names of the MEPs participating in the scheme in order to denounce its allegedly adverse effects on public funds.

85 Next, the same conclusion must be drawn as regards the case-law of the European Court of Human Rights, which ruled that it was not necessary, in a democratic society, to refuse access to information constituting the personal data of an elected official, in the light of the right of journalists to receive and impart information of public interest. It cannot in any way be determined from such a finding whether the measure requested by the applicant is the most appropriate for attaining his objective, or whether it is proportionate to that objective.

86 Lastly, the conclusion reached in paragraph 82 above is also unaffected by the arguments that the applicant made an express link between the aim pursued by his application for access and the necessity of disclosing all the names requested, and that he was not obliged to be more precise in his application, particularly with regard to those MEPs who were members of the Bureau, in view of the possibility of partial disclosure provided for by Article 4(6) of Regulation No 1049/2001. There is nothing in those arguments to demonstrate the necessity of having the names of MEPs participating in the additional pension scheme transferred, as required by Article 8(b) of Regulation No 45/2001.

87 Accordingly, the Court must reject the applicant's arguments regarding the necessity of having the names of MEPs participating in the additional pension scheme transferred in the light of the aim of informing the public and enabling it to take part in a debate on the legitimacy of the scheme; Articles 11 and 42 of the Charter of Fundamental Rights, relating, respectively, to the freedom of expression and to the right of access to documents of the institutions and bodies of the European Union, have not, therefore, been infringed.

88 In the second place, the applicant takes the view that the transfer of personal data at issue is necessary for the purpose of being able to determine whether MEPs' voting behaviour with regard to the additional pension scheme is influenced by their financial interests, the disclosure of all the names of the MEPs participating in the scheme being the only way for the public to hold its representatives accountable for their actions in relation to the scheme.

89 The applicant's arguments are based, both in his confirmatory application and in his written statements, on the necessity of bringing to light possible conflicts of interest of MEPs.

90 First, it must be stated that, in reply to a question put at the hearing, the European Parliament maintained that disclosure of conflicts of interest could not, from a legal perspective, be regarded as a legitimate purpose of the processing of personal data within the meaning of Article 4(1)(b) of Regulation No 45/2001, thereby restating an argument it had put forward in the defence without relating it to that provision. However, it must be noted that the Parliament did not argue, in the contested decision, that transferring the names of MEPs participating in the additional pension scheme would be a processing of personal data that would be incompatible with the legitimate purposes for which the data had been collected. Therefore, that argument must in any event be rejected as having no factual basis, since none of the reasons given for the contested decision includes any such assertion.

91 Secondly, Article 3(1) of the Code of Conduct for Members of the European Parliament with respect to financial interests and conflicts of interest states:

'A conflict of interest exists where [an MEP] has a personal interest that could improperly influence the performance of his or her duties as a Member. A conflict of interest does not exist where a Member benefits only as a member of the general public or of a broad class of persons.'

92 It may also be noted that, for the Council of Europe, a conflict of interest arises from a situation in which a public official has a private interest which is such as to influence, or appear to influence, the impartial and objective performance of his or her official duties, such private interest including any advantage to himself or herself, to his or her family, close relatives, friends and persons or organisations with whom he or she has or has had business or political relations, and also any liability, whether financial or civil, relating thereto (see Article 13 of Recommendation R (2000) 10 of the Committee of Ministers of the Council of Europe to Member States on codes of conduct for public officials, adopted on 11 May 2000).

93 In the case of an elected representative, a conflict of interest therefore presupposes, as the applicant submits, that, when voting on a given subject, that representative's behaviour may be influenced by his private interest. In the present case, the potential conflict of interest lies in the fact that, by voting, MEPs can amend the additional pension scheme or express their views on it in such a way as to promote their interests as beneficiaries of the scheme.

94 In order to be in a position to bring to light potential conflicts of interest of MEPs when they are deciding on the additional pension scheme, it is necessary to know the names of those who are members of the scheme, without the fact that the conflict of interest in question is, as the European Parliament contends, inherent in the duties of members of an elected assembly having any influence on the assessment of the necessity of having the personal data transferred. In itself, that fact cannot in any way establish that the envisaged transfer is not necessary. Such a transfer is therefore the only measure by which the applicant's aim can be attained, no other measure being capable of ensuring that MEPs facing a potential conflict of interest are identified. Consequently, it must be concluded, for the purpose of applying Article 8(b) of Regulation No 45/2001, that the transfer of the names of MEPs participating in the scheme is the most appropriate measure and that it is proportionate for the purpose of determining whether the interests that MEPs have in the scheme can influence their voting behaviour (see, to that effect, judgment in *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraphs 30 and 34).

95 Nevertheless, it must be noted at this stage that, in the present situation, in which the potential conflict of interest lies in the voting behaviour of MEPs, mere disclosure of the identity of those who are members of the additional pension scheme cannot by itself bring the conflict to light. It is also necessary to determine which of the MEPs have been called upon to decide on the scheme in a vote, since the European Parliament maintains that only MEPs who are members of the scheme and of the Bureau — the body which, according to the Parliament, takes decisions on the management of the scheme — could find themselves in a situation in which there is a potential conflict of interest.

96 Yet the applicant did not refer in the confirmatory application only to votes resulting in amendments being made to the management of the additional pension scheme but to any vote in which the European Parliament or one of its bodies decides on the scheme in one way or another. He thus relied on the possible impact of private interests on the voting behaviour of MEPs; the position of MEPs by which they can influence the way in which public funds are used for their benefit; and the lack of any means — other than disclosure of the names of the MEPs who are members of the scheme — of revealing how the elected representatives use their public powers in relation to the scheme.

97 In reply to a measure of organisation of procedure (see paragraph 23 above), the applicant submitted to the Court the measures adopted since 1 October 2005 by which, according to him, the plenary of the European Parliament, the Parliament's Committee on Budgetary Control and the Bureau had made amendments to the additional pension scheme or decided on its management. With regard to the plenary, the acts concerned are Decision 2008/497/EC, Euratom of the European Parliament of 24 April 2007 on the discharge for implementation of the European Union general budget for the financial year 2005, Section I — European Parliament (OJ 2008 L 187, p. 1); Decision 2009/185/EC, Euratom of the European Parliament of 22 April 2008 on discharge in respect of the implementation of the European Union general budget for the financial year 2006, section I — European Parliament (OJ 2009 L 88, p. 1); Decision 2009/628/EC, Euratom of the European Parliament of 23 April 2009 on discharge in respect of the implementation of the European Union general budget for the financial year 2007, Section I — European Parliament (OJ 2009 L 255, p. 1); and Decision 2012/544/EU, Euratom of the European Parliament of 10 May 2012 on discharge in respect of the implementation of the general budget of the European Union for the financial year 2010, Section I — European Parliament (OJ 2012 L 286, p. 1). In the case of the Committee on Budgetary Control, the relevant acts are the draft report of 8 March 2007 on amendments 1 to 21 to the discharge for implementation of the European Union general budget for the financial year 2005, Section I — European Parliament; an information document

concerning the committee's opinion on budgetary discharge for the financial year 2006; and a committee report on budgetary discharge for the financial year 2010. As regards the Bureau, the documents concerned are the decision of 30 November 2005 on the management of the scheme; the decision of 19 May and 9 July 2008 concerning implementing measures for the Statute for Members of the European Parliament (OJ 2009 C 159, p. 1); the decision of 9 March 2009 on the voluntary pension scheme; and the decision of 1 April 2009 on the voluntary pension scheme.

98 Decision 2005/684/EC, Euratom of the European Parliament of 28 September 2005 adopting the Statute for Members of the European Parliament (OJ 2005 L 262, p. 1) must be disregarded at the outset, since that decision is beyond the scope of the application for access to documents made by the applicant, which relates, in particular, to a list of names of MEPs participating in the additional pension scheme after September 2005. The same must apply to the information document on the opinion of the Committee on Budgetary Control on budgetary discharge for the financial year 2006 and that committee's report on budgetary discharge for the financial year 2010, which merely refer indirectly to decisions or votes without identifying them clearly.

99 Next, it must be noted, on reading the replies of the main parties to the measure of organisation of procedure, that the four decisions of the plenary mentioned in paragraph 97 above, each of which contains a decision granting the President of the European Parliament discharge in respect of the implementation of the budget and observations set out in a resolution, were subject to a vote on the discharge decisions themselves and on the resolutions. When questioned at the hearing, the Parliament was unable to specify whether, in respect of each of those decisions and resolutions, votes had been cast as overall votes or as separate votes on particular paragraphs or proposals for amendment of certain paragraphs.

100 The written questions put to the European Parliament after the end of the hearing thus related in particular to the identification of the specific voting procedures applied in respect of the four budgetary discharge decisions mentioned above and the four accompanying resolutions, adopted in plenary.

101 It is apparent from the European Parliament's reply that while each of the four discharge decisions referred to in paragraph 97 above and each of the accompanying resolutions was adopted on the basis of an overall vote in plenary, the votes on the resolutions on discharge for the financial year 2005, held on 24 April 2007, discharge for the financial year 2006, held on 22 April 2008, and discharge for the financial year 2010, held on 10 May 2012, were each preceded by separate votes on amendments and on specific paragraphs of the draft resolutions. In the case of the resolution on discharge for the financial year 2005, paragraphs 74 to 84 of the draft resolution, which concern the additional pension scheme, were the subject of separate votes, during which MEPs expressed their views. In the case of the resolution on discharge for the financial year 2006, paragraphs 70 to 73, which concern the scheme, were adopted in the same way. The same applies in the case of the resolution on discharge for the financial year 2010 with regard to paragraphs 98 and 99 of the draft resolution, which concerned the scheme.

102 It follows from the above that all MEPs forming part of the plenary were entitled to decide on the additional pension scheme on 24 April 2007, on 22 April 2008 and on 10 May 2012.

103 Consequently, in order to enable the applicant to attain his aim of bringing to light potential conflicts of interest of MEPs, the European Parliament would have had to transfer the names of those MEPs participating in the additional pension scheme who were also members of the plenary on the dates mentioned in paragraph 102 above and who actually took part in the votes held on those dates, not just the names of those who took part in the votes organised in accordance with the procedure for voting by roll call provided for by Article 180 of the Rules of Procedure of the Parliament, as the applicant's remarks in his observations lodged on 2 February 2015 might suggest. Irrespective of the

voting procedure used in the votes relating to the scheme, all the MEPs who actually voted and who were members of the scheme could be influenced by their personal interest in that regard (see paragraph 102 above).

104 It follows from the foregoing that it is not necessary to examine the precise voting procedures applied by the Committee on Budgetary Control or the Bureau, since their members are also members of the plenary.

105 Thirdly, in the European Parliament's view it is inherently impossible to determine whether or not MEPs have really been influenced by their own financial interests or by any other — legitimate or illegitimate — motive when called upon to decide on the additional pension scheme, since the identification of MEPs participating in the scheme would not provide any information on the subjective reasons for their votes on the scheme.

106 However, the concept of a conflict of interest does not relate only to a situation in which a public official has a private interest which has actually influenced the impartial and objective performance of his official duties — in this case that of an elected representative in the European Parliament — but also to a situation in which the interest identified may, in the eyes of the public, appear to influence the impartial and objective performance of his official duties. Furthermore, the disclosure of potential conflicts of interest is not aimed only at revealing those cases in which the public official has performed his duties with the intention of satisfying his private interests, but also at informing the public of the risks of public officials being subject to conflicts of interest, so that they act impartially in the performance of their official duties, after, in view of the circumstances in which they find themselves, having declared the potential conflict of interest to which they are subject and taken or proposed measures to resolve or avoid that conflict. Accordingly, the Parliament's argument is unfounded and must be rejected, the subjective reasons for a vote cast by an elected representative being, moreover, inherently unascertainable.

107 Fourthly, for the same reasons as those set out in paragraph 106 above, the Court must reject the European Parliament's argument concerning the applicant's lack of proof of a debate on the potential conflicts of interest of MEPs in relation to the additional pension scheme or on the behaviour of a specific MEP.

108 Fifthly, it is also evident from the reasoning in paragraphs 91 to 106 above that the rule under which it follows from Regulation No 45/2001, as interpreted by the judgment in *Dennekamp* v *Parliament*, cited in paragraph 4 above (EU:T:2011:688, paragraphs 34 and 35), that it is incumbent on the person requesting the transfer of personal data accurately to provide evidence of the fact that that transfer is necessary cannot lead to the consequences that the European Parliament's arguments would imply.

109 First of all, contrary to the European Parliament's contention, it must be noted that the applicant set out the reasons why he needed to find out which MEPs were members of the additional pension scheme, notably as regards the possibility of thereby revealing potential conflicts of interest that might influence the performance of their duties.

110 Next, while the European Parliament seeks to argue that the applicant was obliged accurately to adduce all the evidence of the existence of conflicts of interest in order to establish the necessity of the transfer, it should be noted that, for the purpose of bringing to light the potential conflicts of interest of MEPs voting on the additional pension scheme, the applicant was, as a matter of law, entitled merely to show that they were in that situation because of their dual role as MEPs and as members of the scheme. The concept of a conflict of interest relates to a situation in which the interest identified may, in the eyes of the public, appear to influence the impartial and objective performance of official duties (see paragraph 106 above) and does not, therefore, require the lack of any impartial performance of the duties in question to be demonstrated. More specifically, the applicant cannot be

criticised for not having himself identified the body within the Parliament that was required to decide on the scheme, and thus the group of MEPs concerned, before requesting that the names of the relevant MEPs be transferred.

111 A contrary interpretation would mean that the applicant was required to apply, initially, for access to documents identifying those bodies within which the additional pension scheme had been voted upon, and, in the light of the result obtained, to apply, secondly, for access to the documents identifying the MEPs who actually took part in the vote on that point, and then to the documents identifying the MEPs participating in the scheme. There is nothing in Regulation No 1049/2001 to require an applicant for access to the documents held by an institution or body of the European Union to adopt that approach, nor can it be inferred from the application of Regulation No 45/2001 with respect to documents containing personal data.

112 Sixthly, the European Parliament claims that the interest underpinning the request for the names of MEPs participating in the additional pension scheme to be transferred is based entirely on the assessment of the journalist applying for access to documents — in this instance, the applicant — and not on objective grounds. In so doing, however, the Parliament loses sight of the fact that the applicant relied on the existence of potential conflicts of interest on the part of MEPs who are members of the scheme when it is voted upon, which is not a subjective assessment of a given situation but a statement as to a risk to the impartial and objective performance of official duties by the MEPs concerned.

113 Consequently, it follows from paragraphs 88 to 112 above that the European Parliament made a manifest error of assessment in finding that the applicant had not established the necessity of the transfer of the names of those MEPs participating in the additional pension scheme who, as members of the plenary, had actually voted on the scheme in the votes held on 24 April 2007, 22 April 2008 and 10 May 2012, having regard to the aim of bringing to light potential conflicts of interest.

114 It is appropriate, however, to examine the action further by analysing the arguments relating to the application of the second cumulative condition for the transfer of personal data required by Article 8(b) of Regulation No 45/2001, that is that there is no reason to assume that transferring the names of the members of the plenary participating in the additional pension scheme who took part in a vote on it could prejudice their legitimate interests.

Application of the condition under Article 8(b) of Regulation No 45/2001 relating to the lack of a legitimate interest in the protection of privacy of MEPs

115 The second part of the plea is divided into three claims which overlap. By the first claim, the applicant submits that the MEPs have no legitimate interest in the protection of their privacy for the purposes of Article 8(b) of Regulation No 45/2001, as they open their conduct to a significant degree of public scrutiny. By his second claim, the applicant takes the view that the European Parliament failed in the contested decision to establish that the legitimate interests of the MEPs would be prejudiced by the disclosure of the requested documents. By his third claim, he asserts that even if the Parliament had rightly considered that the requested information fell within the MEPs' private sphere, that would not be sufficient to protect it as a legitimate interest within the meaning of Article 8(b) of Regulation No 45/2001, which requires a weighing up of the interests engaged.

116 It should be noted at the outset that, according to the case-law, once the necessity of having the personal data transferred is established, the institution or body of the European Union in receipt of an application for access to documents containing such data must weigh up the various interests of the parties concerned and verify whether there is any reason to assume that the data subjects' legitimate interests may be prejudiced by that transfer, as required by Article 8(b) of Regulation No 45/2001

(see, to that effect, judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 78, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 30).

117 That requirement must lead the EU institution or body in receipt of the application to refuse to transfer the personal data if it is found that there is the slightest reason to assume that the data subjects' legitimate interests would be prejudiced.

118 In the first place, the applicant's entire argument in support of the second part of the first plea is based on the premiss that the public nature of MEPs' duties and of their status is such that their legitimate interests should not enjoy the same degree of protection as those of individuals who are not public figures. As regards MEPs' interests, a distinction should be made between those falling into the public sphere, which must be subject to a lesser degree of protection when being weighed against an interest that would favour the transfer of personal data, and those forming part of the private sphere, which must be protected.

119 As the European Parliament acknowledges, the distinction which the applicant makes in the case of public figures between the public and private spheres is relevant for the purposes of determining the degree of protection of personal data to which they are entitled under the rules in Regulation No 45/2001, even if that regulation does not contain any such rule. It would be entirely inappropriate for an application for the transfer of personal data to be assessed in the same way irrespective of the identity of the data subject. Public figures have chosen to expose themselves to scrutiny by third parties, particularly the media and, through them, by a lesser or greater general public depending on the policy area, even if such a choice in no way implies that their legitimate interests must be regarded as never being prejudiced by a decision to transfer data relating to them. Thus, public figures have generally already accepted that some of their personal data will be disclosed to the public, and may even have encouraged or made such disclosure themselves. It is necessary therefore to take that environment into account when assessing the risk of the legitimate interests of public figures being prejudiced in the context of the application of Article 8(b) of Regulation No 45/2001, and in weighing those interests against the necessity of transferring the personal data requested.

120 In that context, it is appropriate, for the purposes of assessing the risk of MEPs' legitimate interests being prejudiced in this case — interests which undeniably include certain aspects of their professional activities, such as aspects of remuneration — to take into particular consideration the link between the personal data at issue, namely the names of MEPs participating in the additional pension scheme who have voted on it, and their mandate. The possibility of being a member of the scheme is open only to MEPs. Thus, having a mandate as a Member of the European Parliament is the first condition and is necessary in order to benefit from the additional pension provided under the scheme. For that principal reason, the personal data at issue fall into the public sphere of MEPs.

121 In the light of that feature, which limits the scope of application of the additional pension scheme to MEPs alone, the fact that membership of the scheme is optional and a result of voluntary affiliation, and thus does not arise automatically as a result of their mandate, or that the additional pension is paid after the end of their mandate (which, moreover, is in the very nature of any retirement pension), is not determinative as regards the inclusion of the personal data at issue in the private sphere of MEPs. It is also necessary to take into consideration not only the link with the MEP's mandate, but also all the information given by the applicant (not disputed by the European Parliament and indeed confirmed by the contents of the case-file) concerning the operation of the scheme, namely the Parliament's funding of two thirds of the contributions paid, the fact that it makes up shortfalls in the scheme and its commitment to compensating any losses suffered by the scheme, which, according to the applicant, thus ensures the preservation of the acquired pension rights of MEPs who are members of the scheme. These are matters which reinforce the proposition that the personal data at issue belongs in the public sphere of MEPs, denoting as they do the significant financial and legal commitment of the Parliament to the scheme.

122 Account must also be taken of the case-law according to which the additional pension scheme is part of the statutory provisions which are intended, as a matter of general interest, to ensure the financial independence of MEPs and, moreover, decisions taken in that respect by the competent bodies of the European Parliament must be regarded as measures of internal organisation which are intended to ensure its proper functioning and which fall within the rights conferred by public law on the Parliament so that it is able to perform the tasks entrusted to it, the rights and obligations under that scheme being a matter of public law (see, to that effect, judgments in *Purvis* v *Parliament*, cited in paragraph 26 above, EU:T:2011:600, paragraphs 60 and 61, and of 13 March 2013 in *Inglewood and Others* v *Parliament*, T-229/11 and T-276/11, ECR, EU:T:2013:127, paragraph 61).

123 The European Parliament's argument that contributions to the additional pension scheme relate to the private financial situation of MEPs must be rejected in view of the connection that can be made between the financial elements of the scheme, of which contributions form part, and the public sphere of MEPs. The same reasoning applies in respect of the Parliament's argument that the voting behaviour of MEPs, which is always part of their public sphere, must be distinguished from their membership of the scheme, which, according to the Parliament, falls into their private sphere. Moreover, transferring the names of the MEPs who are members of the scheme merely reveals their affiliation without disclosing any information about their financial situation, including their assets, their savings or the instruments in which the funds paid into the scheme are invested.

124 Having regard to the foregoing, it must therefore be held that, in weighing up the interests engaged, the legitimate interests of the MEPs who are members of the additional pension scheme, which fall into the public sphere of those MEPs, must be subject to a lesser degree of protection than that which, following the logic of Regulation No 45/2001, would be enjoyed by the interests falling into their private sphere.

125 In the second place, it must be borne in mind that, even in that context, personal data are transferred only if there is no reason to assume that the legitimate interests of the data subjects may be prejudiced by that transfer. However, the slightest degree of protection of the names of MEPs who are members of the additional pension scheme has the effect of giving greater weight to the interests represented by the aim of the transfer.

126 As the applicant argues, bringing to light potential conflicts of interest of MEPs, which is the aim of the transfer of data requested, ensures better scrutiny of the actions of MEPs and of the functioning of an EU institution which represents the peoples of the Member States, and improves the transparency of its actions. Contrary to the European Parliament's contention at the hearing, such interests may be lawfully taken into consideration in the weighing up of interests that must be carried out under Article 8(b) of Regulation No 45/2001 (see paragraphs 61 to 63 above). Consequently, in view of the importance of the interests invoked here, which are intended to ensure the proper functioning of the European Union by increasing the confidence that citizens may legitimately place in the institutions, it must be held that the legitimate interests of the MEPs who are members of the additional pension scheme, as defined in paragraphs 120 and 121 above, cannot be prejudiced by the transfer of the personal data at issue.

127 The weighing up of the interests engaged ought therefore to have resulted in approval of the transfer of the names of the MEPs participating in the additional pension scheme who took part in votes on it, since the European Parliament cannot lawfully maintain that there is a legally binding presumption favouring the legitimate interests of the data subjects to whom the personal data to be transferred relate. Nothing in the wording of Article 8(b) of Regulation No 45/2001 militates in favour of such a presumption being recognised, since the assessment of an application for personal data to be transferred requires the interests engaged to be weighed up after the applicant has established that there is a necessity for the data to be transferred (see, to that effect, judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 79, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 34), a condition which is to be

interpreted strictly and requires the applicant to provide express and legitimate reasons for the necessity he invokes. Moreover, the Parliament wrongly relies on Regulation No 1049/2001 in order to justify the existence of such a presumption, noting that the regulation permits exceptions to the right to transparency. While Regulation No 1049/2001 does indeed provide for an exception to the right of access to documents where disclosure would risk undermining the privacy or the integrity of the individual, thus making Regulation No 45/2001 applicable, that does not have the effect of creating a presumption in favour of the legitimate interests of persons whose personal data are protected by the latter regulation.

128 Among the other arguments put forward by the European Parliament, its criticism of the proportionate nature of the measures requested by the applicant is ineffective. In arguing that point, the Parliament challenges the necessity of transferring the names of the MEPs participating in the additional pension scheme for the purpose of attaining the applicant's objectives, and not the weighing up of the interests engaged.

129 Other arguments put forward by the European Parliament must be rejected as unfounded, as, for example, when it contends that, were the applicant's arguments to be accepted, MEPs would no longer be entitled to any privacy, and that the transfer of personal data would endanger the independence of their mandate. No proper evidence is adduced in support of such assertions, whereas the limited nature of the information disclosed by the transfer of data at issue must be emphasised, and there is nothing to explain how the independence of an MEP's mandate would be damaged if the public knew of his membership of the additional pension scheme. The same applies in respect of the argument concerning the fact that MEPs might attract criticism from the public in relation to an alleged conflict of interest. Since such a conflict is inherent in the function of Member of the European Parliament, any criticisms may already be made by any member of the public familiar with the issues concerning the scheme, even if that person is not precisely aware of the names of MEPs potentially affected by such a conflict of interest. Furthermore, it must be noted that the applicant voices such criticism in a representative capacity through his various written pleadings.

130 Accordingly, it must be held that the European Parliament made a manifest error of assessment in finding that the legitimate interests of MEPs participating in the additional pension scheme who took part in a vote on it might be prejudiced by the transfer of their names.

131 It is appropriate to examine the action further, since the European Parliament's error of assessment in applying the two cumulative conditions under Article 8(b) of Regulation No 45/2001 relates only to those members of the plenary who took part in the votes on the additional pension scheme on 24 April 2007, 22 April 2008 and 10 May 2012, and not to those who did not participate in those votes or those not yet, or no longer, in office on the ground, inter alia, that their mandate had previously ended, which includes those who had exercised their pension rights.

Second plea in law, alleging failure to state reasons

132 In essence, the applicant submits that the conclusion of the contested decision, that the obligation to protect privacy in relation to personal data prevails over the requirement of transparency, is vitiated by the failure to state reasons. The European Parliament, he submits, failed to explain how the disclosure of the documents requested would specifically and actually undermine the privacy of the MEPs whose names appeared in those documents.

133 It must be borne in mind that if the institution concerned decides to refuse access to a document which it has been asked to disclose, it must, in principle, explain how disclosure of that document could specifically and actually undermine the interest protected by the exception — among those provided for in Article 4 of Regulation No 1049/2001 — upon which it is relying (judgments in *Sweden* v *MyTravel and Commission*, cited in paragraph 35 above, EU:C:2011:496, paragraph 76, and

of 28 March 2012 in *Egan and Hackett* v *Parliament*, T-190/10, EU:T:2012:165, paragraph 90). Such an explanation cannot therefore consist of a mere assertion that access to certain documents would undermine privacy within the meaning of Article 4(1)(b) of Regulation No 1049/2001 (judgment in *Egan and Hackett* v *Parliament*, EU:T:2012:165, paragraph 91).

134 It should also be borne in mind that, where a request based on Regulation No 1049/2001 seeks access to documents including personal data, Regulation No 45/2001 becomes applicable in its entirety, including Article 8 thereof (judgments in *Commission* v *Bavarian Lager*, cited in paragraph 4 above, EU:C:2010:378, paragraph 63, and *Dennekamp* v *Parliament*, cited in paragraph 4 above, EU:T:2011:688, paragraph 26).

135 Therefore where, as in the present case, Article 8(b) of Regulation No 45/2001 is applicable to an application for access to documents, the examination of the specific and actual nature of the undermining of the interest protected by the exception provided for in Article 4(1)(b) of Regulation No 1049/2001 is indissociable from the assessment of the risk that the legitimate interests of the data subject might be prejudiced by the transfer of personal data, since the legitimate interests referred to in Article 8(b) of Regulation No 45/2001 overlap with the privacy and the integrity of the individual referred to by Article 4(1)(b) of Regulation No 1049/2001, which, through the disclosure of certain aspects thereof to the public, are liable to be prejudiced by the transfer of personal data.

136 Furthermore, it is clear from the case-law that the statement of reasons required by Article 296 TFEU must be appropriate to the act 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 competent Court to exercise its power of review. The requirements to be satisfied by the statement of reasons depend on the circumstances of each case, in particular the content of the measure in question, the nature of the reasons given and the interest which the addressees of the measure, or other parties to whom it is of direct and individual concern, may have in obtaining explanations. 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 296 TFEU 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 (see judgment of 1 February 2007 in *Sison* v *Council*, C-266/05 P, ECR, EU:C:2007:75, paragraph 80 and the case-law cited).

137 According to the applicant, the statement of reasons for the contested decision does not explain how the disclosure of the documents requested would specifically and actually undermine the privacy of the MEPs participating in the additional pension scheme.

138 In the contested decision, the European Parliament took the view that it would not be proportionate to allow the transfer of personal data at issue, given the weight of the data subjects' legitimate interests. It expressed its view that the scope of MEPs' legitimate interests was certainly less far-reaching than those of a private person without any public commitment, while asserting that the protection mechanisms provided for by Regulation No 45/2001 did apply in the present case and that the MEPs had legitimate interests in not having the data at issue disclosed, such data falling into their private sphere and thus constituting a legitimate interest to be protected as data concerning their personal financial situation. According to the Parliament, pension contributions and the resulting pension rights are always private concerns, and the link with the MEP's mandate or the method of funding the additional pension scheme has no relevance. The Parliament went on to find that, if that were not the case, the applicant's proposition would apply to any member of staff of a public authority. It reiterated its view that the transfer of the data at issue, which is based on the general interest of the media and the general public in the personal financial situation of MEPs, was not proportionate, as, if it were otherwise, the media and the public would have access to all the private data of MEPs and of public officials involving public expenditure. It disputed the applicant's argument that the disclosure of the

documents requested would be more appropriate than the measures designed to provide public control of public expenditure. It concluded, in the light of these matters, that the legitimate interests of MEPs should prevail over the alleged necessity of the transfer of the data at issue.

139 It is apparent from the contested decision that the risk of MEPs' legitimate interests, and thus their privacy, being undermined lies in the fact that, falling as they do into the private sphere of MEPs, the personal data at issue constitute a legitimate interest to be protected on the ground that they concern the personal financial situation of MEPs, pension contributions and resulting pension rights being private matters. The other findings made by the European Parliament in weighing up the interests at stake, set out in paragraph 138 above, do not relate to an evaluation of the risk of the legitimate interests or privacy of MEPs being undermined.

140 Since examination of the specific and actual nature of the undermining of the interest protected by the exception provided for in Article 4(1)(b) of Regulation No 1049/2001 is indissociable from the assessment of the risk that the legitimate interests of the data subject might be prejudiced, as referred to in Article 8(b) of Regulation No 45/2001, it must be noted that the European Parliament carried out the latter assessment, stating that the personal data at issue fell into the private sphere of MEPs, were subject to a higher degree of protection under that regulation and therefore had to be protected as legitimate interests. It noted that contributions to a pension scheme and the resulting pension rights were private concerns, irrespective of the scheme in question and of the manner in which it was funded, that the retirement pension under the additional pension scheme was paid after the end of a mandate and that MEPs had to pay a significant personal financial contribution, which was not reimbursed by the Parliament.

141 The European Parliament's reasoning in the contested decision is relatively succinct but none the less allows both the addressee of the decision and the Court to understand the reasons why the Parliament concluded that there was a risk that MEPs' legitimate interests would be prejudiced if the transfer of personal data at issue were authorised. Since such an assessment necessarily encompasses an assessment of the risk of the privacy and the integrity of MEPs being specifically and actually undermined, the applicant's argument, which is somewhat lacking in detail, must, in consequence, be rejected.

142 Accordingly, the second plea in law must be dismissed.

143 It follows from all the foregoing that the action is devoid of purpose in so far as access is sought to the names of the 65 MEPs who were members of the additional pension scheme and applicants in the cases giving rise to the order in *Albertini and Others and Donnelly* v *Parliament*, cited in paragraph 25 above (EU:T:2010:519) and to the judgment in *Purvis* v *Parliament*, cited in paragraph 26 above (EU:T:2011:600); that the contested decision must be annulled in so far as the European Parliament refused to grant access to the names of the MEPs who were members of the scheme and who, as members of the plenary, actually took part in the votes on the scheme held on 24 April 2007, 22 April 2008 and 10 May 2012; and that the action must be dismissed as to the remainder.

Costs

144 Under Article 134(1) 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 However, pursuant to Article 134(2) and (3) of the Rules of Procedure, the Court may order that the costs be shared or decide that the parties are to bear their own costs where each party succeeds on some and fails on other heads.

145 Since the European Parliament has been largely unsuccessful, it must be ordered to bear its own costs and to pay three quarters of those incurred by the applicant. The applicant shall bear one quarter of his own costs.

146 Under Article 138(1) of the Rules of Procedure, the institutions and the Member States which have intervened in the proceedings are to bear their own costs. In the present case, the EDPS, the Republic of Finland and the Kingdom of Sweden shall bear their own costs.

On those grounds,

THE GENERAL COURT (Fifth Chamber)

hereby:

1. Declares that there is no need to adjudicate on the application for annulment of Decision A(2012) 13180 of the European Parliament of 11 December 2012 refusing to grant Mr Gert-Jan Dennekamp access to certain documents relating to the affiliation of certain Members of the European Parliament to the additional pension scheme in so far as access is thereby refused to the names of the 65 Members of the European Parliament who were applicants in the cases giving rise to the order of 15 December 2010 in *Albertini and Others and Donnelly* v *Parliament* (T-219/09 and T-326/09, ECR, EU:T:2010:519) and to the judgment of 18 October 2011 in *Purvis* v *Parliament* (T-439/09, ECR, EU:T:2011:600);

2. Annuls Decision A(2012) 13180 in so far as access is thereby refused to the names of Members participating in the additional pension scheme of the European Parliament who, as members of the Parliament's plenary, actually took part in the votes on that additional pension scheme held on 24 April 2007, 22 April 2008 and 10 May 2012;

3. Dismisses the action as to the remainder;

4. Orders the European Parliament to bear its own costs and to pay three quarters of those incurred by Mr Dennekamp;

5. Orders Mr Dennekamp to bear one quarter of his own costs;

6. Orders the European Data Protection Supervisor (EDPS), the Republic of Finland and the Kingdom of Sweden to bear their own costs.

Dittrich Schwarcz Tomljenović

Delivered in open court in Luxembourg on 15 July 2015.

[Signatures]

Commission, du 7 avril 2004, relatif aux procédures mises en œuvre par la Commission en application des articles 81 [CE] et 82 [CE] (JO L 123, p. 18), rejetant la plainte des requérants relative à des infractions au traité CECA (affaire COMP/37.037-SWSMA).

Dispositif

1) Le recours est rejeté.

2) La Commission européenne supportera, outre ses propres dépens, les dépens de M. Glen Jones et de M^me^ Daphne Jones, ainsi que ceux de Fforch-Y-Garon Coal Co. Ltd.

3) Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, E.ON UK plc et International Power plc supporteront chacun leurs propres dépens.

Arrêt du Tribunal (deuxième chambre) du 23 novembre 2011 — Dennekamp/Parlement

(affaire T-82/09)

« Accès aux documents — Règlement (CE) nº 1049/2001 — Documents relatifs à l'affiliation de certains membres du Parlement européen au régime de pension complémentaire — Refus d'accès — Exception relative à la protection de la vie privée et de l'intégrité de l'individu — Article 8, sous b), du règlement (CE) nº 45/2001 — Transfert de données à caractère personnel »

1. *Union européenne — Institutions — Droit d'accès du public aux documents — Règlement nº 1049/2001 — Exceptions au droit d'accès aux documents — Protection de la vie privée et de l'intégrité de l'individu — Portée — Obligation d'appréciation en conformité avec la législation de l'Union relative à la protection des données à caractère personnel — Applicabilité intégrale des dispositions du règlement nº 45/2001 à toute demande d'accès à des documents comprenant des données à caractère personnel [Règlements du Parlement européen et du Conseil nº 45/2001, art. 8, et nº 1049/2001, art. 4, § 1, b)] (cf. points 21-26, 38-40)*

2. *Rapprochement des législations — Protection des personnes physiques à l'égard du traitement des données à caractère personnel — Traitement de ces données par les institutions et organes de l'Union — Demande d'accès à des documents mentionnant les noms des membres du Parlement affiliés au régime de pension complémentaire — Données à caractère personnel — Demande d'accès auxdits documents au titre du règlement nº 1049/2001 — Obligation d'établir la nécessité du transfert desdites données [Règlements du Parlement européen et du Conseil nº 45/2001, art. 2, a), 5, b) et 8, b), et nº 1049/2001, art. 4, § 1, b)] (cf. points 27-30)*

Objet

Demande d'annulation de la décision A (2008) 22050 du Parlement européen, du 17 décembre 2008, refusant d'accorder au requérant l'accès à certains documents relatifs à l'affiliation de certains membres du Parlement européen au régime de pension complémentaire.

Dispositif

1) Le recours est rejeté.

2) M. Gert-Jan Dennekamp supportera ses propres dépens ainsi que ceux exposés par le Parlement européen.

3) Le Royaume de Danemark, la République de Finlande et le Contrôleur européen de la protection des données (CEPD) supporteront leurs propres dépens.

Arrêt du Tribunal (quatrième chambre) du 23 novembre 2011 — bpost/Commission

(affaire T-514/09)

« Marchés publics de services — Procédure d'appel d'offres de l'OP — Acheminement et distribution quotidiens du Journal officiel, d'ouvrages ainsi que d'autres périodiques et publications — Rejet de l'offre d'un soumissionnaire et décision d'attribuer le marché à un autre soumissionnaire — Critères d'attribution — Obligation de motivation — Erreur manifeste d'appréciation — Responsabilité non contractuelle »

1. *Marchés publics des Communautés européennes — Procédure d'appel d'offres — Procédure de recours contre les décisions du pouvoir adjudicateur d'attribution des marchés publics — Principe du contradictoire — Conciliation avec la protection des secrets d'affaires — Instances responsables des procédures de recours — Obligation de garantir la confidentialité et le droit au respect des secrets d'affaires au regard des informations contenues dans les dossiers communiqués par les parties — Conditions — Conciliation de ladite obligation avec les exigences d'une protection juridique effective et le respect des droits de la défense (Art. 267 TFUE ; règlement du Conseil nº 1605/2002, art. 100, § 2) (cf. points 25-26)*

2. *Marchés publics des Communautés européennes — Procédure d'appel d'offres — Attribution des marchés — Offre économiquement la plus avantageuse — Critères d'attribution — Choix par le pouvoir adjudicateur — Limites — Respect des principes de transparence, d'égalité de traitement et de non-discrimination (Règlement du Conseil nº 1605/2002, art. 97 ; règlement de la Commission nº 2342/2002, art. 138) (cf. points 64, 66)*

JUDGMENT OF THE COURT (Third Chamber)

24 November 2011 *

In Case C-70/10,

REFERENCE for a preliminary ruling under Article 267 TFEU from the cour d'appel de Bruxelles (Belgium), made by decision of 28 January 2010, received at the Court on 5 February 2010, in the proceedings

Scarlet Extended SA

v

Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),

intervening parties:

Belgian Entertainment Association Video ASBL (BEA Video),

* Language of the case: French.

Belgian Entertainment Association Music ASBL (BEA Music),

Internet Service Provider Association ASBL (ISPA),

THE COURT (Third Chamber),

composed of K. Lenaerts, President of the Chamber, J. Malenovský (Rapporteur), R. Silva de Lapuerta, E. Juhász and G. Arestis, Judges,

Advocate General: P. Cruz Villalón,
Registrar: C. Strömholm, Administrator,

having regard to the written procedure and further to the hearing on 13 January 2011,

after considering the observations submitted on behalf of:

— Scarlet Extended SA, by T. De Meese and B. Van Asbroeck, avocats,

— Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Belgian Entertainment Association Video ASBL (BEA Video) and Belgian Entertainment Association Music ASBL (BEA Music), by F. de Visscher, B. Michaux and F. Brison, avocats,

— Internet Service Provider Association ASBL (ISPA), by G. Somers, avocat,

— the Belgian Government, by T. Materne, J.-C. Halleux and C. Pochet, acting as Agents,

— the Czech Government, by M. Smolek and K. Havlíčková, acting as Agents,

— the Italian Government, by G. Palmieri, acting as Agent, assisted by S. Fiorentino, avvocato dello Stato,

— the Netherlands Government, by C. Wissels and B. Koopman, acting as Agents,

— the Polish Government, by M. Szpunar, M. Drwięcki and J. Goliński, acting as Agents,

— the Finnish Government, by M. Pere, acting as Agent,

— the European Commission, by J. Samnadda and C. Vrignon, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 14 April 2011,

gives the following

Judgment

1 This reference for a preliminary ruling concerns the interpretation of Directives:

— 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ 2000 L 178, p. 1);

— 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10);

— 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigendum OJ 2004 L 195, p. 16);

— 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); and

— 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).

2 The reference has been made in proceedings between Scarlet Extended SA ('Scarlet') and the Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) ('SABAM') concerning Scarlet's refusal to install a system for filtering electronic communications which use file-sharing software ('peer-to-peer'), with a view to preventing file sharing which infringes copyright.

Legal context

European Union law

Directive 2000/31

3 Recitals 45 and 47 in the preamble to Directive 2000/31 state:

'(45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such

injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.

…

(47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.'

4 Article 1 of Directive 2000/31 states:

'1. This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.

2. This Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.

…'

5 Article 12 of that directive, which features in Section 4, entitled 'Liability of intermediary service providers', of Chapter II thereof, provides:

'1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission;

and

(c) does not select or modify the information contained in the transmission.

…

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.'

6 Article 15 of Directive 2000/31, which also features in Section 4 of Chapter II, states:

'1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating unlawful activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged unlawful activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.'

Directive 2001/29

7 Recitals 16 and 59 in the preamble to Directive 2001/29 state:

'(16) … This Directive should be implemented within a timescale similar to that for the implementation of [Directive 2000/31], since that Directive provides a harmonised framework of principles and provisions relevant, inter alia, to important parts of this Directive. This Directive is without prejudice to provisions relating to liability in that Directive.

...

(59) In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.'

8 Article 8 of Directive 2001/29 states:

'1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.

...

3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.'

Directive 2004/48

9 Recital 23 in the preamble to Directive 2004/48 provides:

'Without prejudice to any other measures, procedures and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary whose services are being used by a third party to infringe the rightholder's industrial property right. The conditions and procedures relating to such injunctions should be left to the national law of the Member States. As far as infringements of copyright and related rights are concerned, a comprehensive level of harmonisation is already provided for in Directive [2001/29]. Article 8(3) of Directive [2001/29] should therefore not be affected by this Directive.'

10 Article 2(3) of Directive 2004/48 provides as follows:

'This Directive shall not affect:

(a) the Community provisions governing the substantive law on intellectual property … or Directive [2000/31], in general, and Articles 12 to 15 of Directive [2000/31] in particular;

…'

11 Article 3 of Directive 2004/48 provides:

'1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.

2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.'

12 Article 11 of Directive 2004/48 states:

'Member States shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive [2001/29].'

National law

13 Article 87(1), first and second subparagraphs, of the Law of 30 June 1994 on copyright and related rights (*Moniteur belge* of 27 July 1994, p. 19297) states:

'The President of the Tribunal de première instance (Court of First Instance) … shall determine the existence of any infringement of a copyright or related right and shall order that it be brought to an end.

He may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.'

14 Articles 18 and 21 of the Law of 11 March 2003 on certain legal aspects of information society services (*Moniteur belge* of 17 March 2003, p. 12962) transpose Articles 12 and 15 of Directive 2000/31 into national law.

The dispute in the main proceedings and the questions referred for a preliminary ruling

15 SABAM is a management company which represents authors, composers and editors of musical works in authorising the use of their copyright-protected works by third parties.

16 Scarlet is an internet service provider ('ISP') which provides its customers with access to the internet without offering other services such as downloading or file sharing.

17 In the course of 2004, SABAM concluded that internet users using Scarlet's services were downloading works in SABAM's catalogue from the internet, without authorisation and without paying royalties, by means of peer-to-peer networks, which constitute a transparent method of file sharing which is independent, decentralised and features advanced search and download functions.

18 On 24 June 2004, SABAM accordingly brought interlocutory proceedings against Scarlet before the President of the Tribunal de première instance, Brussels, claiming that that company was the best placed, as an ISP, to take measures to bring to an end copyright infringements committed by its customers.

19 SABAM sought, first, a declaration that the copyright in musical works contained in its repertoire had been infringed, in particular the right of reproduction and the right of communication to the public, because of the unauthorised sharing of electronic music files by means of peer-to-peer software, those infringements being committed through the use of Scarlet's services.

20 SABAM also sought an order requiring Scarlet to bring such infringements to an end by blocking, or making it impossible for its customers to send or receive in any way, files containing a musical work using peer-to-peer software without the permission of the rightholders, on pain of a periodic penalty. Lastly, SABAM requested that Scarlet provide it with details of the measures that it would be applying in order to comply with the judgment to be given, on pain of a periodic penalty.

21 By judgment of 26 November 2004, the President of the Tribunal de première instance, Brussels, found that copyright had been infringed, as claimed by SABAM, but, prior to ruling on the application for cessation, appointed an expert to investigate whether the technical solutions proposed by SABAM were technically feasible, whether they would make it possible to filter out only unlawful file sharing, and whether there were other ways of monitoring the use of peer-to-peer software, and to determine the cost of the measures envisaged.

22 In his report, the appointed expert concluded that, despite numerous technical obstacles, the feasibility of filtering and blocking the unlawful sharing of electronic files could not be entirely ruled out.

23 By judgment of 29 June 2007, the President of the Tribunal de première instance, Brussels, accordingly ordered Scarlet to bring to an end the copyright infringements established in the judgment of 26 November 2004 by making it impossible for its customers to send or receive in any way files containing a musical work in SABAM's repertoire by means of peer-to-peer software, on pain of a periodic penalty.

24 Scarlet appealed against that decision to the referring court, claiming, first, that it was impossible for it to comply with that injunction since the effectiveness and permanence of filtering and blocking systems had not been proved and that the installation of the equipment for so doing was faced with numerous practical obstacles, such as problems with the network capacity and the impact on the network. Moreover, any attempt to block the files concerned was, it argued, doomed to fail in the very short term because there were at that time several peer-to-peer software products which made it impossible for third parties to check their content.

25 Scarlet also claimed that that injunction was contrary to Article 21 of the Law of 11 March 2003 on certain legal aspects of information society services, which transposes Article 15 of Directive 2000/31 into national law, because it would impose on Scarlet, *de facto*, a general obligation to monitor communications on its network, inasmuch as any system for blocking or filtering peer-to-peer traffic would necessarily require general surveillance of all the communications passing through its network.

26 Lastly, Scarlet considered that the installation of a filtering system would be in breach of the provisions of European Union law on the protection of personal data and the secrecy of communications, since such filtering involves the processing of IP addresses, which are personal data.

27 In that context, the referring court took the view that, before ascertaining whether a mechanism for filtering and blocking peer-to-peer files existed and could be effective, it had to be satisfied that the obligations liable to be imposed on Scarlet were in accordance with European Union law.

28 In those circumstances, the cour d'appel de Bruxelles decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:

'(1) Do Directives 2001/29 and 2004/48, in conjunction with Directives 95/46, 2000/31 and 2002/58, construed in particular in the light of Articles 8 and 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, permit Member States to authorise a national court, before which substantive proceedings have been brought and on the basis merely of a statutory provision stating that: "They [the national courts] may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right", to order an [ISP] to install, for all its customers, in

abstracto and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent?

(2) If the answer to the [first] question … is in the affirmative, do those directives require a national court, called upon to give a ruling on an application for an injunction against an intermediary whose services are used by a third party to infringe a copyright, to apply the principle of proportionality when deciding on the effectiveness and dissuasive effect of the measure sought?'

Consideration of the questions referred

29 By its questions, the referring court asks, in essence, whether Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction imposed on an ISP to introduce a system for filtering

— all electronic communications passing via its services, in particular those involving the use of peer-to-peer software;

— which applies indiscriminately to all its customers;

— as a preventive measure;

— exclusively at its expense; and

— for an unlimited period,

which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual property rights, with a view to blocking the transfer of files the sharing of which infringes copyright ('the contested filtering system').

30 In that regard, it should first be recalled that, under Article 8(3) of Directive 2001/29 and the third sentence of Article 11 of Directive 2004/48, holders of intellectual property rights may apply for an injunction against intermediaries, such as ISPs, whose services are being used by a third party to infringe their rights.

31 Next, it follows from the Court's case-law that the jurisdiction conferred on national courts, in accordance with those provisions, must allow them to order those intermediaries to take measures aimed not only at bringing to an end infringements already committed against intellectual-property rights using their information-society

services, but also at preventing further infringements (see, to that effect, Case C-324/09 *L'Oréal and Others* [2011] ECR I-6011, paragraph 131).

32 Lastly, it follows from that same case-law that the rules for the operation of the injunctions for which the Member States must provide under Article 8(3) of Directive 2001/29 and the third sentence of Article 11 of Directive 2004/48, such as those relating to the conditions to be met and to the procedure to be followed, are a matter for national law (see, *mutatis mutandis*, *L'Oréal and Others*, paragraph 135).

33 That being so, those national rules, and likewise their application by the national courts, must observe the limitations arising from Directives 2001/29 and 2004/48 and from the sources of law to which those directives refer (see, to that effect, *L'Oréal and Others*, paragraph 138).

34 Thus, in accordance with recital 16 in the preamble to Directive 2001/29 and Article 2(3)(a) of Directive 2004/48, those rules laid down by the Member States may not affect the provisions of Directive 2000/31 and, more specifically, Articles 12 to 15 thereof.

35 Consequently, those rules must, in particular, respect Article 15(1) of Directive 2000/31, which prohibits national authorities from adopting measures which would require an ISP to carry out general monitoring of the information that it transmits on its network.

36 In that regard, the Court has already ruled that that prohibition applies in particular to national measures which would require an intermediary provider, such as an ISP, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual-property rights. Furthermore, such a general monitoring

obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly (see *L'Oréal and Others*, paragraph 139).

37 In those circumstances, it is necessary to examine whether the injunction at issue in the main proceedings, which would require the ISP to install the contested filtering system, would oblige it, as part of that system, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual-property rights.

38 In that regard, it is common ground that implementation of that filtering system would require

— first, that the ISP identify, within all of the electronic communications of all its customers, the files relating to peer-to-peer traffic;

— secondly, that it identify, within that traffic, the files containing works in respect of which holders of intellectual-property rights claim to hold rights;

— thirdly, that it determine which of those files are being shared unlawfully; and

— fourthly, that it block file sharing that it considers to be unlawful.

39 Preventive monitoring of this kind would thus require active observation of all electronic communications conducted on the network of the ISP concerned and, consequently, would encompass all information to be transmitted and all customers using that network.

40 In the light of the foregoing, it must be held that the injunction imposed on the ISP concerned requiring it to install the contested filtering system would oblige it to actively monitor all the data relating to each of its customers in order to prevent any future infringement of intellectual-property rights. It follows that that injunction would require the ISP to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31.

41 In order to assess whether that injunction is consistent with European Union law, account must also be taken of the requirements that stem from the protection of the applicable fundamental rights, such as those mentioned by the referring court.

42 In that regard, it should be recalled that the injunction at issue in the main proceedings pursues the aim of ensuring the protection of copyright, which is an intellectual-property right, which may be infringed by the nature and content of certain electronic communications conducted through the network of the ISP concerned.

43 The protection of the right to intellectual property is indeed enshrined in Article 17(2) of the Charter of Fundamental Rights of the European Union ('the Charter'). There is, however, nothing whatsoever in the wording of that provision or in the Court's case-law to suggest that that right is inviolable and must for that reason be absolutely protected.

44 As paragraphs 62 to 68 of the judgment in Case C-275/06 *Promusicae* [2008] ECR I-271 make clear, the protection of the fundamental right to property, which includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights.

45 More specifically, it follows from paragraph 68 of that judgment that, in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures.

46 Accordingly, in circumstances such as those in the main proceedings, national authorities and courts must, in particular, strike a fair balance between the protection of the intellectual property right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by operators such as ISPs pursuant to Article 16 of the Charter.

47 In the present case, the injunction requiring the installation of the contested filtering system involves monitoring all the electronic communications made through the network of the ISP concerned in the interests of those rightholders. Moreover, that monitoring has no limitation in time, is directed at all future infringements and is intended to protect not only existing works, but also future works that have not yet been created at the time when the system is introduced.

48 Accordingly, such an injunction would result in a serious infringement of the freedom of the ISP concerned to conduct its business since it would require that ISP to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48,

which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly.

49 In those circumstances, it must be held that the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as ISPs.

50 Moreover, the effects of that injunction would not be limited to the ISP concerned, as the contested filtering system may also infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively.

51 It is common ground, first, that the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified.

52 Secondly, that injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to

copyright which vary from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned.

53 Consequently, it must be held that, in adopting the injunction requiring the ISP to install the contested filtering system, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other.

54 In the light of the foregoing, the answer to the questions submitted is that Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an ISP which requires it to install the contested filtering system.

Costs

55 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Third Chamber) hereby rules:

Directives:

— **2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce');**

— **2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society;**

— **2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights ;**

— **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; and**

— **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),**

read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an internet service provider which requires it to install a system for filtering

— **all electronic communications passing via its services, in particular those involving the use of peer-to-peer software;**

— **which applies indiscriminately to all its customers;**

— **as a preventive measure;**

— **exclusively at its expense; and**

— **for an unlimited period,**

which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual-property rights, with a view to blocking the transfer of files the sharing of which infringes copyright.

[Signatures]

JUDGMENT OF THE COURT (Third Chamber)

24 November 2011 *

In Joined Cases C-468/10 and C-469/10,

REFERENCES for a preliminary ruling under Article 267 TFEU from the Tribunal Supremo (Spain), made by decisions of 15 July 2010, received at the Court on 28 September 2010, in the proceedings

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10),

Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10)

v

Administración del Estado,

* Language of the cases: Spanish.

intervening parties:

Unión General de Trabajadores (UGT) (C-468/10 and C-469/10),

Telefónica de España SAU (C-468/10),

France Telecom España SA (C-468/10 and C-469/10),

Telefónica Móviles de España SAU (C-469/10),

Vodafone España SA (C-469/10),

Asociación de Usuarios de la Comunicación (C-469/10),

THE COURT (Third Chamber),

composed of K. Lenaerts (Rapporteur), President of the Chamber, R. Silva de Lapuerta, E. Juhász, T. von Danwitz and D. Šváby, Judges,

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

having regard to the written procedure and further to the hearing on 15 September 2011,

after considering the observations submitted on behalf of:

— Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), by C. Alonso Martínez and A. Creus Carreras, abogados,

— Federación de Comercio Electrónico y Marketing Directo (FECEMD), by R. García del Poyo Vizcaya and M.Á. Serrano Pérez, abogados,

— the Spanish Government, by M. Muñoz Pérez, acting as Agent,

— the European Commission, by I. Martínez del Peral and B. Martenczuk, acting as Agents,

having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,

gives the following

Judgment

1 These references for a preliminary ruling concern the interpretation of Article 7(f) 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 (OJ 1995 L 281, p. 31).

2 The references have been made in two sets of proceedings between, on the one hand, Asociación Nacional de Establecimientos Financieros de Crédito (National Association of Credit Institutions) ('ASNEF'), in the first case, and Federación de Comercio Electrónico y Marketing Directo (Federation of Electronic Commerce and Direct Marketing) ('FECEMD'), in the second case, and, on the other, the Administración del Estado.

Legal context

European Union ('EU') law

Directive 95/46

3 Recitals 7, 8 and 10 in the preamble to Directive 95/46 read as follows:

'(7) … 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; … this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; … this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) …, 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; … this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between

the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market …; … Community action to approximate those laws is therefore needed;

…

(10) … 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 European Convention for the Protection of Human Rights and Fundamental Freedoms [signed in Rome on 4 November 1950 ("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'

4 Article 1 of Directive 95/46, entitled 'Object of the Directive', is drafted in the following 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.'

5 Article 5 of Directive 95/46 is worded as follows:

'Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.'

6 Article 7 of Directive 95/46 states:

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

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

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).'

7 Article 13(1) of Directive 95/46 provides:

'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.'

National law

Organic Law 15/1999

8 Organic Law 15/1999 on the protection of personal data (BOE no 298 of 14 December 1999, p. 43088) transposes Directive 95/46 into Spanish law.

9 Article 3(j) of Organic Law 15/1999 sets out 'public sources' in an exhaustive and restrictive list, which reads as follows:

'… those files that can be consulted by any person, unhindered by a limiting provision or by any requirement other than, where relevant, payment of a fee. Public sources are, exclusively, the electoral roll, telephone directories subject to the conditions laid down in the relevant regulations and lists of persons belonging to professional associations containing only data on the name, title, profession, activity, academic degree, address and an indication of membership of the association. Newspapers and official bulletins and the media are also public sources.'

10 Article 6(1) of Organic Law 15/1999 makes the processing of data subject to the data subject's unambiguous consent, unless otherwise provided by law. Thus, Article 6(2), *in fine*, of Organic Law 15/1999 provides that consent is not required, inter alia, '… when the data are included in public sources and their processing is necessary for the purposes of the legitimate interests pursued by the controller of the file or by the third party to whom the data are disclosed, except where this infringes the fundamental rights and freedoms of the data subject.'

11 Article 11(1) of Organic Law 15/1999 reiterates the need for the data subject's consent in order to disclose personal data to third parties, while Article 11(2), however, provides that that consent is not necessary, inter alia, in relation to data appearing in public sources.

Royal Decree 1720/2007

12 The Spanish Government implemented Organic Law 15/1999 by way of Royal Decree 1720/2007 (BOE No 17 of 19 January 2008, p. 4103).

13 Article 10(1) of Royal Decree 1720/2007 allows the processing and transfer of personal data in cases where the data subject has given prior consent.

14 However, Article 10(2) of Royal Decree 1720/2007 provides:

'… personal data may be processed or transferred without the data subject's consent when:

(a) it is authorised by a regulation having the force of law or under Community law and, in particular, when one of the following situations applies:

— the purpose of the processing or transfer is to satisfy a legitimate interest of the data controller or recipient guaranteed by these rules, as long as the interest or fundamental rights and liberties of the data subjects, as provided in Article 1 of Organic Law 15/1999 of 13 December, are not overriding;

— the processing or transfer of data is necessary in order for the data controller to fulfil a duty imposed upon him by one of those provisions;

(b) the data which are the subject of processing or transfer are in sources accessible to the public and the data controller, or the third party to whom data has been communicated, has a legitimate interest in their processing or knowledge, as long as the fundamental rights and liberties of the data subject are not breached.

The aforesaid notwithstanding, the public administration may communicate the data collected from sources accessible to the public to the data controllers of privately owned files pursuant to this subsection only when they are so authorised by a regulation having the force of law.'

The disputes in the main proceedings and the questions referred for a preliminary ruling

15 ASNEF, on the one hand, and FECEMD, on the other hand, have brought administrative proceedings challenging several articles of Royal Decree 1720/2007.

16 Among the contested provisions are the first indent of Article 10(2)(a) and the first subparagraph of Article 10(2)(b) of Royal Decree 1720/2007, which ASNEF and FECEMD believe are in breach of Article 7(f) of Directive 95/46.

17 In particular, ASNEF and FECEMD take the view that Spanish law adds, to the condition relating to the legitimate interest in data processing without the data subject's consent, a condition, which does not exist in Directive 95/46, to the effect that the data should appear in public sources.

18 The Tribunal Supremo (Supreme Court, Spain) considers that the merits of the actions brought by ASNEF and FECEMD respectively depend to a large extent on the interpretation by the Court of Article 7(f) of Directive 95/46. Accordingly, it states that, if the Court were to hold that Member States are not entitled to add extra conditions to those required by that provision, and if that provision were to be found to have direct effect, Article 10(2)(b) of Royal Decree 1720/2007 would have to be set aside.

19 The Tribunal Supremo explains that, in the absence of the data subject's consent, and in order to allow processing of that data subject's personal data that is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, Spanish law requires not only that the fundamental

rights and freedoms of the data subject be respected, but also that the data appear in the files listed in Article 3(j) of Organic Law 15/1999. In that regard, it takes the view that Organic Law 15/1999 and Royal Decree 1720/2007 restrict the scope of Article 7(f) of Directive 95/46.

20 In the view of the Tribunal Supremo, that restriction constitutes a barrier to the free movement of personal data that is compatible with Directive 95/46 only if the interest or the fundamental rights and freedoms of the data subject so require. It concludes that the only way to avoid a contradiction between Directive 95/46 and Spanish law is to hold that the free movement of personal data appearing in files other than those listed in Article 3(j) of Organic Law 15/1999 infringes the interest or the fundamental rights and freedoms of the data subject.

21 However, the Tribunal Supremo is unsure whether such an interpretation is in accordance with the intention of the EU legislature.

22 In those circumstances, being of the view that the outcome of both the cases before it depends on the interpretation of provisions of EU law, the Tribunal Supremo decided to stay the proceedings and to refer the following questions, which are formulated in identical terms in both cases, to the Court for a preliminary ruling:

‘(1) Must Article 7(f) of [Directive 95/46] be interpreted as precluding the application of national rules which, in the absence of the interested party’s consent, and to allow processing of his personal data that is necessary to pursue a legitimate

interest of the controller or of third parties to whom the data will be disclosed, not only require that fundamental rights and freedoms should not be prejudiced, but also require the data to appear in public sources?

(2) Are the conditions for conferring on it direct effect, set out in the case-law of the Court … met by the abovementioned Article 7(f)?'

23 By order of the President of the Court of 26 October 2010, Cases C-468/10 and C-469/10 were joined for the purposes of the written and oral procedure and the judgment.

Consideration of the questions referred

The first question

24 By its first question, the national court asks, in essence, whether Article 7(f) of Directive 95/46 must be interpreted as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom the data are disclosed, requires not only that the fundamental rights and freedoms of the data subject be respected, but also that the data should appear in public sources.

25 Article 1 of Directive 95/46 requires Member States to ensure the protection of the fundamental rights and freedoms of natural persons, and in particular their privacy, in relation to the handling of personal data (see, to that effect, Case C-524/06 *Huber* [2008] ECR I-9705, paragraph 47).

26 In accordance with the provisions of Chapter II of Directive 95/46, entitled 'General rules on the lawfulness of the processing of personal data', all processing of personal data must, subject to the exceptions permitted under Article 13, comply, first, with the principles relating to data quality set out in Article 6 of Directive 95/46 and, secondly, with one of the six principles for making data processing legitimate listed in Article 7 of Directive 95/46 (see, to that effect, Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, paragraph 65, and *Huber*, paragraph 48).

27 According to recital 7 in the preamble to Directive 95/46, the establishment and functioning of the internal market are liable to be seriously affected by differences in national rules applicable to the processing of personal data (Case C-101/01 *Lindqvist* [2003] ECR I-12971, paragraph 79).

28 In that context, it must be noted that Directive 95/46 is intended, as appears from, inter alia, recital 8 in the preamble thereto, to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. Recital 10 adds that the approximation of the national laws applicable in this area 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 EU (see, to that effect, *Lindqvist*, paragraph 95, and *Huber*, paragraph 50).

29 Accordingly, it has been held that the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete. It is upon that view that Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of the individuals to whom such data relate (*Lindqvist*, paragraph 96).

30 Consequently, it follows from the objective of ensuring an equivalent level of protection in all Member States that Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful.

31 That interpretation is corroborated by the term 'may be processed only if' and its juxtaposition with 'or' contained in Article 7 of Directive 95/46, which demonstrate the exhaustive and restrictive nature of the list appearing in that article.

32 It follows that Member States cannot add new principles relating to the lawfulness of the processing of personal data to Article 7 of Directive 95/46 or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7.

33 The foregoing interpretation is not brought into question by Article 5 of Directive 95/46. Article 5 merely authorises Member States to specify, within the limits of Chapter II of that directive and, accordingly, Article 7 thereof, the conditions under which the processing of personal data is lawful.

34 The margin of discretion which Member States have pursuant to Article 5 can therefore be used only in accordance with the objective pursued by Directive 95/46 of maintaining a balance between the free movement of personal data and the protection of private life (*Lindqvist*, paragraph 97).

35 Directive 95/46 includes rules with a degree of flexibility and, in many instances, leaves to the Member States the task of deciding the details or choosing between options (*Lindqvist*, paragraph 83). A distinction, consequently, must be made between national measures that provide for additional requirements amending the scope of a principle referred to in Article 7 of Directive 95/46, on the one hand, and national measures which provide for a mere clarification of one of those principles, on the other hand. The first type of national measure is precluded. It is only in the context of the second type of national measure that Member States have, pursuant to Article 5 of Directive 95/46, a margin of discretion.

36 It follows that, under Article 5 of Directive 95/46, Member States also cannot introduce principles relating to the lawfulness of the processing of personal data other than those listed in Article 7 thereof, nor can they amend, by additional requirements, the scope of the six principles provided for in Article 7.

37 In the present cases, Article 7(f) of Directive 95/46 provides that the processing of personal data is lawful if it 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)'.

38 Article 7(f) sets out two cumulative conditions that must be fulfilled in order for the processing of personal data to be lawful: firstly, the processing of the personal data must be 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; and, secondly, such interests must not be overridden by the fundamental rights and freedoms of the data subject.

39 It follows that, in relation to the processing of personal data, Article 7(f) of Directive 95/46 precludes any national rules which, in the absence of the data subject's consent, impose requirements that are additional to the two cumulative conditions set out in the preceding paragraph.

40 However, account must be taken of the fact that the second of those conditions necessitates a balancing of the opposing rights and interests concerned which depends, in principle, on the individual circumstances of the particular case in question and in the context of which the person or the institution which carries out the balancing must take account of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

41 In this regard, it must be noted that Article 8(1) of the Charter states that '[e]veryone has the right to the protection of personal data concerning him or her'. That fundamental right is closely connected with the right to respect for private life expressed in Article 7 of the Charter (Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paragraph 47).

42 According to the Court's case-law, the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual (*Volker*

und Markus Schecke and Eifert, paragraph 52). However, it follows from Articles 8(2) and 52(1) of the Charter that, under certain conditions, limitations may be imposed on that right.

43 Moreover, Member States must, when transposing Directive 95/46, take care to rely on an interpretation of that directive which allows a fair balance to be struck between the various fundamental rights and freedoms protected by the EU legal order (see, by analogy, Case C-275/06 *Promusicae* [2008] ECR I-271, paragraph 68).

44 In relation to the balancing which is necessary pursuant to Article 7(f) of Directive 95/46, it is possible to take into consideration the fact that the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources.

45 Unlike the processing of data appearing in public sources, the processing of data appearing in non-public sources necessarily implies that information relating to the data subject's private life will thereafter be known by the data controller and, as the case may be, by the third party or parties to whom the data are disclosed. This more serious infringement of the data subject's rights enshrined in Articles 7 and 8 of the Charter must be properly taken into account by being balanced against the legitimate interest pursued by the data controller or by the third party or parties to whom the data are disclosed.

46 In that regard, it must be noted that there is nothing to preclude Member States, in the exercise of their discretion laid down in Article 5 of Directive 95/46, from establishing guidelines in respect of that balancing.

47 However, it is no longer a precision within the meaning of Article 5 of Directive 95/46 if national rules exclude the possibility of processing certain categories of personal data by definitively prescribing, for those categories, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case.

48 Consequently, without prejudice to Article 8 of Directive 95/46 concerning the processing of particular categories of data, a provision which is not at issue in the main proceedings, Article 7(f) of that directive precludes a Member State from excluding, in a categorical and generalised manner, the possibility of processing certain categories of personal data, without allowing the opposing rights and interests at issue to be balanced against each other in a particular case.

49 In light of those considerations, the answer to the first question is that Article 7(f) of Directive 95/46 must be interpreted as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also that those data should appear in public sources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources.

The second question

50 By its second question, the national court asks, in essence, whether Article 7(f) of Directive 95/46 has direct effect.

51 In that regard, it must be recalled that, according to settled case-law of the Court, whenever the provisions of a directive appear, so far as their subject-matter is concerned, to be unconditional and sufficiently precise, they may be relied on before the national courts by individuals against the State where the latter has failed to implement that directive in domestic law by the end of the period prescribed or where it has failed to implement that directive correctly (see Case C-203/10 *Auto Nikolovi* [2011] ECR I-1083, paragraph 61 and the case-law cited).

52 It must be stated that Article 7(f) of Directive 95/46 is a provision that is sufficiently precise to be relied on by an individual and applied by the national courts. Moreover, while that directive undoubtedly confers on the Member States a greater or lesser discretion in the implementation of some of its provisions, Article 7(f), for its part, states an unconditional obligation (see, by analogy, *Österreichischer Rundfunk and Others*, paragraph 100).

53 The use of the expression 'except where' in the actual text of Article 7(f) of Directive 95/46 is not such, by itself, as to cast doubt on the unconditional nature of that provision, within the meaning of that case-law.

54 That expression is intended to establish one of the two cumulative elements provided for in Article 7(f) of Directive 95/46 to which the possibility of processing personal data without the data subject's consent is subject. As that element is defined, it does not deprive Article 7(f) of its precise and unconditional nature.

55 The answer to the second question is therefore that Article 7(f) of Directive 95/46 has direct effect.

Costs

56 Since these proceedings are, for the parties to the main proceedings, a step in the actions pending before the national court, the decisions on costs are a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Third Chamber) hereby rules:

1. **Article 7(f) 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 must be interpreted as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest of the data**

controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also that the data should appear in public sources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources.

2. Article 7(f) of Directive 95/46 has direct effect.

[Signatures]

Reports of Cases

JUDGMENT OF THE COURT (Third Chamber)

16 February 2012 *

(Information society — Copyright — Internet — Hosting service provider — Processing of information stored on an online social networking platform — Introducing a system for filtering that information in order to prevent files being made available which infringe copyright — No general obligation to monitor stored information)

In Case C-360/10,

REFERENCE for a preliminary ruling under Article 267 TFEU from the rechtbank van eerste aanleg te Brussel (Belgium), made by decision of 28 June 2010, received at the Court on 19 July 2010, in the proceedings

Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)

v

Netlog NV,

THE COURT (Third Chamber),

composed of K. Lenaerts, President of the Chamber, J. Malenovský (Rapporteur), R. Silva de Lapuerta, G. Arestis and D. Šváby, Judges,

Advocate General: P. Cruz Villalón,

Registrar: M. Ferreira, Principal Administrator,

having regard to the written procedure and further to the hearing on 7 July 2011,

after considering the observations submitted on behalf of:

— Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM), by B. Michaux, F. de Visscher and F. Brison, advocaten,

— Netlog NV, by P. Van Eecke, advocaat,

— the Belgian Government, by T. Materne and J.-C. Halleux, acting as Agents,

— the Italian Government, by G. Palmieri, acting as Agent, assisted by S. Fiorentino, avvocato dello Stato,

— the Netherlands Government, by C. Wissels, acting as Agent,

* Language of the case: Dutch.

— the United Kingdom Government, by S. Ossowski, acting as Agent,

— the European Commission, by A. Nijenhuis and J. Samnadda, acting as Agents,

having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,

gives the following

Judgment

1 This reference for a preliminary ruling concerns the interpretation of:

— Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ 2000 L 178, p. 1);

— Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10);

— Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigenda OJ 2004 L 195, p. 16, and OJ 2007 L 204, p. 27);

— 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); and

— 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).

2 The reference has been made in proceedings between Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) ('SABAM') and Netlog NV ('Netlog'), the owner of an online social networking platform, concerning Netlog's obligation to introduce a system for filtering information stored on its platform in order to prevent files being made available which infringe copyright.

Legal context

European Union (EU) law

Directive 2000/31

3 Under recitals 45, 47 and 48 in the preamble to Directive 2000/31:

'(45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.

…

(47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.

(48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.'

4 Article 14 of Directive 2000/31, headed 'Hosting', states:

'(1) Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

(2) Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

(3) This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.'

5 Under Article 15 of Directive 2000/31:

'(1) Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

(2) Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.'

Directive 2001/29

6 Under recitals 16 and 59 in the preamble to Directive 2001/29:

'(16) … This Directive should be implemented within a timescale similar to that for the implementation of [Directive 2000/31], since that Directive provides a harmonised framework of principles and provisions relevant inter alia to important parts of this Directive. This Directive is without prejudice to provisions relating to liability in that Directive.

…

(59) In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.'

7 Under Article 3(1) of Directive 2001/29:

'Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.'

8 Article 8 of that directive provides:

'(1) Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.

…

(3) Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.'

Directive 2004/48

9 Recital 23 in the preamble to Directive 2004/48 is worded as follows:

'Without prejudice to any other measures, procedures and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary whose services are being used by a third party to infringe the rightholder's industrial property right. The conditions and procedures relating to such injunctions should be left to the national law of the Member States. As far as infringements of copyright and related rights are concerned, a comprehensive level of harmonisation is already provided for in Directive [2001/29]. Article 8(3) of Directive [2001/29] should therefore not be affected by this Directive.'

10 Under Article 2(3) of Directive 2004/48:

'This Directive shall not affect:

(a) the Community provisions governing the substantive law on intellectual property, Directive 95/46/EC … or Directive 2000/31/EC, in general, and Articles 12 to 15 of Directive 2000/31/EC in particular;

…'

11 Article 3 of Directive 2004/48 states:

'(1) Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.

(2) Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.'

12 The third sentence of Article 11 of Directive 2004/48 states:

'Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive [2001/29].'

National law

13 Article 87(1), first and second subparagraphs, of the Law of 30 June 1994 on copyright and related rights (*Belgisch Staatsblad*, 27 July 1994, p. 19297), which transposes Article 8(3) of Directive 2001/29 and Article 11 of Directive 2004/48 into national law, states:

'The President of the Tribunal de première instance (Court of First Instance) … shall determine the existence of any infringement of a copyright or related right and shall order that it be brought to an end.

He may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.'

14 Articles 20 and 21 of the Law of 11 March 2003 on certain legal aspects of information society services (*Belgisch Staatsblad*, 17 March 2003, p. 12962) transpose Articles 14 and 15 of Directive 2000/31 into national law.

The dispute in the main proceedings and the question referred for a preliminary ruling

15 SABAM is a management company which represents authors, composers and publishers of musical works. On that basis, it is responsible for, inter alia, authorising the use by third parties of copyright-protected works of those authors, composers and publishers.

16 Netlog runs an online social networking platform where every person who registers acquires a personal space known as a 'profile' which the user can complete himself and which becomes available globally.

17 The most important function of that platform, which is used by tens of millions of individuals on a daily basis, is to build virtual communities through which those individuals can communicate with each other and thereby develop friendships. On their profile, users can, inter alia, keep a diary, indicate their hobbies and interests, show who their friends are, display personal photos or publish video clips.

18 However, SABAM claimed that Netlog's social network also offers all users the opportunity to make use, by means of their profile, of the musical and audio-visual works in SABAM's repertoire, making those works available to the public in such a way that other users of that network can have access to them without SABAM's consent and without Netlog paying it any fee.

19 During February 2009, SABAM approached Netlog with a view to concluding an agreement regarding the payment of a fee by Netlog for the use of the SABAM repertoire.

20 By letter of 2 June 2009, SABAM gave notice to Netlog that it should give an undertaking to cease and desist from making available to the public musical and audio-visual works from SABAM's repertoire without the necessary authorisation.

21 On 23 June 2009, SABAM had Netlog summoned before the President of the rechtbank van eerste aanleg te Brussel (Court of First Instance, Brussels) in injunction proceedings under Article 87(1) of the Law of 30 June 1994 on copyright and related rights, requesting inter alia that Netlog be ordered immediately to cease unlawfully making available musical or audio-visual works from SABAM's repertoire and to pay a penalty of EUR 1000 for each day of delay in complying with that order.

22 In that regard, Netlog submitted that granting SABAM's injunction would be tantamount to imposing on Netlog a general obligation to monitor, which is prohibited by Article 21(1) of the Law of 11 March 2003 on certain legal aspects of information society services, which transposes Article 15(1) of Directive 2000/31 into national law.

23 In addition, Netlog claimed, without being contradicted by SABAM, that the granting of such an injunction could result in the imposition of an order that it introduce, for all its customers, *in abstracto* and as a preventative measure, at its own cost and for an unlimited period, a system for filtering most of the information which is stored on its servers in order to identify on its servers electronic files containing musical, cinematographic or audio-visual work in respect of which SABAM claims to hold rights, and subsequently that it block the exchange of such files.

24 It is possible that introducing such a filtering system would mean that personal data would have to be processed which would have to satisfy the provisions of EU law relating to the protection of personal data and the confidentiality of communications.

25 In those circumstances, the rechtbank van eerste aanleg te Brussel decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:

'Do Directives 2001/29 and 2004/48, in conjunction with Directives 95/46, 2000/31 and 2002/58, construed in particular in the light of Articles 8 and 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms [signed in Rome on 4 November 1950], permit Member States to authorise a national court, before which substantive proceedings have been brought and on the basis merely of a statutory provision stating that "[the national courts] may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right", to order a hosting service provider to introduce, for all its customers, *in abstracto* and as a preventive measure, at its own cost and for an unlimited period, a system for filtering most of the information which is stored on its servers in order to identify on its servers electronic files containing musical, cinematographic or audio-visual work in respect of which SABAM claims to hold rights, and subsequently to block the exchange of such files?'

Consideration of the question referred

26 By its question, the referring court asks, in essence, whether Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, are to be interpreted as precluding a national court from issuing an injunction against a hosting service provider which requires it to install a system for filtering:

— information which is stored on its servers by its service users;

— which applies indiscriminately to all of those users;

— as a preventative measure;

— exclusively at its expense; and

— for an unlimited period,

which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright ('the contested filtering system').

27 In that regard, first, it is not in dispute that the owner of an online social networking platform - such as Netlog - stores information provided by the users of that platform, relating to their profile, on its servers, and that it is thus a hosting service provider within the meaning of Article 14 of Directive 2000/31.

28 Next, it should be borne in mind that, according to Article 8(3) of Directive 2001/29 and the third sentence of Article 11 of Directive 2004/48, holders of intellectual property rights may apply for an injunction against operators of online social networking platforms, such as Netlog, who act as intermediaries within the meaning of those provisions, given that their services may be exploited by users of those platforms to infringe intellectual property rights.

29 In addition, it follows from the Court's case-law that the jurisdiction conferred on national courts, in accordance with those provisions, must allow them to order those intermediaries to take measures aimed not only at bringing to an end infringements already committed against intellectual-property rights using their information-society services, but also at preventing further infringements (see Case C-70/10 *Scarlet Extended* [2011] ECR I-11959, paragraph 31).

30 Lastly, it follows from that same case-law that the rules for the operation of the injunctions for which the Member States must provide under Article 8(3) of Directive 2001/29 and the third sentence of Article 11 of Directive 2004/48, such as those relating to the conditions to be met and to the procedure to be followed, are a matter for national law (see *Scarlet Extended*, paragraph 32).

31 Nevertheless, the rules established by the Member States, and likewise their application by the national courts, must observe the limitations arising from Directives 2001/29 and 2004/48 and from the sources of law to which those directives refer (see *Scarlet Extended*, paragraph 33).

32 Thus, in accordance with recital 16 in the preamble to Directive 2001/29 and Article 2(3)(a) of Directive 2004/48, those rules may not affect the provisions of Directive 2000/31 and, more specifically, Articles 12 to 15 thereof (see *Scarlet Extended*, paragraph 34).

33 Consequently, those rules must, in particular, respect Article 15(1) of Directive 2000/31, which prohibits national authorities from adopting measures which would require a hosting service provider to carry out general monitoring of the information that it stores (see, by analogy, *Scarlet Extended*, paragraph 35).

34 In that regard, the Court has already ruled that that prohibition applies in particular to national measures which would require an intermediary provider, such as a hosting service provider, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual-property rights. Furthermore, such a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly (see *Scarlet Extended*, paragraph 36).

35 In those circumstances, it is necessary to examine whether the injunction at issue in the main proceedings, which would require the hosting service provider to introduce the contested filtering system, would oblige it, as part of that system, to actively monitor all the data of each of its service users in order to prevent any future infringement of intellectual-property rights.

36 In that regard, it is common ground that implementation of that filtering system would require:

— first, that the hosting service provider identify, within all of the files stored on its servers by all its service users, the files which are likely to contain works in respect of which holders of intellectual-property rights claim to hold rights;

— next, that it determine which of those files are being stored and made available to the public unlawfully; and

— lastly, that it prevent files that it considers to be unlawful from being made available.

37 Preventive monitoring of this kind would thus require active observation of files stored by users with the hosting service provider and would involve almost all of the information thus stored and all of the service users of that provider (see, by analogy, *Scarlet Extended*, paragraph 39).

38 In the light of the foregoing, it must be held that the injunction imposed on the hosting service provider requiring it to install the contested filtering system would oblige it to actively monitor almost all the data relating to all of its service users in order to prevent any future infringement of intellectual-property rights. It follows that that injunction would require the hosting service provider to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31 (see, by analogy, *Scarlet Extended*, paragraph 40).

39 In order to assess whether that injunction is consistent with EU law, account must also be taken of the requirements that stem from the protection of the applicable fundamental rights, such as those mentioned by the referring court.

40 In that regard, it should be borne in mind that the injunction at issue in the main proceedings pursues the aim of ensuring the protection of copyright, which is an intellectual-property right, which may be infringed by the nature and content of certain information stored and made available to the public by means of the service offered by the hosting service provider.

41 The protection of the right to intellectual property is indeed enshrined in Article 17(2) of the Charter of Fundamental Rights of the European Union ('the Charter'). There is, however, nothing whatsoever in the wording of that provision or in the Court's case-law to suggest that that right is inviolable and must for that reason be absolutely protected (*Scarlet Extended*, paragraph 43).

42 As paragraphs 62 to 68 of the judgment in Case C-275/06 *Promusicae* [2008] ECR I-271 make clear, the protection of the fundamental right to property, which includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights.

43 More specifically, it follows from paragraph 68 of that judgment that, in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures.

44 Accordingly, in circumstances such as those in the main proceedings, national authorities and courts must, in particular, strike a fair balance between the protection of the intellectual property right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by operators such as hosting service providers pursuant to Article 16 of the Charter (see *Scarlet Extended*, paragraph 46).

45 In the main proceedings, the injunction requiring the installation of the contested filtering system involves monitoring all or most of the information stored by the hosting service provider concerned, in the interests of those rightholders. Moreover, that monitoring has no limitation in time, is directed at all future infringements and is intended to protect not only existing works, but also works that have not yet been created at the time when the system is introduced.

46 Accordingly, such an injunction would result in a serious infringement of the freedom of the hosting service provider to conduct its business since it would require that hosting service provider to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly (see, by analogy, *Scarlet Extended*, paragraph 48).

47 In those circumstances, it must be held that the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as hosting service providers (see, by analogy, *Scarlet Extended*, paragraph 49).

48 Moreover, the effects of that injunction would not be limited to the hosting service provider, as the contested filtering system may also infringe the fundamental rights of that hosting service provider's service users, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively.

49 Indeed, the injunction requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users. The information connected with those profiles is protected personal data because, in principle, it allows those users to be identified (see, by analogy, *Scarlet Extended*, paragraph 51).

50 Moreover, that injunction could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. In addition, in some Member States certain works fall within the public domain or may be posted online free of charge by the authors concerned (see, by analogy, *Scarlet Extended*, paragraph 52).

51 Consequently, it must be held that, in adopting the injunction requiring the hosting service provider to install the contested filtering system, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other (see, by analogy, *Scarlet Extended*, paragraph 53).

52 In the light of the foregoing, the answer to the question referred is that Directives 2000/31, 2001/29 and 2004/48, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against a hosting service provider which requires it to install the contested filtering system.

Costs

53 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds,

the Court (Third Chamber)

hereby rules:

Directives:

— **2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce);**

— **2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; and**

— **2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights,**

read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding a national court from issuing an injunction against a hosting service provider which requires it to install a system for filtering:

— **information which is stored on its servers by its service users;**

— **which applies indiscriminately to all of those users;**

— **as a preventative measure;**

— **exclusively at its expense; and**

— **for an unlimited period,**

which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright.

[Signatures]

Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

6 October 2015 *

(Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities)

In Case C-362/14,

REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings

Maximillian Schrems

v

Data Protection Commissioner,

joined party:

Digital Rights Ireland Ltd,

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), S. Rodin and K. Jürimäe, Presidents of Chambers, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen and C. Lycourgos, Judges,

Advocate General: Y. Bot,

Registrar: L. Hewlett, Principal Administrator,

having regard to the written procedure and further to the hearing on 24 March 2015,

after considering the observations submitted on behalf of:

— Mr Schrems, by N. Travers, Senior Counsel, P. O'Shea, Barrister-at-Law, G. Rudden, Solicitor, and H. Hofmann, Rechtsanwalt,

— the Data Protection Commissioner, by P. McDermott, Barrister-at-Law, S. More O'Ferrall and D. Young, Solicitors,

* Language of the case: English.

— Digital Rights Ireland Ltd, by F. Crehan, Barrister-at-Law, and S. McGarr and E. McGarr, Solicitors,

— Ireland, by A. Joyce, B. Counihan and E. Creedon, acting as Agents, and D. Fennelly, Barrister-at-Law,

— the Belgian Government, by J.-C. Halleux and C. Pochet, acting as Agents,

— the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,

— the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,

— the Austrian Government, by G. Hesse and G. Kunnert, acting as Agents,

— the Polish Government, by M. Kamejsza, M. Pawlicka and B. Majczyna, acting as Agents,

— the Slovenian Government, by A. Grum and V. Klemenc, acting as Agents,

— the United Kingdom Government, by L. Christie and J. Beeko, acting as Agents, and J. Holmes, Barrister,

— the European Parliament, by D. Moore, A. Caiola and M. Pencheva, acting as Agents,

— the European Commission, by B. Schima, B. Martenczuk, B. Smulders and J. Vondung, acting as Agents,

— the European Data Protection Supervisor (EDPS), by C. Docksey, A. Buchta and V. Pérez Asinari, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 23 September 2015,

gives the following

Judgment

1 This request for a preliminary ruling relates to the interpretation, in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union ('the Charter'), of Articles 25(6) and 28 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 (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 (OJ 2003 L 284, p. 1) ('Directive 95/46'), and, in essence, to the validity of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

2 The request has been made in proceedings between Mr Schrems and the Data Protection Commissioner ('the Commissioner') concerning the latter's refusal to investigate a complaint made by Mr Schrems regarding the fact that Facebook Ireland Ltd ('Facebook Ireland') transfers the personal data of its users to the United States of America and keeps it on servers located in that country.

Legal context

Directive 95/46

3 Recitals 2, 10, 56, 57, 60, 62 and 63 in the preamble to Directive 95/46 are worded as follows:

‘(2) ... data-processing systems are designed to serve man; … they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to … the well-being of individuals;

…

(10) … 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 European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950,] 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;

…

(56) … cross-border flows of personal data are necessary to the expansion of international trade; … the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; … the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) … on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

…

(60) … in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

…

(62) … the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) … such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; ...’

4 Articles 1, 2, 25, 26, 28 and 31 of Directive 95/46 provide:

‘*Article 1*

Object of the Directive

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.

...

Article 2

Definitions

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;

...

(d) “controller” shall mean 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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

...

Article 25

Principles

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.

Article 26

Derogations

1. 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.

2. Without prejudice to paragraph 1, a Member State may authorise 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), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorisations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2).

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

...

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

— investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

— effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

— the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

...

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

...

Article 31

...

2. Where reference is made to this Article, Articles 4 and 7 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)] shall apply, having regard to the provisions of Article 8 thereof.

...'

Decision 2000/520

5 Decision 2000/520 was adopted by the Commission on the basis of Article 25(6) of Directive 95/46.

6 Recitals 2, 5 and 8 in the preamble to that decision are worded as follows:

'(2) The Commission may find that a third country ensures an adequate level of protection. In that case personal data may be transferred from the Member States without additional guarantees being necessary.

…

(5) The adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the safe harbour privacy principles for the protection of personal data transferred from a Member State to the United States (hereinafter "the Principles") and the frequently asked questions (hereinafter "the FAQs") providing guidance for the implementation of the Principles issued by the Government of the United States on 21 July 2000. Furthermore the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs.

…

(8) In the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection.'

7 Articles 1 to 4 of Decision 2000/520 provide:

‘*Article 1*

1. For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the “Safe Harbour Privacy Principles” (hereinafter “the Principles”), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked questions (hereinafter “the FAQs”) issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States, having regard to the following documents issued by the US Department of Commerce:

(a) the safe harbour enforcement overview set out in Annex III;

(b) a memorandum on damages for breaches of privacy and explicit authorisations in US law set out in Annex IV;

(c) a letter from the Federal Trade Commission set out in Annex V;

(d) a letter from the US Department of Transportation set out in Annex VI.

2. In relation to each transfer of data the following conditions shall be met:

(a) the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs; and

(b) the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles implemented in accordance with the FAQs.

3. The conditions set out in paragraph 2 are considered to be met for each organisation that self-certifies its adherence to the Principles implemented in accordance with the FAQs from the date on which the organisation notifies to the US Department of Commerce (or its designee) the public disclosure of the commitment referred to in paragraph 2(a) and the identity of the government body referred to in paragraph 2(b).

Article 2

This Decision concerns only the adequacy of protection provided in the United States under the Principles implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect the application of other provisions of that Directive that pertain to the processing of personal data within the Member States, in particular Article 4 thereof.

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 an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

(a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or

(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned 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 under the circumstances to provide the organisation with notice and an opportunity to respond.

The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.

2. Member States shall inform the Commission without delay when measures are adopted on the basis of paragraph 1.

3. The Member States and the Commission shall also inform each other of cases where the action of bodies responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States fails to secure such compliance.

4. If the information collected under paragraphs 1, 2 and 3 provides evidence that any body responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States is not effectively fulfilling its role, the Commission shall inform the US Department of Commerce and, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC with a view to reversing or suspending the present Decision or limiting its scope.

Article 4

1. This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation.

The Commission shall in any case evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection within the meaning of Article 25 of Directive 95/46/EC and any evidence that the present Decision is being implemented in a discriminatory way.

2. The Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC.'

8 Annex I to Decision 2000/520 is worded as follows:

‘Safe Harbour Privacy Principles issued by the US Department of Commerce on 21 July 2000 ... the Department of Commerce is issuing this document and Frequently Asked Questions (“the Principles”) under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of “adequacy” it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. … Decisions by organisations to qualify for the safe harbour are entirely voluntary, and organisations may qualify for the safe harbour in different ways. ... Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation; or (c) if the effect of the Directive [or] Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organisations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or US law, organisations are expected to opt for the higher protection where possible. ...’

9 Annex II to Decision 2000/520 reads as follows:

‘Frequently Asked Questions (FAQs)

... FAQ 6 — Self-Certification

Q: *How does an organisation self-certify that it adheres to the Safe Harbour Principles?*

A: Safe harbour benefits are assured from the date on which an organisation self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.

To self-certify for the safe harbour, organisations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organisation that is joining the safe harbour, that contains at least the following information:

1. name of organisation, mailing address, e-mail address, telephone and fax numbers;

2. description of the activities of the organisation with respect to personal information received from the [European Union]; and

3. description of the organisation’s privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbour, (d) the specific statutory body that has jurisdiction to hear any claims against the organisation regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the

annex to the Principles), (e) name of any privacy programmes in which the organisation is a member, (f) method of verification (e.g. in-house, third party) …, and (g) the independent recourse mechanism that is available to investigate unresolved complaints.

Where the organisation wishes its safe harbour benefits to cover human resources information transferred from the [European Union] for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organisation arising out of human resources information that is listed in the annex to the Principles. ...

The Department (or its designee) will maintain a list of all organisations that file such letters, thereby assuring the availability of safe harbour benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. ...

... FAQ 11 — Dispute Resolution and Enforcement

Q: *How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organisation's persistent failure to comply with the Principles be handled?*

A: The Enforcement Principle sets out the requirements for safe harbour enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ on verification (FAQ 7). This FAQ 11 addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organisations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programmes that incorporate the Safe Harbour Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their authorised representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are additional to the requirements set forth in paragraph 3 of the introduction to the Principles that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.

Recourse Mechanisms

Consumers should be encouraged to raise any complaints they may have with the relevant organisation before proceeding to independent recourse mechanisms. ...

...

FTC Action

The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organisations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbour Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. ... …'

10 Annex IV to Decision 2000/520 states:

'Damages for Breaches of Privacy, Legal Authorisations and Mergers and Takeovers in US Law

This responds to the request by the European Commission for clarification of US law with respect to (a) claims for damages for breaches of privacy, (b) "explicit authorisations" in US law for the use of personal information in a manner inconsistent with the safe harbour principles, and (c) the effect of mergers and takeovers on obligations undertaken pursuant to the safe harbour principles.

...

B. Explicit Legal Authorisations The safe harbour principles contain an exception where statute, regulation or case-law create "conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the principles is limited to the extent necessary to meet the overriding legitimate interests further[ed] by such authorisation". Clearly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law. As for explicit authorisations, while the safe harbour principles are intended to bridge the differences between the US and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers. The limited exception from strict adherence to the safe harbour principles seeks to strike a balance to accommodate the legitimate interests on each side. The exception is limited to cases where there is an explicit authorisation. Therefore, as a threshold matter, the relevant statute, regulation or court decision must affirmatively authorise the particular conduct by safe harbour organisations ... In other words, the exception would not apply where the law is silent. In addition, the exception would apply only if the explicit authorisation conflicts with adherence to the safe harbour principles. Even then, the exception "is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation". By way of illustration, where the law simply authorises a company to provide personal information to government authorities, the exception would not apply. Conversely, where the law specifically authorises the company to provide personal information to government agencies without the individual's consent, this would constitute an "explicit authorisation" to act in a manner that conflicts with the safe harbour principles. Alternatively, specific exceptions from affirmative requirements to provide notice and consent would fall within the exception (since it would be the equivalent of a specific authorisation to disclose the information without notice and consent). For example, a statute which authorises doctors to provide their patients' medical records to health officials without the patients' prior consent might permit an exception from the notice and choice principles. This authorisation would not permit a doctor to provide the same medical records to health maintenance organisations or commercial pharmaceutical research laboratories, which would be beyond the scope of the purposes authorised by the law and therefore beyond the scope of the exception ... The legal authority in question can be a "stand alone" authorisation to do specific things with personal information, but, as the examples below illustrate, it is likely to be an exception to a broader law which proscribes the collection, use, or disclosure of personal information. ...'

Communication COM(2013) 846 final

11 On 27 November 2013 the Commission adopted the communication to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final) ('Communication COM(2013) 846 final'). The communication was accompanied by the 'Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection', also dated 27 November 2013. That report was drawn up, as stated in point 1 thereof, in cooperation with the United States after the existence in that country of a number of surveillance programmes involving the large-scale collection and processing of personal data had been revealed. The report contained inter alia a detailed analysis of United States law as regards, in particular, the legal bases authorising the existence of surveillance programmes and the collection and processing of personal data by United States authorities.

12 In point 1 of Communication COM(2013) 846 final, the Commission stated that '[c]ommercial exchanges are addressed by Decision [2000/520]', adding that '[t]his Decision provides a legal basis for transfers of personal data from the [European Union] to companies established in the [United States] which have adhered to the Safe Harbour Privacy Principles'. In addition, the Commission underlined in point 1 the increasing relevance of personal data flows, owing in particular to the development of the digital economy which has indeed 'led to exponential growth in the quantity, quality, diversity and nature of data processing activities'.

13 In point 2 of that communication, the Commission observed that 'concerns about the level of protection of personal data of [Union] citizens transferred to the [United States] under the Safe Harbour scheme have grown' and that '[t]he voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement'.

14 It further stated in point 2 that '[t]he personal data of [Union] citizens sent to the [United States] under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the [European Union] and the purposes for which it was transferred to the [United States]' and that '[a] majority of the US internet companies that appear to be more directly concerned by [the surveillance] programmes are certified under the Safe Harbour scheme'.

15 In point 3.2 of Communication COM(2013) 846 final, the Commission noted a number of weaknesses in the application of Decision 2000/520. It stated, first, that some certified United States companies did not comply with the principles referred to in Article 1(1) of Decision 2000/520 ('the safe harbour principles') and that improvements had to be made to that decision regarding 'structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception'. It observed, secondly, that 'Safe Harbour also acts as a conduit for the transfer of the personal data of EU citizens from the [European Union] to the [United States] by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes'.

16 The Commission concluded in point 3.2 that whilst, '[g]iven the weaknesses identified, the current implementation of Safe Harbour cannot be maintained, ... its revocation would[, however,] adversely affect the interests of member companies in the [European Union] and in the [United States]'. Finally, the Commission added in that point that it would 'engage with the US authorities to discuss the shortcomings identified'.

Communication COM(2013) 847 final

17 On the same date, 27 November 2013, the Commission adopted the communication to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the [European Union] (COM(2013) 847 final) ('Communication COM(2013) 847 final'). As is clear from point 1 thereof, that communication was based inter alia on information received in the ad hoc EU-US Working Group and followed two Commission assessment reports published in 2002 and 2004 respectively.

18 Point 1 of Communication COM(2013) 847 final explains that the functioning of Decision 2000/520 'relies on commitments and self-certification of adhering companies', adding that '[s]igning up to these arrangements is voluntary, but the rules are binding for those who sign up'.

19 In addition, it is apparent from point 2.2 of Communication COM(2013) 847 final that, as at 26 September 2013, 3 246 companies, falling within many industry and services sectors, were certified. Those companies mainly provided services in the EU internal market, in particular in the internet

sector, and some of them were EU companies which had subsidiaries in the United States. Some of those companies processed the data of their employees in Europe which was transferred to the United States for human resource purposes.

20 The Commission stated in point 2.2 that '[a]ny gap in transparency or in enforcement on the US side results in responsibility being shifted to European data protection authorities and to the companies which use the scheme'.

21 It is apparent, in particular, from points 3 to 5 and 8 of Communication COM(2013) 847 final that, in practice, a significant number of certified companies did not comply, or did not comply fully, with the safe harbour principles.

22 In addition, the Commission stated in point 7 of Communication COM(2013) 847 final that 'all companies involved in the PRISM programme [a large-scale intelligence collection programme], and which grant access to US authorities to data stored and processed in the [United States], appear to be Safe Harbour certified' and that '[t]his has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the [European Union]'. In that regard, the Commission noted in point 7.1 of that communication that 'a number of legal bases under US law allow large-scale collection and processing of personal data that is stored or otherwise processed [by] companies based in the [United States]' and that '[t]he large-scale nature of these programmes may result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in [Decision 2000/520]'.

23 In point 7.2 of Communication COM(2013) 847 final, headed 'Limitations and redress possibilities', the Commission noted that 'safeguards that are provided under US law are mostly available to US citizens or legal residents' and that, '[m]oreover, there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes'.

24 According to point 8 of Communication COM(2013) 847 final, the certified companies included '[w]eb companies such as Google, Facebook, Microsoft, Apple, Yahoo', which had 'hundreds of millions of clients in Europe' and transferred personal data to the United States for processing.

25 The Commission concluded in point 8 that 'the large-scale access by intelligence agencies to data transferred to the [United States] by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data is transferred to the [United States]'.

The dispute in the main proceedings and the questions referred for a preliminary ruling

26 Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network ('Facebook') since 2008.

27 Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland's users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing.

28 On 25 June 2013 Mr Schrems made a complaint to the Commissioner by which he in essence asked the latter to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the United States. He contended in his complaint that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency ('the NSA').

29 Since the Commissioner took the view that he was not required to investigate the matters raised by Mr Schrems in the complaint, he rejected it as unfounded. The Commissioner considered that there was no evidence that Mr Schrems' personal data had been accessed by the NSA. He added that the allegations raised by Mr Schrems in his complaint could not be profitably put forward since any question of the adequacy of data protection in the United States had to be determined in accordance with Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection.

30 Mr Schrems brought an action before the High Court challenging the decision at issue in the main proceedings. After considering the evidence adduced by the parties to the main proceedings, the High Court found that the electronic surveillance and interception of personal data transferred from the European Union to the United States serve necessary and indispensable objectives in the public interest. However, it added that the revelations made by Edward Snowden had demonstrated a 'significant over-reach' on the part of the NSA and other federal agencies.

31 According to the High Court, Union citizens have no effective right to be heard. Oversight of the intelligence services' actions is carried out within the framework of an *ex parte* and secret procedure. Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and interception carried out by them on a large scale.

32 The High Court stated that Irish law precludes the transfer of personal data outside national territory save where the third country ensures an adequate level of protection for privacy and fundamental rights and freedoms. The importance of the rights to privacy and to inviolability of the dwelling, which are guaranteed by the Irish Constitution, requires that any interference with those rights be proportionate and in accordance with the law.

33 The High Court held that the mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution. In order for interception of electronic communications to be regarded as consistent with the Irish Constitution, it would be necessary to demonstrate that the interception is targeted, that the surveillance of certain persons or groups of persons is objectively justified in the interests of national security or the suppression of crime and that there are appropriate and verifiable safeguards. Thus, according to the High Court, if the main proceedings were to be disposed of on the basis of Irish law alone, it would then have to be found that, given the existence of a serious doubt as to whether the United States ensures an adequate level of protection of personal data, the Commissioner should have proceeded to investigate the matters raised by Mr Schrems in his complaint and that the Commissioner was wrong in rejecting the complaint.

34 However, the High Court considers that this case concerns the implementation of EU law as referred to in Article 51 of the Charter and that the legality of the decision at issue in the main proceedings must therefore be assessed in the light of EU law. According to the High Court, Decision 2000/520 does not satisfy the requirements flowing both from Articles 7 and 8 of the Charter and from the principles set out by the Court of Justice in the judgment in *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238). The right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be

rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards.

35 The High Court further observes that in his action Mr Schrems in reality raises the legality of the safe harbour regime which was established by Decision 2000/520 and gives rise to the decision at issue in the main proceedings. Thus, even though Mr Schrems has not formally contested the validity of either Directive 95/46 or Decision 2000/520, the question is raised, according to the High Court, as to whether, on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether Article 8 of the Charter authorised the Commissioner to break free, if appropriate, from such a finding.

36 In those circumstances the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?

(2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?'

Consideration of the questions referred

37 By its questions, which it is appropriate to examine together, the referring court asks, in essence, whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, prevents a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

The powers of the national supervisory authorities, within the meaning of Article 28 of Directive 95/46, when the Commission has adopted a decision pursuant to Article 25(6) of that directive

38 It should be recalled first of all that the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter (see judgments in *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 68; and *Ryneš*, C-212/13, EU:C:2014:2428, paragraph 29).

39 It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms. The importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8 thereof, is, moreover, emphasised in the case-law of the Court (see judgments in *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 47; *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 53; and *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraphs, 53, 66, 74 and the case-law cited).

40 As regards the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU (see, to this effect, judgments in *Commission* v *Austria*, C-614/10, EU:C:2012:631, paragraph 36, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 47).

41 The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data (see judgments in *Commission* v *Germany*, C-518/07, EU:C:2010:125, paragraph 25, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 48 and the case-law cited).

42 In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data (see, to this effect, judgments in *Commission* v *Germany*, C-518/07, EU:C:2010:125, paragraph 24, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 51).

43 The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings.

44 It is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, so that they do not have powers on the basis of Article 28 in respect of processing of such data carried out in a third country.

45 However, the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive 95/46 (see, to this effect, judgment in *Parliament* v *Council and Commission*, C-317/04 and C-318/04, EU:C:2006:346, paragraph 56) carried out in a Member State. That provision defines ‘processing of

personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means' and mentions, by way of example, 'disclosure by transmission, dissemination or otherwise making available'.

46 Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to the directive. In that regard, Chapter IV of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data (see, to this effect, judgment in *Lindqvist*, C-101/01, EU:C:2003:596, paragraph 63).

47 As, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46.

48 Whilst acknowledging, in recital 56 in its preamble, that transfers of personal data from the Member States to third countries are necessary for the expansion of international trade, Directive 95/46 lays down as a principle, in Article 25(1), that such transfers may take place only if the third country ensures an adequate level of protection.

49 Furthermore, recital 57 states that transfers of personal data to third countries not ensuring an adequate level of protection must be prohibited.

50 In order to control transfers of personal data to third countries according to the level of protection accorded to it in each of those countries, Article 25 of Directive 95/46 imposes a series of obligations on the Member States and the Commission. It is apparent, in particular, from that article that the finding that a third country does or does not ensure an adequate level of protection may, as the Advocate General has observed in point 86 of his Opinion, be made either by the Member States or by the Commission.

51 The Commission may adopt, on the basis of Article 25(6) of Directive 95/46, a decision finding that a third country ensures an adequate level of protection. In accordance with the second subparagraph of that provision, such a decision is addressed to the Member States, who must take the measures necessary to comply with it. Pursuant to the fourth paragraph of Article 288 TFEU, it is binding on all the Member States to which it is addressed and is therefore binding on all their organs (see, to this effect, judgments in *Albako Margarinefabrik*, 249/85, EU:C:1987:245, paragraph 17, and *Mediaset*, C-69/13, EU:C:2014:71, paragraph 23) in so far as it has the effect of authorising transfers of personal data from the Member States to the third country covered by it.

52 Thus, until such time as the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality (judgment in *Commission* v *Greece*, C-475/01, EU:C:2004:585, paragraph 18 and the case-law cited).

53 However, a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, such as Decision 2000/520, cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim, within the meaning of

Article 28(4) of that directive, concerning the protection of their rights and freedoms in regard to the processing of that data. Likewise, as the Advocate General has observed in particular in points 61, 93 and 116 of his Opinion, a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive.

54 Neither Article 8(3) of the Charter nor Article 28 of Directive 95/46 excludes from the national supervisory authorities' sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46.

55 In particular, the first subparagraph of Article 28(4) of Directive 95/46, under which the national supervisory authorities are to hear 'claims lodged by any person … concerning the protection of his rights and freedoms in regard to the processing of personal data', does not provide for any exception in this regard where the Commission has adopted a decision pursuant to Article 25(6) of that directive.

56 Furthermore, it would be contrary to the system set up by Directive 95/46 and to the objective of Articles 25 and 28 thereof for a Commission decision adopted pursuant to Article 25(6) to have the effect of preventing a national supervisory authority from examining a person's claim concerning the protection of his rights and freedoms in regard to the processing of his personal data which has been or could be transferred from a Member State to the third country covered by that decision.

57 On the contrary, Article 28 of Directive 95/46 applies, by its very nature, to any processing of personal data. Thus, even if the Commission has adopted a decision pursuant to Article 25(6) of that directive, the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive.

58 If that were not so, persons whose personal data has been or could be transferred to the third country concerned would be denied the right, guaranteed by Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights (see, by analogy, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 68).

59 A claim, within the meaning of Article 28(4) of Directive 95/46, by which a person whose personal data has been or could be transferred to a third country contends, as in the main proceedings, that, notwithstanding what the Commission has found in a decision adopted pursuant to Article 25(6) of that directive, the law and practices of that country do not ensure an adequate level of protection must be understood as concerning, in essence, whether that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.

60 In this connection, the Court's settled case-law should be recalled according to which the European Union is a union based on the rule of law in which all acts of its institutions are subject to review of their compatibility with, in particular, the Treaties, general principles of law and fundamental rights (see, to this effect, judgments in *Commission and Others* v *Kadi*, C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518, paragraph 66; *Inuit Tapiriit Kanatami and Others* v *Parliament and Council*, C-583/11 P, EU:C:2013:625, paragraph 91; and *Telefónica* v *Commission*, C-274/12 P, EU:C:2013:852, paragraph 56). Commission decisions adopted pursuant to Article 25(6) of Directive 95/46 cannot therefore escape such review.

61 That said, the Court alone has jurisdiction to declare that an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, is invalid, the exclusivity of that jurisdiction having the purpose of guaranteeing legal certainty by ensuring that EU law is applied uniformly (see judgments in *Melki and Abdeli*, C-188/10 and C-189/10, EU:C:2010:363, paragraph 54, and *CIVAD*, C-533/10, EU:C:2012:347, paragraph 40).

62 Whilst the national courts are admittedly entitled to consider the validity of an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, they are not, however, endowed with the power to declare such an act invalid themselves (see, to this effect, judgments in *Foto-Frost*, 314/85, EU:C:1987:452, paragraphs 15 to 20, and *IATA and ELFAA*, C-344/04, EU:C:2006:10, paragraph 27). A fortiori, when the national supervisory authorities examine a claim, within the meaning of Article 28(4) of that directive, concerning the compatibility of a Commission decision adopted pursuant to Article 25(6) of the directive with the protection of the privacy and of the fundamental rights and freedoms of individuals, they are not entitled to declare that decision invalid themselves.

63 Having regard to those considerations, where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, as in the main proceedings, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence.

64 In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded and therefore rejects it, the person who lodged the claim must, as is apparent from the second subparagraph of Article 28(3) of Directive 95/46, read in the light of Article 47 of the Charter, have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. Having regard to the case-law cited in paragraphs 61 and 62 of the present judgment, those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded (see, to this effect, judgment in *T & L Sugars and Sidul Açúcares* v *Commission*, C-456/13 P, EU:C:2015:284, paragraph 48 and the case-law cited).

65 In the converse situation, where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded, that authority must, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46, read in the light in particular of Article 8(3) of the Charter, be able to engage in legal proceedings. It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity.

66 Having regard to the foregoing considerations, the answer to the questions referred is that Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the

processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

The validity of Decision 2000/520

67 As is apparent from the referring court's explanations relating to the questions submitted, Mr Schrems contends in the main proceedings that United States law and practice do not ensure an adequate level of protection within the meaning of Article 25 of Directive 95/46. As the Advocate General has observed in points 123 and 124 of his Opinion, Mr Schrems expresses doubts, which the referring court indeed seems essentially to share, concerning the validity of Decision 2000/520. In such circumstances, having regard to what has been held in paragraphs 60 to 63 of the present judgment and in order to give the referring court a full answer, it should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter.

The requirements stemming from Article 25(6) of Directive 95/46

68 As has already been pointed out in paragraphs 48 and 49 of the present judgment, Article 25(1) of Directive 95/46 prohibits transfers of personal data to a third country not ensuring an adequate level of protection.

69 However, for the purpose of overseeing such transfers, the first subparagraph of Article 25(6) of Directive 95/46 provides that the Commission 'may find … 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 …, for the protection of the private lives and basic freedoms and rights of individuals'.

70 It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that 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' and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.

71 However, first, as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed 'for the protection of the private lives and basic freedoms and rights of individuals'.

72 Thus, Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.

73 The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the

high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.

74 It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.

75 Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country.

76 Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard.

77 Moreover, as the Advocate General has stated in points 134 and 135 of his Opinion, when the validity of a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision's adoption.

78 In this regard, it must be stated that, in view of, first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, secondly, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection, the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict (see, by analogy, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 47 and 48).

Article 1 of Decision 2000/520

79 The Commission found in Article 1(1) of Decision 2000/520 that the principles set out in Annex I thereto, implemented in accordance with the guidance provided by the FAQs set out in Annex II, ensure an adequate level of protection for personal data transferred from the European Union to organisations established in the United States. It is apparent from that provision that both those principles and the FAQs were issued by the United States Department of Commerce.

80 An organisation adheres to the safe harbour principles on the basis of a system of self-certification, as is apparent from Article 1(2) and (3) of Decision 2000/520, read in conjunction with FAQ 6 set out in Annex II thereto.

81 Whilst recourse by a third country to a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection 'by reason of its domestic law or … international commitments', the reliability of such a system, in the light of that requirement, is founded essentially

on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice.

82 In the present instance, by virtue of the second paragraph of Annex I to Decision 2000/520, the safe harbour principles are 'intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of "adequacy" it creates'. Those principles are therefore applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them.

83 Moreover, Decision 2000/520, pursuant to Article 2 thereof, 'concerns only the adequacy of protection provided in the United States under the [safe harbour principles] implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive [95/46]', without, however, containing sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive, by reason of its domestic law or its international commitments.

84 In addition, under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'.

85 In this connection, Decision 2000/520 states in Part B of Annex IV, with regard to the limits to which the safe harbour principles' applicability is subject, that, '[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law'.

86 Thus, Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.

87 In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 33 and the case-law cited).

88 In addition, Decision 2000/520 does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.

89 Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind. As the Advocate General has observed in points 204 to 206 of his Opinion, procedures before the Federal Trade Commission — the powers of which, described in particular in FAQ 11 set

out in Annex II to that decision, are limited to commercial disputes — and the private dispute resolution mechanisms concern compliance by the United States undertakings with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.

90 Moreover, the foregoing analysis of Decision 2000/520 is borne out by the Commission's own assessment of the situation resulting from the implementation of that decision. Particularly in points 2 and 3.2 of Communication COM(2013) 846 final and in points 7.1, 7.2 and 8 of Communication COM(2013) 847 final, the content of which is set out in paragraphs 13 to 16 and paragraphs 22, 23 and 25 of the present judgment respectively, the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

91 As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55 and the case-law cited).

92 Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52 and the case-law cited).

93 Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).

94 In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39).

95 Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an

effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (see, to this effect, judgments in *Les Verts* v *Parliament*, 294/83, EU:C:1986:166, paragraph 23; *Johnston*, 222/84, EU:C:1986:206, paragraphs 18 and 19; *Heylens and Others*, 222/86, EU:C:1987:442, paragraph 14; and *UGT-Rioja and Others*, C-428/06 to C-434/06, EU:C:2008:488, paragraph 80).

96 As has been found in particular in paragraphs 71, 73 and 74 of the present judgment, in order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment.

97 However, the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments.

98 Consequently, without there being any need to examine the content of the safe harbour principles, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid.

Article 3 of Decision 2000/520

99 It is apparent from the considerations set out in paragraphs 53, 57 and 63 of the present judgment that, under Article 28 of Directive 95/46, read in the light in particular of Article 8 of the Charter, the national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him. That is in particular the case where, in bringing such a claim, that person raises questions regarding the compatibility of a Commission decision adopted pursuant to Article 25(6) of that directive with the protection of the privacy and of the fundamental rights and freedoms of individuals.

100 However, the first subparagraph of Article 3(1) of Decision 2000/520 lays down specific rules regarding the powers available to the national supervisory authorities in the light of a Commission finding relating to an adequate level of protection, within the meaning of Article 25 of Directive 95/46.

101 Under that provision, the national supervisory authorities may, '[w]ithout 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], … suspend data flows to an organisation that has self-certified its adherence to the [principles of Decision 2000/520]', under restrictive conditions establishing a high threshold for intervention. Whilst that provision is without prejudice to the powers of those authorities to take action to ensure compliance with national provisions adopted pursuant to Directive 95/46, it excludes, on the other hand, the possibility of them taking action to ensure compliance with Article 25 of that directive.

102 The first subparagraph of Article 3(1) of Decision 2000/520 must therefore be understood as denying the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person, in bringing a claim under that provision, puts forward matters that may call into question whether a Commission decision that has found, on the basis of Article 25(6) of the directive, that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.

103 The implementing power granted by the EU legislature to the Commission in Article 25(6) of Directive 95/46 does not confer upon it competence to restrict the national supervisory authorities' powers referred to in the previous paragraph of the present judgment.

104 That being so, it must be held that, in adopting Article 3 of Decision 2000/520, the Commission exceeded the power which is conferred upon it in Article 25(6) of Directive 95/46, read in the light of the Charter, and that Article 3 of the decision is therefore invalid.

105 As Articles 1 and 3 of Decision 2000/520 are inseparable from Articles 2 and 4 of that decision and the annexes thereto, their invalidity affects the validity of the decision in its entirety.

106 Having regard to all the foregoing considerations, it is to be concluded that Decision 2000/520 is invalid.

Costs

107 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

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

1. **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 as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.**

2. **Decision 2000/520 is invalid.**

[Signatures]

Recueil de la jurisprudence

ARRÊT DU TRIBUNAL DE LA FONCTION PUBLIQUE DE L'UNION EUROPÉENNE (deuxième chambre)

21 octobre 2015 *

« Fonction publique — Fonctionnaires — Règlement nº 45/2001 — Traitement de données à caractère personnel obtenues à des fins privées — Enquête administrative — Procédure disciplinaire — Droits de la défense — Devoir de motivation — Sanction disciplinaire — Proportionnalité »

Dans l'affaire F-57/14,

ayant pour objet un recours introduit au titre de l'article 270 TFUE, applicable au traité CEEA en vertu de son article 106 bis,

AQ, fonctionnaire de la Commission européenne, demeurant à Bruxelles (Belgique), représenté, initialement, par M^e^ L. Massaux, avocat, puis par M^e^ H. Mignard, avocat,

partie requérante,

contre

Commission européenne, représentée par M. J. Currall et M^me^ C. Ehrbar, en qualité d'agents,

partie défenderesse,

LE TRIBUNAL DE LA FONCTION PUBLIQUE (deuxième chambre),

composé de MM. K. Bradley, président, H. Kreppel et M^me^ M. I. Rofes i Pujol (rapporteur), juges,

greffier : M. P. Cullen, administrateur,

vu la procédure écrite et à la suite de l'audience du 30 juin 2015,

rend le présent

Arrêt

1 Par requête parvenue au greffe du Tribunal le 20 juin 2014, AQ demande, d'une part, l'annulation de la décision de l'autorité investie du pouvoir de nomination (ci-après l'« AIPN ») de la Commission européenne, du 19 mars 2014, de rejet de sa réclamation, ainsi que, pour autant que de besoin, l'annulation de la décision du 6 septembre 2013 lui infligeant la sanction disciplinaire du blâme et, d'autre part, la condamnation de la Commission à lui verser la somme de 5 000 euros, évaluée ex æquo et bono, à titre de dommages et intérêts.

* Langue de procédure : le français.

Cadre juridique

Les dispositions relatives à la protection des données à caractère personnel

2 L'article 8, intitulé « Protection des données à caractère personnel », de la Charte des droits fondamentaux de l'Union européenne établit ce qui suit :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. […]

[…] »

3 Le 18 décembre 2000, le Parlement européen et le Conseil de l'Union européenne ont adopté le règlement (CE) nº 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes [de l'Union européenne] et à la libre circulation de ces données (JO 2001 L 8, p. 1).

4 Conformément au considérant 7 du règlement nº 45/2001 :

« Les personnes susceptibles d'être protégées sont celles dont les données à caractère personnel sont traitées par les institutions ou organes [de l'Union] dans quelque contexte que ce soit, par exemple parce que ces personnes sont employées par ces institutions ou organes. »

5 En vertu de l'article 2 du règlement nº 45/2001 :

« Aux fins du présent règlement, on entend par :

a) 'données à caractère personnel' : toute information concernant une personne physique identifiée ou identifiable […]

[…] »

6 L'article 3 du règlement nº 45/2001 est libellé comme suit :

« 1. Le présent règlement s'applique au traitement de données à caractère personnel par toutes les institutions et tous les organes [de l'Union], dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit [de l'Union].

2. Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. »

7 L'article 4 du règlement nº 45/2001 dispose, en ce qui concerne la qualité des données :

« 1. Les données à caractère personnel doivent être :

a) traitées loyalement et licitement ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que le

responsable du traitement prévoie des garanties appropriées, afin de veiller, en particulier, à ce que les données ne soient traitées pour aucune autre finalité et qu'elles ne soient pas utilisées à l'appui de dispositions ou décisions concernant une personne en particulier ;

[…] »

8 L'article 5 du règlement nº 45/2001 prévoit, pour ce qui est de la licéité du traitement de données à caractère personnel :

« Le traitement de données à caractère personnel ne peut être effectué que si :

a) le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant [l'Union européenne] ou d'autres actes législatifs adoptés sur la base de ces traités ou relevant de l'exercice légitime de l'autorité publique dont est investi l'institution ou l'organe [de l'Union] ou le tiers auquel les données sont communiquées, ou

b) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou

c) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci, ou

d) la personne concernée a indubitablement donné son consentement, ou

e) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée. »

9 D'après le libellé de l'article 49 du règlement nº 45/2001 :

« Tout manquement aux obligations auxquelles un fonctionnaire ou un autre agent [de l'Union] est tenu en vertu du présent règlement, commis intentionnellement ou par négligence, l'expose à une sanction disciplinaire, conformément aux dispositions du statut des fonctionnaires [de l'Union européenne] ou aux régimes qui sont applicables aux autres agents. »

Les dispositions statutaires relatives à la discipline

10 En vertu de l'article 12 du statut des fonctionnaires de l'Union européenne, dans sa version applicable au litige (ci-après le « statut ») :

« Le fonctionnaire s'abstient de tout acte et de tout comportement qui puissent porter atteinte à la dignité de sa fonction. »

11 L'article 86 du statut établit :

« 1. Tout manquement aux obligations auxquelles le fonctionnaire ou l'ancien fonctionnaire est tenu, au titre du présent statut, commis volontairement ou par négligence, l'expose à une sanction disciplinaire.

2. L'[AIPN] ou l'Office européen de lutte antifraude peuvent ouvrir une enquête administrative, en vue de vérifier l'existence d'un manquement au sens du paragraphe 1, lorsque des éléments de preuve laissant présumer l'existence d'un manquement ont été portés à leur connaissance.

[…] »

12 Conformément à l'article 2, paragraphe 2, de l'annexe IX du statut, relative à la procédure disciplinaire :

« L'[AIPN] informe l'intéressé de la fin de l'enquête et lui communique les conclusions du rapport d'enquête et, sur sa demande et sous réserve de la protection des intérêts légitimes de tierces parties, tous les documents qui sont en rapport direct avec les allégations formulées à son encontre. »

13 L'article 3 de l'annexe IX du statut dispose :

« Sur la base du rapport d'enquête, après avoir communiqué au fonctionnaire concerné toutes les pièces du dossier et après l'avoir entendu, l'[AIPN] peut :

a) décider qu'aucune charge ne peut être retenue contre le fonctionnaire concerné, auquel cas ce dernier en est alors informé par écrit ; ou

b) décider, même en cas de manquement ou de manquement présumé aux obligations, qu'il convient de n'adopter aucune sanction disciplinaire et, le cas échéant, adresser au fonctionnaire une mise en garde ; ou

c) en cas de manquement aux obligations, conformément à l'article 86 du statut,

i) décider de l'ouverture de la procédure disciplinaire prévue à la section 4 de la présente annexe, ou

ii) décider de l'ouverture d'une procédure disciplinaire devant le conseil de discipline. »

14 L'article 9 de l'annexe IX du statut est libellé comme suit :

« 1. L'[AIPN] peut appliquer une des sanctions suivantes :

a) l'avertissement par écrit ;

b) le blâme ;

[…] »

15 L'article 10 de l'annexe IX du statut précise :

« La sanction disciplinaire infligée est proportionnelle à la gravité de la faute commise. Pour déterminer la gravité de la faute et décider de la sanction disciplinaire à infliger, il est tenu compte notamment :

a) de la nature de la faute et des circonstances dans lesquelles elle a été commise ;

b) de l'importance du préjudice porté à l'intégrité, à la réputation ou aux intérêts des institutions en raison de la faute commise ;

c) du degré d'intentionnalité ou de négligence dans la faute commise ;

d) des motifs ayant amené le fonctionnaire à commettre la faute ;

e) du grade et de l'ancienneté du fonctionnaire ;

f) du degré de responsabilité personnelle du fonctionnaire ;

g) du niveau des fonctions et responsabilités du fonctionnaire ;

h) de la récidive de l'acte ou du comportement fautif ;

i) de la conduite du fonctionnaire tout au long de sa carrière. »

16 L'article 11 de l'annexe IX du statut prévoit :

« L'[AIPN] peut décider de la sanction d'avertissement par écrit ou de blâme sans consultation du conseil [de discipline]. Le fonctionnaire concerné est préalablement entendu par l'[AIPN]. »

Faits à l'origine du litige

17 Le requérant est fonctionnaire de la Commission depuis 1988. Lors de l'introduction du recours, il était classé au grade AD 13.

18 Il ressort du dossier que, le vendredi 5 mars 2010, à 12 h 25, le requérant a envoyé un courriel au service « Sélection/Recrutement » de la direction des ressources humaines de la direction générale (DG) « Personnel et administration » (ci-après le « service 'Sélection/Recrutement' ») du Conseil, à partir de son adresse IP (« Internet Protocol ») à la Commission. Ce courriel, rédigé en anglais, dont la rubrique « Objet » mentionnait « Coordonnées de M. [A] », était libellé comme suit :

« Chers [c]ollègues,

Nous sommes à la recherche des coordonnées de M. [A], qui a récemment réussi un concours de [chef d'unité] organisé par le [s]ecrétariat [g]énéral du Conseil pour l'unité [BB] afin de l'inviter à une conférence[. P]ourriez-vous, s'il vous plaît, nous envoyer ses coordonnées ?

Merci d'avance pour votre coopération.

[…] »

19 Le courriel était signé par le requérant, à savoir qu'il mentionnait son prénom et son patronyme suivis de la mention de ses fonctions d'administrateur principal d'une direction générale de la Commission et comprenait son adresse administrative, son numéro de téléphone et son adresse électronique professionnelle. Un agent du service « Sélection/Recrutement » du Conseil a répondu au requérant le même jour et lui a fourni l'adresse électronique privée de M. A.

20 Le même 5 mars 2010, à 14 h 36, le requérant a envoyé, à partir de son adresse IP à la Commission et à l'adresse électronique privée de M. A qui venait de lui être communiquée, un courriel, rédigé en langue anglaise, mentionnant, à la rubrique « Objet », « Invitation à de futures conférences », et dont le libellé était le suivant :

« Cher [c]ollègue,

Nous sommes informés de ce que vous allez prendre vos fonctions comme [chef d'unité] suite au concours organisé par le [s]ecrétariat [g]énéral du Conseil pour l'unité [BB]. Nous aimerions vous inviter à de futures conférences. Pourriez-vous, s'il vous plaît, nous envoyer votre curriculum vitæ à jour ?

Merci d'avance pour votre coopération.

[…] »

21 Le courriel était signé par le requérant, à savoir qu'il mentionnait son prénom et son patronyme, suivis de la mention de ses fonctions d'administrateur principal.

22 Le courriel en réponse de M. A, envoyé le même 5 mars 2010 à partir de l'adresse électronique privée communiquée par l'agent du service « Sélection/Recrutement » du Conseil et qu'avait utilisée le requérant, avait la teneur suivante :

« Cher [Monsieur],

Je vous remercie pour votre courriel. Je [vous] rappelle que je n'ai pas encore été nommé sur le poste de [c]hef d'[u]nité. Cependant, en supposant qu'il ne s'agit que d'une question de temps, oui, cela m'intéresse d'être invité à des conférences. Puis-je vous demander dans quel but vous avez l'intention d'utiliser mon [curriculum vitæ] et aussi si je devrais le présenter dans un format particulier ?

[…] »

23 Le requérant a répondu à M. A par la même voie, toujours à partir de son adresse IP à la Commission et avec l'indication de ses fonctions d'administrateur principal, le lundi 8 mars 2010. Le libellé de ce courriel était le suivant :

« Cher futur collègue,

Je vous remercie pour votre réponse rapide. En fait, à la Commission […], les postes de [chef d'unité] sont des postes de gestion et vous serez invité à des conférences dans le futur en tant que conférencier ou en tant que participant, en fonction du contenu de votre [curriculum vitæ]. Afin de nous permettre de vous inviter, pourriez-vous, s'il vous plaît, nous transmettre votre [curriculum vitæ] actualisé (il n'y a pas de format particulier prévu) ?

Merci d'avance pour votre coopération.

[…] »

24 Le 10 mars 2010, M. A a adressé au requérant, à partir de son adresse électronique privée, un courriel dans lequel il indiquait :

« […]

Veuillez trouver ci-joint mon [curriculum vitæ]. Il n'est pas destiné à être publié à l'extérieur et il ne peut être utilisé pour aucune finalité autre que celle pour laquelle vous l'avez demandé, à savoir exclusivement pour l'usage interne des institutions de l'[Union européenne] dans le but de leur permettre de m'inviter à des conférences.

[…] »

25 Le 11 mars 2010, un nouvel échange de courriels a eu lieu entre le requérant et M. A. Le requérant, à partir de son adresse IP à la Commission, avec mention, pour la signature, de ses prénom et nom suivis de l'indication de ses fonctions d'administrateur principal, a écrit à M. A ce qui suit :

« […]

Merci de nous avoir envoyé votre [curriculum vitæ]. Je me permets de vous signaler que, dans le cadre des conférences organisées dans le contexte des institutions de l'[Union européenne], il est habituel de publier le [curriculum vitæ] des orateurs concernés. Bien entendu, pour éviter tout problème de

cohérence, les données que vous indiquez dans votre [curriculum vitæ] devraient toujours coïncider avec [celles] que vous avez fournies dans le passé ainsi qu'avec [celles] que vous transmettrez dans le futur. Le moment venu, vous recevrez éventuellement les invitations.

[…] »

26 M. A a répondu au courriel du requérant mentionné au point précédent dans les termes suivants :

« […]

Merci. Je suis convaincu que mon [curriculum vitæ] est cohérent, etc. Cependant, le [curriculum vitæ] que je vous ai transmis n'est pas destiné à être publié, car il est rédigé aux seules fins d'évaluation par d'éventuels employeurs. Si vous le souhaitez, je vous fournirai un [curriculum vitæ] pour publication en rapport avec des conférences, mais uniquement après que j'aurai été engagé par la Commission […]. Par conséquent, je vous fais confiance pour respecter les conditions d'utilisation que j'ai indiquées explicitement dans mon courriel du 10 mars 2010.

J'espère que vous comprendrez également que ma position n'est pas déraisonnable, compte tenu de ce que, à ce jour, je ne fais pas partie du personnel des institutions de l'[Union européenne].

[…] »

27 Le requérant conteste avoir reçu le courriel de M. A mentionné au point précédent et que la Commission a produit en annexe au mémoire en défense.

28 Le 16 juin 2011, M. A, qui avait entre-temps été nommé chef de l'unité BB à la Commission, a envoyé un courriel à l'Office d'investigation et de discipline de la Commission (IDOC) dans lequel il décrit un entretien qu'il a eu la veille avec un des membres de son unité, M[me] E. Au cours de cet entretien, cette dernière se serait plainte du fait que le requérant, avec qui elle avait entretenu une relation personnelle dans le passé, serait entré à son domicile sans sa permission, le 11 juin 2011, et l'aurait ensuite empêchée d'en sortir. Ces faits auraient été portés à la connaissance de la police.

29 Dans son courriel à l'IDOC du 16 juin 2011, M. A indique que, en entendant le nom du requérant, il s'est souvenu des courriels échangés avec celui-ci en mars 2010 et qu'il a alors communiqué cette information à M[me] E. Celle-ci, qui, en mars 2010, occupait le poste de M. A en tant que chef de l'unité BB faisant fonction, lui aurait déclaré avoir eu connaissance des données de son curriculum vitæ avant qu'il n'arrive à la Commission, car le requérant le lui avait transmis. En annexe à son courriel à l'IDOC, M. A a joint le courriel, mentionné aux points 18 et 19 du présent arrêt, envoyé au requérant par un membre du service « Sélection/Recrutement » du Conseil le 5 mars 2010 à 14 h 20, ainsi que l'échange de courriels repris aux points 20 à 26 du présent arrêt.

30 Dans son courriel à l'IDOC du 16 juin 2011, M. A a fait part, en outre, de ses griefs envers le requérant et, en premier lieu, de ce qu'il avait obtenu de la part du Conseil, sous de faux prétextes, son adresse électronique privée. À son avis, si le requérant avait été autorisé à disposer de cette information, il aurait dû l'obtenir de la Commission elle-même. En deuxième lieu, le requérant aurait manqué aux règles en matière d'éthique et de professionnalisme et aurait agi de manière illégale en utilisant son adresse IP à la Commission et en se présentant comme administrateur principal dans cette institution afin d'obtenir des informations personnelles le concernant, informations dont il se serait servi à des fins étrangères aux intérêts de la Commission. Troisièmement, le requérant n'aurait pas respecté la condition à laquelle M. A avait soumis l'envoi de son curriculum vitæ et, contrairement à ses souhaits quant à la diffusion autorisée, il l'aurait transmis à M[me] E.

31 Le 24 novembre 2011, le directeur général de la DG « Ressources humaines et sécurité » a envoyé une note au directeur de l'IDOC pour l'informer de sa décision, en accord avec le secrétaire général de la Commission, d'ouvrir une enquête administrative et de charger l'IDOC d'y procéder. Cette enquête administrative visait à déterminer, d'une part, si le requérant, alors fonctionnaire de grade AD 12, avait eu un comportement contraire à la dignité de sa fonction en agressant physiquement M^me^ E à son domicile en juin 2011 (ci-après le « premier volet du mandat d'enquête ») et, d'autre part, s'il avait enfreint les règles relatives à la protection des données personnelles en se procurant, de façon mensongère, le curriculum vitæ de M. A en vue d'en faire un usage autre que celui auquel il prétendait le destiner (ci-après le « second volet du mandat d'enquête »).

32 Le 6 décembre 2011, l'IDOC a adressé une note au requérant l'informant de la décision susmentionnée d'ouverture d'une enquête administrative et du mandat donné à l'IDOC pour conduire ladite enquête. Par cette note, le requérant a également a été informé de l'objet de l'enquête administrative, du nom des personnes qui allaient l'auditionner dans le cadre de l'enquête administrative, de la date à laquelle son audition était prévue, à savoir le 18 janvier 2012 à 10 h 30, et de ce que l'audition se déroulerait en anglais. Une copie du chapitre 10 du manuel de l'IDOC intitulé « Le dossier disciplinaire et la protection des données personnelles » était annexée à la note.

33 Il ressort du procès-verbal de l'audition du requérant par l'IDOC que l'audition a débuté en anglais et que, bien que la plupart des questions lui aient été posées dans cette langue, à partir de sa réponse à la deuxième question, posée en anglais, le requérant s'est exprimé en français. Il ressort des déclarations du requérant qu'il est membre d'une association depuis 2006, qu'il a rencontré M^me^ E dans le cadre des activités de cette association en 2008 et qu'ils ont eu une relation personnelle. À l'époque à laquelle il avait demandé à M. A de lui communiquer son curriculum vitæ, M^me^ E était le chef de l'unité BB faisant fonction, poste auquel M. A allait être nommé. M^me^ E voulait se renseigner sur son futur supérieur hiérarchique et, n'ayant pas réussi à se procurer son curriculum vitæ au sein de la Commission, elle aurait donné le nom et l'adresse électronique privée de M. A au requérant, lequel aurait agi dans le but de lui rendre service, sans savoir que ses agissements pouvaient porter atteinte aux règles relatives à la protection des données personnelles.

34 Il ressort également du procès-verbal de l'audition du requérant par l'IDOC que le requérant a déclaré ne pas se souvenir d'avoir contacté, en mars 2010, le service « Sélection/Recrutement » du Conseil afin d'obtenir l'adresse électronique privée de M. A, que la prise de contact avec M. A s'était produite dans un cadre privé et qu'il avait utilisé une formule standard qu'il employait d'habitude pour les intervenants des conférences qu'il organisait, ce qui, à son avis, « n'était pas cohérent avec les finalités de [M^me^ E] à l'époque ». Dans ce contexte, le requérant a déclaré que le « [curriculum vitæ de M. A] n'avait pas servi dans le cadre de la réclamation de [M^me^ E] contre la décision du jury de ne pas donner suite à sa demande de participation au poste de [chef d'unité] ».

35 Le requérant a été à nouveau entendu dans le cadre de l'enquête administrative, le 6 juin 2012, dans le but de compléter les déclarations faites lors de l'audition précédente.

36 Le 7 août 2012, l'IDOC a transmis au requérant une note à son attention, mentionnant, à la rubrique « Objet », « [Références de l'enquête administrative –] Communication des faits vous concernant dans le projet de rapport d'enquête [dont les références figurent en objet] », avec, en annexe, une « note sur les faits » divisée en deux parties (ci-après la « note sur les faits »). Il était indiqué dans la première partie que la plainte pour harcèlement de M^me^ E à l'égard du requérant, objet du premier volet du mandat d'enquête, avait été classée sans suite, le comportement de ce dernier ne pouvant pas être considéré comme contraire à l'article 12 du statut. La seconde partie reprenait les faits objet du second volet du mandat d'enquête concernant le requérant, établis par l'enquête administrative, afin de permettre à ce dernier de présenter ses observations avant la finalisation du rapport d'enquête et sa transmission à l'AIPN. Le délai dans lequel le requérant pouvait transmettre ses observations avait été fixé au 10 septembre 2012.

37 Dans la note sur les faits, les circonstances dans lesquelles le requérant avait obtenu le curriculum vitæ de M. A et l'utilisation qu'il en avait faite étaient décrites comme suit :

« [Le requérant] s'est procuré le [curriculum vitæ] de M. [A] en lui faisant croire que celui-ci serait utilisé pour l'organisation de conférences auxquelles participe le personnel d'encadrement de la Commission. L'envoi des messages depuis son adresse IP à la Commission et la mention de ses fonctions d'administrateur principal ont contribué à renforcer l'impression qu'il s'agissait d'une demande officielle des services de la Commission à des fins professionnelles.

M. [A] a clairement limité l'utilisation de son [curriculum vitæ] à des fins professionnelles en précisant qu'il ne pouvait servir qu'aux institutions européennes dans le but de l'inviter à participer à des conférences. Il était dès lors clair pour [le requérant] qu'il ne pouvait s'en servir ni le conserver à des fins privées, que ce soit dans le but d'aider M[me] [E] comme il l'a prétendu lors de son audition de janvier 2012 ou de faciliter l'organisation de conférences organisées par des associations privées dans des domaines culturels ou autres comme il l'a indiqué en juin 2012.

[Le requérant] a obtenu, détenu et utilisé le [curriculum vitæ] de M. [A] dans un but différent de celui pour lequel il l'avait reçu. Il en a également donné une copie à M[me] [E] sans l'accord de M. [A], ce qui constitue un transfert illicite de données personnelles au sens du règlement n° 45/2001.

[Le requérant] a enfreint les règles relatives à la protection des données personnelles. Lors de son audition en janvier 2012, [le requérant] a déclaré avoir une 'connaissance générale' de ces règles. Sans connaître dans le détail des règles qui sont toutefois régulièrement rappelées à l'attention des fonctionnaires et qui sont accessibles sur le site [Internet] Europa de la Commission, [le requérant] ne pouvait ignorer qu'il faisait un usage abusif des informations qu'il avait obtenues de M. [A] à des fins strictement professionnelles.

La façon dont [le requérant] a obtenu le [curriculum vitæ] de M. [A] était délibérément trompeuse. Un tel comportement à l'égard d'un futur collègue, ignorant des pratiques de la Commission, porte atteinte à l'image et à la réputation de l'institution et de son personnel au sens de l'article 12 du statut. »

38 Le requérant a présenté ses observations sur les faits le concernant, tels que relatés dans la note sur les faits, le 8 août 2012. Après avoir émis, à titre liminaire, l'avis que « les deux affaires en question rel[evaient] de la sphère de la vie privée et, dès lors, qu'il n'appart[enait] pas à l'administration d'intervenir », il a soulevé plusieurs arguments, notamment : que le curriculum vitæ de M. A ne constituait pas un document officiel de la Commission rentrant dans le champ d'application du règlement n° 45/2001, mais qu'il s'agissait d'un document envoyé à titre privé dans le cadre d'un échange de correspondance privée entre deux futurs collègues, voire deux collègues ; que ces courriels avaient été envoyés à l'adresse privée de M. A pour l'inviter à titre privé à des conférences organisées par des réseaux culturels ; qu'il n'avait jamais signé les courriels avec sa signature officielle de la Commission ; que M. A avait marqué son accord pour participer à des conférences et qu'il lui avait envoyé son curriculum vitæ ; que, depuis son entrée en fonctions à la Commission, M. A ne l'avait jamais contacté pour avoir des renseignements ou des explications sur les courriels de mars 2010 ; que le fait d'avoir envoyé ces courriels depuis son adresse IP à la Commission avec mention de ses fonctions d'administrateur principal ne portait pas à croire qu'il s'agissait d'une demande officielle des services de la Commission à des fins professionnelles ; que le curriculum vitæ de M. A n'avait pas été utilisé à des fins privées, le requérant l'ayant effacé à peine reçu du fait qu'il manquait d'utilité ; que, le curriculum vitæ de M. A n'étant pas un document à traiter au titre du règlement n° 45/2011, le requérant n'avait pas pu faire un usage abusif des données qu'il avait obtenues à des fins privées ; que le fait d'avoir reçu le curriculum vitæ à des fins strictement privées excluait qu'il l'ait obtenu de façon trompeuse et, également, que M. A avait attendu près de deux ans avant de porter plainte. Dans sa note d'observations, le requérant a, en outre, demandé à « l'administration de [lui] communiquer les

éléments nécessaires ou de lui laisser accéder aux dossiers administratifs afin de lui permettre [de] comprendre la [note de l'IDOC] contestée du 7 août 2012 et en particulier les intentions et la motivation de la plainte de M. [A] ».

39 Dans le rapport soumis à l'AIPN à la fin de l'enquête administrative (ci-après le « rapport d'enquête »), le 3 octobre 2012, l'IDOC a conclu que le comportement du requérant sur lequel portait le second volet du mandat d'enquête constituait une violation des règles relatives à la protection des données personnelles définies par le règlement nº 45/2001 et un comportement contraire à la dignité de la fonction au sens de l'article 12 du statut et a recommandé l'audition du requérant au titre de l'article 3 de l'annexe IX du statut.

40 Au vu du rapport d'enquête, le directeur général de la DG « Ressources humaines et sécurité » a envoyé, le 9 octobre 2012, une note au directeur de l'IDOC par laquelle elle lui communiquait sa décision d'auditionner le requérant au titre de l'article 3 de l'annexe IX du statut, le but de cette audition étant de lui permettre d'apprécier les charges qui pourraient être retenues contre lui et de décider si elles justifiaient l'ouverture d'une procédure disciplinaire.

41 Par décision du 22 octobre 2012, l'AIPN a notamment refusé de faire droit à la demande du requérant, reprise au point 38 in fine du présent arrêt. Ce refus est fondé tant sur la circonstance que les droits du requérant auraient été limités, lorsqu'il a introduit ladite demande, à la connaissance de l'ouverture de l'enquête administrative et des faits le concernant, afin de lui permettre de présenter ses observations, que sur le fait que la procédure d'enquête administrative n'avait pas encore été clôturée.

42 Par une note du 25 janvier 2013, l'IDOC a informé le requérant de la décision de l'AIPN d'ouvrir la procédure prévue à l'article 3 de l'annexe IX du statut. Il ressort de cette note qu'étaient joints en annexe le rapport d'enquête ainsi qu'un courriel adressé par le requérant à M. A le 23 janvier 2012 et un courriel du Conseil, du 28 février 2012, qui reprenait l'échange de courriels entre le requérant et le service « Sélection/Recrutement » du Conseil du 5 mars 2010. Par la même note, le requérant a été convoqué à une audition le 8 février 2013.

43 Lors de son audition au titre de l'article 3 de l'annexe IX du statut, également diligentée par l'IDOC pour le compte de l'AIPN, le requérant a confirmé avoir demandé le curriculum vitæ de M. A tant dans le but de l'inviter à des conférences que dans celui d'aider M^me^ E ; avoir fait ladite demande à titre privé ; avoir montré le curriculum vitæ à M^me^ E et l'avoir détruit par la suite ; avoir utilisé son adresse IP à la Commission pour une communication privée, ce qui ne serait pas interdit ; avoir indiqué ses fonctions d'administrateur principal afin que le destinataire sache qu'ils étaient des collègues de grades élevés ; ne pas avoir utilisé le logo de la Commission dont il se servait pour des messages officiels et professionnels ; ne pas avoir donné d'indication amenant à penser qu'il agissait en tant qu'organisateur officiel de conférences ; ne pas avoir reçu le courriel de M. A du 11 mars 2010 (mentionné au point 26 du présent arrêt) ; avoir utilisé le logo de la Commission dans son courriel du 5 mars 2010, envoyé au service « Sélection/Recrutement » du Conseil, du fait que la communication était interinstitutionnelle et que, en tout état de cause, l'adresse courriel privée de M. A était accessible au public ; ne pas avoir compris le message de M. A relatif à l'utilisation limitée et conditionnelle de son curriculum vitæ, faute pour lui d'avoir indiqué qu'il était confidentiel ; avoir été incité dans son initiative par M^me^ E, laquelle avait un intérêt à connaître le profil de M. A, et avoir demandé son curriculum vitæ en dehors du champ d'application du règlement nº 45/2001. À la fin de sa déposition, le requérant a déclaré regretter ses agissements, dans l'hypothèse où il aurait mal agi, et ne pas avoir eu de mauvaise intention.

44 Par note du 26 avril 2013, notifiée au requérant le 30 avril suivant, le directeur général de la DG « Ressources humaines et sécurité » a informé le requérant que, au vu du procès-verbal de l'audition du 8 février 2013 au titre de l'article 3 de l'annexe IX du statut, en sa qualité d'AIPN, elle avait décidé l'ouverture d'une procédure disciplinaire sans consultation du conseil de discipline pour des faits relatifs à un traitement abusif de données personnelles et un comportement ayant des répercussions

négatives sur la réputation de l'institution et de son personnel contraire à l'article 12 du statut. Un rapport disciplinaire (« disciplinary report ») préparé par l'IDOC, daté du 25 avril 2013 et comprenant onze annexes (ci-après le « rapport disciplinaire »), était joint à cette note aux fins de préparer la procédure disciplinaire. Par la même note, le requérant a été informé qu'il allait être auditionné conformément à l'article 11 de l'annexe IX du statut.

45 L'audition du requérant par l'AIPN, au titre de l'article 11 de l'annexe IX du statut, a eu lieu le 18 juin 2013. Le procès-verbal de cette audition n'a pas été versé au dossier.

46 Par décision du 6 septembre 2013, l'AIPN a infligé au requérant la sanction de blâme prévue à l'article 9, paragraphe 1, sous b), de l'annexe IX du statut. Dans cette décision, les faits considérés par l'AIPN comme établis à l'égard du requérant sont : la demande adressée au service « Sélection/Recrutement » du Conseil le 5 mars 2010, le courriel envoyé le même jour à M. A à partir de son adresse IP à la Commission dans les termes repris au point 20 du présent arrêt et la communication à M[me] E du curriculum vitæ de M. A, alors que ce dernier avait expressément limité l'utilisation qui pouvait en être faite. Les éléments et les circonstances aggravantes et atténuantes dont l'AIPN a tenu compte pour la détermination de la gravité de la sanction sont indiqués au point 13 de la décision.

47 La décision du 6 septembre 2013 a été contestée par le requérant par une réclamation du 20 novembre 2013. La réclamation a été rejetée par décision de l'AIPN du 19 mars 2014, dont le requérant a reçu notification le lendemain (ci-après la « décision de rejet de la réclamation »).

Conclusions des parties

48 Le requérant conclut à ce qu'il plaise au Tribunal :

— annuler la décision de rejet de la réclamation et, pour autant que de besoin, la décision du 6 septembre 2013 ;

— condamner la Commission à lui verser une somme évaluée ex æquo et bono à 5 000 euros à titre de dommages et intérêts ;

— condamner la Commission aux dépens.

49 La Commission conclut à ce qu'il plaise au Tribunal :

— rejeter le recours ;

— condamner le requérant aux dépens.

En droit

Sur les conclusions en annulation de la décision de rejet de la réclamation

50 Selon une jurisprudence constante, des conclusions en annulation formellement dirigées contre la décision de rejet d'une réclamation ont, dans le cas où cette décision est dépourvue de contenu autonome, pour effet de saisir le Tribunal de l'acte contre lequel la réclamation a été présentée (voir, en ce sens, arrêt du 17 janvier 1989, Vainker/Parlement, 293/87, EU:C:1989:8, point 8). En l'espèce, la décision du 19 mars 2014 par laquelle l'AIPN a rejeté la réclamation du requérant confirme la décision de l'AIPN du 6 septembre 2013 de lui infliger la sanction disciplinaire de blâme, en ajoutant des arguments venant au support de celle-ci.

51 En pareille hypothèse, c'est bien la légalité de l'acte initial faisant grief qui doit être examinée en prenant en considération la motivation figurant dans la décision de rejet de la réclamation, cette motivation étant censée coïncider avec cet acte (voir, en ce sens, arrêt du 9 décembre 2009, Commission/Birkhoff, T-377/08 P, EU:T:2009:485, points 58 et 59). Par conséquent, les conclusions en annulation dirigées contre la décision de rejet de la réclamation sont dépourvues de contenu autonome et le recours doit être regardé comme formellement dirigé contre la décision initiale, du 6 septembre 2013, infligeant la sanction de blâme, telle que précisée par la décision de rejet de la réclamation (ci-après la « décision attaquée ») (voir, en ce sens, arrêts du 10 juin 2004, Eveillard/Commission, T-258/01, EU:T:2004:177, points 29 à 32, et du 18 avril 2012, Buxton/Parlement, F-50/11, EU:F:2012:51, point 21).

52 Il s'ensuit qu'il n'y a pas lieu d'examiner séparément les conclusions en annulation de la décision de rejet de la réclamation.

Sur les conclusions en annulation de la décision d'ouvrir une procédure disciplinaire sans consultation du conseil de discipline ainsi que du rapport disciplinaire

53 Le Tribunal constate que, dans le cadre du premier moyen soulevé à l'appui de ses conclusions en annulation de la décision attaquée, le requérant demande également l'annulation de la décision d'ouvrir une procédure disciplinaire sans consultation du conseil de discipline ainsi que celle du rapport disciplinaire.

54 À cet égard, et sans qu'il soit nécessaire d'examiner si ces deux derniers actes constituent des actes faisant grief au requérant, il suffit de constater qu'il ne ressort pas du dossier que le requérant a suivi la procédure établie aux articles 90 et 91 du statut pour pouvoir contester utilement ces actes. Par conséquent, ces chefs de conclusions doivent être déclarés irrecevables.

Sur les conclusions en annulation de la décision attaquée

55 Le requérant soulève cinq moyens d'annulation, chacun divisé en plusieurs branches, que le Tribunal examinera successivement selon l'ordre de la requête.

Sur le premier moyen, divisé en quatre branches, tirées, la première, de la violation de l'article 41 de la Charte ; la deuxième, de la violation du principe du respect des droits de la défense ; la troisième, de la violation de l'article 6 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales et, la quatrième, du principe de bonne administration

– Arguments des parties

56 Au soutien du premier moyen, le requérant fait valoir que, alors que plusieurs documents relatifs à la procédure d'enquête administrative émanant de l'AIPN ont été rédigés en français, langue dans laquelle il s'est exprimé tant lors de ses auditions, même lorsque des questions lui ont été posées en anglais, que par écrit, ce qui indiquerait qu'il avait choisi le français comme langue de procédure, l'AIPN a décidé de mener la procédure disciplinaire en anglais. Même s'il parle l'anglais, le requérant considère être mieux à même de nuancer ses propos en français plutôt qu'en anglais.

57 La Commission conclut au rejet du premier moyen.

– Appréciation du Tribunal

58 L'argumentation soulevée par le requérant ne saurait prospérer. En effet, en premier lieu, s'il est vrai que notamment la note de l'IDOC du 6 décembre 2011, dont le contenu est repris au point 32 du présent arrêt, par laquelle le requérant a été informé de la décision d'ouverture de l'enquête administrative ; la note du 26 avril 2013 du directeur général de la DG « Ressources humaines et sécurité », dont le contenu est repris au point 44 du présent arrêt, par laquelle le requérant a été informé de la décision d'ouverture d'une procédure disciplinaire ; le rapport disciplinaire préparé par l'IDOC, mentionné au point 44 du présent arrêt, et la décision attaquée, reprise au point 46 du présent arrêt, ont été rédigés en anglais, il n'en demeure pas moins qu'il s'agit dans tous les cas de documents qui ont l'administration pour auteur et que, tel qu'il ressort du dossier, le requérant n'a pas été contraint de s'exprimer dans cette langue ni oralement ni par écrit. En effet, lorsqu'il a été entendu par les enquêteurs de l'IDOC le 18 janvier 2012, il a pu répondre en français aux questions qui lui ont été posées en anglais ; lorsqu'il a été entendu par les enquêteurs de l'IDOC le 6 juin 2012, les questions lui ont été posées en français et, s'il est vrai qu'il a répondu en anglais aux questions qui lui ont été posées dans cette langue au cours de l'audition du 8 février 2013, il demeure qu'il n'a pas indiqué avoir besoin de s'exprimer en français. Le requérant ne saurait donc valablement soutenir avoir été empêché d'apporter les nuances qu'il estimait nécessaires à ses déclarations orales lorsqu'il a exercé ses droits de la défense en présentant ses observations, car il a pu, à chaque fois, s'exprimer dans la langue de sa préférence. Il convient d'ajouter, en outre, que le requérant a été informé, dès réception de la note du 6 décembre 2011 par laquelle il a été invité à une audition le 18 janvier 2012, du fait que cette audition allait se dérouler en anglais, ce à quoi il ne s'est pas opposé, alors qu'il a disposé de plus d'un mois pour demander, s'il l'avait considéré nécessaire, à être entendu dans une autre langue.

59 En tout état de cause, le Tribunal relève qu'il ressort de plusieurs documents versés au dossier que le requérant a un niveau élevé de connaissance de la langue anglaise. Ainsi, selon le système informatique de gestion du personnel appelé « SysPer 2 » de la Commission, la troisième langue du requérant est l'anglais, après l'allemand et sa langue maternelle ; dans son rapport d'évaluation pour l'année 2013, le requérant a écrit, à la page 3, sous la rubrique « Auto-évaluation » du point 4, « Utilisation des langues », qu'il « dispose de compétences linguistiques dans cinq langues [de l'Union] étant donné [s]es connaissances approfondies de [l'allemand, de l'anglais, du français, du portugais et du polonais et qu'il] utilise quotidiennement les langues [allemande], [anglaise] et [française] dans [s]on travail […] », et, parmi les exigences du poste occupé par le requérant, telles que reprises dans le formulaire de description de poste, figurent des connaissances aussi approfondies d'allemand et de français que d'anglais.

60 En deuxième lieu, il n'y a pas eu non plus violation de l'article 41, paragraphe 4, de la Charte, qui dispose que toute personne peut s'adresser aux institutions de l'Union dans une des langues des traités et doit recevoir une réponse dans la même langue.

61 Il y a lieu de rappeler, à cet égard, qu'il ressort de la jurisprudence que, s'il incombe aux institutions, en vertu du devoir de sollicitude, de s'adresser à un fonctionnaire dans une langue que celui-ci maîtrise de façon approfondie, il ne peut être déduit de l'article 41, paragraphe 4, de la Charte que toute décision adressée par une institution de l'Union à un de ses fonctionnaires devrait être rédigée dans la langue du choix de ce dernier. En effet, cette disposition ne s'applique aux relations entre les institutions et leurs agents que lorsque ceux-ci adressent une correspondance aux institutions en leur seule qualité de citoyens de l'Union et non en leur qualité de fonctionnaire ou d'agent (ordonnances du 7 octobre 2009, Marcuccio/Commission, F-122/07, EU:F:2009:134, points 63 et 65, et Marcuccio/Commission, F-3/08, EU:F:2009:135, points 31 et 33). Par suite, le requérant ne saurait se prévaloir utilement dans le cadre du présent recours de la disposition précitée de la Charte.

62 En troisième lieu, il n'y a pas eu non plus violation de l'article 6, paragraphe 3, sous a), de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, qui prévoit, notamment, que tout accusé a le droit d'être informé, dans une langue

qu'il comprend, de la nature et de la cause de l'accusation portée contre lui. En effet, il ressort d'une jurisprudence établie du juge de l'Union que la disposition précitée n'est applicable qu'en matière pénale (arrêt du 8 mai 2008, Weiss und Partner, C-14/07, EU:C:2008:264, point 57).

63 Il s'ensuit que le premier moyen doit être rejeté comme non fondé.

Sur le deuxième moyen, divisé en plusieurs branches, tirées, la première, de la violation des articles 2 et 3 de l'annexe IX du statut ; la deuxième, de la violation de l'article 41 de la Charte, du principe du respect des droits de la défense et de l'article 6 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales ; la troisième, de la violation du principe de bonne administration ; la quatrième, de la violation du devoir de motivation ; la cinquième, de la violation du principe de sécurité juridique et, la sixième, du détournement de pouvoir

64 Le Tribunal constate que, dans ses écrits, le requérant ne développe son argumentation qu'à l'égard des première et deuxième branches du deuxième moyen, tirées respectivement de la violation des articles 2 et 3 de l'annexe IX du statut et de la violation des droits de la défense dans le cadre de l'enquête administrative et au cours de la procédure disciplinaire. Les troisième, quatrième, cinquième et sixième branches ne sont qu'énoncées et ne sont aucunement étayées par une quelconque argumentation, contrairement à la règle prévue à l'article 35, paragraphe 1, sous e), du règlement de procédure en vigueur au moment de l'introduction du présent recours [devenu, après modification, l'article 50, paragraphe 1, sous e), du règlement de procédure]. Il y a donc lieu de les déclarer irrecevables.

– Arguments des parties

65 À l'appui des deux premières branches du deuxième moyen, le requérant fait valoir que l'AIPN a agi en violation des articles 2 et 3 de l'annexe IX du statut ainsi que de ses droits de la défense, car ni dans le cadre de l'enquête administrative menée par l'IDOC ni pendant la procédure disciplinaire il n'a eu communication de toutes les pièces du dossier. Ainsi, la copie du procès-verbal de l'audition de M^me^ E, avec laquelle le requérant a un conflit d'ordre privé, lui aurait été refusée ; plusieurs passages du rapport d'enquête auraient été noircis, voire supprimés, et il en irait de même en ce qui concerne la transcription de l'audition de M. A, alors que ces deux personnes, M^me^ E et M. A, auraient été à l'origine de la décision d'ouverture de l'enquête administrative et de celle d'ouvrir la procédure disciplinaire. Le requérant ajoute, à cet égard, que le courriel que M. A a transmis à l'IDOC le 16 juin 2011 n'a été porté à sa connaissance que le 30 avril 2013, lorsqu'il lui a été communiqué en annexe au rapport disciplinaire, transmis avec la note du 26 avril 2013 du directeur général de la DG « Ressources humaines et sécurité », relative à l'ouverture d'une procédure disciplinaire.

66 La Commission conclut au rejet du deuxième moyen.

– Appréciation du Tribunal

67 En ce qui concerne le grief relatif à la violation de l'article 2 de l'annexe IX du statut et des droits de la défense du requérant dans le cadre de l'enquête administrative, il résulte du libellé de cette disposition, qui renvoie à l'article 1^er^ de la même annexe, que, au cours d'une enquête administrative, l'intéressé est tenu informé de son implication pour autant que cette information ne nuise pas au bon déroulement de ladite enquête.

68 En l'espèce, il ressort du dossier, en premier lieu, que le requérant, comme cela a d'ailleurs été exposé ci-dessus (voir point 32 du présent arrêt), a été informé de l'ouverture de l'enquête administrative par la note de l'IDOC du 6 décembre 2011 et, au plus tard le jour de sa première audition, le 18 janvier 2012, qu'il a été informé des faits qui lui étaient reprochés, conformément à l'article 1^er^, premier

alinéa, de l'annexe IX du statut. Il ressort, en deuxième lieu, du dossier que les faits que les enquêteurs de l'IDOC ont estimé établis concernant le requérant étaient ceux qui faisaient l'objet du second volet du mandat d'enquête, à savoir l'obtention du curriculum vitæ de M. A et l'usage que le requérant en a fait, que ces faits ont été communiqués à ce dernier le 7 août 2012 et qu'il a présenté des observations le lendemain. Les observations du requérant ont été jointes au rapport d'enquête envoyé par l'IDOC à l'AIPN.

69 En troisième lieu, c'est bien le rapport d'enquête, expurgé de toute mention du premier volet du mandat d'enquête, qui a été communiqué au requérant le 25 janvier 2013, ce qui va au-delà de l'obligation imposée à l'AIPN par l'article 2, paragraphe 2, de l'annexe IX du statut, lequel ne prévoit que la communication à l'intéressé des conclusions du rapport de l'enquête administrative.

70 En ce qui concerne, en quatrième lieu, le grief du requérant relatif à la violation par l'AIPN de l'article 2 de l'annexe IX du statut du fait de ne pas lui avoir transmis le procès-verbal de l'audition de M^me^ E, le Tribunal constate que c'est uniquement à la fin de l'enquête administrative que l'intéressé peut demander les documents en rapport direct avec les allégations formulées à son égard et qu'il ressort du dossier que, lorsque le requérant a introduit une telle demande, à savoir le 8 août 2012, l'enquête administrative n'avait pas encore été clôturée.

71 Il s'ensuit que, en l'espèce, il n'y a pas eu violation par l'AIPN de l'article 2 de l'annexe IX du statut ni des droits de la défense du requérant dans le cadre de l'enquête administrative.

72 Pour ce qui est, ensuite, de la violation par l'AIPN de l'article 3 de l'annexe IX du statut, lequel prévoit la communication au fonctionnaire concerné de toutes les pièces du dossier avant de décider de l'ouverture d'une procédure disciplinaire, et de la violation des droits de la défense du requérant au cours de la procédure disciplinaire, le requérant se plaint du fait de ne pas avoir eu communication du procès-verbal de l'audition de M^me^ E, d'avoir reçu un rapport d'enquête incomplet ainsi qu'une transcription incomplète de l'audition de M. A et d'avoir reçu le courriel que M. A avait transmis à l'IDOC le 16 juin 2011 seulement le 30 avril 2013, lorsqu'il lui a été communiqué en annexe au rapport disciplinaire, transmis avec la note du 26 avril 2013 du directeur général de la DG « Ressources humaines et sécurité », relative à l'ouverture d'une procédure disciplinaire.

73 En ce qui concerne le premier grief, il est constant que l'AIPN n'a pas transmis au requérant de copie du procès-verbal de l'audition de M^me^ E. Toutefois, s'il est vrai que l'article 3 de l'annexe IX du statut impose à l'AIPN l'obligation de communiquer au fonctionnaire concerné toutes les pièces du dossier préalablement à son audition avant de décider de l'ouverture d'une procédure disciplinaire, il n'en demeure pas moins que, lorsqu'elle donne accès à une personne au dossier qui la concerne, l'administration est également tenue, en vertu de l'article 41, paragraphe 2, sous b), de la Charte, de respecter les intérêts légitimes de la confidentialité.

74 Or, en l'espèce, d'une part, en ce qui concerne le requérant, l'enquête administrative a démontré que le premier volet du mandat d'enquête, à savoir déterminer si le requérant avait eu un comportement contraire à la dignité de sa fonction à l'égard de M^me^ E, a été classé sans suite, faute de preuve de harcèlement au travail, ce qui est indiqué dans la note sur les faits, jointe à la note de l'IDOC du 7 août 2012, dont le requérant a reçu notification le même jour. Au vu de ce que la procédure disciplinaire n'a pas porté sur les comportements que M^me^ E reprochait au requérant, la protection des intérêts légitimes de cette dernière est susceptible de justifier la confidentialité de sa déposition et, partant, la non-communication au requérant du rapport d'audition de M^me^ E établi dans le cadre de l'enquête administrative.

75 D'autre part, le second volet du mandat d'enquête portait sur l'obtention par le requérant du curriculum vitæ de M. A et l'usage qu'il a en fait : il est constant que le requérant n'a pas nié avoir demandé son curriculum vitæ à M. A et l'avoir ensuite communiqué à M^me^ E, mais qu'il a indiqué avoir agi à l'instigation de M^me^ E.

76 Dans la mesure où le rapport d'enquête, tel que communiqué au requérant, a repris, dans les deux derniers tirets de la page 4, les propos tenus par M[me] E, lors de son audition dans le cadre de l'enquête administrative, à l'égard du requérant et que ce dernier a pu réagir et apporter les preuves qu'il considérait comme pertinentes à sa décharge, ce qui ressort du procès-verbal de son audition du 8 février 2013, avant même que l'AIPN adopte la décision d'ouverture d'une procédure disciplinaire, il y a lieu de conclure que le fait pour le requérant de ne pas avoir eu accès au procès-verbal de l'audition de M[me] E n'a pas affecté ses droits de la défense.

77 La même conclusion doit être tirée du fait que l'AIPN a transmis au requérant une version expurgée du rapport d'enquête et une version expurgée du procès-verbal de l'audition de M. A. En effet, il ressort de ces deux documents, tel qu'ils ont été communiqués au requérant, qu'ils contiennent la description circonstanciée des faits qui lui étaient reprochés relatifs à l'obtention du curriculum vitæ de M. A et à l'usage qu'il en a fait, seuls faits sur lesquels se fonde la décision de l'AIPN du 26 avril 2013 d'ouvrir une procédure disciplinaire.

78 Le requérant se plaint, enfin, du fait que le courriel de M. A, envoyé le 16 juin 2011, par lequel ce dernier a porté à la connaissance de l'IDOC les démarches entamées par le requérant afin de se procurer son curriculum vitæ et l'usage qu'il en a fait, ne lui a été communiqué que le 30 avril 2013, en tant qu'annexe au rapport disciplinaire, lequel lui avait été notifié aux fins de préparer la procédure disciplinaire.

79 À cet égard, il convient de constater que, s'il est vrai que le courriel de M. A à l'origine de la décision d'ouverture de l'enquête administrative n'a été communiqué au requérant qu'une fois que la décision d'ouvrir une procédure disciplinaire avait été adoptée, il n'en demeure pas moins que, tel que cela ressort du procès-verbal de l'audition du requérant par l'IDOC du 18 janvier 2012, dès cette date et avant même de commencer l'audition, le requérant a été mis au courant par les enquêteurs des deux volets du mandat d'enquête et des faits qui lui étaient reprochés, faits sur lesquels ont porté les questions qui lui ont été posées. Dans ces conditions, dans la mesure où le requérant a disposé dès le début de la procédure d'enquête administrative des informations qui le concernaient, qui figuraient dans le courriel de M. A, la communication dudit courriel seulement le 30 avril 2013 plutôt qu'avant son audition du 8 février 2013 n'a pas été susceptible de nuire à ses droits de la défense.

80 Par conséquent, il n'y a pas eu violation par l'AIPN de l'article 3 de l'annexe IX du statut ni des droits de la défense du requérant pendant la procédure disciplinaire.

81 Il résulte de ce qui précède que le deuxième moyen doit être rejeté comme étant, en partie, irrecevable et, en partie, dépourvu de fondement.

Sur le troisième moyen, divisé en plusieurs branches, tirées, la première, de la violation de l'article 41 de la Charte ; la deuxième, de la violation du principe de bonne administration ; la troisième, de la violation du devoir de motivation ; la quatrième, de la violation du principe de sécurité juridique ; la cinquième, du détournement de pouvoir et, la sixième, de l'erreur manifeste d'appréciation

82 Le Tribunal constate que, dans ses écrits, le requérant ne développe son argumentation qu'à l'égard de la troisième branche du troisième moyen, tirée d'une violation du devoir de l'AIPN de motiver correctement la décision attaquée. Les deuxième, quatrième, cinquième et sixième branches du moyen sont simplement énoncées et ne sont aucunement étayées par une quelconque argumentation, contrairement à la règle prévue à l'article 35, paragraphe 1, sous e), du règlement de procédure en vigueur lors de l'introduction du recours [devenu, après modification, l'article 50, paragraphe 1, sous e), du règlement de procédure]. Il y a donc lieu de les déclarer irrecevables. Le même sort doit être réservé à la première branche du troisième moyen, tirée de la violation de l'article 41 de la Charte, cet article étant composé de plusieurs points visant à protéger des droits distincts et le requérant n'ayant pas identifié lequel d'entre eux aurait été violé par l'AIPN.

– Arguments des parties

83 À l'appui de la troisième branche du troisième moyen, le requérant soutient que les dispositions de l'article 8 de la Charte ainsi que celles du règlement nº 45/2001, sur lesquelles l'AIPN s'est fondée pour adopter la décision attaquée, s'adressent soit aux institutions et organes de l'Union soit aux autorités nationales lorsqu'elles mettent en œuvre le droit de l'Union et ne trouvent pas à s'appliquer dans le cadre d'un litige concernant deux fonctionnaires de l'Union. Il ajoute que le règlement nº 45/2001 s'applique au traitement de données à caractère personnel par les institutions et organes de l'Union, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit de l'Union. Or, le requérant ne pourrait pas être considéré comme étant un organe de l'Union au sens dudit règlement et n'aurait pas pour mission de récolter ou de traiter des données à caractère personnel. Pour cette raison, la motivation de la décision attaquée ne serait pas adéquate et son fondement légal devrait être écarté. En outre, le requérant fait valoir que les membres du personnel de la Commission sont autorisés à utiliser leur adresse électronique professionnelle à des fins purement privées et qu'il n'a jamais dépassé les limites acceptables de l'utilisation de son adresse électronique professionnelle à des fins privées.

84 La Commission conclut au rejet du troisième moyen.

– Appréciation du Tribunal

85 Il ressort de l'article 3 du règlement nº 45/2001 que ce règlement trouve à s'appliquer au traitement de données à caractère personnel par, notamment, toutes les institutions de l'Union, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit de l'Union. En vertu de l'article 2 dudit règlement, la notion de « données à caractère personnel » s'entend, aux fins dudit règlement, comme toute information concernant une personne physique identifiée ou identifiable. Conformément au considérant 7 du même règlement, les personnes susceptibles d'être protégées sont celles dont les données à caractère personnel sont traitées par les institutions ou organes de l'Union, dans quelque contexte que ce soit. L'article 49 du règlement nº 45/2001 dispose, quant à lui, que tout manquement aux obligations auxquelles un fonctionnaire ou un agent de l'Union est tenu en vertu de ce règlement l'expose à une sanction disciplinaire. La Charte, dont les dispositions s'adressent notamment aux institutions, organes et organismes de l'Union, reconnaît, à l'article 8, le droit de toute personne à la protection des données à caractère personnel la concernant et à ce que ces données soient traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi.

86 En l'espèce, il résulte des faits repris aux points 18 à 25 du présent arrêt, qui n'ont pas été contestés par le requérant, que, à partir de son adresse IP à la Commission et en signant en tant qu'administrateur principal dans une des directions générales de l'institution avec mention de son adresse professionnelle postale, de son numéro de téléphone professionnel et de son adresse IP à la Commission, le requérant s'est procuré auprès du service « Sélection/Recrutement » du Conseil l'adresse électronique privée de M. A en indiquant audit service qu'il en avait besoin pour l'inviter à une conférence ; que, toujours en sa qualité d'administrateur principal et à partir de son adresse IP à la Commission, le requérant s'est servi de l'adresse électronique privée de M. A pour lui demander de lui transmettre un curriculum vitæ à jour, prétendument dans le but de l'inviter à des conférences ; que ce dernier a envoyé au requérant son curriculum vitæ en précisant qu'il ne pouvait être utilisé pour une autre finalité que celle pour laquelle il lui avait été demandé, à savoir dans le but de permettre aux institutions de l'Union de l'inviter à des conférences, et que, le 11 mars 2010, le requérant a accusé réception dudit curriculum vitæ ainsi que des conditions d'utilisation imposées par M. A.

87 Il résulte également de la description des faits reprise aux points 33 et 43 du présent arrêt que, lors de ses auditions dans le cadre de l'enquête administrative, le requérant a déclaré, s'agissant de l'obtention du curriculum vitæ de M. A, avoir agi dans le but de rendre service à M[me] E, laquelle était à l'époque chef de l'unité BB faisant fonction dans l'attente de la nomination de M. A, et avoir ainsi montré le curriculum vitæ de M. A à M[me] E.

88 Il est vrai que, tel que le soutient le requérant, l'article 8 de la Charte ainsi que le règlement n° 45/2001, dispositions sur lesquelles se fonde la décision attaquée et qui reconnaissent aux personnes des droits juridiquement protégés, s'appliquent au traitement de données à caractère personnel par, notamment, les institutions de l'Union dans l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit de l'Union. C'est bien dans ce cadre que l'article 49 du règlement n° 45/2001 prévoit l'application de sanctions disciplinaires aux fonctionnaires et agents en cas de manquement à leurs obligations en vertu dudit règlement, que ce soit intentionnel ou par négligence.

89 Or, en l'espèce, même si le requérant s'est procuré les données personnelles de M. A à des fins strictement privées, il demeure que, pour les obtenir, il a choisi, tant lorsqu'il s'est adressé au service « Sélection/Recrutement » du Conseil que lorsqu'il a écrit à M. A, d'utiliser son adresse IP à la Commission et de signer en tant qu'administrateur principal ; que, tant dans l'un que dans l'autre de ces deux courriels, le requérant a affirmé demander les données personnelles de M. A dans le but de l'inviter à des conférences en tant que futur collègue et que, lorsque M. A lui a envoyé son curriculum vitæ, M. A a limité l'utilisation de ses données au but pour lequel le requérant les lui avait demandées, à savoir être invité à des conférences par les institutions de l'Union.

90 S'étant donc présenté comme « destinataire » des données à caractère personnel au sens du règlement n° 45/2001, tant à l'égard du service « Sélection/Recrutement » du Conseil qu'à l'égard de M. A, aux fins de l'obtention de telles données de ce dernier, le requérant était soumis à la fois à l'article 8 de la Charte et aux dispositions du règlement n° 45/2001, notamment à l'obligation imposée à l'article 4, paragraphe 1, sous b), dudit règlement, en vertu duquel les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.

91 Il y a lieu d'ajouter, à cet égard, que l'argument du requérant selon lequel il n'aurait pas reçu le courriel de M. A, daté du 11 mars 2010 et dont le libellé est repris au point 26 du présent arrêt, est inopérant, M. A ayant déjà indiqué au requérant, dans le courriel qu'il lui avait envoyé le 10 mars 2010, la finalité pour laquelle son curriculum vitæ pouvait être utilisé.

92 Il s'ensuit que, le requérant ayant montré le curriculum vitæ de M. A à M[me] E, alors qu'il l'avait obtenu de la part de M. A en vue d'éventuelles invitations à des conférences et que la transmission par ce dernier s'accompagnait d'une limitation quant à son utilisation, la motivation de la décision attaquée, qui a considéré que les faits entraient bien dans le champ d'application de l'article 8 de la Charte et du règlement n° 45/2001, n'est pas erronée.

93 Il y a lieu d'ajouter à cet égard que l'argument du requérant selon lequel les membres du personnel de la Commission sont autorisés à utiliser leur adresse IP professionnelle pour envoyer des courriels à des fin privées est sans pertinence, au vu de ce que le requérant n'a pas été censuré par l'AIPN du fait d'avoir envoyé des courriels privés à partir de son adresse IP à la Commission.

94 Par conséquent, le troisième moyen doit être rejeté comme étant, en partie, irrecevable, et, en partie, mal fondé.

Sur le quatrième moyen, divisé en plusieurs branches, tirées, la première, de la violation de l'article 1er de l'annexe IX du statut ; la deuxième, de la violation de l'article 41 de la Charte ; la troisième, de la violation du principe de bonne administration ; la quatrième, de la violation du devoir de motivation ; la cinquième, de la violation du principe de sécurité juridique ; la sixième, d'un détournement de pouvoir ; la septième, d'une erreur manifeste d'appréciation ; la huitième, de la violation du devoir de sollicitude incombant à l'administration ; la neuvième, de la violation de l'obligation de l'administration d'exercer son pouvoir disciplinaire avec soin et impartialité et, la dixième, de la violation des droits de la défense

95 Le Tribunal constate que, dans ses écrits, le requérant ne développe son argumentation qu'à l'égard des septième et neuvième branches du quatrième moyen, tirées respectivement d'une erreur manifeste d'appréciation et de la violation du devoir d'impartialité de l'administration en matière disciplinaire. Les autres branches du moyen sont simplement énoncées et ne sont aucunement étayées par une quelconque argumentation, contrairement à la règle prévue à l'article 35, paragraphe 1, sous e), du règlement de procédure en vigueur lors de l'introduction du recours [devenu, après modification, l'article 50, paragraphe 1, sous e), du règlement de procédure]. Il y a donc lieu de les déclarer irrecevables.

– Arguments des parties

96 Le requérant fait valoir que l'AIPN a commis une erreur manifeste d'appréciation à deux égards : en premier lieu, lorsqu'elle a indiqué, dans la décision de rejet de la réclamation, que la décision attaquée « a été prise après que l'AIPN a considéré prouvé que le requérant s'est prévalu de sa position et de son grade au sein de la Commission pour obtenir de façon fallacieuse le [curriculum vitæ] de M. [A] à des fins privées, alors que M. [A] en avait clairement limité l'usage à des conférences organisées par les institutions européennes », dans la mesure où l'obtention de « façon fallacieuse » dudit curriculum vitæ n'a pas été démontrée. En second lieu, l'AIPN n'aurait pas prouvé que le requérant a fait un usage illicite du curriculum vitæ de M. A, qu'il aurait par ailleurs détruit, le requérant s'étant limité à montrer ledit curriculum vitæ à Mme E sans qu'aucune publicité ne soit intervenue par la suite.

97 Le requérant se plaint également du manque d'indépendance dont l'IDOC et l'AIPN auraient fait preuve au cours de l'enquête administrative et de la procédure disciplinaire. Il est d'avis que les explications qu'il a apportées n'ont pas été prises en considération et que l'administration aurait dû accueillir avec précaution les plaintes de Mme E à son égard ainsi que les déclarations de cette dernière et de M. A en ce qui concerne l'obtention, la détention et l'utilisation du curriculum vitæ de ce dernier. La partialité de l'IDOC se serait manifestée lorsque le requérant a été entendu dans le cadre de l'enquête administrative, le 18 janvier 2012 et le 6 juin 2012, sans avoir eu accès ni aux déclarations de Mme E ni au courriel de M. A du 16 juin 2011. L'AIPN n'aurait pas non plus respecté les obligations que lui imposent l'article 1er, paragraphe 3, et l'article 2, paragraphe 2, de l'annexe IX du statut dans la mesure où le requérant n'a pas été informé du fait que le premier volet du mandat d'enquête avait été classé sans suite.

98 La Commission conclut au rejet du quatrième moyen.

– Appréciation du Tribunal

99 En ce qui concerne les arguments du requérant relatifs à une éventuelle erreur manifeste d'appréciation de la part de l'AIPN, il convient de relever, en premier lieu, que, tel que repris aux points 33 et 34 du présent arrêt, lors de son audition du 18 janvier 2012 par les enquêteurs de l'IDOC, le requérant a déclaré avoir demandé son curriculum vitæ à M. A ; en deuxième lieu, que c'est le requérant lui-même qui a joint, en annexe à la requête, la plupart des courriels qu'il a échangés avec M. A à partir de son adresse IP à la Commission, courriels qu'il a signés en tant qu'administrateur principal et dans lesquels il a demandé son curriculum vitæ à M. A aux fins de

l'inviter à des conférences, et, en troisième lieu, que, tel qu'il ressort du point 43 du présent arrêt, le requérant a déclaré, lors de son audition le 8 février 2013, avoir montré le curriculum vitæ de M. A à M^me^ E pour des raisons autres que celles pour lesquelles le curriculum vitæ avait été communiqué au requérant par l'intéressé.

100 Dans ces conditions, force est de constater que l'AIPN n'a pas commis d'erreur manifeste d'appréciation lorsqu'elle a conclu, aux points 11 et 12 de la décision attaquée, dans sa formulation initiale du 6 septembre 2013, puis l'a confirmé dans la décision de rejet de la réclamation, que le requérant avait trompé M. A en vue de l'obtention de son curriculum vitæ à des fins privées et qu'il l'avait ensuite utilisé pour des fins autres que celles pour lesquelles M. A le lui avait communiqué.

101 Pour ce qui est de l'éventuel manque d'indépendance de l'IDOC et de l'AIPN au cours de l'enquête administrative et de la procédure disciplinaire dont le requérant se plaint, en premier lieu, le Tribunal constate que ce n'est pas sur le fondement des seules accusations de M^me^ E et de M. A que le requérant a été sanctionné, mais à la suite d'une procédure d'enquête administrative et d'une procédure disciplinaire régulièrement menées, au cours desquelles tant M^me^ E et M. A que le requérant ont été entendus, ce dernier ayant également été invité à présenter des observations écrites avant la finalisation du rapport d'enquête, en vue de l'exposé, dans ce dernier, des faits considérés comme établis. Le fait que, à la fin de la procédure disciplinaire, le requérant se soit vu imposer une sanction ne signifie pas pour autant que ses déclarations et ses explications n'ont pas été prises en considération.

102 En deuxième lieu, le Tribunal relève que, par application de son devoir de sollicitude à l'égard de tout le personnel de l'institution et non pas seulement à l'égard du requérant, l'AIPN a, à bon droit, pu se considérer obligée d'ordonner l'ouverture d'une enquête administrative en vue de vérifier si les faits portés à sa connaissance dans le courriel de M. A du 16 juin 2011 étaient constitutifs d'un manquement à ses obligations de la part du fonctionnaire concerné.

103 En troisième lieu, en ce qui concerne le grief relatif au défaut de communication au requérant, préalablement à ses auditions des 18 janvier 2012 et 6 juin 2012, des déclarations de M^me^ E et du courriel de M. A du 16 juin 2011, le Tribunal renvoie aux points 70 et 71 du présent arrêt, desquels il résulte que les règles statutaires applicables ne prévoient qu'un droit d'accès restreint à certains documents pour le fonctionnaire faisant l'objet d'une enquête administrative, et ce uniquement à la fin de l'enquête, alors que, tel qu'il ressort du dossier, le seul moment auquel le requérant a demandé à l'administration l'accès au dossier a été le 8 août 2012 et que l'enquête administrative n'a été clôturée que le 3 octobre 2012.

104 En quatrième lieu, le grief du requérant selon lequel il n'aurait pas été informé de ce que le premier volet du mandat d'enquête avait été classé sans suite manque en fait, ce qui ressort clairement de la première partie de la note sur les faits, dans laquelle il est indiqué que « [l]a plainte pour harcèlement déposée par M^me^ [E] a été classée sans suite, ce dont [le requérant] a été informé ». Cette information a donc été portée à la connaissance du requérant avant même la fin de l'enquête administrative.

105 Le requérant ne peut donc pas valablement soutenir qu'il y aurait eu violation par l'administration des obligations que lui imposent l'article 1^er^, paragraphe 3, et l'article 2, paragraphe 2, de l'annexe IX du statut.

106 Il s'ensuit que le requérant n'a pas démontré la violation du devoir d'impartialité de la part de l'IDOC et de l'AIPN au cours de l'enquête administrative et de la procédure disciplinaire.

107 Les branches du quatrième moyen tirées de l'erreur manifeste d'appréciation et de la violation du devoir d'impartialité de l'administration n'ayant pas été établies, il convient de rejeter le quatrième moyen comme étant, en partie, irrecevable et, en partie, mal fondé.

Sur le cinquième moyen, divisé en plusieurs branches, tirées, la première, de la violation des articles 3, 9 et 10 de l'annexe IX du statut ; la deuxième, de la violation de l'article 41 de la Charte ; la troisième, de la violation du principe de bonne administration ; la quatrième, de la violation de l'obligation de motivation ; la cinquième, de la violation du principe de sécurité juridique ; la sixième, du détournement de pouvoir ; la septième, de l'erreur manifeste d'appréciation et, la huitième, de la violation du principe de proportionnalité de la sanction disciplinaire

108 Le Tribunal constate que, dans ses écrits, le requérant ne développe son argumentation qu'à l'égard des quatrième et huitième branches du cinquième moyen, tirées, respectivement, de la violation de l'obligation de motivation et de la violation du principe de proportionnalité de toute sanction disciplinaire. Les autres branches du moyen ne sont qu'énoncées et ne sont aucunement étayées par une quelconque argumentation, contrairement à la règle prévue à l'article 35, paragraphe 1, sous e), du règlement de procédure en vigueur lors de l'introduction du recours [devenu, après modification, l'article 50, paragraphe 1, sous e), du règlement de procédure]. Il y a donc lieu de les déclarer irrecevables.

– Arguments des parties

109 Le requérant conteste la motivation relative à « la fixation de la hauteur de la sanction » telle que reprise dans la décision attaquée, dans sa formulation initiale du 6 septembre 2013. Cette motivation, fort succincte et qui manquerait totalement de pertinence, serait erronée tant en droit qu'en fait. En outre, la problématique du curriculum vitæ n'ayant eu aucun impact et la réputation des institutions de l'Union n'ayant pas été entachée, l'absence de pertinence serait évidente.

110 Le requérant fait également valoir que, « [a]u vu des éléments développés ci-dessus », aucune sanction ne se justifierait et il ajoute, à titre subsidiaire, que, si un manquement devait être retenu, une mise en garde aurait amplement suffi et que, en tout état de cause, la sanction serait disproportionnée.

111 La Commission conclut au rejet du cinquième moyen.

– Appréciation du Tribunal

112 Selon une jurisprudence constante, la motivation d'une décision faisant grief doit permettre au juge d'exercer son contrôle sur la légalité de la décision et doit fournir à l'intéressé les indications nécessaires pour savoir si la décision est bien fondée (arrêt du 17 juillet 2012, BG/Médiateur, F-54/11, EU:F:2012:114, point 96, confirmé sur pourvoi par arrêt du 22 mai 2014, BG/Médiateur, T-406/12 P, EU:T:2014:273).

113 La question de savoir si la motivation de la décision de l'AIPN imposant une sanction satisfait à ces exigences doit être appréciée au regard non seulement de son libellé, mais également de son contexte ainsi que de l'ensemble des règles juridiques régissant la matière concernée. À cet égard, si l'AIPN doit indiquer de manière précise les faits retenus à la charge du fonctionnaire, ainsi que les considérations qui l'ont amenée à adopter la sanction choisie, il n'est pas pour autant exigé qu'elle discute tous les points de fait et de droit qui ont été soulevés par l'intéressé au cours de la procédure (arrêt du 8 novembre 2007, Andreasen/Commission, F-40/05, EU:F:2007:189, point 260).

114 En l'espèce, il ressort du libellé de la décision du 6 septembre 2013, infligeant la sanction de blâme au requérant, que l'AIPN s'est bien acquittée de son obligation de motivation. En effet, l'analyse détaillée de la matérialité et de l'appréciation des faits ainsi que les griefs reprochés au requérant figurent aux points 1 à 12 de ladite décision, tandis que le point 13 reprend de manière précise les considérations, y compris les circonstances aggravantes et atténuantes, qui ont amené l'AIPN à imposer au requérant la sanction prévue à l'article 9, paragraphe 1, sous b), de l'annexe IX du statut.

115 Par conséquent, il y a lieu de conclure que la décision du 6 septembre 2013, telle que précisée par la décision de rejet de la réclamation, et le contexte dans lequel elle a été adoptée ont fourni au requérant les indications nécessaires lui permettant de connaître les motifs à l'origine de ladite décision et ont permis au juge d'exercer son contrôle sur la légalité de cette dernière. Il s'ensuit que la quatrième branche du cinquième moyen, tirée de l'absence de motivation de la décision attaquée, n'est pas fondée.

116 En ce qui concerne la huitième branche du cinquième moyen, par laquelle le requérant fait grief à l'AIPN de lui avoir infligé une sanction et, subsidiairement, de lui avoir infligé une sanction disproportionnée, il y a lieu de rappeler que l'article 86 du statut prévoit que tout manquement aux obligations auxquelles le fonctionnaire est tenu, au titre du statut, commis volontairement ou par négligence, l'expose à une sanction disciplinaire.

117 En l'espèce, la réalité de certains des faits reprochés au requérant dans le second volet du mandat d'enquête étant établie, notamment par des preuves écrites ainsi que des déclarations du requérant lui-même, il appartenait à l'AIPN de décider, dans l'exercice de son pouvoir d'appréciation, si ces faits étaient constitutifs d'un manquement du requérant à ses obligations au sens de l'article 86, paragraphe 1, du statut et, dans l'affirmative, de lui infliger une sanction proportionnée à la faute commise.

118 S'agissant d'apprécier si la sanction disciplinaire infligée est proportionnelle à la gravité des faits établis, il y a lieu de rappeler que, s'il est vrai que le statut ne prévoit pas de rapport fixe entre les sanctions prévues à l'article 9 de l'annexe IX du statut et les catégories possibles de manquements commis par les fonctionnaires, il n'en demeure pas moins que l'article 10 de l'annexe IX du statut contient une liste non exhaustive de critères, y compris des circonstances pouvant atténuer ou aggraver le comportement du fonctionnaire, dont l'AIPN doit tenir compte pour déterminer la gravité de la faute et décider de la sanction disciplinaire.

119 En l'espèce, le Tribunal relève, en premier lieu, que, sur le fondement du rapport d'enquête, l'AIPN a décidé de l'ouverture d'une procédure disciplinaire sans consultation du conseil de discipline, ce qui, par application de l'article 11 de l'annexe IX du statut, implique que la sanction éventuellement imposée ne pouvait être que l'avertissement par écrit ou le blâme, à savoir l'une des deux sanctions disciplinaires les plus faibles dans l'échelle des sanctions.

120 En second lieu, le Tribunal constate que, dans la décision attaquée, après avoir examiné la nature de la faute et les circonstances dans lesquelles elle a été commise, l'AIPN a tenu compte, d'une part, du fait que le comportement du requérant avait eu un impact limité sur la réputation de l'institution ainsi que sur la situation personnelle de M. A, de ce qu'il ne s'était pas reproduit et de ce que le requérant semblait avoir respecté ses obligations statutaires dans le passé. D'autre part, l'AIPN a considéré que le comportement du requérant avait entraîné un risque pour M. A de se former un avis négatif sur la conduite des fonctionnaires de l'Union, alors qu'il était en cours de recrutement à la Commission ; que le requérant avait délibérément trompé M. A afin d'obtenir son curriculum vitæ à des fins privées ; que le grade élevé du requérant ainsi que sa longue expérience à la Commission l'obligeaient tout particulièrement à respecter le niveau le plus haut de conduite qui s'impose aux fonctionnaires de l'Union. Enfin, l'AIPN a tenu compte du refus répété du requérant d'admettre que son comportement constituait un manquement à ses obligations statutaires.

121 Il s'ensuit que, ayant été choisie dans le respect des dispositions de l'article 10 de l'annexe IX du statut, la sanction de blâme infligée au requérant par l'AIPN est proportionnée par rapport aux faits établis à son encontre.

122 Il y a donc lieu de rejeter le cinquième moyen comme étant, en partie, irrecevable et, en partie, non fondé.

123 Il convient, par conséquent, de rejeter les conclusions en annulation de la décision attaquée.

Sur les conclusions indemnitaires

Arguments des parties

124 Le requérant fait valoir que la décision attaquée est une décision arbitraire qui lui aurait porté un préjudice tant moral que matériel. En effet, même s'il ne s'agit que d'une sanction légère, elle serait susceptible de nuire à la poursuite de sa carrière. Il demande au Tribunal de condamner la Commission à lui verser, à titre de dommages et intérêts, évaluée ex æquo et bono, la somme de 5 000 euros.

125 La Commission conclut au rejet de la demande indemnitaire.

Appréciation du Tribunal

126 Selon une jurisprudence constante, lorsque le préjudice dont un requérant se prévaut trouve son origine dans l'adoption d'une décision faisant l'objet de conclusions en annulation, le rejet de ces conclusions en annulation entraîne, par principe, le rejet des conclusions indemnitaires, ces dernières leur étant étroitement liées (arrêt du 23 octobre 2012, Eklund/Commission, F-57/11, EU:F:2012:145, point 106).

127 Les conclusions indemnitaires visant la réparation du préjudice matériel et moral qu'aurait causé la décision attaquée au requérant doivent donc être rejetées dans la mesure où les conclusions en annulation de la décision attaquée ont été rejetées.

128 Il découle de ce qui précède que le recours doit être rejeté dans sa totalité.

Sur les dépens

129 Aux termes de l'article 101 du règlement de procédure, sous réserve des autres dispositions du chapitre huitième du titre deuxième dudit règlement, toute partie qui succombe supporte ses propres dépens et est condamnée aux dépens exposés par l'autre partie, s'il est conclu en ce sens. En vertu de l'article 102, paragraphe 1, du même règlement, le Tribunal peut décider, lorsque l'équité l'exige, qu'une partie qui succombe supporte ses propres dépens, mais n'est condamnée que partiellement aux dépens exposés par l'autre partie, voire qu'elle ne doit pas être condamnée à ce titre.

130 Il résulte des motifs énoncés dans le présent arrêt que le requérant a succombé en son recours. En outre, la Commission a, dans ses conclusions, expressément demandé que le requérant soit condamné aux dépens. Les circonstances de l'espèce ne justifiant pas l'application des dispositions de l'article 102, paragraphe 1, du règlement de procédure, le requérant doit supporter ses propres dépens et est condamné à supporter les dépens exposés par la Commission.

Par ces motifs,

LE TRIBUNAL DE LA FONCTION PUBLIQUE (deuxième chambre)

déclare et arrête :

1) **Le recours est rejeté.**

2) **AQ supporte ses propres dépens et est condamné à supporter les dépens exposés par la Commission européenne.**

Bradley Kreppel Rofes i Pujol

Ainsi prononcé en audience publique à Luxembourg, le 21 octobre 2015.

Le greffier
W. Hakenberg

Le président
K. Bradley

Reports of Cases

JUDGMENT OF THE GENERAL COURT (Sixth Chamber)

3 December 2015 *

(Non-contractual liability — Petition addressed to the Parliament — Dissemination of certain personal data on the Parliament's website — Absence of a sufficiently serious breach of a rule of law conferring rights on individuals)

In Case T-343/13,

CN, residing in Brumath (France), represented by M. Velardo, lawyer,

applicant,

supported by

European Data Protection Supervisor (EDPS), represented initially by A. Buchta and V. Pozzato, then by A. Buchta, M. Pérez Asinari, F. Polverino, M. Guglielmetti and U. Kallenberger, acting as Agents,

intervener,

v

European Parliament, represented by N. Lorenz and S. Seyr, acting as Agents,

defendant,

APPLICATION for compensation to make good the damage allegedly suffered by the applicant following the dissemination on the Parliament's website of certain personal data relating to the applicant,

THE GENERAL COURT (Sixth Chamber),

composed of S. Frimodt Nielsen, President, F. Dehousse and A.M. Collins (Rapporteur), Judges,

Registrar: J. Palacio González, Principal Administrator,

having regard to the written part of the procedure and further to the hearing on 24 March 2015,

gives the following

* Language of the case: Italian.

Judgment

Background to the dispute

1 Until 2011, the applicant, CN, was an official of the Council of the European Union. On 23 September 2009, he submitted a petition to the European Parliament, on the subject of the support granted to disabled family members of a European official, the difficulties encountered by European officials suffering health problems during their careers and the mistreatment of his case by the Council, by means of a form available online on the Parliament's website.

2 On 8 January 2010, the European Commission was consulted pursuant to Rule 202(6) of the Rules of Procedure of the European Parliament (OJ 2011 L 116, p. 1, 'the Rules of Procedure'), now Rule 216(6) of the Rules of Procedure in its version of July 2014.

3 On 15 January 2010, the Committee on Petitions of the Parliament informed the applicant that his petition had been declared admissible.

4 After receiving the response from the Commission on 15 March 2010, the Committee on Petitions decided to close the petition and informed the applicant accordingly on 14 June 2010.

5 After rejecting the petition, the Parliament published on its website a document concerning the petition entitled 'notice to members' ('the notice'). The notice provided a summary description of the content of the petition and the Commission's response. In particular, it gave the name of the applicant and stated that he was suffering from a serious, life-threatening illness and that his son had a severe mental or physical disability.

6 In May 2011, the applicant was placed on sick leave by the Council on account of his state of health.

7 In April 2012, the applicant sent an email to the Commission's 'Europe Direct Contact Centre', which forwarded it to the Parliament on 10 April 2012. In that email, the applicant requested that the notice be removed from the Parliament's website.

8 On 20 April 2012, the Parliament replied to the applicant, stating that it had removed the notice from the internet.

9 On 31 August 2012, the applicant reiterated his request through his counsel, as, according to him, the personal data in question could still be viewed on the Parliament's website.

10 On 24 September 2012, the Parliament replied that the publication of the notice was lawful. It added that the applicant's personal data would nevertheless be erased from the internet even though there was no legal obligation to do so.

11 The Parliament has stated, in response to a written question from the Court, that the most recent erasure operations in respect of common search engines took place on 8 October 2012.

12 On 4 December 2012, the applicant's counsel reiterated the request, pointing out that the personal data in question could still be viewed on the internet.

13 On 10 January 2013, the Parliament replied to the applicant's counsel, stating that it considered its conduct to be lawful. It added that all the documents on its website had nevertheless been processed or were currently being processed in order to erase the applicant's personal data.

14 According the applicant, the personal data in question were available on the internet at least until that latter date.

Procedure and forms of order sought

15 By application lodged at the Court Registry on 28 June 2013, the applicant brought the present action.

16 By document lodged at the Court Registry on 4 October 2013, the European Data Protection Supervisor (EDPS) applied for leave to intervene in the present case in support of the form of order sought by the applicant. By order of 21 November 2013, the President of the Sixth Chamber granted the EDPS leave to intervene. The EDPS lodged his statement in intervention on 7 February 2014. The parties lodged their observations on that statement within the prescribed period.

17 The applicant claims that the Court should:

— order the European Union and the Parliament to pay a sum of EUR 1 000 in compensation for material damage suffered and EUR 40 000 in compensation for non-material damage suffered, plus interest calculated at the rate of 6.75%;

— order the European Union and the Parliament to pay the costs.

18 The Parliament contends that the Court should:

— dismiss the action as unfounded;

— order the applicant to pay the costs.

19 On a proposal from the Judge-Rapporteur, the Court (Sixth Chamber) decided to open the oral part of the procedure and, in the context of the measures of organisation of procedure provided for in Article 64 of the Rules of Procedure of the General Court of 2 May 1991, requested the parties to lodge certain documents and put a number of questions to them in writing, requesting them to reply before the hearing. The parties complied with those requests within the prescribed time limits.

20 The parties presented oral argument and replied to the oral questions put by the Court at the hearing on 24 March 2015.

Law

21 In support of his action, the applicant puts forward a single plea in law, alleging the non-contractual liability of the European Union. In his view, the three conditions giving rise to such liability are met in the present case, namely that the Parliament's conduct is unlawful, damage has been suffered, and there is a causal link between the unlawful conduct and the damage.

22 The EDPS supports the applicant's claims regarding the unlawfulness of the Parliament's conduct.

23 The Parliament claims that the action is unfounded in its entirety.

1. *The unlawfulness of the Parliament's conduct*

Arguments of the parties

24 As a preliminary point, the applicant asserts that, according to case-law, where unlawful conduct occurs in an area in which the institution concerned enjoys a wide discretion, the non-contractual liability of the European Union is subject to the establishment of a sufficiently serious breach of a rule of law intended to confer rights on individuals. The decisive test for finding that a breach is sufficiently serious is whether the institution manifestly and gravely disregarded the limits on its discretion.

25 Conversely, according to the applicant, where an institution has only considerably reduced, or even no, discretion, the mere infringement of EU law may be sufficient to establish the existence of a sufficiently serious breach.

26 The applicant asserts that, with regard to the decision to publish the notice on the Parliament's website, the Parliament did not enjoy any discretion in view of the applicable legal framework (Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950 (ECHR), Article 8(1) of the Charter of Fundamental Rights of the European Union, Article 22 of the United Nations Convention on the Rights of Persons with Disabilities, adopted on 13 December 2006 and ratified by the European Union on 23 December 2010 ('the Convention on the Rights of Persons with Disabilities'), and 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)).

27 The applicant submits that the Parliament infringed those provisions by publishing information on his state of health, his son's state of health and his professional life.

28 In particular, the applicant relies on Article 5(d) and Articles 10 and 16 of Regulation No 45/2001. It is not clear from the document in which he consented to public consideration of his petition that he unambiguously agreed to publication of personal data or that he expressly agreed to publication of data relating to his state of health and to the presence of a person with disabilities in his family.

29 In addition, even though the applicant requested the removal of personal data from the Parliament's website, the Parliament initially responded negatively and granted the request only following the intervention of his counsel, in contravention of the right to erasure of personal data. Furthermore, the fact that the Parliament agreed to erase the data suggests that it implicitly acknowledged the unlawfulness of the publication. Article 16 of Regulation No 45/2001 only provides for the erasure of data whose processing is unlawful.

30 The Parliament's duty of transparency cannot justify the disclosure of personal data relating to the state of health and the presence of a person with disabilities in his family. Even assuming publication of a summary of petitions in order to provide information on the activities of the EU institutions to be a legitimate interest, the infringement of the applicant's rights is disproportionate.

31 In the reply, the applicant adds that the Parliament also infringed Article 12 of the Bureau decision of 22 June 2005 on Implementing rules relating to Regulation No 45/2001 (OJ 2005 C 308, p. 1, 'the Implementing rules relating to Regulation No 45/2001'), which provides that a request for erasure must be processed within 15 working days and that, if erasure is accepted, it must be acted upon 'immediately'. In this case, the procedure lasted almost ten months.

32 According to the applicant, Rule 203 of the Rules of Procedure neither requires nor authorises the publication of information such as that at issue. Furthermore, the Rules of Procedure, an internal organisation document, cannot derogate from Regulation No 45/2001.

33 The Parliament asserts that its conduct was lawful.

34 As regards the initial phase of the public consideration of the petition, the Parliament argues that its conduct was consistent with Article 5(b) (processing necessary for compliance with a legal obligation), Article 5(d) (processing based on unambiguously given consent), Article 10(2)(a) (express consent to the processing of sensitive data) and Article 10(2)(d) (processing of sensitive data which are manifestly made public by the data subject) of Regulation No 45/2001.

35 First, with particular regard to the argument concerning Article 5(b) of Regulation No 45/2001, the Parliament submits that Rule 203 of the Rules of Procedure (now Rule 217) establishes as a general principle that notice is to be given of petitions. Under Rule 201(9) (now Rule 215(9)), petitions as a general rule become public documents, and the name of the petitioner and the contents of the petition may be published by the Parliament for reasons of transparency. Consequently, the submission of a petition implies, in principle, that notice is given thereof, allowing other citizens to support the signatory. In addition, the Parliament maintains that under Articles 10 and 11 TEU and Articles 15 and 232 TFEU, its work should be conducted mainly in public.

36 Second, according to the Parliament, the processing of personal data was consistent with Article 5(d) of Regulation No 45/2001, since the applicant had unambiguously given his consent to the public consideration of his petition. The applicant was duly informed and did not avail himself of the option available to him to request anonymous or confidential processing of his petition.

37 Third, the Parliament asserts that the consent given by the applicant in the conditions described above was express consent to the processing of sensitive data within the meaning of Article 10(2)(a) of Regulation No 45/2001.

38 As regards the phase subsequent to the publication of the data, which concerns the request for erasure, the Parliament submits that the main condition for the data subject obtaining the erasure of his data on the basis of Article 16 of Regulation No 45/2001 is that the processing of the data was unlawful, which was not the case in this instance. Nevertheless, the Parliament erased the applicant's data as a mere courtesy.

39 The Parliament also maintains that Regulation No 45/2001 does not contain any rule providing for the possibility of withdrawing the consent given. If such withdrawal were possible, it could have effects only for the future. In addition, it is impossible retroactively to erase certain data, such as those in the minutes of Parliament proceedings, which are published in the *Official Journal of the European Union*.

40 In his statement in intervention, the EDPS focuses on the condition relating to the allegedly unlawful conduct of the Parliament.

41 The EDPS argues that to be valid consent must be informed and specific, that is to say, connected with a processing operation of which the individual has been informed. In the view of the EDPS, these conditions were not met in the present case. None of the information provided in the online form made clear the precise consequences of the envisaged processing to the petitioner. In particular, there was no mention in the form that sensitive data would be made accessible on the internet. The EDPS adds that Article 10(2)(a) of Regulation No 45/2001 offers additional protection to Article 5(d) of the regulation in so far as it requires that the information given to the individual with a view to obtaining his consent clearly mentions sensitive data and the envisaged processing operation. According to the EDPS, any other interpretation would deprive Article 5(d) of that regulation of its substance.

42 In the light of the above considerations, the EDPS takes the view that the Parliament did not obtain the express consent of the applicant in accordance with Article 10(2)(a) of Regulation No 45/2001.

Findings of the Court

43 Under the second sentence of Article 340 TFEU, '[i]n the case of non-contractual liability, the Union shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its institutions or by its servants in the performance of their duties'.

44 The Court has ruled that in order for the Union to incur non-contractual liability under the second sentence of Article 340 TFEU for unlawful conduct of its institutions a number of conditions must be satisfied: the institution's conduct must be unlawful, actual damage must have been suffered and there must be a causal link between the conduct and the damage pleaded (judgments of 11 July 1997 in *Oleifici Italiani* v *Commission*, T-267/94, ECR, EU:T:1997:113, paragraph 20, and 9 September 2008 in *MyTravel* v *Commission*, T-212/03, ECR, EU:T:2008:315, paragraph 35). The condition of unlawful conduct of the Union's institutions requires a sufficiently serious breach of a rule of law intended to confer rights on individuals (judgment in *MyTravel* v *Commission*, EU:T:2008:315, paragraph 37). The decisive test for finding that a breach of EU law is sufficiently serious is whether the EU institution manifestly and gravely disregarded the limits on its discretion (judgment of 5 March 1996 in *Brasserie du pêcheur and Factortame*, C-46/93 and C-48/93, ECR, EU:C:1996:79, paragraph 55).

45 With regard to the condition concerning the unlawfulness of the institutions' conduct, it must be examined, first, whether the rules of law relied on by the applicant are intended to confer rights on individuals and, second, whether the Parliament committed a sufficiently serious breach of those rules.

46 In the application, the applicant relies on provisions relating to the protection of personal data contained in the Charter of Fundamental Rights, Regulation No 45/2001 and the Implementing rules relating to Regulation No 45/2001 and also on provisions relating to the protection of private life contained in the ECHR and the Convention on the Rights of Persons with Disabilities.

The rules relating to the protection of personal data

47 The right to the protection of personal data enshrined in Article 8 of the Charter of Fundamental Rights is developed by Regulation No 45/2001 in respect of acts of EU institutions and bodies and by the Implementing rules relating to Regulation No 45/2001 in respect of the Parliament in particular. These various provisions are intended to confer rights on individuals. They may therefore be relied on by the applicant in his action for compensation.

48 As regards the existence of an alleged sufficiently serious breach of those rules, the arguments put forward by the applicant mainly concern the application of Regulation No 45/2001 and its Implementing rules. He does not dispute, in particular, that those rules are compatible with the right established by the Charter of Fundamental Rights. Consequently, and contrary to the claim made by the applicant, the judgment of 9 November 2010 in *Volker und Markus Schecke and Eifert* (C-92/09 and C-93/09, ECR, EU:C:2010:662) is not relevant to the outcome of these proceedings.

49 Furthermore, according to case-law, it is clear from the first sentence of recital 15 of Regulation No 45/2001 that a reference to other provisions was not found necessary for processing carried out in the exercise of activities within the scope of that regulation, given that, in such cases, it is clearly Regulation No 45/2001 itself which applies (judgment of 29 June 2010 in *Commission* v *Bavarian Lager*, C-28/08 P, ECR, EU:C:2010:378, paragraph 62). Consequently, for the purposes of the present action, it is necessary to consider the provisions of Regulation No 45/2001 and its Implementing rules.

50 It has been held that the expression 'data concerning health' must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual (see, by analogy, judgment of 6 November 2003 in *Lindqvist*, C-101/01, ECR, EU:C:2003:596, paragraph 50, regarding 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)). However, that notion cannot be extended to include expressions which do not give rise to the disclosure of any data regarding a person's health or medical condition (see, to that effect, judgment of 31 May 2005 in *Dionyssopoulou* v *Council*, T-105/03, ECR-SC, EU:T:2005:189, paragraph 33).

51 In the light of these considerations it is necessary to examine, first, the initial publication of the personal data in question and, second, the Parliament's response to the applicant's request to remove the data from its website.

– Dissemination of personal data on the internet

52 It should be noted as a preliminary point that in this case the Parliament carried out a series of operations for the processing of personal data within the meaning of Article 2(b) of Regulation No 45/2001. Dissemination of personal data, including dissemination on the internet, constitutes such a processing operation for the purposes of that provision.

53 The notice published on the Parliament's website stated, among other things, that the applicant, who was named, had recently suffered a serious, potentially life-threatening illness and that his son had a disability. The notice also contained certain information relating to the applicant's career.

54 It must therefore be stated that the processing of data by the Parliament related to the applicant's personal data (including information on his career) and sensitive personal data concerning the health of the applicant and of his son. The processing of these different sets of personal data should be examined separately.

55 First, the processing of sensitive personal data relating to the applicant must be examined in the light of Article 10 of Regulation No 45/2001.

56 Under Article 10(1) of Regulation No 45/2001, the processing of personal data revealing data concerning health is prohibited. However, Article 10(2)(a) of that regulation provides that this prohibition does not apply, inter alia, where the data subject has given his or her express consent.

57 Against this background, it should be observed that Article 2(h) of Regulation No 45/2001 defines the data subject's consent as 'any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed'.

58 In this instance, it must be ascertained whether, as the Parliament claims, the applicant had given his express consent to the publication of his sensitive personal data on the internet.

59 In this case, since Article 2(h) of Regulation No 45/2001 does not lay down any conditions as to form, the lodging of the petition may be regarded as an indication of the applicant's wishes.

60 In addition, the applicant does not put forward any argument to call into question the fact that the petition was freely submitted, without coercion, duress, intimidation or deception.

61 Under the same provision, the consent must be specific, that is to say, connected with a processing operation (or series of processing operations) for precise purposes. That provision also stipulates that to be valid consent must be informed, which means that, when he gives his consent, the data subject has the essential information concerning the fundamental aspects of the processing, in the light of the context of the specific case.

62 Lastly, it is clear from Article 10(2)(a) of Regulation No 45/2001 that where the consent relates to the processing of sensitive data, it must be express. In other words, consent must be explicit, ruling out the possibility of inferring it implicitly from the actions of the person concerned.

63 The present case must be examined in the light of those considerations.

64 It should be noted that the Parliament's website recommends that petitioners read the 'online help' before submitting a petition. That 'online help' contains the following statement, under the heading 'Publication of petitions':

'Petitioners are advised that minutes are published in the Official Journal. Certain details, including the name of the petitioner and the number of the petition are consequently available on the Internet. This has implications for the protection of individual data and petitioners' attention is drawn to this specifically. If, as a petitioner, you do not wish your name to be disclosed, the European Parliament will respect your privacy, but such requests must be clear and explicitly mentioned in your petition. Similarly, if you wish your petition to be treated in confidence it should also be clearly requested. The Committee attaches importance to the transparency of its meetings which may be web-streamed. Proceedings may therefore be observed on any normal computer via the EP website. Committee meetings are held in public and petitioners are able to attend if they so request, if and when their petition is discussed.'

65 In addition, when he submitted his petition through the Parliament's website, the applicant completed a form by answering the following questions in the affirmative:

'If the Committee on Petitions declares your petition admissible, do you agree to its being considered in public?'

'Do you consent to your name being recorded on a public register, accessible through Internet?'

66 Account must also be taken of the following factors.

67 First, the Court must take into consideration the scheme and the purpose of the right of petition to the Parliament under Articles 24 and 227 TFEU. That right of petition is expressly conceived as an instrument of democratic participation, which is intended to be transparent in order to permit other citizens to support it, if appropriate, and thus to generate a public debate. Reference should also be made to Articles 15 and 232 TFEU, which provide that the Parliament's work should be conducted mainly in public. It is in this context that the rules governing the exercise of the right of petition, in particular those in Rule 201 et seq. of the Rules of Procedure (now Rule 215 et seq.), are intended to be applied.

68 Second, reference should be made to the ordinary meaning of the expression 'considered in public' for an average person who is required to complete a form when he lodges his petition.

69 Third, it should be noted that, at the time of submission, the applicant was informed by the Parliament that he could request anonymous or even confidential processing of his petition, that minutes were published in the Official Journal, that 'certain details', including the name of the petitioner, were available on the internet, that there was a public register, accessible through the internet, and that the meetings of the Committee on Petitions could be web-streamed.

70 Fourth, regard should be had to the specific content of the petition at issue, namely the fact that an EU institution had purportedly failed to take due account of the applicant's illness (and his son's disability) for the purposes of his career, a matter which, in principle, has a degree of public interest. It should be added that the acknowledgement of receipt expressly confirmed that this was precisely the subject of the petition. Consequently, the publication of this information concerned the specific contents of the petition, and not incidental or extraneous elements.

71 In this regard, Rule 201(9) of the Rules of Procedure provides that '[p]etitions, once registered, shall as a general rule become public documents, and the name of the petitioner and the contents of the petition may be published by Parliament for reasons of transparency'. Rule 201(10) provides that '[n]otwithstanding the provisions contained in paragraph 9, the petitioner may request that his or her name be withheld in order to protect his or her privacy, in which case Parliament must comply with the request'.

72 Under Rule 203 of the Rules of Procedure on notice of petitions:

'1. Notice shall be given in Parliament of the petitions entered in the register referred to in Rule [201](6) and the main decisions on the procedure to be followed in relation to specific petitions. Such announcements shall be entered in the minutes of proceedings.

2. The title and a summary of the texts of petitions entered in the register, together with the texts of the opinions and the most important decisions forwarded in connection with the examination of the petitions, shall be made available to the public in a database, provided the petitioner agrees. Confidential petitions shall be preserved in the records of Parliament, where they shall be available for inspection by Members.'

73 More specifically, petitions are, in principle, public documents, even though an exception to this rule may be applied at the request of the person concerned. As the Parliament stated at the hearing, any other conclusion would effectively impose on it an obligation of censorship in relation to the contents of the petition submitted by the applicant.

74 Consequently, it must be stated that in the present case, having regard to all the specific circumstances mentioned in paragraphs 64 to 73 above, the applicant provided a 'freely given and informed indication' of his wishes. A careful reading of the information provided by the Parliament should have enabled a reasonably observant petitioner to assess the full significance and consequences of his action. Furthermore, that indication of wishes was specific, as the Parliament informed the applicant that his complaint, the subject of which related inherently to the considerations mentioned in paragraph 70 above, would be accessible on the internet. Lastly, the applicant gave his express consent by ticking the boxes on the form relating to public consideration and recording on a register accessible on the internet, without the need for his consent to be inferred implicitly from any action.

75 All these circumstances mean that this case is fundamentally different from *V* v *Parliament* (judgment of 5 July 2011 in *V* v *Parliament*, F-46/09, ECR-SC, EU:F:2011:101, paragraph 138), in which the data subject had not given any consent to the transfer by the Commission to the Parliament of medical data concerning her.

76 In the light of all the above considerations, the Court holds that in the present case the applicant had given his express consent to the disclosure of the sensitive information in question in accordance with Article 10(2)(a) of Regulation No 45/2001.

77 Second, with regard to the personal data not mentioned in Article 10(1) of Regulation No 45/2001 (such as data relating to the applicant's career), processing is subject to the rules in Article 5 of Regulation No 45/2001. Under Article 5(d) of the regulation, data may be processed, inter alia, where the data subject has unambiguously given his or her consent. In other words, data may be processed where the data subject has given his or her consent with certainty and without ambiguity.

78 Whereas Article 10(2)(a) of Regulation No 45/2001 requires the consent to be express, under Article 5(d) of that regulation consent must be unambiguously given. As the EDPS has pointed out, it is logical, given the nature of sensitive personal data, that the conditions required for consent under Article 5(d) of Regulation No 45/2001 cannot be stricter than those laid down in Article 10(2)(a) of that regulation.

79 Consequently, reference should be made to the statements made in paragraphs 57 to 74 above, which must be applied *mutatis mutandis* in the present case to the processing of personal data other than the sensitive personal data concerning the applicant. In particular, as far as the objective of the petition is concerned, it relates specifically to the fact that an EU institution had not duly taken into account the applicant's personal situation for the purposes of his career.

80 In these circumstances, the Court considers that the applicant had unambiguously provided a 'freely given specific and informed indication' of his wishes in relation to the processing of his personal data by the Parliament, including their disclosure in the context of the processing of a petition by the Parliament.

81 As the justifications given in Article 5 of Regulation No 45/2001 for the processing of data are not cumulative, as is clear from the wording of that provision, there is no need to examine whether the processing of personal data was also justified under another of the provisions relied on by the Parliament.

82 Accordingly, the Court holds that the Parliament did not commit a sufficiently serious breach of a rule of law by disseminating the personal data in question on the internet.

83 Third, in so far as it states that the applicant's son has a severe mental or physical disability, the notice also contains sensitive personal data relating to the applicant's son, even though he is not named.

84 In the absence of any indication that the applicant is the legal representative of his son, the express consent given by him cannot justify the processing of those data by the Parliament under Article 10(2)(a) of Regulation No 45/2001.

85 However, the applicant's son is not a party to the present action. Furthermore, as has just been explained, there is no evidence that the applicant is the legal representative of his son or that he has been authorised to bring the present action on his behalf.

86 According to case-law, in order to ensure the effectiveness of the condition relating to the breach of a rule of law conferring rights on individuals, the protection offered by the rule invoked must be effective vis-à-vis the person who invokes it and that person must therefore be among those on whom the rule in question confers rights. A rule which does not protect the individual against the unlawfulness invoked by him, but protects another individual, cannot be accepted as a source of compensation (judgments of 12 September 2007 in *Nikolaou* v *Commission*, T-259/03, EU:T:2007:254, paragraph 44, and 9 July 2009 in *Ristic and Others* v *Commission*, T-238/07, EU:T:2009:263, paragraph 60). It follows that in his action for compensation the applicant cannot invoke unlawfulness resulting from the alleged breach of rights of a third party, namely his son.

– Subsequent to the request to remove the data from the website

87 It must then be examined whether the Parliament's conduct subsequent to the request to remove the applicant's personal data from its website could constitute a sufficiently serious breach of a rule of law intended to confer rights on individuals.

88 According to the applicant, when he requested the removal of personal data from the Parliament's website, the Parliament initially responded negatively and granted the request only following the intervention of his counsel, in contravention of the right to erasure of personal data. Furthermore, the fact that the Parliament agreed to erase the data suggests that it implicitly acknowledged the unlawfulness of the publication. Lastly, the applicant adds that the Parliament infringed Article 12 of the Implementing rules relating to Regulation No 45/2001.

89 In essence, the applicant's arguments raise two questions: first, whether he had the right to the removal of his personal data and, second, whether the Parliament dealt with that request diligently.

90 As regards the first question, it should be noted that Article 16 of Regulation No 45/2001 confers the right to seek the erasure of personal data only if the processing is unlawful (see, to that effect, judgment of 16 September 2009 in *Vinci* v *ECB*, F-130/07, ECR-SC, EU:F:2009:114, paragraphs 66 and 67), as the applicant himself recognises. That provision cannot therefore be relied on in support of request for erasure where the processing is lawful, as in the present case (see paragraph 52 et seq.). The fact that the Parliament decided to grant the request does not in itself imply recognition of the unlawfulness of the initial publication. It should be noted in this regard that the Parliament has explained that it erased the data as a courtesy.

91 Furthermore, under Article 18 of Regulation No 45/2001, the data subject has the right to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her, except where, inter alia, he or she has unambiguously given his consent in accordance with Article 5(d) of that regulation.

92 In addition, in so far as the processing of data in the present case was based on the consent of the data subject, it should be observed that Regulation No 45/2001 does not expressly provide for the possibility of withdrawing the consent initially given.

93 In the light of the above considerations, the Court considers that the applicant was not able to invoke a right of erasure of the personal data in question on the basis of Regulation No 45/2001. It should be added that the applicant has not legitimately invoked any other ground for his request for erasure. In any event the Parliament removed the data from its website even though there was no binding obligation to do so.

94 Lastly, it should be noted that *Google Spain and Google* (C-131/12, ECR, EU:C:2014:317), which concerned the 'right to be forgotten' on the internet, related to very different factual and legal circumstances to the present case. In particular, even though in that judgment the Court held, in essence, that such a right could exist in certain conditions, the provisions of Directive 95/46 on which the Court based its reasoning (Article 7(f), Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46) differ significantly from those at issue in this case, which is connected, in essence, with the issue of the consent of the data subject. Unlike in the present case, in *Google* the data subject had not given his consent to the initial publication of his personal data.

95 As regards the second question, the applicant has not claimed the breach of a rule or principle of law in the event that the initial publication by the Parliament was lawful, as was the case in this instance.

96 It should be noted that Article 12 of the Implementing rules relating to Regulation No 45/2001, relating to the right of erasure, provides in paragraph 3:

'The data controller shall reply within 15 working days of receiving a request for erasure. If the request is accepted, it shall be acted upon immediately. If the data controller deems the request unjustified, he or she shall have 15 working days within which to inform the data subject by means of a letter stating the grounds for the decision.'

97 It follows from that provision that the Parliament has 15 working days to reply to a request for erasure, whether or not it is well founded. In the present case, the applicant sent his request to the Commission's 'Europe Direct Contact Centre', which forwarded it to the Parliament on 10 April 2012. The Parliament replied to the request within the prescribed time limit. Contrary to the claim made by the applicant, the Parliament never rejected the request. In actual fact, as is clear from the replies of 20 April 2012, 24 September 2012 and 10 January 2013, the Parliament agreed to erase the data, whilst rightly stating that the publication was lawful.

98 The personal data were erased on around 8 October 2012, according to the Parliament, and on around 10 January 2013, according to the applicant.

99 In its defence, the Parliament stated that some time was needed to track down the documents which contained the applicant's data and to take the necessary technical measures. As the Parliament explained at the hearing in response to the Court's questions, complete removal from the internet is a technically difficult process. The Court considers that these technical difficulties explain the time needed by the Parliament, whose technical services had to take action on several occasions, to erase the data in question and that the Parliament did not initially refuse the applicant's request.

100 Article 12(3) of the Implementing rules relating to Regulation No 45/2001 provides that if the request is accepted, it must be acted upon immediately. That provision applies to situations in which the request is accepted because it is justified, namely because the processing is unlawful. In those circumstances, it is logical that it must be acted upon immediately. However, where, as in this case, the request is not justified, but is accepted as a courtesy, there is no reason to impose an obligation to act 'immediately'. In this case the Parliament is required only to act upon its undertaking within a reasonable period. In view of the explanations provided by the Parliament, the Court considers that in this instance it did not commit an unlawful act in the processing of the request for erasure, including in acting upon that request.

101 Accordingly, the Court holds that the Parliament did not commit a sufficiently serious breach of a rule of law subsequent to the request for erasure made by the applicant.

Rules relating to the protection of private life

102 With regard to the provisions relating to the protection of private life relied on by the applicant, under Article 6(3) TEU, fundamental rights, as guaranteed by the ECHR, constitute general principles of the Union's law, even though the Union is not party to the ECHR. On the other hand, the Convention on the Rights of Persons with Disabilities has been ratified by the Union.

103 However, irrespective of whether, having regard to their nature and general scheme (judgments of 23 November 1999 in *Portugal* v *Council*, C-149/96, ECR, EU:C:1999:574, paragraph 47, and 3 February 2005 in *Chiquita Brands and Others* v *Commission*, T-19/01, ECR, EU:T:2005:31, paragraph 114), the ECHR and the Convention on the Rights of Persons with Disabilities contain provisions intended to confer rights on individuals, it must be stated that the applicant simply claims an infringement of Article 22 of the Convention on the Rights of Persons with Disabilities without offering any specific arguments in support of that claim.

104 The same holds for the alleged infringement of Article 8 of the ECHR. In this regard, the applicant merely cites three judgments of the European Court of Human Rights which, in his view, show that the right to respect for private life includes the right to keep his state of health secret (European Court of Human Rights, *S. and Marper v. United Kingdom*, no. 30562/04 and 30566/04, 4 December 2008) and the right to non-disclosure of data concerning professional life (European Court of Human Rights, *Amann v. Switzerland*, no. 27798/95, 16 February 2000, and *Rotaru v. Romania*, no. 28341/95, 4 May 2000). However, those judgments concern situations which are very different from the situation in the present case, specifically the storage of biometric data of persons suspected of criminal offences, the interception of a business telephone call and the creation by the public authorities of a file containing various personal information.

105 Furthermore, the judgment of 5 October 1994 in *X* v *Commission* (C-404/92 P, ECR, EU:C:1994:361), cited by the applicant in support of his claims, also concerns a very different matter, in particular the Commission's refusal to recruit an individual who had allowed tests to be carried out which could point to possible infection with the Aids virus, despite his objection to such tests being performed. It should be stated that *V* v *Parliament*, cited in paragraph 75 above (EU:F:2011:101, paragraph 110 et seq.), also concerns a situation which is not comparable as it relates to the transfer of medical data of a former Commission employee to the Parliament without her consent, which led to the withdrawal of the offer of employment by the Parliament.

106 Consequently, in the light of the above considerations, it is difficult to identify a parallelism or similarity between the facts in those cases and the present situation which could support the applicant's arguments.

107 In addition, for the reasons given in paragraph 52 et seq., 'interference by a public authority' in private life within the meaning of Article 8 of the ECHR cannot be considered to exist where the applicant gives his consent to the disclosure of information as in the present case.

108 Consequently, the Court considers that the applicant has not established the existence of an infringement of the Convention on the Rights of Persons with Disabilities or of the ECHR by the Parliament.

109 Accordingly, the arguments relating to the unlawfulness of the Parliament's conduct must be rejected.

110 As the three conditions relating to the non-contractual liability of the European Union are cumulative (judgment of 10 July 2014 in *Nikolaou* v *Court of Auditors*, C-220/13 P, ECR, EU:C:2014:2057, paragraph 52), the action must be dismissed in its entirety, without it being necessary to examine the arguments relating to damage and the causal link. Nevertheless, the Court considers it appropriate to examine those arguments in the present case.

2. *Damage and the causal link*

Arguments of the parties

111 The applicant asserts that the unlawful conduct of the Parliament has caused him material and non-material damage.

112 First, the applicant submits that he was compelled to have recourse to the services of a legal counsel and that it was only after two letters of formal notice sent by his counsel that the Parliament removed the document from its website. The applicant thus incurred fees amounting to EUR 1 000, which represents his material damage.

113 Second, with regard to non-material damage, the applicant maintains that it stems from the Parliament's dismissive and dilatory attitude, which hurt him deeply and caused him considerable stress, as he was concerned that his son, who suffers from severe mental illness and is very fragile, could become aware of the published information. He estimates the non-material damage on an equitable basis at EUR 40 000.

114 In the reply, the applicant claims that the time which passed between publication and the request for erasure is irrelevant. He also asserts that he submitted his request for erasure immediately, as soon as he became aware of the publication of the data.

115 The applicant argues that there is a direct causal link between the unlawful conduct and the damage, as the damage is the result of the publication of the information by the Parliament and of the difficulties in obtaining the removal of the information.

116 The Parliament does not dispute that if the existence of unlawful conduct were established, the applicant would have suffered material damage of EUR 1 000 in respect of legal fees. However, it asserts that the applicant has not demonstrated that non-material damage exists.

117 Lastly, the Parliament does not dispute the existence of a causal link if the Court were to hold that there was unlawful conduct and that the applicant has suffered damage.

Findings of the Court

118 It should first be recalled that, according to case-law, with regard to the condition that damage must have been suffered, such damage must be actual and certain. By contrast, purely hypothetical and indeterminate damage does not give a right to compensation (judgment of 28 April 2010 in *BST* v *Commission*, T-452/05, ECR, EU:T:2010:167, paragraph 165). However, the requirement relating to the existence of certain damage is met where the damage is imminent and foreseeable with sufficient certainty, even if the damage cannot yet be precisely assessed (judgment of 14 January 1987 in *Zuckerfabrik Bedburg and Others* v *Council and Commission*, 281/84, ECR, EU:C:1987:3, paragraph 14).

119 It is for the party seeking to establish the European Union's liability to adduce proof as to the existence or extent of the damage alleged and to establish a sufficiently direct causal link between that damage and the conduct complained of on the part of the institution concerned (judgment in *BST* v *Commission*, cited in paragraph 118 above, EU:T:2010:167, paragraph 167).

120 The Parliament does not dispute the existence of the material damage claimed by the applicant, namely the fees for his legal counsel, if unlawful conduct were to exist.

121 With regard to non-material damage, on the other hand, the applicant has not demonstrated the existence of such damage. He has merely claimed that the Parliament's dismissive and dilatory attitude hurt him deeply and caused him considerable stress, without providing any evidence in support of this claim. Consequently, it cannot be accepted.

122 Accordingly, the applicant's arguments relating to the existence of non-material damage must be rejected.

123 Lastly, the existence of a causal link is accepted where there is a direct link of cause and effect between the wrongful act of the institution concerned and the damage pleaded, in respect of which applicants bear the burden of proof (judgment of 28 September 1999 in *Hautem* v *EIB*, T-140/97, ECR-SC,

EU:T:1999:176, paragraph 85). It is settled case-law that the damage must be a sufficiently direct consequence of the conduct complained of (judgment of 25 June 1997 in *Perillo* v *Commission*, T-7/96, ECR, EU:T:1997:94, paragraph 41).

124 According to case-law, although it is not possible to prohibit those concerned from seeking legal advice at the pre-litigation stage, it is their own decision and the institution concerned cannot be held liable for the consequences (judgments of 9 March 1978 in *Herpels* v *Commission*, 54/77, ECR, EU:C:1978:45, paragraph 48; 28 June 2007 in *Internationaler Hilfsfonds* v *Commission*, C-331/05 P, ECR, EU:C:2007:390, paragraph 24, and 8 July 2008 in *Franchet and Byk* v *Commission*, T-48/05, ECR, EU:T:2008:257, paragraph 415). The costs thus freely incurred by the person concerned cannot therefore be imputed to the Parliament (see, to that effect, judgment in *Internationaler Hilfsfonds* v *Commission*, EU:C:2007:390, paragraph 27). Consequently, there is no causal link between the alleged material damage suffered by the applicant and the actions by the Parliament.

125 The applicant's arguments concerning the causal link between the alleged unlawful conduct and the material damage must also therefore be rejected.

126 In those circumstances, the applicant's request for compensation for damage allegedly suffered must be rejected as unfounded.

Costs

127 Under Article 134(1) of the Rules of Procedure of the General Court, 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 applicant has been unsuccessful, he must be ordered to pay the costs, as applied for by the Parliament.

128 Under Article 138(1) of the Rules of Procedure, the EDPS must bear his own costs.

On those grounds,

THE GENERAL COURT (Sixth Chamber)

hereby:

1. Dismisses the action;

2. Orders CN to pay the costs of the European Parliament and to bear his own costs;

3. Orders the European Data Protection Supervisor (EDPS) to bear his own costs.

Frimodt Nielsen Dehousse Collins

Delivered in open court in Luxembourg on 3 December 2015.

[Signatures]

Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

21 December 2016*

(Reference for a preliminary ruling — Electronic communications — Processing of personal data — Confidentiality of electronic communications — Protection — Directive 2002/58/EC — Articles 5, 6 and 9 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 11 and Article 52(1) — National legislation — Providers of electronic communications services — Obligation relating to the general and indiscriminate retention of traffic and location data — National authorities — Access to data — No prior review by a court or independent administrative authority — Compatibility with EU law)

In Joined Cases C-203/15 and C-698/15,

REQUESTS for a preliminary ruling under Article 267 TFEU, made by the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England & Wales) (Civil Division) (United Kingdom), by decisions, respectively, of 29 April 2015 and 9 December 2015, received at the Court on 4 May 2015 and 28 December 2015, in the proceedings

Tele2 Sverige AB (C-203/15)

v

Post- och telestyrelsen,

and

Secretary of State for the Home Department (C-698/15)

v

Tom Watson,

Peter Brice,

Geoffrey Lewis,

interveners:

Open Rights Group,

Privacy International,

The Law Society of England and Wales,

* * Languages of the case: English and Swedish.

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, A. Tizzano, Vice-President, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), J.L. da Cruz Vilaça, E. Juhász and M. Vilaras, Presidents of the Chamber, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen and C. Lycourgos, Judges,

Advocate General: H. Saugmandsgaard Øe,

Registrar: C. Strömholm, Administrator,

having regard to the decision of the President of the Court of 1 February 2016 that Case C-698/15 should be determined pursuant to the expedited procedure provided for in Article 105(1) of the Rules of Procedure of the Court,

having regard to the written procedure and further to the hearing on 12 April 2016,

after considering the observations submitted on behalf of:

— Tele2 Sverige AB, by M. Johansson and N. Torgerzon, advokater, and by E. Lagerlöf and S. Backman,

— Mr Watson, by J. Welch and E. Norton, Solicitors, I. Steele, Advocate, B. Jaffey, Barrister, and D. Rose QC,

— Mr Brice and Mr Lewis, by A. Suterwalla and R. de Mello, Barristers, R. Drabble QC, and S. Luke, Solicitor,

— Open Rights Group and Privacy International, by D. Carey, Solicitor, and by R. Mehta and J. Simor, Barristers,

— The Law Society of England and Wales, by T. Hickman, Barrister, and by N. Turner,

— the Swedish Government, by A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren and L. Swedenborg, acting as Agents,

— the United Kingdom Government, by S. Brandon, L. Christie and V. Kaye, acting as Agents, and by D. Beard QC, G. Facenna QC, J. Eadie QC and S. Ford, Barrister,

— the Belgian Government, by J.-C. Halleux, S. Vanrie and C. Pochet, acting as Agents,

— the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,

— the Danish Government, by C. Thorning and M. Wolff, acting as Agents,

— the German Government, by T. Henze, M. Hellmann and J. Kemper, acting as Agents, and by M. Kottmann and U. Karpenstein, Rechtsanwalte,

— the Estonian Government, by K. Kraavi-Käerdi, acting as Agent,

— Ireland, by E. Creedon, L. Williams and A. Joyce, acting as Agents, and by D. Fennelly BL,

— the Spanish Government, by A. Rubio González, acting as Agent,

— the French Government, by G. de Bergues, D. Colas, F.-X. Bréchot and C. David, acting as Agents,

— the Cypriot Government, by K. Kleanthous, acting as Agent,

— the Hungarian Government, by M. Fehér and G. Koós, acting as Agents,

— the Netherlands Government, by M. Bulterman, M. Gijzen and. J. Langer, acting as Agents,

— the Polish Government, by B. Majczyna, acting as Agent,

— the Finnish Government, by J. Heliskoski, acting as Agent,

— the European Commission, by H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira and J. Vondung, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 19 July 2016,

gives the following

Judgment

1 These requests for a preliminary ruling concern the interpretation of Article 15(1) 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), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) ('Directive 2002/58'), read in the light of Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter').

2 The requests have been made in two proceedings between (i) Tele2 Sverige AB and Post- och telestyrelsen (the Swedish Post and Telecom Authority; 'PTS'), concerning an order sent by PTS to Tele2 Sverige requiring the latter to retain traffic and location data in relation to its subscribers and registered users (Case C-203/15), and (ii) Mr Tom Watson, Mr Peter Brice and Mr Geoffrey Lewis, on the one hand, and the Secretary of State for the Home Department (United Kingdom of Great Britain and Northern Ireland), on the other, concerning the conformity with EU law of Section 1 of the Data Retention and Investigatory Powers Act 2014 ('DRIPA') (Case C-698/15).

Legal context

EU law

Directive 2002/58

3 Recitals 2, 6, 7, 11, 21, 22, 26 and 30 of Directive 2002/58 state:

'(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by [the Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

...

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

...

(11) Like 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)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

...

(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.

(22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. ...

...

(26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data … may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the

publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. ...

...

(30) Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. ...'

4 Article 1 of Directive 2002/58, headed 'Scope and aim', provides:

'1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.'

5 Article 2 of Directive 2002/58, headed 'Definitions', provides:

'Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.

The following definitions shall also apply:

...

(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) "location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

...'

6 Article 3 of Directive 2002/58, headed ‘Services concerned’, provides:

‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.’

7 Article 4 of that directive, headed ‘Security of processing’, is worded as follows:

‘1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

1a. Without prejudice to Directive [95/46], the measures referred to in paragraph 1 shall at least:

— ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,

— protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and

— ensure the implementation of a security policy with respect to the processing of personal data.

...’

8 Article 5 of Directive 2002/58, headed ‘Confidentiality of the communications’, provides:

‘1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

...

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’

9 Article 6 of Directive 2002/58, headed ‘Traffic data’, provides:

‘1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

...

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.'

10 Article 9(1) of that directive, that article being headed 'Location data other than traffic data', provides:

'Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. …'

11 Article 15 of that directive, headed 'Application of certain provisions of Directive [95/46]', states:

'1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

...

1b. Providers shall establish internal procedures for responding to requests for access to users' personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive [95/46] shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

…’

Directive 95/46

12 Article 22 of Directive 95/46, which is in Chapter III of that directive, is worded as follows:

‘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.’

Directive 2006/24/EC

13 Article 1(2) of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), that article being headed ‘Subject matter and scope’, provided:

‘This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.’

14 Article 3 of that directive, headed ‘Obligation to retain data’, provided:

‘1. By way of derogation from Articles 5, 6 and 9 of [Directive 2002/58], Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.’

Swedish law

15 It is apparent from the order for reference in Case C-203/15 that the Swedish legislature, in order to transpose Directive 2006/24 into national law, amended the lagen (2003:389) om elektronisk kommunikation [Law (2003:389) on electronic communications; ‘the LEK’] and the förordningen (2003:396) om elektronisk kommunikation [Regulation (2003:396) on electronic communications]. Both of those texts, in the versions applicable to the dispute in the main proceedings, contain rules on the retention of electronic communications data and on access to that data by the national authorities.

16 Access to that data is, in addition, regulated by the lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Law (2012:278) on gathering of data relating to electronic communications as part of intelligence gathering by law enforcement authorities: ‘Law 2012:278’) and by the rättegångsbalken (Code of Judicial Procedure; ‘the RB’).

The obligation to retain electronic communications data

17 According to the information provided by the referring court in Case C-203/15, the provisions of Paragraph 16a of Chapter 6 of the LEK, read together with Paragraph 1 of Chapter 2 of that law, impose an obligation on providers of electronic communications services to retain data the retention of which was required by Directive 2006/24. The data concerned is that relating to subscriptions and all electronic communications necessary to trace and identify the source and destination of a communication; to determine its date, time, and type; to identify the communications equipment used and to establish the location of mobile communication equipment used at the start and end of each communication. The data which there is an obligation to retain is data generated or processed in the context of telephony services, telephony services which use a mobile connection, electronic messaging systems, internet access services and internet access capacity (connection mode) provision services. The obligation extends to data relating to unsuccessful communications. The obligation does not however extend to the content of communications.

18 Articles 38 to 43 of Regulation (2003:396) on electronic communications specify the categories of data that must be retained. As regards telephony services, there is the obligation to retain data relating to calls and numbers called and the identifiable dates and times of the start and end of the communication. As regards telephony services which use a mobile connection, additional obligations are imposed, covering, for example, the retention of location data at the start and end of the communication. As regards telephony services using an IP packet, data to be retained includes, in addition to data mentioned above, data relating to the IP addresses of the caller and the person called. As regards electronic messaging systems, data to be retained includes data relating to the numbers of senders and recipients, IP addresses or other messaging addresses. As regards internet access services, data to be retained includes, for example, data relating to the IP addresses of users and the traceable dates and times of logging into and out of the internet access service.

Data retention period

19 In accordance with Paragraph 16d of Chapter 6 of the LEK, the data covered by Paragraph 16a of that Chapter must be retained by the providers of electronic communications services for six months from the date of the end of communication. The data must then be immediately erased, unless otherwise provided in the second subparagraph of Paragraph 16d of that Chapter.

Access to retained data

20 Access to retained data by the national authorities is governed by the provisions of Law 2012:278, the LEK and the RB.

– Law 2012:278

21 In the context of intelligence gathering, the national police, the Säkerhetspolisen (the Swedish Security Service), and the Tullverket (the Swedish Customs Authority) may, on the basis of Paragraph 1 of Law 2012:278, on the conditions prescribed by that law and without informing the provider of an electronic communications network or a provider of an electronic communications service authorised under the LEK, undertake the collection of data relating to messages transmitted by an electronic communications network, the electronic communications equipment located in a specified geographical area and the geographical areas(s) where electronic communications equipment is or was located.

22 In accordance with Paragraphs 2 and 3 of Law 2012:278, data may, as a general rule, be collected if, depending on the circumstances, the measure is particularly necessary in order to avert, prevent or detect criminal activity involving one or more offences punishable by a term of imprisonment of at least two years, or one of the acts listed in Paragraph 3 of that law, referring to offences punishable by a term of imprisonment of less than two years. Any grounds supporting that measure must outweigh considerations relating to the harm or prejudice that may be caused to the person affected by that measure or to an interest opposing that measure. In accordance with Paragraph 5 of that law, the duration of the measure must not exceed one month.

23 The decision to implement such a measure is to be taken by the director of the authority concerned or by a person to whom that responsibility is delegated. The decision is not subject to prior review by a judicial authority or an independent administrative authority.

24 Under Paragraph 6 of Law 2012:278, the Säkerhets och integritetsskyddsnämnden (the Swedish Commission on Security and Integrity Protection) must be informed of any decision authorising the collection of data. In accordance with Paragraph 1 of Lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Law (2007:980) on the supervision of certain law enforcement activities), that authority is to oversee the application of the legislation by the law enforcement authorities.

– The LEK

25 Under Paragraph 22, first subparagraph, point 2, of Chapter 6 of the LEK, all providers of electronic communications services must disclose data relating to a subscription at the request of the prosecution authority, the national police, the Security Service or any other public law enforcement authority, if that data is connected with a presumed criminal offence. On the information provided by the referring court in Case C-203/15, it is not necessary that the offence be a serious crime.

– The RB

26 The RB governs the disclosure of retained data to the national authorities within the framework of preliminary investigations. In accordance with Paragraph 19 of Chapter 27 of the RB, 'placing electronic communications under surveillance' without the knowledge of third parties is, as a general rule, permitted within the framework of preliminary investigations that relate to, inter alia, offences punishable by a sentence of imprisonment of at least six months. The expression 'placing electronic communications under surveillance', under Paragraph 19 of Chapter 27 of the RB, means obtaining data without the knowledge of third parties that relates to a message transmitted by an electronic communications network, the electronic communications equipment located or having been located in a specific geographical area, and the geographical area(s) where specific electronic communications equipment is or has been located.

27 According to what is stated by the referring court in Case C-203/15, information on the content of a message may not be obtained on the basis of Paragraph 19 of Chapter 27 of the RB. As a general rule, placing electronic communications under surveillance may be ordered, under Paragraph 20 of Chapter 27 of the RB, only where there are reasonable grounds for suspicion that an individual has committed an offence and that the measure is particularly necessary for the purposes of the investigation: the subject of that investigation must moreover be an offence punishable by a sentence of imprisonment of at least two years, or attempts, preparation or conspiracy to commit such an offence. In accordance with Paragraph 21 of Chapter 27 of the RB, the prosecutor must, other than in cases of urgency, request from the court with jurisdiction authority to place electronic communications under surveillance.

The security and protection of retained data

28 Under Paragraph 3a of Chapter 6 of the LEK, providers of electronic communications services who are subject to an obligation to retain data must take appropriate technical and organisational measures to ensure the protection of data during processing. On the information provided by the referring court in Case C-203/15, Swedish law does not, however, make any provision as to where the data is to be retained.

United Kingdom law

DRIPA

29 Section 1 of DRIPA, headed 'Powers for retention of relevant communications data subject to safeguards', provides:

'(1) The Secretary of State may by notice (a "retention notice") require a public telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of the Regulation of Investigatory Powers Act 2000 (purposes for which communications data may be obtained).

(2) A retention notice may:

(a) relate to a particular operator or any description of operators;

(b) require the retention of all data or any description of data;

(c) specify the period or periods for which data is to be retained;

(d) contain other requirements, or restrictions, in relation to the retention of data;

(e) make different provision for different purposes;

(f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.

(3) The Secretary of State may by regulations make further provision about the retention of relevant communications data.

(4) Such provision may, in particular, include provision about:

(a) requirements before giving a retention notice;

(b) the maximum period for which data is to be retained under a retention notice;

(c) the content, giving, coming into force, review, variation or revocation of a retention notice;

(d) the integrity, security or protection of, access to, or the disclosure or destruction of, data retained by virtue of this section;

(e) the enforcement of, or auditing compliance with, relevant requirements or restrictions;

(f) a code of practice in relation to relevant requirements or restrictions or relevant power;

(g) the reimbursement by the Secretary of State (with or without conditions) of expenses incurred by public telecommunications operators in complying with relevant requirements or restrictions;

(h) the [Data Retention (EC Directive) Regulations 2009] ceasing to have effect and the transition to the retention of data by virtue of this section.

(5) The maximum period provided for by virtue of subsection (4)(b) must not exceed 12 months beginning with such day as is specified in relation to the data concerned by regulations under subsection (3).

...'

30 Section 2 of DRIPA defines the expression 'relevant communications data' as meaning 'communications data of the kind mentioned in the Schedule to the [Data Retention (EC Directive) Regulations 2009] so far as such data is generated or processed in the United Kingdom by public telecommunications operators in the process of supplying the telecommunications services concerned'.

RIPA

31 Section 21(4) of the Regulation of Investigatory Powers Act 2000 ('RIPA'), that section being in Chapter II of that act and headed 'Lawful acquisition and disclosure of communications data', states:

'In this Chapter "communications data" means any of the following:

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person:

(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service'.

32 On the information provided in the order for reference in Case C-698/15, that data includes 'user location data', but not data relating to the content of a communication.

33 As regards access to retained data, Section 22 of RIPA provides:

'(1) This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data.

(2) It is necessary on grounds falling within this subsection to obtain communications data if it is necessary:

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing disorder;

(c) in the interests of the economic well-being of the United Kingdom;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

(g) or the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

(h) or any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

…

(4) Subject to subsection (5), where it appears to the designated person that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice to the postal or telecommunications operator, require the operator:

(a) if the operator is not already in possession of the data, to obtain the data; and

(b) in any case, to disclose all of the data in his possession or subsequently obtained by him.

(5) The designated person shall not grant an authorisation under subsection (3) or give a notice under subsection (4), unless he believes that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining the data.'

34 Under Section 65 of RIPA, complaints may be made to the Investigatory Powers Tribunal (United Kingdom) if there is reason to believe that data has been acquired inappropriately.

The Data Retention Regulations 2014

35 The Data Retention Regulations 2014 ('the 2014 Regulations'), adopted on the basis of DRIPA, are divided into three parts, Part 2 containing regulations 2 to 14 of that legislation. Regulation 4, headed 'Retention notices', provides:

'(1) A retention notice must specify:

(a) the public telecommunications operator (or description of operators) to whom it relates,

(b) the relevant communications data which is to be retained,

(c) the period or periods for which the data is to be retained,

(d) any other requirements, or any restrictions, in relation to the retention of the data.

(2) A retention notice must not require any data to be retained for more than 12 months beginning with:

(a) in the case of traffic data or service use data, the day of the communication concerned, and

(b) in the case of subscriber data, the day on which the person concerned leaves the telecommunications service concerned or (if earlier) the day on which the data is changed.

...'

36 Regulation 7 of the 2014 Regulations, headed 'Data integrity and security', provides:

'(1) A public telecommunications operator who retains communications data by virtue of section 1 of [DRIPA] must:

(a) secure that the data is of the same integrity and subject to at least the same security and protection as the data on any system from which it is derived,

(b) secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and

(c) protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure.

(2) A public telecommunications operator who retains communications data by virtue of section 1 of [DRIPA] must destroy the data if the retention of the data ceases to be authorised by virtue of that section and is not otherwise authorised by law.

(3) The requirement in paragraph (2) to destroy the data is a requirement to delete the data in such a way as to make access to the data impossible.

(4) It is sufficient for the operator to make arrangements for the deletion of the data to take place at such monthly or shorter intervals as appear to the operator to be practicable.'

37 Regulation 8 of the 2014 Regulations, headed Disclosure of retained data', provides:

'(1) A public telecommunications operator must put in place adequate security systems (including technical and organisational measures) governing access to communications data retained by virtue of section 1 of [DRIPA] in order to protect against any disclosure of a kind which does not fall within section 1(6)(a) of [DRIPA].

(2) A public telecommunications operator who retains communications data by virtue of section 1 of [DRIPA] must retain the data in such a way that it can be transmitted without undue delay in response to requests.'

38 Regulation 9 of the 2014 Regulations, headed 'Oversight by the Information Commissioner', states:

'The Information Commissioner must audit compliance with requirements or restrictions imposed by this Part in relation to the integrity, security or destruction of data retained by virtue of section 1 of [DRIPA].'

The Code of Practice

39 The Acquisition and Disclosure of Communications Data Code of Practice ('the Code of Practice') contains, in paragraphs 2.5 to 2.9 and 2.36 to 2.45, guidance on the necessity for and proportionality of obtaining communications data. As explained by the referring court in Case C-698/15, particular attention must, in accordance with paragraphs 3.72 to 3.77 of that code, be paid to necessity and proportionality where the communications data sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information.

40 Under paragraph 3.78 to 3.84 of that code, a court order is required in the specific case of an application for communications data that is made in order to identify a journalist's source. Under paragraphs 3.85 to 3.87 of that code, judicial approval is required when an application for access is made by local authorities. No authorisation, on the other hand, need be obtained from a court or any independent body with respect to access to communications data protected by legal professional privilege or relating to doctors of medicine, Members of Parliament or ministers of religion.

41 Paragraph 7.1 of the Code of Practice provides that communications data acquired or obtained under the provisions of RIPA, and all copies, extracts and summaries of that data, must be handled and stored securely. In additions, the requirements of the Data Protection Act must be adhered to.

42 In accordance with paragraph 7.18 of the Code of Practice, where a United Kingdom public authority is considering the possible disclosure to overseas authorities of communications data, it must, inter alia, consider whether that data will be adequately protected. However, it is stated in paragraph 7.22 of that code that a transfer of data to a third country may take place where that transfer is necessary for reasons of substantial public interest, even where the third country does not provide an adequate level of protection. On the information given by the referring court in Case C-698/15, the Secretary of State for the Home Department may issue a national security certificate that exempts certain data from the provisions of the legislation.

43 In paragraph 8.1 of that code, it is stated that RIPA established the Interception of Communications Commissioner (United Kingdom), whose remit is, inter alia, to provide independent oversight of the exercise and performance of the powers and duties contained in Chapter II of Part I of RIPA. As is stated in paragraph 8.3 of the code, the Commissioner may, where he can 'establish that an individual has been adversely affected by any wilful or reckless failure', inform that individual of suspected unlawful use of powers.

The disputes in the main proceedings and the questions referred for a preliminary ruling

Case C-203/15

44 On 9 April 2014, Tele2 Sverige, a provider of electronic communications services established in Sweden, informed the PTS that, following the ruling in the judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12; 'the *Digital Rights* judgment', EU:C:2014:238) that Directive 2006/24 was invalid, it would cease, as from 14 April 2014, to retain electronic communications data, covered by the LEK, and that it would erase data retained prior to that date.

45 On 15 April 2014, the Rikspolisstyrelsen (the Swedish National Police Authority, Sweden) sent to the PTS a complaint to the effect that Tele2 Sverige had ceased to send to it the data concerned.

46 On 29 April 2014, the justitieminister (Swedish Minister for Justice) appointed a special reporter to examine the Swedish legislation at issue in the light of the *Digital Rights* judgment. In a report dated 13 June 2014, entitled 'Datalagring, EU-rätten och svensk rätt, Ds 2014:23' (Data retention, EU law

and Swedish law; 'the 2014 report'), the special reporter concluded that the national legislation on the retention of data, as set out in Paragraphs 16a to 16f of the LEK, was not incompatible with either EU law or the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 ('the ECHR'). The special reporter emphasised that the *Digital Rights* judgment could not be interpreted as meaning that the general and indiscriminate retention of data was to be condemned as a matter of principle. From his perspective, neither should the *Digital Rights* judgment be understood as meaning that the Court had established, in that judgment, a set of criteria all of which had to be satisfied if legislation was to be able to be regarded as proportionate. He considered that it was necessary to assess all the circumstances in order to determine the compatibility of the Swedish legislation with EU law, such as the extent of data retention in the light of the provisions on access to data, on the duration of retention, and on the protection and the security of data.

47 On that basis, on 19 June 2014 the PTS informed Tele2 Sverige that it was in breach of its obligations under the national legislation in failing to retain the data covered by the LEK for six months, for the purpose of combating crime. By an order of 27 June 2014, the PTS ordered Tele2 Sverige to commence, by no later than 25 July 2014, the retention of that data.

48 Tele2 Sverige considered that the 2014 report was based on a misinterpretation of the *Digital Rights* judgment and that the obligation to retain data was in breach of the fundamental rights guaranteed by the Charter, and therefore brought an action before the Förvaltningsrätten i Stockholm (Administrative Court, Stockholm) challenging the order of 27 June 2014. Since that court dismissed the action, by judgment of 13 October 2014, Tele2 Sverige brought an appeal against that judgment before the referring court.

49 In the opinion of the referring court, the compatibility of the Swedish legislation with EU law should be assessed with regard to Article 15(1) of Directive 2002/58. While that directive establishes the general rule that traffic and location data should be erased or made anonymous when no longer required for the transmission of a communication, Article 15(1) of that directive introduces a derogation from that general rule since it permits the Member States, where justified on one of the specified grounds, to restrict that obligation to erase or render anonymous, or even to make provision for the retention of data. Accordingly, EU law allows, in certain situations, the retention of electronic communications data.

50 The referring court nonetheless seeks to ascertain whether a general and indiscriminate obligation to retain electronic communications data, such as that at issue in the main proceedings, is compatible, taking into consideration the *Digital Rights* judgment, with Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter. Given that the opinions of the parties differ on that point, it is necessary that the Court give an unequivocal ruling on whether, as maintained by Tele2 Sverige, the general and indiscriminate retention of electronic communications data is per se incompatible with Articles 7 and 8 and Article 52(1) of the Charter, or whether, as stated in the 2014 Report, the compatibility of such retention of data is to be assessed in the light of provisions relating to access to the data, the protection and security of the data and the duration of retention.

51 In those circumstances the Kammarrätten i Stockholm (Administrative Court of Appeal of Stockholm, Sweden) decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:

'(1) Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime … compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter?

(2) If the answer to question 1 is in the negative, may the retention nevertheless be permitted where:

(a) access by the national authorities to the retained data is determined as [described in paragraphs 19 to 36 of the order for reference], and

(b) data protection and security requirements are regulated as [described in paragraphs 38 to 43 of the order for reference], and

(c) all relevant data is to be retained for six months, calculated as from the day when the communication is ended, and subsequently erased as [described in paragraph 37 of the order for reference]?'

Case C-698/15

52 Mr Watson, Mr Brice and Mr Lewis each lodged, before the High Court of Justice (England & Wales), Queen's Bench Division (Divisional Court) (United Kingdom), applications for judicial review of the legality of Section 1 of DRIPA, claiming, inter alia, that that section is incompatible with Articles 7 and 8 of the Charter and Article 8 of the ECHR.

53 By judgment of 17 July 2015, the High Court of Justice (England & Wales), Queen's Bench Division (Divisional Court) held that the *Digital Rights* judgment laid down 'mandatory requirements of EU law' applicable to the legislation of Member States on the retention of communications data and access to such data. According to the High Court of Justice, since the Court, in that judgment, held that Directive 2006/24 was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. It follows from the underlying logic of the *Digital Rights* judgment that legislation that establishes a general body of rules for the retention of communications data is in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation is complemented by a body of rules for access to the data, defined by national law, which provides sufficient safeguards to protect those rights. Accordingly, Section 1 of DRIPA is not compatible with Articles 7 and 8 of the Charter in so far as it does not lay down clear and precise rules providing for access to and use of retained data and in so far as access to that data is not made dependent on prior review by a court or an independent administrative body.

54 The Secretary of State for the Home Department brought an appeal against that judgment before the Court of Appeal (England & Wales) (Civil Division) (United Kingdom).

55 That court states that Section 1(1) of DRIPA empowers the Secretary of State for the Home Department to adopt, without any prior authorisation from a court or an independent administrative body, a general regime requiring public telecommunications operators to retain all data relating to any postal service or any telecommunications service for a maximum period of 12 months if he/she considers that such a requirement is necessary and proportionate to achieve the purposes stated in the United Kingdom legislation. Even though that data does not include the content of a communication, it could be highly intrusive into the privacy of users of communications services.

56 In the order for reference and in its judgment of 20 November 2015, delivered in the appeal procedure, wherein it decided to send to the Court this request for a preliminary ruling, the referring court considers that the national rules on the retention of data necessarily fall within the scope of Article 15(1) of Directive 2002/58 and must therefore conform to the requirements of the Charter. However, as stated in Article 1(3) of that directive, the EU legislature did not harmonise the rules relating to access to retained data.

57 As regards the effect of the *Digital Rights* judgment on the issues raised in the main proceedings, the referring court states that, in the case that gave rise to that judgment, the Court was considering the validity of Directive 2006/24 and not the validity of any national legislation. Having regard, inter alia, to the close relationship between the retention of data and access to that data, it was essential that that directive should incorporate a set of safeguards and that the *Digital Rights* judgment should analyse, when examining the lawfulness of the data retention regime established by that directive, the rules relating to access to that data. The Court had not therefore intended to lay down, in that judgment, mandatory requirements applicable to national legislation on access to data that does not implement EU law. Further, the reasoning of the Court was closely linked to the objective pursued by Directive 2006/24. National legislation should, however, be assessed in the light of the objectives pursued by that legislation and its context.

58 As regards the need to refer questions to the Court for a preliminary ruling, the referring court draws attention to the fact that, when the order for reference was issued, six courts in other Member States, five of those courts being courts of last resort, had declared national legislation to be invalid on the basis of the *Digital Rights* judgment. The answer to the questions referred is therefore not obvious, although the answer is required to give a ruling on the cases brought before that court.

59 In those circumstances, the Court of Appeal (England & Wales) (Civil Division) decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:

‘(1) Does [the *Digital Rights* judgment] (including, in particular, paragraphs 60 to 62 thereof) lay down mandatory requirements of EU law applicable to a Member State’s domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of [the Charter]?

(2) Does [the *Digital Rights* judgment] expand the scope of Articles 7 and/or 8 of [the Charter] beyond that of Article 8 of the European Convention of Human Rights … as established in the jurisprudence of the European Court of Human Rights …?’

The procedure before the Court

60 By order of 1 February 2016, *Davis and Others* (C-698/15, not published, EU:C:2016:70), the President of the Court decided to grant the request of the Court of Appeal (England & Wales) (Civil Division) that Case C-698/15 should be dealt with under the expedited procedure provided for in Article 105(1) of the Court’s Rules of Procedure.

61 By decision of the President of the Court of 10 March 2016, Cases C-203/15 and C-698/15 were joined for the purposes of the oral part of the procedure and the judgment.

Consideration of the questions referred for a preliminary ruling

The first question in Case C-203/15

62 By the first question in Case C-203/15, the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm) seeks, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter, must be interpreted as precluding national legislation such as that at issue in the main proceedings that provides, for the purpose of fighting crime, for general and indiscriminate retention of all traffic and location data of all subscribers and registered users with respect to all means of electronic communications.

63 That question arises, in particular, from the fact that Directive 2006/24, which the national legislation at issue in the main proceedings was intended to transpose, was declared to be invalid by the *Digital Rights* judgment, though the parties disagree on the scope of that judgment and its effect on that legislation, given that it governs the retention of traffic and location data and access to that data by the national authorities.

64 It is necessary first to examine whether national legislation such as that at issue in the main proceeding falls within the scope of EU law.

The scope of Directive 2002/58

65 The Member States that have submitted written observations to the Court have differed in their opinions as to whether and to what extent national legislation on the retention of traffic and location data and access to that data by the national authorities, for the purpose of combating crime, falls within the scope of Directive 2002/58. Whereas, in particular, the Belgian, Danish, German and Estonian Governments, Ireland and the Netherlands Government have expressed the opinion that the answer is that it does, the Czech Government has proposed that the answer is that it does not, since the sole objective of such legislation is to combat crime. The United Kingdom Government, for its part, argues that only legislation relating to the retention of data, but not legislation relating to the access to that data by the competent national law enforcement authorities, falls within the scope of that directive.

66 As regards, finally, the Commission, while it maintained, in its written observations submitted to the Court in Case C-203/15, that the national legislation at issue in the main proceedings falls within the scope of Directive 2002/58, the Commission argues, in its written observations in Case C-698/15, that only national rules relating to the retention of data, and not those relating to the access of the national authorities to that data, fall within the scope of that directive. The latter rules should, however, according to the Commission, be taken into consideration in order to assess whether national legislation governing the retention of data by providers of electronic communications services constitutes a proportionate interference in the fundamental rights guaranteed in Articles 7 and 8 of the Charter.

67 In that regard, it must be observed that a determination of the scope of Directive 2002/58 must take into consideration, inter alia, the general structure of that directive.

68 Article 1(1) of Directive 2002/58 indicates that the directive provides, inter alia, for the harmonisation of the provisions of national law required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector.

69 Article 1(3) of that directive excludes from its scope 'activities of the State' in specified fields, including the activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters (see, by analogy, with respect to the first indent of Article 3(2) of Directive 95/46, judgments of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596, paragraph 43, and of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, EU:C:2008:727, paragraph 41).

70 Article 3 of Directive 2002/58 states that the directive is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices ('electronic communications services'). Consequently, that directive must be regarded as regulating the activities of the providers of such services.

71 Article 15(1) of Directive 2002/58 states that Member States may adopt, subject to the conditions laid down, 'legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 [of that directive]'. The second sentence of Article 15(1) of that directive identifies, as an example of measures that may thus be adopted by Member States, measures 'providing for the retention of data'.

72 Admittedly, the legislative measures that are referred to in Article 15(1) of Directive 2002/58 concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 51). Moreover, the objectives which, under that provision, such measures must pursue, such as safeguarding national security, defence and public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that directive.

73 However, having regard to the general structure of Directive 2002/58, the factors identified in the preceding paragraph of this judgment do not permit the conclusion that the legislative measures referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.

74 Further, the legislative measures referred to in Article 15(1) of Directive 2002/58 govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services. Accordingly, Article 15(1), read together with Article 3 of that directive, must be interpreted as meaning that such legislative measures fall within the scope of that directive.

75 The scope of that directive extends, in particular, to a legislative measure, such as that at issue in the main proceedings, that requires such providers to retain traffic and location data, since to do so necessarily involves the processing, by those providers, of personal data.

76 The scope of that directive also extends to a legislative measure relating, as in the main proceedings, to the access of the national authorities to the data retained by the providers of electronic communications services.

77 The protection of the confidentiality of electronic communications and related traffic data, guaranteed in Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies. As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, including 'any data related to such communications', in order to protect the confidentiality of electronic communications.

78 In those circumstances, a legislative measure whereby a Member State, on the basis of Article 15(1) of Directive 2002/58, requires providers of electronic communications services, for the purposes set out in that provision, to grant national authorities, on the conditions laid down in such a measure, access to the data retained by those providers, concerns the processing of personal data by those providers, and that processing falls within the scope of that directive.

79 Further, since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained by the providers of electronic communications services.

80 That interpretation is confirmed by Article 15(1b) of Directive 2002/58, which provides that providers are to establish internal procedures for responding to requests for access to users' personal data, based on provisions of national law adopted pursuant to Article 15(1) of that directive.

81 It follows from the foregoing that national legislation, such as that at issue in the main proceedings in Cases C-203/15 and C-698/15, falls within the scope of Directive 2002/58.

The interpretation of Article 15(1) of Directive 2002/58, in the light of Articles 7, 8, 11 and Article 52(1) of the Charter

82 It must be observed that, according to Article 1(2) of Directive 2002/58, the provisions of that directive 'particularise and complement' Directive 95/46. As stated in its recital 2, Directive 2002/58 seeks to ensure, in particular, full respect for the rights set out in Articles 7 and 8 of the Charter. In that regard, it is clear from the explanatory memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 final), which led to Directive 2002/58, that the EU legislature sought 'to ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used'.

83 To that end, Directive 2002/58 contains specific provisions designed, as is apparent from, in particular, recitals 6 and 7 of that directive, to offer to the users of electronic communications services protection against risks to their personal data and privacy that arise from new technology and the increasing capacity for automated storage and processing of data.

84 In particular, Article 5(1) of that directive provides that the Member States must ensure, by means of their national legislation, the confidentiality of communications effected by means of a public communications network and publicly available electronic communications services, and the confidentiality of the related traffic data.

85 The principle of confidentiality of communications established by Directive 2002/58 implies, inter alia, as stated in the second sentence of Article 5(1) of that directive, that, as a general rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons lawfully authorised in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 47).

86 Accordingly, as confirmed by recitals 22 and 26 of Directive 2002/58, under Article 6 of that directive, the processing and storage of traffic data are permitted only to the extent necessary and for the time necessary for the billing and marketing of services and the provision of value added services (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraphs 47 and 48). As regards, in particular, the billing of services, that processing is permitted only up to the end of the period during which the bill may be lawfully challenged or legal proceedings brought to obtain payment. Once that period has elapsed, the data processed and stored must be erased or made anonymous. As regards location data other than traffic data, Article 9(1) of that directive provides that that data may be processed only subject to certain conditions and after it has been made anonymous or the consent of the users or subscribers obtained.

87 The scope of Article 5, Article 6 and Article 9(1) of Directive 2002/58, which seek to ensure the confidentiality of communications and related data, and to minimise the risks of misuse, must moreover be assessed in the light of recital 30 of that directive, which states: 'Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum'.

88 Admittedly, Article 15(1) of Directive 2002/58 enables the Member States to introduce exceptions to the obligation of principle, laid down in Article 5(1) of that directive, to ensure the confidentiality of personal data, and to the corresponding obligations, referred to in Articles 6 and 9 of that directive (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 50).

89 Nonetheless, in so far as Article 15(1) of Directive 2002/58 enables Member States to restrict the scope of the obligation of principle to ensure the confidentiality of communications and related traffic data, that provision must, in accordance with the Court's settled case-law, be interpreted strictly (see, by analogy, judgment of 22 November 2012, *Probst*, C-119/12, EU:C:2012:748, paragraph 23). That provision cannot, therefore, permit the exception to that obligation of principle and, in particular, to the prohibition on storage of data, laid down in Article 5 of Directive 2002/58, to become the rule, if the latter provision is not to be rendered largely meaningless.

90 It must, in that regard, be observed that the first sentence of Article 15(1) of Directive 2002/58 provides that the objectives pursued by the legislative measures that it covers, which derogate from the principle of confidentiality of communications and related traffic data, must be 'to safeguard national security — that is, State security — defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system', or one of the other objectives specified in Article 13(1) of Directive 95/46, to which the first sentence of Article 15(1) of Directive 2002/58 refers (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 53). That list of objectives is exhaustive, as is apparent from the second sentence of Article 15(1) of Directive 2002/58, which states that the legislative measures must be justified on 'the grounds laid down' in the first sentence of Article 15(1) of that directive. Accordingly, the Member States cannot adopt such measures for purposes other than those listed in that latter provision.

91 Further, the third sentence of Article 15(1) of Directive 2002/58 provides that '[a]ll the measures referred to [in Article 15(1)] shall be in accordance with the general principles of [European Union] law, including those referred to in Article 6(1) and (2) [EU]', which include the general principles and fundamental rights now guaranteed by the Charter. Article 15(1) of Directive 2002/58 must, therefore, be interpreted in the light of the fundamental rights guaranteed by the Charter (see, by analogy, in relation to Directive 95/46, judgments of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; of 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 68, and of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 38).

92 In that regard, it must be emphasised that the obligation imposed on providers of electronic communications services, by national legislation such as that at issue in the main proceedings, to retain traffic data in order, when necessary, to make that data available to the competent national authorities, raises questions relating to compatibility not only with Articles 7 and 8 of the Charter, which are expressly referred to in the questions referred for a preliminary ruling, but also with the freedom of expression guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraphs 25 and 70).

93 Accordingly, the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 of the Charter, as derived from the Court's case-law (see, to that effect, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 39 and the case-law cited), must be taken into consideration in interpreting Article 15(1) of

Directive 2002/58. The same is true of the right to freedom of expression in the light of the particular importance accorded to that freedom in any democratic society. That fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (see, to that effect, judgments of 12 June 2003, *Schmidberger*, C-112/00, EU:C:2003:333, paragraph 79, and of 6 September 2011, *Patriciello*, C-163/10, EU:C:2011:543, paragraph 31).

94 In that regard, it must be recalled that, under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of those rights and freedoms. With due regard to the principle of proportionality, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (judgment of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 50).

95 With respect to that last issue, the first sentence of Article 15(1) of Directive 2002/58 provides that Member States may adopt a measure that derogates from the principle of confidentiality of communications and related traffic data where it is a 'necessary, appropriate and proportionate measure within a democratic society', in view of the objectives laid down in that provision. As regards recital 11 of that directive, it states that a measure of that kind must be 'strictly' proportionate to the intended purpose. In relation to, in particular, the retention of data, the requirement laid down in the second sentence of Article 15(1) of that directive is that data should be retained 'for a limited period' and be 'justified' by reference to one of the objectives stated in the first sentence of Article 15(1) of that directive.

96 Due regard to the principle of proportionality also derives from the Court's settled case-law to the effect that the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary (judgments of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, EU:C:2008:727, paragraph 56; of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 77; the *Digital Rights* judgment, paragraph 52, and of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 92).

97 As regards whether national legislation, such as that at issue in Case C-203/15, satisfies those conditions, it must be observed that that legislation provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions. As stated in the order for reference, the categories of data covered by that legislation correspond, in essence, to the data whose retention was required by Directive 2006/24.

98 The data which providers of electronic communications services must therefore retain makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment. That data includes, inter alia, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data makes it possible, in particular, to identify the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. Further, that data makes it possible to know how often the subscriber or registered user communicated with certain persons in a given period (see, by analogy, with respect to Directive 2006/24, the *Digital Rights* judgment, paragraph 26).

99 That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, by analogy, in relation to Directive 2006/24, the *Digital Rights judgment*, paragraph 27). In particular, that data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.

100 The interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 37).

101 Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 39), the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 28).

102 Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 60).

103 Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 51).

104 In that regard, it must be observed, first, that the effect of such legislation, in the light of its characteristic features as described in paragraph 97 of the present judgment, is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.

105 Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraphs 57 and 58).

106 Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 59).

107 National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

108 However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.

109 In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 54 and the case-law cited).

110 Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

111 As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.

112 Having regard to all of the foregoing, the answer to the first question referred in Case C-203/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

The second question in Case C-203/15 and the first question in Case C-698/15

113 It must, at the outset, be noted that the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm) referred the second question in Case C-203/15 only in the event that the answer to the first question in that case was negative. That second question, however, arises irrespective of whether retention of data is generalised or targeted, as set out in paragraphs 108 to 111 of this judgment. Accordingly, the Court must answer the second question in Case C-203/15 together with the first question in Case C-698/15, which is referred regardless of the extent of the obligation to retain data that is imposed on providers of electronic communications services.

114 By the second question in Case C-203/15 and the first question in Case C-698/15, the referring courts seek, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data, and more particularly, the access of the competent national authorities to retained data, where that legislation does not restrict that access solely to the objective of fighting serious crime, where that access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

115 As regards objectives that are capable of justifying national legislation that derogates from the principle of confidentiality of electronic communications, it must be borne in mind that, since, as stated in paragraphs 90 and 102 of this judgment, the list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58 is exhaustive, access to the retained data must correspond, genuinely and strictly, to one of those objectives. Further, since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data.

116 As regards compatibility with the principle of proportionality, national legislation governing the conditions under which the providers of electronic communications services must grant the competent national authorities access to the retained data must ensure, in accordance with what was stated in paragraphs 95 and 96 of this judgment, that such access does not exceed the limits of what is strictly necessary.

117 Further, since the legislative measures referred to in Article 15(1) of Directive 2002/58 must, in accordance with recital 11 of that directive, 'be subject to adequate safeguards', a data retention measure must, as follows from the case-law cited in paragraph 109 of this judgment, lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law.

118 In order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in Article 15(1) of Directive 2002/58, even if that objective is to fight serious crime. That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 61).

119 Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the

circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime (see, by analogy, ECtHR, 4 December 2015, *Zakharov v. Russia*, CE:ECHR:2015:1204JUD004714306, § 260). However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.

120 In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 62; see also, by analogy, in relation to Article 8 of the ECHR, ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary*, CE:ECHR:2016:0112JUD003713814, §§ 77 and 80).

121 Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed (see, by analogy, judgments of 7 May 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 52, and of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 95).

122 With respect to the rules relating to the security and protection of data retained by providers of electronic communications services, it must be noted that Article 15(1) of Directive 2002/58 does not allow Member States to derogate from Article 4(1) and Article 4(1a) of that directive. Those provisions require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraphs 66 to 68).

123 In any event, the Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data (see, to that effect, the *Digital Rights* judgment, paragraph 68, and the judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraphs 41 and 58).

124 It is the task of the referring courts to determine whether and to what extent the national legislation at issue in the main proceedings satisfies the requirements stemming from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as set out in paragraphs 115 to 123 of this judgment, with respect to both the access of the competent national authorities to the retained data and the protection and level of security of that data.

125 Having regard to all of the foregoing, the answer to the second question in Case C-203/15 and to the first question in Case C-698/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

The second question in Case C-698/15

126 By the second question in Case C-698/15, the Court of Appeal (England & Wales) (Civil Division) seeks in essence to ascertain whether, in the *Digital Rights* judgment, the Court interpreted Articles 7 and/or 8 of the Charter in such a way as to expand the scope conferred on Article 8 ECHR by the European Court of Human Rights.

127 As a preliminary point, it should be recalled that, whilst, as Article 6(3) TEU confirms, fundamental rights recognised by the ECHR constitute general principles of EU law, the ECHR does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law (see, to that effect, judgment of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 45 and the case-law cited).

128 Accordingly, the interpretation of Directive 2002/58, which is at issue in this case, must be undertaken solely in the light of the fundamental rights guaranteed by the Charter (see, to that effect, judgment of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 46 and the case-law cited).

129 Further, it must be borne in mind that the explanation on Article 52 of the Charter indicates that paragraph 3 of that article is intended to ensure the necessary consistency between the Charter and the ECHR, 'without thereby adversely affecting the autonomy of Union law and … that of the Court of Justice of the European Union' (judgment of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 47). In particular, as expressly stated in the second sentence of Article 52(3) of the Charter, the first sentence of Article 52(3) does not preclude Union law from providing protection that is more extensive then the ECHR. It should be added, finally, that Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR.

130 However, in accordance with the Court's settled case-law, the justification for making a request for a preliminary ruling is not for advisory opinions to be delivered on general or hypothetical questions, but rather that it is necessary for the effective resolution of a dispute concerning EU law (see, to that effect, judgments of 24 April 2012, *Kamberaj*, C-571/10, EU:C:2012:233, paragraph 41; of 26 February 2013, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, paragraph 42, and of 27 February 2014, *Pohotovosť*, C-470/12, EU:C:2014:101 paragraph 29).

131 In this case, in view of the considerations set out, in particular, in paragraphs 128 and 129 of the present judgment, the question whether the protection conferred by Articles 7 and 8 of the Charter is wider than that guaranteed in Article 8 of the ECHR is not such as to affect the interpretation of Directive 2002/58, read in the light of the Charter, which is the matter in dispute in the proceedings in Case C-698/15.

132 Accordingly, it does not appear that an answer to the second question in Case C-698/15 can provide any interpretation of points of EU law that is required for the resolution, in the light of that law, of that dispute.

133 It follows that the second question in Case C-698/15 is inadmissible.

Costs

134 Since these proceedings are, for the parties to the main proceedings, a step in the actions pending before the national courts, the decision on costs is a matter for those courts. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

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

1. **Article 15(1) 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), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.**

2. **Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.**

3. **The second question referred by the Court of Appeal (England & Wales) (Civil Division) is inadmissible.**

Lenaerts	Tizzano	Silva de Lapuerta
von Danwitz	Da Cruz Vilaça Juhász	Vilaras
Borg Barthet	Malenovský	Levits
Bonichot	Arabadjiev	Rodin

Biltgen Lycourgos

Delivered in open court in Luxembourg on 21 December 2016.

A. Calot Escobar
Registrar

K. Lenaerts
President

Reports of Cases

JUDGMENT OF THE COURT (Fourth Chamber)

17 October 2013 *

(Reference for a preliminary ruling — Area of freedom, security and justice — Biometric passport — Fingerprints — Regulation (EC) No 2252/2004 — Article 1(2) — Validity — Legal basis — Procedure for adopting — Articles 7 and 8 of the Charter of Fundamental Rights of the European Union — Right to respect for private life — Right to the protection of personal data — Proportionality)

In Case C-291/12,

REQUEST for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Gelsenkirchen (Germany), made by decision of 15 May 2012, received at the Court on 12 June 2012, in the proceedings

Michael Schwarz

v

Stadt Bochum,

THE COURT (Fourth Chamber),

composed of L. Bay Larsen, President of the Chamber, M. Safjan, J. Malenovský (Rapporteur), U. Lõhmus and A. Prechal, Judges,

Advocate General: P. Mengozzi,

Registrar: K. Malacek, Administrator,

having regard to the written procedure and further to the hearing on 13 March 2013,

after considering the observations submitted on behalf of:

— Mr Schwarz, on his own behalf, and by W. Nešković, Rechtsanwalt,

— the Stadt Bochum, by S. Sondermann, acting as Agent,

— the German Government, by T. Henze and A. Wiedmann, acting as Agents,

— the Polish Government, by B. Majczyna, acting as Agent,

— the European Parliament, by U. Rösslein and P. Schonard, acting as Agents,

— the Council of the European Union, by I. Gurov and Z. Kupčová, acting as Agents,

* Language of the case: German.

— the European Commission, by B. Martenczuk and G. Wils, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 13 June 2013,

gives the following

Judgment

1 This request for a preliminary ruling concerns the validity of Article 1(2) of Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OJ 2004 L 385, p. 1), as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009 (OJ 2009 L 142, p. 1; corrigendum: OJ 2009 L 188, p. 127) ('Regulation No 2252/2004').

2 The request has been made in proceedings between Mr Schwarz and the Stadt Bochum (city of Bochum) concerning the latter's refusal to issue him with a passport unless his fingerprints were taken at the same time so that they could be stored on that passport.

Legal context

3 Article 2 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 (OJ 1995 L 281, p. 31) 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;

…'

4 Article 7(e) of Directive 95/46 provides:

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

…

(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'.

5 Recitals 2, 3 and 8 in the preamble to Regulation No 2252/2004 state:

‘(2) Minimum security standards for passports were introduced by a Resolution of the representatives of the Governments of the Member States, meeting within the Council, on 17 October 2000 [supplementing the resolutions of 23 June 1981, 30 June 1982, 14 July 1986 and 10 July 1995 as regards the security characteristics of passports and other travel documents (OJ 2000 C 310, p. 1)]. It is now appropriate to upgrade this Resolution by a Community measure in order to achieve enhanced harmonised security standards for passports and travel documents to protect against falsification. At the same time biometric identifiers should be integrated in the passport or travel document in order to establish a reliable link between the genuine holder and the document.

(3) The harmonisation of security features and the integration of biometric identifiers is an important step towards the use of new elements in the perspective of future developments at European level, which render the travel document more secure and establish a more reliable link between the holder and the passport and the travel document as an important contribution to ensuring that it is protected against fraudulent use. The specifications of the International Civil Aviation Organisation (ICAO), and in particular those set out in Document 9303 on machine readable travel documents, should be taken into account.

…

(8) With regard to the personal data to be processed in the context of passports and travel documents, Directive [95/46] applies. It should be ensured that no further information shall be stored in the passport unless provided for in this Regulation, its annex or unless it is mentioned in the relevant travel document.’

6 Under recital 5 in the preamble to Regulation No 444/2009:

‘Regulation [No 2252/2004] requires biometric data to be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. This is without prejudice to any other use or storage of these data in accordance with national legislation of Member States. Regulation [No 2252/2004] does not provide a legal base for setting up or maintaining databases for storage of those data in Member States, which is strictly a matter of national law.’

7 Under Article 1(1) to (2a) of Regulation No 2252/2004:

‘1. Passports and travel documents issued by Member States shall comply with the minimum security standards set out in the Annex.

…

2. Passports and travel documents shall include a highly secure storage medium which shall contain a facial image. Member States shall also include two fingerprints taken flat in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.

2a. The following persons shall be exempt from the requirement to give fingerprints:

(a) Children under the age of 12 years.

…

(b) persons, where fingerprinting is physically impossible.’

8 Article 2(a) of that regulation provides:

‘Additional technical specifications … for passports and travel documents relating to the following shall be established in accordance with the procedure referred to in Article 5(2):

(a) additional security features and requirements including enhanced anti-forgery, counterfeiting and falsification standards’.

9 Article 3(1) of that regulation provides:

‘In accordance with the procedure referred to in Article 5(2) it may be decided that the specifications referred to in Article 2 shall be secret and not be published. In that case, they shall be made available only to the bodies designated by the Member States as responsible for printing and to persons duly authorised by a Member State or the [European] Commission.’

10 Under Article 4(3) of that regulation:

‘Biometric data shall be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. For the purpose of this Regulation the biometric features in passports and travel documents shall only be used for verifying:

(a) the authenticity of the passport or travel document;

(b) the identity of the holder by means of directly available comparable features when the passport or travel document is required to be produced by law.

The checking of the additional security features shall be carried out without prejudice to Article 7(2) of Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) [(OJ 2006 L 105, p. 1)]. The failure of the matching in itself shall not affect the validity of the passport or travel document for the purpose of the crossing of external borders.’

The dispute in the main proceedings and the question referred for a preliminary ruling

11 Mr Schwarz applied to the Stadt Bochum for a passport, but refused at that time to have his fingerprints taken. After the Stadt Bochum rejected his application, Mr Schwarz brought an action before the referring court in which he requested that the city be ordered to issue him with a passport without taking his fingerprints.

12 Before that court, Mr Schwarz disputes the validity of the regulation (Regulation No 2252/2004) which created the obligation to take the fingerprints of persons applying for passports. He submits that that regulation does not have an appropriate legal basis and is vitiated by a procedural defect. In addition, he claims that Article 1(2) of that regulation infringes the right to the protection of personal data laid down, in general terms, in Article 7 of the Charter of Fundamental Rights of the European Union (‘the Charter’), which relates to the right to respect for private life, and explicitly in Article 8 thereof.

13 In those circumstances the Verwaltungsgericht Gelsenkirchen (Administrative Court, Gelsenkirchen) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:

‘Is Article 1(2) of [Regulation No 2252/2004] to be considered valid?’

Consideration of the question referred

14 By its question, read in the light of the order for reference, the referring court asks, in essence, whether Article 1(2) of Regulation No 2252/2004 is invalid on the grounds, in the first place, that the regulation has an inappropriate legal basis; in the second, that the procedure for adopting that regulation is vitiated by a defect and, in the third, that Article 1(2) of that regulation breaches certain fundamental rights of the holders of passports issued in accordance with that provision.

Legal basis of Regulation No 2252/2004

15 The referring court seeks to establish whether it was permissible for the Council to adopt Regulation No 2252/2004 on the basis of Article 62(2)(a) EC, given that that provision does not explicitly refer to any power to regulate issues relating to passports and travel documents issued to citizens of the Union ('passports').

16 In that regard, it should be noted that Article 62(2)(a) EC, in the version applicable from 1 May 1999 to 30 November 2009, on the basis of which Regulation No 2252/2004 was adopted, was part of Title IV of the EC Treaty, entitled 'Visas, asylum, immigration and other policies related to free movement of persons'. That provision stated that the Council of the European Union, acting in accordance with the procedure referred to in Article 67 EC, was, within a period of five years after the entry into force of the Treaty of Amsterdam, to adopt 'measures on the crossing of the external borders of the Member States which shall establish … standards and procedures to be followed by Member States in carrying out checks on persons at such borders'.

17 It is clear from both the wording and the aim of Article 62(2)(a) EC that this provision authorised the Council to regulate how checks were to be carried out at the external borders of the European Union in order to ascertain the identity of persons crossing those borders. Such checks necessarily requiring documents to be presented that make it possible to establish that identity, Article 62(2)(a) EC therefore authorised the Council to adopt legal provisions relating to such documents and to passports in particular.

18 As to whether Article 62(2)(a) EC authorised the Council to adopt measures establishing standards and procedures in connection with the issuing of passports to citizens of the Union, it should be noted, first, that the provision referred to checks on 'persons' without providing further details. Thus, it must be presumed that the provision was intended to cover not only third-country nationals, but also citizens of the Union and, hence, their passports.

19 Second, as also confirmed by the Explanatory Memorandum to the proposal for a Council Regulation on standards for security features and biometrics in EU citizens passports [(COM(2004) 116 final)] as submitted by the Commission, harmonised security standards for passports may be required in order to avoid passports having security features which lag behind those provided for by the uniform format for visas and residence permits for third-country nationals. In those circumstances, the EU legislature has the authority to provide for similar security features in respect of passports held by EU citizens, in so far as such authority helps to prevent those passports from becoming targets for falsification or fraudulent use.

20 It follows that Article 62(2)(a) EC was an appropriate legal basis for adopting Regulation No 2252/2004 and, in particular, Article 1(2) thereof.

Procedure for adopting Regulation No 2252/2004

21 The referring court seeks to establish whether Article 1(2) of Regulation No 2252/2004 is valid in view of the procedural requirements listed in Article 67(1) EC. In that regard, that court refers to the line of argument put forward by the applicant, who is of the view that, contrary to the requirements of the latter provision, the European Parliament was not properly consulted in the course of the legislative procedure. According to Mr Schwarz, the Commission's proposal submitted to the Parliament for consultation purposes provided for the storage of images of fingerprints on passports to be merely an option for the Member States, changing into an obligation after the Parliament had been consulted. That represented a significant amendment; as a result, under Article 67 EC, further consultation of the Parliament was necessary.

22 However, it is common ground that Regulation No 444/2009 has replaced the wording of Article 1(2) of Regulation No 2252/2004 – on the subject of which, according to the applicant, the Parliament was not consulted – with new wording which reproduces the obligation to store images of fingerprints in passports. Regulation No 444/2009 being applicable to the facts in the case before the referring court and adopted following the joint decision procedure and, so, with the full involvement of the Parliament in its role as co-legislator, the ground for invalidity relied on by the applicant in that regard is ineffective.

Fundamental rights to respect for private life and the protection of personal data

23 First, the Court must examine whether taking fingerprints and storing them in passports, as provided for in Article 1(2) of Regulation No 2252/2004, constitutes a threat to the rights to respect for private life and the protection of personal data. If so, it must then be ascertained whether such a threat can be justified.

Whether such a threat exists

24 Article 7 of the Charter states, inter alia, that everyone has the right to respect for his or her private life. Under Article 8(1) thereof, everyone has the right to the protection of personal data concerning him or her.

25 It follows from a joint reading of those articles that, as a general rule, any processing of personal data by a third party may constitute a threat to those rights.

26 From the outset, it should be borne in mind that the right to respect for private life with regard to the processing of personal data concerns any information relating to an identified or identifiable individual (Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paragraph 52, and Joined Cases C-468/10 and C-469/10 *ASNEF and FECEMD* [2011] ECR I-12181, paragraph 42).

27 Fingerprints constitute personal data, as they objectively contain unique information about individuals which allows those individuals to be identified with precision (see, to that effect, in particular, European Court of Human Rights judgment in *S. and Marper v. United Kingdom*, §§ 68 and 84, ECHR 2008).

28 In addition, as can be seen from Article 2(b) of Directive 95/46, processing of personal data means any operation performed upon such data by a third party, such as the collecting, recording, storage, consultation or use thereof.

29 Applying Article 1(2) of Regulation No 2252/2004 means that national authorities are to take a person's fingerprints and that those fingerprints are to be kept in the storage medium in that person's passport. Such measures must therefore be viewed as a processing of personal data.

30 In those circumstances, the taking and storing of fingerprints by the national authorities which is governed by Article 1(2) of Regulation No 2252/2004 constitutes a threat to the rights to respect for private life and the protection of personal data. Accordingly, it must be ascertained whether that twofold threat is justified.

Justification

31 Under Article 8(2) of the Charter, personal data cannot be processed except on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

32 First of all, concerning the condition requiring the consent of persons applying for passports before their fingerprints can be taken, it should be noted that, as a general rule, it is essential for citizens of the Union to own a passport in order, for example, to travel to non-member countries and that that document must contain fingerprints pursuant to Article 1(2) of Regulation No 2252/2004. Therefore, citizens of the Union wishing to make such journeys are not free to object to the processing of their fingerprints. In those circumstances, persons applying for passports cannot be deemed to have consented to that processing.

33 Next, regarding whether the processing of fingerprints can be justified on the basis of some other legitimate basis laid down by law, it should be borne in mind from the outset that the rights recognised by Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, *Volker und Markus Schecke and Eifert*, paragraph 48, and Case C-543/09 *Deutsche Telekom* [2011] ECR I-3441, paragraph 51).

34 Indeed, Article 52(1) of the Charter allows for limitations of the exercise of those rights, so long as those limitations are provided for by law, respect the essence of those rights, and, in accordance with the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

35 First, in the present case, it is common ground that the limitation arising from the taking and storing of fingerprints when issuing passports must be considered to be provided for by law, for the purposes of Article 52(1) of the Charter, since those operations are provided for by Article 1(2) of Regulation No 2252/2004.

36 Second, concerning the objective of general interest underlying that limitation, it can be seen that Article 1(2) of Regulation No 2252/2004, when read in the light of recitals 2 and 3 of that regulation, has two specific aims: the first, to prevent the falsification of passports and the second, to prevent fraudulent use thereof, that is to say, use by persons other than their genuine holders.

37 Accordingly, Article 1(2) is designed, through pursuit of those aims, to prevent, inter alia, illegal entry into the European Union.

38 In those circumstances, it must be found that Article 1(2) of Regulation No 2252/2004 pursues an objective of general interest recognised by the Union.

39 Third, it is not apparent from the evidence available to the Court, nor has it been claimed, that the limitations placed on the exercise of the rights recognised by Articles 7 and 8 of the Charter in the present case do not respect the essence of those rights.

40 Fourth, the Court must establish whether the limitations placed on those rights are proportionate to the aims pursued by Regulation No 2252/2004 and, by extension, to the objective of preventing illegal entry into the European Union. It must therefore be ascertained whether the measures implemented by that regulation are appropriate for attaining those aims and do not go beyond what is necessary to achieve them (see *Volker und Markus Schecke and Eifert*, paragraph 74).

41 As to whether Article 1(2) of Regulation No 2252/2004 is appropriate for attaining the aim of preventing the falsification of passports, it is common ground that the storage of fingerprints on a highly secure storage medium as provided for by that provision requires sophisticated technology. Therefore such storage is likely to reduce the risk of passports being falsified and to facilitate the work of the authorities responsible for checking the authenticity of passports at EU borders.

42 Mr Schwarz submits that the method of ascertaining identity using fingerprints is not appropriate for attaining the aim of preventing fraudulent use of passports, since there have been mistakes when implementing that method in practice; given that no two digital copies of a set of fingerprints are ever identical, systems using that method are not sufficiently accurate, resulting in not inconsiderable rates of unauthorised persons being incorrectly accepted and of authorised persons being incorrectly rejected.

43 In that regard, however, it must be held that the fact that the method is not wholly reliable is not decisive. Although that method does not prevent all unauthorised persons from being accepted, it is enough that it significantly reduces the likelihood of such acceptance that would exist if that method were not used.

44 Although it is true that the use of fingerprints as a means of ascertaining identity may, on an exceptional basis, lead to authorised persons being rejected by mistake, the fact remains that a mismatch between the fingerprints of the holder of a passport and the data in that document does not mean that the person concerned will automatically be refused entry to the European Union, as is pointed out in the second subparagraph of Article 4(3) of Regulation No 2252/2004. A mismatch of that kind will simply draw the competent authorities attention to the person concerned and will result in a more detailed check of that person in order definitively to establish his identity.

45 In the light of the foregoing, the taking and storing of fingerprints referred to in Article 1(2) of Regulation No 2252/2004 are appropriate for attaining the aims pursued by that regulation and, by extension, the objective of preventing illegal entry to the European Union.

46 Next, in assessing whether such processing is necessary, the legislature is obliged, inter alia, to examine whether it is possible to envisage measures which will interfere less with the rights recognised by Articles 7 and 8 of the Charter but will still contribute effectively to the objectives of the European Union rules in question (see, to that effect, *Volker und Markus Schecke and Eifert*, paragraph 86).

47 In that context, with regard to the aim of protecting against the fraudulent use of passports, it must in the first place be considered whether the threat posed by the measure of taking fingerprints does not go beyond what is necessary in order to achieve that aim.

48 In this respect, it is be borne in mind, on the one hand, that that action involves no more than the taking of prints of two fingers, which can, moreover, generally be seen by others, so that this is not an operation of an intimate nature. Nor does it cause any particular physical or mental discomfort to the person affected any more than when that person's facial image is taken.

49 It is true that those fingerprints are to be taken in addition to the facial image. However, the combination of two operations designed to identify persons may not *a priori* be regarded as giving rise in itself to a greater threat to the rights recognised by Articles 7 and 8 of the Charter than if each of those two operations were to be considered in isolation.

50 Thus, as regards the case in the main proceedings, nothing in the case file submitted to the Court permits a finding that the fact that fingerprints and a facial image are taken at the same time would, by reason of that fact alone, give rise to greater interference with those rights.

51 On the other hand, it should also be noted that the only real alternative to the taking of fingerprints raised in the course of the proceedings before the Court is an iris scan. Nothing in the case file submitted to the Court suggests that the latter procedure would interfere less with the rights recognised by Articles 7 and 8 of the Charter than the taking of fingerprints.

52 Furthermore, with regard to the effectiveness of those two methods, it is common ground that iris-recognition technology is not yet as advanced as fingerprint-recognition technology. In addition, the procedure for iris recognition is currently significantly more expensive than the procedure for comparing fingerprints and is, for that reason, less suitable for general use.

53 In those circumstances, the Court has not been made aware of any measures which would be both sufficiently effective in helping to achieve the aim of protecting against the fraudulent use of passports and less of a threat to the rights recognised by Articles 7 and 8 of the Charter than the measures deriving from the method based on the use of fingerprints.

54 In the second place, in order for Article 1(2) of Regulation No 2252/2004 to be justified in the light of that aim, it is also crucial that the processing of any fingerprints taken pursuant to that provision should not go beyond what is necessary to achieve that aim.

55 In that regard, the legislature must ensure that there are specific guarantees that the processing of such data will be effectively protected from misuse and abuse (see, to that effect, European Court of Human Rights judgment, *S. and Marper*, § 103).

56 In that respect, it should be noted that Article 4(3) of Regulation No 2252/2004 explicitly states that fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder.

57 In addition, that regulation ensures protection against the risk of data including fingerprints being read by unauthorised persons. In that regard, Article 1(2) of that regulation makes it clear that such data are to be kept in a highly secure storage medium in the passport of the person concerned.

58 However, the referring court is uncertain, in the light of its assessment, whether Article 1(2) of Regulation No 2252/2004 is proportionate in view of the risk that, once fingerprints have been taken pursuant to that provision, the – extremely high quality – data will be stored, perhaps centrally, and used for purposes other than those provided for by that regulation.

59 In that regard, it is true that fingerprints play a particular role in the field of identifying persons in general. Thus, the identification techniques of comparing fingerprints taken in a particular place with those stored in a database make it possible to establish whether a certain person is in that particular place, whether in the context of a criminal investigation or in order to monitor that person indirectly.

60 However, it should be borne in mind that Article 1(2) of Regulation No 2252/2004 does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone.

61 The regulation not providing for any other form or method of storing those fingerprints, it cannot in and of itself, as is pointed out by recital 5 of Regulation No 444/2009, be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the European Union.

62 In those circumstances, the arguments put forward by the referring court concerning the risks linked to possible centralisation cannot, in any event, affect the validity of that regulation and would have, should the case arise, to be examined in the course of an action brought before the competent courts against legislation providing for a centralised fingerprint base.

63 In the light of the foregoing, it must be held that Article 1(2) of Regulation No 2252/2004 does not imply any processing of fingerprints that would go beyond what is necessary in order to achieve the aim of protecting against the fraudulent use of passports.

64 It follows that the interference arising from Article 1(2) of Regulation No 2252/2004 is justified by its aim of protecting against the fraudulent use of passports.

65 In those circumstances, there is no longer any need to examine whether the measures put into effect by that regulation are necessary in view of its other aim (namely, preventing the falsification of passports).

66 In the light of all the foregoing considerations, the answer to the question referred is that examination of that question has revealed nothing capable of affecting the validity of Article 1(2) of Regulation No 2252/2004.

Costs

67 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Fourth Chamber) hereby rules:

Examination of the question referred has revealed nothing capable of affecting the validity of Article 1(2) of Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009.

[Signatures]

Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

8 April 2014*

(Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union)

In Joined Cases C-293/12 and C-594/12,

REQUESTS for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) and the Verfassungsgerichtshof (Austria), made by decisions of 27 January and 28 November 2012, respectively, received at the Court on 11 June and 19 December 2012, in the proceedings

Digital Rights Ireland Ltd (C-293/12)

v

Minister for Communications, Marine and Natural Resources,

Minister for Justice, Equality and Law Reform,

Commissioner of the Garda Síochána,

Ireland,

The Attorney General,

intervener:

Irish Human Rights Commission,

and

Kärntner Landesregierung (C-594/12),

Michael Seitlinger,

Christof Tschohl and others,

* Languages of the case: English and German.

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), E. Juhász, A. Borg Barthet, C.G. Fernlund and J.L. da Cruz Vilaça, Presidents of Chambers, A. Rosas, G. Arestis, J.-C. Bonichot, A. Arabadjiev, C. Toader and C. Vajda, Judges,

Advocate General: P. Cruz Villalón,

Registrar: K. Malacek, Administrator,

having regard to the written procedure and further to the hearing on 9 July 2013,

after considering the observations submitted on behalf of:

— Digital Rights Ireland Ltd, by F. Callanan, Senior Counsel, and F. Crehan, Barrister-at-Law, instructed by S. McGarr, Solicitor,

— Mr Seitlinger, by G. Otto, Rechtsanwalt,

— Mr Tschohl and Others, by E. Scheucher, Rechtsanwalt,

— the Irish Human Rights Commission, by P. Dillon Malone, Barrister-at-Law, instructed by S. Lucey, Solicitor,

— Ireland, by E. Creedon and D. McGuinness, acting as Agents, assisted by E. Regan, Senior Counsel, and D. Fennelly, Barrister-at-Law,

— the Austrian Government, by G. Hesse and G. Kunnert, acting as Agents,

— the Spanish Government, by N. Díaz Abad, acting as Agent,

— the French Government, by G. de Bergues and D. Colas and by B. Beaupère-Manokha, acting as Agents,

— the Italian Government, by G. Palmieri, acting as Agent, assisted by A. De Stefano, avvocato dello Stato,

— the Polish Government, by B. Majczyna and M. Szpunar, acting as Agents,

— the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,

— the United Kingdom Government, by L. Christie, acting as Agent, assisted by S. Lee, Barrister,

— the European Parliament, by U. Rösslein and A. Caiola and by K. Zejdová, acting as Agents,

— the Council of the European Union, by J. Monteiro and E. Sitbon and by I. Šulce, acting as Agents,

— the European Commission, by D. Maidani, B. Martenczuk and M. Wilderspin, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 12 December 2013,

gives the following

Judgment

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

2 The request made by the High Court (Case C-293/12) concerns proceedings between (i) Digital Rights Ireland Ltd. ('Digital Rights') and (ii) the Minister for Communications, Marine and Natural Resources, the Minister for Justice, Equality and Law Reform, the Commissioner of the Garda Síochána, Ireland and the Attorney General, regarding the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications.

3 The request made by the Verfassungsgerichtshof (Constitutional Court) (Case C-594/12) concerns constitutional actions brought before that court by the Kärntner Landesregierung (Government of the Province of Carinthia) and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants regarding the compatibility with the Federal Constitutional Law (Bundes-Verfassungsgesetz) of the law transposing Directive 2006/24 into Austrian national law.

Legal context

Directive 95/46/EC

4 The object 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 (OJ 1995 L 281, p. 31), according to Article 1(1) thereof, is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with regard to the processing of personal data.

5 As regards the security of processing such data, Article 17(1) of that directive provides:

'Member States shall provide that the controller must implement appropriate technical and organi[s]ational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.'

Directive 2002/58/EC

6 The aim 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), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11, 'Directive 2002/58), according to Article 1(1) thereof, is to harmonise the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and to confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such

data and of electronic communication equipment and services in the European Union. According to Article 1(2), the provisions of that directive particularise and complement Directive 95/46 for the purposes mentioned in Article 1(1).

7 As regards the security of data processing, Article 4 of Directive 2002/58 provides:

'1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

— ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,

— protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,

— ensure the implementation of a security policy with respect to the processing of personal data,

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.'

8 As regards the confidentiality of the communications and of the traffic data, Article 5(1) and (3) of that directive provide:

'1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

…

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.'

9 Article 6(1) of Directive 2002/58 states:

'Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).'

10 Article 15 of Directive 2002/58 states in paragraph 1:

'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.'

Directive 2006/24

11 After having launched a consultation with representatives of law enforcement authorities, the electronic communications industry and data protection experts, on 21 September 2005 the Commission presented an impact assessment of policy options in relation to the rules on the retention of traffic data ('the impact assessment'). That assessment served as the basis for the drawing up of the 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/EC (COM(2005) 438 final, 'the proposal for a directive'), also presented on 21 September 2005, which led to the adoption of Directive 2006/24 on the basis of Article 95 EC.

12 Recital 4 in the preamble to Directive 2006/24 states:

'Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.'

13 According to the first sentence of recital 5 in the preamble to Directive 2006/24, '[s]everal Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences'.

14 Recitals 7 to 11 in the preamble to Directive 2006/24 read as follows:

'(7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

(9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) [signed in Rome on 4 November 1950], everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. …

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.'

15 Recitals 16, 21 and 22 in the preamble to Directive 2006/24 state:

'(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.

(21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(22) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.'

16 Directive 2006/24 lays down the obligation on the providers of publicly available electronic communications services or of public communications networks to retain certain data which are generated or processed by them. In that context, Articles 1 to 9, 11 and 13 of the directive state:

‘Article 1

Subject matter and scope

1. This Directive aims to harmonise Member States’ provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2

Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) …, and in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive:

(a) “data” means traffic data and location data and the related data necessary to identify the subscriber or user;

(b) “user” means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

(c) “telephone service” means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

(d) “user ID” means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;

(e) “cell ID” means the identity of the cell from which a mobile telephony call originated or in which it terminated;

(f) “unsuccessful call attempt” means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

Article 3

Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4

Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of EU law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5

Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

  (1) concerning fixed network telephony and mobile telephony:

    (i) the calling telephone number;

    (ii) the name and address of the subscriber or registered user;

  (2) concerning Internet access, Internet e-mail and Internet telephony:

    (i) the user ID(s) allocated;

    (ii) the user ID and telephone number allocated to any communication entering the public telephone network;

    (iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;

and

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8

Storage requirements for retained data

Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9

Supervisory authority

1. Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.

2. The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

…

Article 11

Amendment of Directive 2002/58/EC

The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:

“1a. Paragraph 1 shall not apply to data specifically required by [Directive 2006/24/EC] to be retained for the purposes referred to in Article 1(1) of that Directive.”

…

Article 13

Remedies, liability and penalties

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.’

The actions in the main proceedings and the questions referred for a preliminary ruling

Case C-293/12

17 On 11 August 2006, Digital Rights brought an action before the High Court in which it claimed that it owned a mobile phone which had been registered on 3 June 2006 and that it had used that mobile phone since that date. It challenged the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications and asked the national court, in particular, to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, which requires telephone communications service providers to retain traffic and location data relating to those providers for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State.

18 The High Court, considering that it was not able to resolve the questions raised relating to national law unless the validity of Directive 2006/24 had first been examined, decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

‘1. Is the restriction on the rights of the [p]laintiff in respect of its use of mobile telephony arising from the requirements of Articles 3, 4 … and 6 of Directive 2006/24/EC incompatible with [Article 5(4)] TEU in that it is disproportionate and unnecessary or inappropriate to achieve the legitimate aims of:

(a) Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime?

and/or

(b) Ensuring the proper functioning of the internal market of the European Union?

2. Specifically,

(i) Is Directive 2006/24 compatible with the right of citizens to move and reside freely within the territory of the Member States laid down in Article 21 TFEU?

(ii) Is Directive 2006/24 compatible with the right to privacy laid down in Article 7 of the [Charter of Fundamental Rights of the European Union (“the Charter”)] and Article 8 ECHR?

(iii) Is Directive 2006/24 compatible with the right to the protection of personal data laid down in Article 8 of the Charter?

(iv) Is Directive 2006/24 compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR?

(v) Is Directive 2006/24 compatible with the right to [g]ood [a]dministration laid down in Article 41 of the Charter?

3. To what extent do the Treaties — and specifically the principle of loyal cooperation laid down in [Article 4(3) TEU] — require a national court to inquire into, and assess, the compatibility of the national implementing measures for [Directive 2006/24] with the protections afforded by the [Charter], including Article 7 thereof (as informed by Article 8 of the ECHR)?’

Case C–594/12

19 The origin of the request for a preliminary ruling in Case C-594/12 lies in several actions brought before the Verfassungsgerichtshof by the Kärntner Landesregierung and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants, respectively, seeking the annulment of Paragraph 102a of the 2003 Law on telecommunications (Telekommunikationsgesetz 2003), which was inserted into that 2003 Law by the federal law amending it (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 — TKG 2003 geändert wird, BGBl I, 27/2011) for the purpose of transposing Directive 2006/24 into Austrian national law. They take the view, inter alia, that Article 102a of the Telekommunikationsgesetz 2003 infringes the fundamental right of individuals to the protection of their data.

20 The Verfassungsgerichtshof wonders, in particular, whether Directive 2006/24 is compatible with the Charter in so far as it allows the storing of many types of data in relation to an unlimited number of persons for a long time. The Verfassungsgerichtshof takes the view that the retention of data affects almost exclusively persons whose conduct in no way justifies the retention of data relating to them. Those persons are exposed to a greater risk that authorities will investigate the data relating to them, become acquainted with the content of those data, find out about their private lives and use those data for multiple purposes, having regard in particular to the unquantifiable number of persons having access to the data for a minimum period of six months. According to the referring court, there are doubts as to whether that directive is able to achieve the objectives which it pursues and as to the proportionality of the interference with the fundamental rights concerned.

21 In those circumstances the Verfassungsgerichtshof decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

‘1. Concerning the validity of acts of institutions of the European Union:

Are Articles 3 to 9 of [Directive 2006/24] compatible with Articles 7, 8 and 11 of the [Charter]?

2. Concerning the interpretation of the Treaties:

(a) In the light of the explanations relating to Article 8 of the Charter, which, according to Article 52(7) of the Charter, were drawn up as a way of providing guidance in the interpretation of the Charter and to which regard must be given by the Verfassungsgerichtshof, must [Directive 95/46] and 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] be taken into account, for the purposes of assessing the permissibility of interference, as being of equal standing to the conditions under Article 8(2) and Article 52(1) of the Charter?

(b) What is the relationship between “Union law”, as referred to in the final sentence of Article 52(3) of the Charter, and the directives in the field of the law on data protection?

(c) In view of the fact that [Directive 95/26] and Regulation … No 45/2001 contain conditions and restrictions with a view to safeguarding the fundamental right to data protection under the Charter, must amendments resulting from subsequent secondary law be taken into account for the purpose of interpreting Article 8 of the Charter?

(d) Having regard to Article 52(4) of the Charter, does it follow from the principle of the preservation of higher levels of protection in Article 53 of the Charter that the limits applicable under the Charter in relation to permissible restrictions must be more narrowly circumscribed by secondary law?

(e) Having regard to Article 52(3) of the Charter, the fifth paragraph in the preamble thereto and the explanations in relation to Article 7 of the Charter, according to which the rights guaranteed in that article correspond to those guaranteed by Article 8 of the [ECHR], can assistance be derived from the case-law of the European Court of Human Rights for the purpose of interpreting Article 8 of the Charter such as to influence the interpretation of that latter article?'

22 By decision of the President of the Court of 11 June 2013, Cases C-293/12 and C-594/12 were joined for the purposes of the oral procedure and the judgment.

Consideration of the questions referred

The second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12

23 By the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12, which should be examined together, the referring courts are essentially asking the Court to examine the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter.

The relevance of Articles 7, 8 and 11 of the Charter with regard to the question of the validity of Directive 2006/24

24 It follows from Article 1 and recitals 4, 5, 7 to 11, 21 and 22 of Directive 2006/24 that the main objective of that directive is to harmonise Member States' provisions concerning the retention, by providers of publicly available electronic communications services or of public communications networks, of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism, in compliance with the rights laid down in Articles 7 and 8 of the Charter.

25 The obligation, under Article 3 of Directive 2006/24, on providers of publicly available electronic communications services or of public communications networks to retain the data listed in Article 5 of the directive for the purpose of making them accessible, if necessary, to the competent national authorities raises questions relating to respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for freedom of expression under Article 11 of the Charter.

26 In that regard, it should be observed that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

27 Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.

28 In such circumstances, even though, as is apparent from Article 1(2) and Article 5(2) of Directive 2006/24, the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.

29 The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article (Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* EU:C:2010:662, paragraph 47).

30 Whereas the references for a preliminary ruling in the present cases raise, in particular, the question of principle as to whether or not, in the light of Article 7 of the Charter, the data of subscribers and registered users may be retained, they also concern the question of principle as to whether Directive 2006/24 meets the requirements for the protection of personal data arising from Article 8 of the Charter.

31 In the light of the foregoing considerations, it is appropriate, for the purposes of answering the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12, to examine the validity of the directive in the light of Articles 7 and 8 of the Charter.

Interference with the rights laid down in Articles 7 and 8 of the Charter

32 By requiring the retention of the data listed in Article 5(1) of Directive 2006/24 and by allowing the competent national authorities to access those data, Directive 2006/24, as the Advocate General has pointed out, in particular, in paragraphs 39 and 40 of his Opinion, derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, directives which provided for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication, unless they are necessary for billing purposes and only for as long as so necessary.

33 To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that effect, Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 75).

34 As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.

35 Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right (see, as regards Article 8 of the ECHR, Eur. Court H.R., *Leander v. Sweden*, 26 March 1987, § 48, Series A no 116; *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI). Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.

36 Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data.

37 It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

Justification of the interference with the rights guaranteed by Articles 7 and 8 of the Charter

38 Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

39 So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.

40 Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.

41 As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonise Member States' provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security.

42 It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest (see, to that effect, Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission* EU:C:2008:461, paragraph 363, and Cases C-539/10 P and C-550/10 P *Al-Aqsa* v *Council* EU:C:2012:711, paragraph 130). The same is true of the fight against serious crime in order to ensure public security (see, to that effect, Case C-145/09 *Tsakouridis* EU:C:2010:708, paragraphs 46 and 47). Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.

43 In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that, because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.

44 It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.

45 In those circumstances, it is necessary to verify the proportionality of the interference found to exist.

46 In that regard, according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives (see, to that effect, Case C-343/09 *Afton Chemical* EU:C:2010:419, paragraph 45; *Volker und Markus Schecke and Eifert* EU:C:2010:662, paragraph 74; Cases C-581/10 and C-629/10 *Nelson and Others* EU:C:2012:657, paragraph 71; Case C-283/11 *Sky Österreich* EU:C:2013:28, paragraph 50; and Case C-101/12 *Schaible* EU:C:2013:661, paragraph 29).

47 With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V).

48 In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

49 As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.

50 That assessment cannot be called into question by the fact relied upon in particular by Mr Tschohl and Mr Seitlinger and by the Portuguese Government in their written observations submitted to the Court that there are several methods of electronic communication which do not fall within the scope of Directive 2006/24 or which allow anonymous communication. Whilst, admittedly, that fact is such

as to limit the ability of the data retention measure to attain the objective pursued, it is not, however, such as to make that measure inappropriate, as the Advocate General has pointed out in paragraph 137 of his Opinion.

51 As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

52 So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12 *IPI* EU:C:2013:715, paragraph 39 and the case-law cited).

53 In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter.

54 Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, § 62 and 63; *Rotaru v. Romania*, § 57 to 59, and *S. and Marper v. the United Kingdom*, § 99).

55 The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, *S. and Marper v. the United Kingdom*, § 103, and *M. K. v. France*, 18 April 2013, no. 19522/09, § 35).

56 As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

57 In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

58 Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

59 Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

60 Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

61 Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

62 In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

63 Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

64 Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

65 It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

66 Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

67 Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

68 In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 *Commission* v *Austria* EU:C:2012:631, paragraph 37).

69 Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.

70 In those circumstances, there is no need to examine the validity of Directive 2006/24 in the light of Article 11 of the Charter.

71 Consequently, the answer to the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12 is that Directive 2006/24 is invalid.

The first question and the second question, parts (a) and (e), and the third question in Case C-293/12 and the second question in Case C-594/12

72 It follows from what was held in the previous paragraph that there is no need to answer the first question, the second question, parts (a) and (e), and the third question in Case C-293/12 or the second question in Case C-594/12.

Costs

73 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national courts, the decision on costs is a matter for those courts. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

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

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid.

[Signatures]

Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

13 May 2014*

(Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8)

In Case C-131/12,

REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Nacional (Spain), made by decision of 27 February 2012, received at the Court on 9 March 2012, in the proceedings

Google Spain SL,

Google Inc.

v

Agencia Española de Protección de Datos (AEPD),

Mario Costeja González,

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, M. Ilešič (Rapporteur), L. Bay Larsen, T. von Danwitz, M. Safjan, Presidents of Chambers, J. Malenovský, E. Levits, A. Ó Caoimh, A. Arabadjiev, M. Berger, A. Prechal and E. Jarašiūnas Judges,

Advocate General: N. Jääskinen,

Registrar: M. Ferreira, Principal Administrator,

having regard to the written procedure and further to the hearing on 26 February 2013,

after considering the observations submitted on behalf of:

— Google Spain SL and Google Inc., by F. González Díaz, J. Baño Fos and B. Holles, abogados,

— Mr Costeja González, by J. Muñoz Rodríguez, abogado,

— the Spanish Government, by A. Rubio González, acting as Agent,

* Language of the case: Spanish.

— the Greek Government, by E.-M. Mamouna and K. Boskovits, acting as Agents,

— the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,

— the Austrian Government, by G. Kunnert and C. Pesendorfer, acting as Agents,

— the Polish Government, by B. Majczyna and M. Szpunar, acting as Agents,

— the European Commission, by I. Martínez del Peral and B. Martenczuk, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 25 June 2013,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 2(b) and (d), Article 4(1)(a) and (c), Article 12(b) and subparagraph (a) of the first paragraph of Article 14 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 (OJ 1995 L 281, p. 31) and of Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

2 The request has been made in proceedings between, on the one hand, Google Spain SL ('Google Spain') and Google Inc. and, on the other, the Agencia Española de Protección de Datos (Spanish Data Protection Agency; 'the AEPD') and Mr Costeja González concerning a decision by the AEPD upholding the complaint lodged by Mr Costeja González against those two companies and ordering Google Inc. to adopt the measures necessary to withdraw personal data relating to Mr Costeja González from its index and to prevent access to the data in the future.

Legal context

European Union law

3 Directive 95/46 which, according to Article 1, has the object of protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and of removing obstacles to the free flow of such data, states in recitals 2, 10, 18 to 20 and 25 in its preamble:

'(2) … data-processing systems are designed to serve man; … they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to … the well-being of individuals;

...

(10) … 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 European Convention for the Protection of Human Rights and Fundamental Freedoms [, signed in Rome on 4 November 1950,] 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;

...

(18) … in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; … in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) … establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; … the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor in this respect; … when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) … the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; … in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

...

(25) … the principles of protection must be reflected, on the one hand, in the obligations imposed on persons … responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances'.

4 Article 2 of Directive 95/46 states that '[f]or 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;

...

(d) "controller" shall mean 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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

...'

5 Article 3 of Directive 95/46, entitled 'Scope', states in paragraph 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.'

6 Article 4 of Directive 95/46, entitled 'National law applicable', provides:

'1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.'

7 In Section I (entitled 'Principles relating to data quality') of Chapter II of Directive 95/46, Article 6 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. 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;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(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. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

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

8 In Section II (entitled 'Criteria for making data processing legitimate') of Chapter II of Directive 95/46, Article 7 provides:

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

...

(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).'

9 Article 9 of Directive 95/46, entitled 'Processing of personal data and freedom of expression', provides:

'Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.'

10 Article 12 of Directive 95/46, entitled 'Rights of access', provides:

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

...

(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;

...'

11 Article 14 of Directive 95/46, entitled 'The data subject's right to object', provides:

'Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

...'

12 Article 28 of Directive 95/46, entitled 'Supervisory authority', is worded as follows:

'1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

...

3. Each authority shall in particular be endowed with:

— investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

— effective powers of intervention, such as, for example, that … of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing …

— …

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

…

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

…'

Spanish law

13 Directive 95/46 was transposed into Spanish Law by Organic Law No 15/1999 of 13 December 1999 on the protection of personal data (BOE No 298 of 14 December 1999, p. 43088).

The dispute in the main proceedings and the questions referred for a preliminary ruling

14 On 5 March 2010, Mr Costeja González, a Spanish national resident in Spain, lodged with the AEPD a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, in particular in Catalonia (Spain) ('La Vanguardia'), and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr Costeja González's name in the search engine of the Google group ('Google Search'), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

15 By that complaint, Mr Costeja González requested, first, that La Vanguardia be required either to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. Second, he requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to La Vanguardia. Mr Costeja González stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant.

16 By decision of 30 July 2010, the AEPD rejected the complaint in so far as it related to La Vanguardia, taking the view that the publication by it of the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.

17 On the other hand, the complaint was upheld in so far as it was directed against Google Spain and Google Inc. The AEPD considered in this regard that operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society. The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties. The AEPD considered that that obligation may be owed directly by operators of search engines, without it being necessary to erase the data or information from the website where they appear, including when retention of the information on that site is justified by a statutory provision.

18 Google Spain and Google Inc. brought separate actions against that decision before the Audiencia Nacional (National High Court). The Audiencia Nacional joined the actions.

19 That court states in the order for reference that the actions raise the question of what obligations are owed by operators of search engines to protect personal data of persons concerned who do not wish that certain information, which is published on third parties' websites and contains personal data relating to them that enable that information to be linked to them, be located, indexed and made available to internet users indefinitely. The answer to that question depends on the way in which Directive 95/46 must be interpreted in the context of these technologies, which appeared after the directive's publication.

20 In those circumstances, the Audiencia Nacional decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. With regard to the territorial application of Directive [95/46] and, consequently, of the Spanish data protection legislation:

(a) must it be considered that an "establishment", within the meaning of Article 4(1)(a) of Directive 95/46, exists when any one or more of the following circumstances arise:

— when the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State,

or

— when the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking,

or

— when the office or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to data protection, even where such collaboration is engaged in voluntarily?

(b) Must Article 4(1)(c) of Directive 95/46 be interpreted as meaning that there is "use of equipment … situated on the territory of the said Member State":

— when a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in that Member State,

or

— when it uses a domain name pertaining to a Member State and arranges for searches and the results thereof to be based on the language of that Member State?

(c) Is it possible to regard as a use of equipment, in the terms of Article 4(1)(c) of Directive 95/46, the temporary storage of the information indexed by internet search engines? If the answer to that question is affirmative, can it be considered that that connecting factor is present when the undertaking refuses to disclose the place where it stores those indexes, invoking reasons of competition?

(d) Regardless of the answers to the foregoing questions and particularly in the event that the Court … considers that the connecting factors referred to in Article 4 of [Directive 95/46] are not present:

must Directive 95/46 … be applied, in the light of Article 8 of the [Charter], in the Member State where the centre of gravity of the conflict is located and more effective protection of the rights of … Union citizens is possible?

2. As regards the activity of search engines as providers of content in relation to Directive 95/46 …:

(a) in relation to the activity of [Google Search], as a provider of content, consisting in locating information published or included on the net by third parties, indexing it automatically, storing it temporarily and finally making it available to internet users according to a particular order of preference, when that information contains personal data of third parties: must an activity like the one described be interpreted as falling within the concept of "processing of … data" used in Article 2(b) of Directive 95/46?

(b) If the answer to the foregoing question is affirmative, and once again in relation to an activity like the one described:

must Article 2(d) of Directive 95/46 be interpreted as meaning that the undertaking managing [Google Search] is to be regarded as the "controller" of the personal data contained in the web pages that it indexes?

(c) In the event that the answer to the foregoing question is affirmative:

may the [AEPD], protecting the rights embodied in [Article] 12(b) and [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, directly impose on [Google Search] a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located?

(d) In the event that the answer to the foregoing question is affirmative:

would the obligation of search engines to protect those rights be excluded when the information that contains the personal data has been lawfully published by third parties and is kept on the web page from which it originates?

3. Regarding the scope of the right of erasure and/or the right to object, in relation to the "derecho al olvido" (the "right to be forgotten"), the following question is asked:

must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?'

Consideration of the questions referred

Question 2(a) and (b), concerning the material scope of Directive 95/46

21 By Question 2(a) and (b), which it is appropriate to examine first, the referring court asks, in essence, whether Article 2(b) of Directive 95/46 is to be interpreted as meaning that the activity of a search engine as a provider of content which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of that provision when that information contains personal data. If the answer is in the affirmative, the referring court seeks to ascertain furthermore whether Article 2(d) of Directive 95/46 is to be interpreted as meaning that the operator of a search engine must be regarded as the 'controller' in respect of that processing of the personal data, within the meaning of that provision.

22 According to Google Spain and Google Inc., the activity of search engines cannot be regarded as processing of the data which appear on third parties' web pages displayed in the list of search results, given that search engines process all the information available on the internet without effecting a selection between personal data and other information. Furthermore, even if that activity must be classified as 'data processing', the operator of a search engine cannot be regarded as a 'controller' in respect of that processing since it has no knowledge of those data and does not exercise control over the data.

23 On the other hand, Mr Costeja González, the Spanish, Italian, Austrian and Polish Governments and the European Commission consider that that activity quite clearly involves 'data processing' within the meaning of Directive 95/46, which is distinct from the data processing by the publishers of websites and pursues different objectives from such processing. The operator of a search engine is the 'controller' in respect of the data processing carried out by it since it is the operator that determines the purposes and means of that processing.

24 In the Greek Government's submission, the activity in question constitutes such 'processing', but inasmuch as search engines serve merely as intermediaries, the undertakings which operate them cannot be regarded as 'controllers', except where they store data in an 'intermediate memory' or 'cache memory' for a period which exceeds that which is technically necessary.

25 Article 2(b) of Directive 95/46 defines 'processing of personal data' as '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'.

26 As regards in particular the internet, the Court has already had occasion to state that the operation of loading personal data on an internet page must be considered to be such 'processing' within the meaning of Article 2(b) of Directive 95/46 (see Case C-101/01 *Lindqvist* EU:C:2003:596, paragraph 25).

27 So far as concerns the activity at issue in the main proceedings, it is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus 'personal data' within the meaning of Article 2(a) of that directive.

28 Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data.

29 Nor is the foregoing finding affected by the fact that those data have already been published on the internet and are not altered by the search engine.

30 The Court has already held that the operations referred to in Article 2(b) of Directive 95/46 must also be classified as such processing where they exclusively concern material that has already been published in unaltered form in the media. It has indeed observed in that regard that a general derogation from the application of Directive 95/46 in such a case would largely deprive the directive of its effect (see, to this effect, Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* EU:C:2008:727, paragraphs 48 and 49).

31 Furthermore, it follows from the definition contained in Article 2(b) of Directive 95/46 that, whilst the alteration of personal data indeed constitutes processing within the meaning of the directive, the other operations which are mentioned there do not, on the other hand, in any way require that the personal data be altered.

32 As to the question whether the operator of a search engine must be regarded as the 'controller' in respect of the processing of personal data that is carried out by that engine in the context of an activity such as that at issue in the main proceedings, it should be recalled that Article 2(d) of Directive 95/46 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'.

33 It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d).

34 Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.

35 In this connection, it should be pointed out that the processing of personal data carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page.

36 Moreover, it is undisputed that that activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published.

37 Also, the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users' access to that information may, when users carry out their search on the basis of an individual's name, result in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the internet enabling them to establish a more or less detailed profile of the data subject.

38 Inasmuch as the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.

39 Finally, the fact that publishers of websites have the option of indicating to operators of search engines, by means in particular of exclusion protocols such as 'robot.txt' or codes such as 'noindex' or 'noarchive', that they wish specific information published on their site to be wholly or partially excluded from the search engines' automatic indexes does not mean that, if publishers of websites do not so indicate, the operator of a search engine is released from its responsibility for the processing of personal data that it carries out in the context of the engine's activity.

40 That fact does not alter the position that the purposes and means of that processing are determined by the operator of the search engine. Furthermore, even if that option for publishers of websites were to mean that they determine the means of that processing jointly with that operator, this finding would not remove any of the latter's responsibility as Article 2(d) of Directive 95/46 expressly provides that that determination may be made 'alone or jointly with others'.

41 It follows from all the foregoing considerations that the answer to Question 2(a) and (b) is that Article 2(b) and (d) of Directive 95/46 are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).

Question 1(a) to (d), concerning the territorial scope of Directive 95/46

42 By Question 1(a) to (d), the referring court seeks to establish whether it is possible to apply the national legislation transposing Directive 95/46 in circumstances such as those at issue in the main proceedings.

43 In this respect, the referring court has established the following facts:

— Google Search is offered worldwide through the website 'www.google.com'. In numerous States, a local version adapted to the national language exists. The version of Google Search in Spanish is offered through the website 'www.google.es', which has been registered since 16 September 2003. Google Search is one of the most used search engines in Spain.

— Google Search is operated by Google Inc., which is the parent company of the Google Group and has its seat in the United States.

— Google Search indexes websites throughout the world, including websites located in Spain. The information indexed by its 'web crawlers' or robots, that is to say, computer programmes used to locate and sweep up the content of web pages methodically and automatically, is stored temporarily on servers whose State of location is unknown, that being kept secret for reasons of competition.

— Google Search does not merely give access to content hosted on the indexed websites, but takes advantage of that activity and includes, in return for payment, advertising associated with the internet users' search terms, for undertakings which wish to use that tool in order to offer their goods or services to the internet users.

— The Google group has recourse to its subsidiary Google Spain for promoting the sale of advertising space generated on the website 'www.google.com'. Google Spain, which was established on 3 September 2003 and possesses separate legal personality, has its seat in Madrid (Spain). Its activities are targeted essentially at undertakings based in Spain, acting as a commercial agent for the Google group in that Member State. Its objects are to promote, facilitate and effect the sale of on-line advertising products and services to third parties and the marketing of that advertising.

— Google Inc. designated Google Spain as the controller, in Spain, in respect of two filing systems registered by Google Inc. with the AEPD; those filing systems were intended to contain the personal data of the customers who had concluded contracts for advertising services with Google Inc.

44 Specifically, the main issues raised by the referring court concern the notion of 'establishment', within the meaning of Article 4(1)(a) of Directive 95/46, and of 'use of equipment situated on the territory of the said Member State', within the meaning of Article 4(1)(c).

Question 1(a)

45 By Question 1(a), the referring court asks, in essence, whether Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when one or more of the following three conditions are met:

— the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State, or

— the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking, or

— the branch or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to protection of personal data, even where such collaboration is engaged in voluntarily.

46 So far as concerns the first of those three conditions, the referring court states that Google Search is operated and managed by Google Inc. and that it has not been established that Google Spain carries out in Spain an activity directly linked to the indexing or storage of information or data contained on third parties' websites. Nevertheless, according to the referring court, the promotion and sale of advertising space, which Google Spain attends to in respect of Spain, constitutes the bulk of the Google group's commercial activity and may be regarded as closely linked to Google Search.

47 Mr Costeja González, the Spanish, Italian, Austrian and Polish Governments and the Commission submit that, in the light of the inextricable link between the activity of the search engine operated by Google Inc. and the activity of Google Spain, the latter must be regarded as an establishment of the former and the processing of personal data is carried out in context of the activities of that establishment. On the other hand, according to Google Spain, Google Inc. and the Greek Government, Article 4(1)(a) of Directive 95/46 is not applicable in the case of the first of the three conditions listed by the referring court.

48 In this regard, it is to be noted first of all that recital 19 in the preamble to Directive 95/46 states that 'establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements' and that 'the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor'.

49 It is not disputed that Google Spain engages in the effective and real exercise of activity through stable arrangements in Spain. As it moreover has separate legal personality, it constitutes a subsidiary of Google Inc. on Spanish territory and, therefore, an 'establishment' within the meaning of Article 4(1)(a) of Directive 95/46.

50 In order to satisfy the criterion laid down in that provision, it is also necessary that the processing of personal data by the controller be 'carried out in the context of the activities' of an establishment of the controller on the territory of a Member State.

51 Google Spain and Google Inc. dispute that this is the case since the processing of personal data at issue in the main proceedings is carried out exclusively by Google Inc., which operates Google Search without any intervention on the part of Google Spain; the latter's activity is limited to providing support to the Google group's advertising activity which is separate from its search engine service.

52 Nevertheless, as the Spanish Government and the Commission in particular have pointed out, Article 4(1)(a) of Directive 95/46 does not require the processing of personal data in question to be carried out 'by' the establishment concerned itself, but only that it be carried out 'in the context of the activities' of the establishment.

53 Furthermore, in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words cannot be interpreted restrictively (see, by analogy, Case C-324/09 *L'Oréal and Others* EU:C:2011:474, paragraphs 62 and 63).

54 It is to be noted in this context that it is clear in particular from recitals 18 to 20 in the preamble to Directive 95/46 and Article 4 thereof that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope.

55 In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.

56 In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.

57 As has been stated in paragraphs 26 to 28 of the present judgment, the very display of personal data on a search results page constitutes processing of such data. Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory.

58 That being so, it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure (see, by analogy, *L'Oréal and Others* EU:C:2011:474, paragraphs 62 and 63), in particular their right to privacy, with respect to the processing of personal data, a right to which the directive accords special importance as is confirmed in particular by Article 1(1) thereof and recitals 2 and 10 in its preamble (see, to this effect, Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 70; Case C-553/07 *Rijkeboer* EU:C:2009:293, paragraph 47; and Case C-473/12 *IPI* EU:C:2013:715, paragraph 28 and the case-law cited).

59 Since the first of the three conditions listed by the referring court suffices by itself for it to be concluded that an establishment such as Google Spain satisfies the criterion laid down in Article 4(1)(a) of Directive 95/46, it is unnecessary to examine the other two conditions.

60 It follows from the foregoing that the answer to Question 1(a) is that Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

Question 1(b) to (d)

61 In view of the answer given to Question 1(a), there is no need to answer Question 1(b) to (d).

Question 2(c) and (d), concerning the extent of the responsibility of the operator of a search engine under Directive 95/46

62 By Question 2(c) and (d), the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information

relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

63 Google Spain and Google Inc. submit that, by virtue of the principle of proportionality, any request seeking the removal of information must be addressed to the publisher of the website concerned because it is he who takes the responsibility for making the information public, who is in a position to appraise the lawfulness of that publication and who has available to him the most effective and least restrictive means of making the information inaccessible. Furthermore, to require the operator of a search engine to withdraw information published on the internet from its indexes would take insufficient account of the fundamental rights of publishers of websites, of other internet users and of that operator itself.

64 According to the Austrian Government, a national supervisory authority may order such an operator to erase information published by third parties from its filing systems only if the data in question have been found previously to be unlawful or incorrect or if the data subject has made a successful objection to the publisher of the website on which that information was published.

65 Mr Costeja González, the Spanish, Italian and Polish Governments and the Commission submit that the national authority may directly order the operator of a search engine to withdraw from its indexes and intermediate memory information containing personal data that has been published by third parties, without having to approach beforehand or simultaneously the publisher of the web page on which that information appears. Furthermore, according to Mr Costeja González, the Spanish and Italian Governments and the Commission, the fact that the information has been published lawfully and that it still appears on the original web page has no effect on the obligations of that operator under Directive 95/46. On the other hand, according to the Polish Government that fact is such as to release the operator from its obligations.

66 First of all, it should be remembered that, as is apparent from Article 1 and recital 10 in the preamble, Directive 95/46 seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (see, to this effect, *IPI* EU:C:2013:715, paragraph 28).

67 According to recital 25 in the preamble to Directive 95/46, the principles of protection laid down by the directive are reflected, on the one hand, in the obligations imposed on persons responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority and the circumstances under which processing can be carried out, and, on the other hand, in the rights conferred on individuals whose data are the subject of processing to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.

68 The Court has already held that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter (see, in particular, Case C-274/99 P *Connolly* v *Commission* EU:C:2001:127, paragraph 37, and *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 68).

69 Article 7 of the Charter guarantees the right to respect for private life, whilst Article 8 of the Charter expressly proclaims the right to the protection of personal data. Article 8(2) and (3) specify that 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, that everyone has the right of access to

data which have been collected concerning him or her and the right to have the data rectified, and that compliance with these rules is to be subject to control by an independent authority. Those requirements are implemented inter alia by Articles 6, 7, 12, 14 and 28 of Directive 95/46.

70 Article 12(b) of Directive 95/46 provides that Member States are to guarantee every data subject the right to obtain from the controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of Directive 95/46, in particular because of the incomplete or inaccurate nature of the data. As this final point relating to the case where certain requirements referred to in Article 6(1)(d) of Directive 95/46 are not observed is stated by way of example and is not exhaustive, it follows that non-compliant nature of the processing, which is capable of conferring upon the data subject the right guaranteed in Article 12(b) of the directive, may also arise from non-observance of the other conditions of lawfulness that are imposed by the directive upon the processing of personal data.

71 In this connection, it should be noted that, subject to the exceptions permitted under Article 13 of Directive 95/46, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (see *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 65; Joined Cases C-468/10 and C-469/10 *ASNEF and FECEMD* EU:C:2011:777, paragraph 26; and Case C-342/12 *Worten* EU:C:2013:355, paragraph 33).

72 Under Article 6 of Directive 95/46 and without prejudice to specific provisions that the Member States may lay down in respect of processing for historical, statistical or scientific purposes, the controller has the task of ensuring that personal data are processed 'fairly and lawfully', that they are 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes', that they are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed', that they are 'accurate and, where necessary, kept up to date' and, finally, that they are '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'. In this context, the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified.

73 As regards legitimation, under Article 7 of Directive 95/46, of processing such as that at issue in the main proceedings carried out by the operator of a search engine, that processing is capable of being covered by the ground in Article 7(f).

74 This provision permits the processing of personal data where it 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 — in particular his right to privacy with respect to the processing of personal data — which require protection under Article 1(1) of the directive. Application of Article 7(f) thus necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter (see *ASNEF and FECEMD*, EU:C:2011:777, paragraphs 38 and 40).

75 Whilst the question whether the processing complies with Articles 6 and 7(f) of Directive 95/46 may be determined in the context of a request as provided for in Article 12(b) of the directive, the data subject may, in addition, rely in certain conditions on the right to object laid down in subparagraph (a) of the first paragraph of Article 14 of the directive.

76 Under subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, Member States are to grant the data subject the right, at least in the cases referred to in Article 7(e) and (f) of the directive, to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. The

balancing to be carried out under subparagraph (a) of the first paragraph of Article 14 thus enables account to be taken in a more specific manner of all the circumstances surrounding the data subject's particular situation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.

77 Requests under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 may be addressed by the data subject directly to the controller who must then duly examine their merits and, as the case may be, end processing of the data in question. Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly.

78 In this connection, it is to be noted that it is clear from Article 28(3) and (4) of Directive 95/46 that each supervisory authority is to hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data and that it has investigative powers and effective powers of intervention enabling it to order in particular the blocking, erasure or destruction of data or to impose a temporary or definitive ban on such processing.

79 It is in the light of those considerations that it is necessary to interpret and apply the provisions of Directive 95/46 governing the data subject's rights when he lodges with the supervisory authority or judicial authority a request such as that at issue in the main proceedings.

80 It must be pointed out at the outset that, as has been found in paragraphs 36 to 38 of the present judgment, processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C-509/09 and C-161/10 *eDate Advertising and Others* EU:C:2011:685, paragraph 45).

81 In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing. However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

82 Following the appraisal of the conditions for the application of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 which is to be carried out when a request such as that at issue in the main proceedings is lodged with it, the supervisory authority or judicial authority may order the operator of the search engine to remove from the list of results displayed following a search made on the basis of a person's name links to web pages published by third parties containing

information relating to that person, without an order to that effect presupposing the previous or simultaneous removal of that name and information — of the publisher's own accord or following an order of one of those authorities — from the web page on which they were published.

83 As has been established in paragraphs 35 to 38 of the present judgment, inasmuch as the data processing carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites and affects the data subject's fundamental rights additionally, the operator of the search engine as the controller in respect of that processing must ensure, within the framework of its responsibilities, powers and capabilities, that that processing meets the requirements of Directive 95/46, in order that the guarantees laid down by the directive may have full effect.

84 Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites.

85 Furthermore, the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit, by virtue of Article 9 of Directive 95/46, from derogations from the requirements laid down by the directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine. It cannot therefore be ruled out that in certain circumstances the data subject is capable of exercising the rights referred to in Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 against that operator but not against the publisher of the web page.

86 Finally, it must be stated that not only does the ground, under Article 7 of Directive 95/46, justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, the outcome of the weighing of the interests at issue to be carried out under Article 7(f) and subparagraph (a) of the first paragraph of Article 14 of the directive may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page is at issue, given that, first, the legitimate interests justifying the processing may be different and, second, the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same.

87 Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page.

88 In the light of all the foregoing considerations, the answer to Question 2(c) and (d) is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

Question 3, concerning the scope of the data subject's rights guaranteed by Directive 95/46

89 By Question 3, the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as enabling the data subject to require the operator of a search engine to remove from the list of results displayed following a search made on the basis of his name links to web pages published lawfully by third parties and containing true information relating to him, on the ground that that information may be prejudicial to him or that he wishes it to be 'forgotten' after a certain time.

90 Google Spain, Google Inc., the Greek, Austrian and Polish Governments and the Commission consider that this question should be answered in the negative. Google Spain, Google Inc., the Polish Government and the Commission submit in this regard that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 confer rights upon data subjects only if the processing in question is incompatible with the directive or on compelling legitimate grounds relating to their particular situation, and not merely because they consider that that processing may be prejudicial to them or they wish that the data being processed sink into oblivion. The Greek and Austrian Governments submit that the data subject must approach the publisher of the website concerned.

91 According to Mr Costeja González and the Spanish and Italian Governments, the data subject may oppose the indexing by a search engine of personal data relating to him where their dissemination through the search engine is prejudicial to him and his fundamental rights to the protection of those data and to privacy — which encompass the 'right to be forgotten' — override the legitimate interests of the operator of the search engine and the general interest in freedom of information.

92 As regards Article 12(b) of Directive 95/46, the application of which is subject to the condition that the processing of personal data be incompatible with the directive, it should be recalled that, as has been noted in paragraph 72 of the present judgment, such incompatibility may result not only from the fact that such data are inaccurate but, in particular, also from the fact that they are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.

93 It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.

94 Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.

95 So far as concerns requests as provided for by Article 12(b) of Directive 95/46 founded on alleged non-compliance with the conditions laid down in Article 7(f) of the directive and requests under subparagraph (a) of the first paragraph of Article 14 of the directive, it must be pointed out that in each case the processing of personal data must be authorised under Article 7 for the entire period during which it is carried out.

96 In the light of the foregoing, when appraising such requests made in order to oppose processing such as that at issue in the main proceedings, it should in particular be examined whether the data subject has a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name. In this connection, it must be pointed out that it is not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data subject.

97 As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held, as follows in particular from paragraph 81 of the present judgment, that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.

98 As regards a situation such as that at issue in the main proceedings, which concerns the display, in the list of results that the internet user obtains by making a search by means of Google Search on the basis of the data subject's name, of links to pages of the on-line archives of a daily newspaper that contain announcements mentioning the data subject's name and relating to a real-estate auction connected with attachment proceedings for the recovery of social security debts, it should be held that, having regard to the sensitivity for the data subject's private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list. Accordingly, since in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, a matter which is, however, for the referring court to establish, the data subject may, by virtue of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, require those links to be removed from the list of results.

99 It follows from the foregoing considerations that the answer to Question 3 is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

Costs

100 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

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

1. **Article 2(b) and (d) 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 are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).**

2. **Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.**

3. **Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.**

4. **Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.**

[Signatures]

Reports of Cases

JUDGMENT OF THE COURT (Third Chamber)

17 July 2014*

(Request for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Articles 2, 12 and 13 — Concept of 'personal data' — Scope of the right of access of a data subject — Data relating to the applicant for a residence permit and legal analysis contained in an administrative document preparatory to the decision — Charter of Fundamental Rights of the European Union — Articles 8 and 41)

In Joined Cases C-141/12 and C-372/12,

REQUESTS for a preliminary ruling under Article 267 TFEU from the Rechtbank Middelburg (C-141/12) and from the Raad van State (C-372/12) (Netherlands), made by decisions of 15 March 2012 and 1 August 2012 respectively, received at the Court on 20 March 2012 and 3 August 2012, in the proceedings

YS (C-141/12)

v

Minister voor Immigratie, Integratie en Asiel,

and

Minister voor Immigratie, Integratie en Asiel (C-372/12)

v

M,

S,

THE COURT (Third Chamber),

composed of M. Ilešič (Rapporteur), President of the Chamber, C.G. Fernlund, A. Ó Caoimh, C. Toader and E. Jarašiūnas, Judges,

Advocate General: E. Sharpston,

Registrar: M. Ferreira, Principal Administrator,

having regard to the written procedure and further to the hearing on 3 July 2013,

* Language of the case: Dutch.

after considering the observations submitted on behalf of:

— YS, M and S, by B. Scholten, J. Hoftijzer and I. Oomen, advocaten,

— the Netherlands Government, by B. Koopman and C. Wissels, acting as Agents,

— the Czech Government, by M. Smolek, acting as Agent,

— the Greek Government, by E.-M. Mamouna and D. Tsagkaraki, acting as Agents,

— the French Government, by D. Colas and S. Menez, acting as Agents,

— the Austrian Government, by C. Pesendorfer, acting as Agent,

— the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,

— the European Commission, by B. Martenczuk, P. van Nuffel and C. ten Dam, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 12 December 2013,

gives the following

Judgment

1 These requests for a preliminary ruling concern the interpretation of Articles 2(a), 12(a) and 13(1)(d), (f) and (g) 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 (OJ 1995 L 281, p. 31), and of Articles 8(2) and 41(2)(b) of the Charter of Fundamental Rights of the European Union ('the Charter').

2 The requests have been made in two sets of proceedings between YS, a third country national who applied for a residence permit for a fixed period in the Netherlands, and the Minister voor Immigratie, Integratie en Asiel (Minister for Immigration, Integration and Asylum, 'the Minister') and between the Minister and M and S, also third country nationals who made the same type of application, concerning the Minister's refusal to communicate to those nationals a copy of an administrative document drafted before the adoption of the decisions on their applications for residence permits.

Legal context

EU law

3 Directive 95/46, the object of which, according to Article 1, is to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, and to remove obstacles to the free flow of personal data, states in recitals 25 and 41 in its preamble:

'(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons ... responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the

data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

...

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; ...'

4 The concept of 'personal data' is defined in Article 2(a) of Directive 95/46 as 'any information relating to an identified or identifiable natural person ("data subject")'.

5 Article 12 of that directive, entitled 'Right of access', provides as follows:

'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,

...

(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.'

6 Article 13(1) of that directive, entitled 'Exemptions and restrictions', provides:

'Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in [Article] ... 12 ... when such a restriction constitutes a necessary [measure] to safeguard:

...

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

...

(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.'

7 Article 14 of the directive provides that Member States are to grant the data subject the right, in certain circumstances, to object to the processing of data relating to him.

8 Under Articles 22 and 23(1) of the directive, Member States are to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question and to provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the directive is entitled to receive compensation from the controller for the damage suffered.

Netherlands law

9 Articles 2, 12 and 13 of Directive 95/46 were transposed into national law by Articles 1, 35 and 43 respectively of the Law on the Protection of Personal Data (Wet bescherming persoonsgegevens, 'the Wbp').

10 Article 35 of the Wbp is worded as follows:

'The data subject shall have the right to apply to the controller without restraint and at reasonable intervals to be notified as to whether data relating to him are being processed. The controller shall notify the data subject in writing within four weeks if data relating to him are being processed.

Where such data are being processed, such notification shall contain a full overview thereof in an intelligible form, a description of the purpose or purposes of the processing, the categories of data concerned and the recipients or categories of recipients, as well as any available information as to the source of the data.'

11 Under Article 43(e) of the Wbp, the controller can exclude application of Article 35 of the Wbp in so far as is necessary in the interests of protecting the data subject or the rights and freedoms of others.

12 Under Article 29(1)(a) of the Law on Foreign Nationals 2000 (Vreemdelingenwet 2000, the 'Vw 2000'), a residence permit for a fixed period may be granted to a foreign national who is a refugee. Under Article 29(1)(b) of that law, such a permit may also be granted to a foreign national who has proved that he has good grounds for believing that if he is expelled he will run a real risk of being subjected to the death penalty or execution, to torture, inhuman or degrading treatment or punishment, or to serious and individual threat to a civilian's life or person by reason of indiscriminate violence in situations of international or internal armed conflict.

The disputes in the main proceedings and the questions referred for a preliminary ruling

13 The case officer of the Immigration and Naturalisation Service responsible for dealing with an application for a residence permit draws up, where he is not authorised to sign the decision, a draft decision which is submitted for assessment to a reviser in that service. The case officer attaches a document in which he explains to the reviser the reasons for his draft decision ('the minute'). Where the case officer has the authority to sign, the minute is not submitted to a reviser but is used as an explanatory memorandum of the decision making process to justify the decision internally. The minute is part of the preparatory process within that service but not of the final decision, even though some points mentioned in it may reappear in the statement of reasons of that decision.

14 Generally, the minute contains the following information: name, telephone and office number of the case officer responsible for preparing the decision; boxes for the initials and names of revisers; data relating to the applicant, such as name, date of birth, nationality, gender, ethnicity, religion and

language; details of the procedural history; details of the statements made by the applicant and the documents submitted; the legal provisions which are applicable; and, finally, an assessment of the foregoing information in the light of the applicable legal provisions. This assessment is referred to as the 'legal analysis'.

15 Depending on the case, the legal analysis may be more or less extensive, varying from a few sentences to several pages. In an in-depth analysis, the case officer responsible for the preparation of the decision addresses, inter alia, the credibility of the statements made and explains why he considers an applicant eligible or not for a residence permit. A summary analysis may merely refer to the application of a particular policy line.

16 Until 14 July 2009, the Minister's policy was to make the minute available upon mere request. Taking the view that the large number of those requests resulted in too great a work load, that the data subjects often misinterpreted the legal analyses contained in the minutes which were made available to them and that, because of that availability, the exchange of views within the Immigration and Naturalisation Service was recorded less frequently in the minutes, the Minister abandoned that policy.

17 Since then, requests for the communication of minutes have been systematically refused. Instead of obtaining a copy of the minute, the applicant now receives a summary of the personal data contained in the document, including information relating to the origin of those data and, where relevant, the bodies to which they were disclosed.

Case C-141/12

18 On 13 January 2009, YS submitted an application for a residence permit for a fixed period under asylum law. The application was rejected by decision of 9 June 2009. That decision was withdrawn by letter of 9 April 2010, and the application was once again rejected by decision of 6 July 2010.

19 By letter of 10 September 2010, YS asked for the minute relating to the decision of 6 July 2010 to be communicated to him.

20 By decision of 24 September 2010, that was refused. However, the decision did give a summary of the data contained in the minute, the origin of those data and the bodies to which the data had been disclosed. YS lodged an objection against the refusal to communicate the minute, which itself was rejected by decision of 22 March 2011.

21 YS then brought an action against that rejection decision before the Rechtbank Middelburg (District Court, Middelburg), on the ground that he could not lawfully be refused access to that minute.

22 In those circumstances, the Rechtbank Middelburg decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'1. Are the data reproduced in the minute concerning the data subject and which relate to the data subject personal data within the meaning of Article 2(a) of [Directive 95/46]?

2. Does the legal analysis included in the minute constitute personal data within the meaning of the aforementioned provision?

3. If the Court of Justice confirms that the data described above are personal data, should the processor/government body grant access to those personal data pursuant to Article 12 of [Directive 95/46] and Article 8(2) of the Charter?

4. In that context, may the data subject rely directly on Article 41(2)(b) of the Charter, and if so, must the phrase "while respecting the legitimate interests of confidentiality [in decision-making]" included therein be interpreted in such a way that the right of access to the minute may be refused on that ground?

5. When the data subject requests access to the minute, should the processor/government body provide a copy of that document in order to do justice to the right of access?'

Case C-372/12

The dispute concerning M

23 By decision of 28 October 2009, the Minister granted M a residence permit for a fixed period as asylum seeker on the basis of Article 29(1)(b) of the Vw 2000. The reasons for that decision were not given, in that it did not set out the manner in which the case had been assessed by the Immigration and Naturalisation Service.

24 By letter of 30 October 2009, M, on the basis of Article 35 of the Wbp, requested access to the minute relating to that decision.

25 By decision of 4 November 2009, the Minister refused M access to the minute. He based the refusal on Article 43(e) of the Wbp, since he was of the view that access to such a document was liable adversely to affect the freedom of the case worker responsible for compiling it to include certain arguments and considerations in the minute which could be relevant in the decision-making process.

26 The objection to that refusal having been rejected by decision of 3 December 2010, M brought an action against that decision before the Rechtbank Middelburg. By decision of 16 June 2011, that court took the view that the interest relied on by the Minister to refuse access to the minute did not amount to an interest protected by Article 43(e) of the Wbp, and annulled the Minister's decision as being based on reasoning that was wrong in law. It also found that there was no reason to maintain the legal effects of the decision, since the Minister, contrary to Article 35(2) of the Wbp, had not given access to the legal analysis in the minute from which it might have become evident why M could not be considered to be a refugee for the purposes of Article 29(1)(a) of the Vw 2000.

The dispute concerning S

27 By decision of 10 February 2010, which did not state reasons, the Minister granted S an ordinary residence permit for a fixed period on the ground of 'dramatic circumstances'. By letter of 19 February 2010, S, on the basis of Article 35 of the Wbp, requested the minute relating to that decision.

28 The request was rejected by decision of 31 March 2010, which was confirmed by decision of 21 October 2010 following an objection. In the decision of 21 October 2010, the Minister took the position that the decision of 31 March 2010 had already stated which personal data were included in the minute and that the request for access to the minute had thus been met. Furthermore, he was of the opinion that the Wbp does not confer any rights of access to the minute.

29 By decision of 4 August 2011, the Rechtbank Amsterdam (District Court, Amsterdam) declared well-founded the action brought by S against the decision of 21 October 2010 and annulled that decision. That court found, inter alia, that the minute in question did not contain any information other than personal data of S, that he had a right of access to those data under the Wbp, and that the Minister's refusal to allow access was not validly based.

30 The Minister decided to appeal to the Raad van State (Council of State) both in the dispute concerning M and in that concerning S.

31 In those circumstances, the Raad van State decided to join the cases concerning M and S, to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

‘1. Should the second indent of Article 12(a) of [Directive 95/46] be interpreted to mean that there is a right to a copy of documents in which personal data have been processed, or is it sufficient if a full summary, in an intelligible form, of the personal data that have undergone processing in the documents concerned is provided?

2. Should the words “right of access” in Article 8(2) of [the Charter] be interpreted to mean that there is a right to a copy of documents in which personal data have been processed, or is it sufficient if there is provision of a full summary, in an intelligible form, of the personal data that have undergone processing in the documents concerned within the meaning of the second indent of Article 12(a) of [Directive 95/46]?

3. Is Article 41(2)(b) of [the Charter] also addressed to the Member States of the European Union in so far as they are implementing EU law within the meaning of Article 51(1) of that Charter?

4. Does the consequence that, as a result of the granting of access to “minutes”, the reasons why a particular decision is proposed are no longer recorded therein, which is not in the interests of the internal undisturbed exchange of views within the public authority concerned and of orderly decision-making, constitute a legitimate interest of confidentiality within the meaning of Article 41(2)(b) of [the Charter]?

5. Can a legal analysis, as set out in a “minute”, be regarded as personal data within the meaning of Article 2(a) of [Directive 95/46]?

6. Does the protection of the rights and freedoms of others, within the meaning of Article 13(1)(g) of [Directive 95/46] …, also cover the interest in an internal undisturbed exchange of views within the public authority concerned? If the answer to that is in the negative, can that interest then be covered by Article 13(1)(d) or (f) of that directive?’

32 By decision of 30 April 2013, Cases C-141/12 and C-372/12 were joined for the purposes of the oral procedure and of the judgment.

Consideration of the questions referred

The first and second questions in Case C-141/12 and the fifth question in Case C-372/12, concerning the concept of ‘personal data’

33 By the first and second questions in Case C-141/12 and the fifth question in Case C-372/12, which it is appropriate to examine together, the referring courts ask, in essence, whether Article 2(a) of Directive 95/46 must be interpreted as meaning that the data relating to the applicant for a residence permit and the legal analysis included in the minute are ‘personal data’ within the meaning of that provision.

34 Although all interested parties who adopted a view on this point consider that the data relating to the applicant for a residence permit included in the minute correspond to the concept of ‘personal data’ and propose, consequently, that a positive reply be given to the first question in Case C-141/12, opinions differ in relation to the legal analysis in that administrative document, which is the subject of the second question in that case and the fifth question in Case C-372/12.

35 YS, M and S, the Greek, Austrian and Portuguese Governments and the European Commission consider that, in so far as the legal analysis refers to a specific natural person and is based on the situation and that person's individual characteristics, it also comes under the concept of 'personal data'. The Greek Government and the Commission state, however, that that applies solely to legal analyses which contain information concerning an individual and not to those which contain only an abstract legal interpretation, while M and S consider that even such an abstract interpretation falls within the scope of that provision if it is decisive for the assessment of the application for a residence permit and is applied to the specific case of the applicant.

36 By contrast, according to the Netherlands, Czech and French Governments, the legal analysis in a minute does not come under the concept of 'personal data'.

37 In this respect, it should be noted that Article 2(a) of Directive 95/46 defines personal data as 'any information relating to an identified or identifiable natural person'.

38 There is no doubt that the data relating to the applicant for a residence permit and contained in a minute, such as the applicant's name, date of birth, nationality, gender, ethnicity, religion and language, are information relating to that natural person, who is identified in that minute in particular by his name, and must consequently be considered to be 'personal data' (see, to that effect, inter alia the judgment in *Huber*, C-524/06, EU:C:2008:724, paragraphs 31 and 43).

39 As regards, on the other hand, the legal analysis in a minute, it must be stated that, although it may contain personal data, it does not in itself constitute such data within the meaning of Article 2(a) of Directive 95/46.

40 As the Advocate General noted in essence in point 59 of her Opinion, and as the Netherlands, Czech and French Governments noted, such a legal analysis is not information relating to the applicant for a residence permit, but at most, in so far as it is not limited to a purely abstract interpretation of the law, is information about the assessment and application by the competent authority of that law to the applicant's situation, that situation being established inter alia by means of the personal data relating to him which that authority has available to it.

41 That interpretation of the concept of 'personal data' for the purposes of Directive 95/46 not only follows from the wording of Article 2(a) but is also borne out by the objective and general scheme of that directive.

42 In accordance with Article 1 of that directive, its purpose is to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data, and thus to permit the free flow of personal data between Member States.

43 According to recital 25 in the preamble to Directive 95/46, the principles of protection of natural persons provided therein are reflected, on the one hand, in the obligations imposed on those responsible for processing data concerning those persons and, on the other hand, in the rights conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.

44 As regards those rights of the data subject, referred to in Directive 95/46, it must be noted that the protection of the fundamental right to respect for private life means, inter alia, that that person may be certain that the personal data concerning him are correct and that they are processed in a lawful manner. As is apparent from recital 41 in the preamble to that directive, it is in order to carry out the necessary checks that the data subject has, under Article 12(a) of the directive, a right of access to the data relating to him which are being processed. That right of access is necessary, inter alia, to enable the data subject to obtain, depending on the circumstances, the rectification, erasure or blocking of

his data by the controller and consequently to exercise the right set out in Article 12(b) of that directive (see, to that effect, the judgment in *Rijkeboer*, C-553/07, EU:C:2009:293, paragraphs 49 and 51).

45 In contrast to the data relating to the applicant for a residence permit which is in the minute and which may constitute the factual basis of the legal analysis contained therein, such an analysis, as the Netherlands and French Governments have noted, is not in itself liable to be the subject of a check of its accuracy by that applicant and a rectification under Article 12(b) of Directive 95/46.

46 In those circumstances, extending the right of access of the applicant for a residence permit to that legal analysis would not in fact serve the directive's purpose of guaranteeing the protection of the applicant's right to privacy with regard to the processing of data relating to him, but would serve the purpose of guaranteeing him a right of access to administrative documents, which is not however covered by Directive 95/46.

47 In an analogous context, as regards the processing of personal data by the EU institutions, governed on the one hand by 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), and on the other by Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ 2001 L 145, p. 43), the Court has previously held, in paragraph 49 of the judgment in *Commission* v *Bavarian Lager*, C-28/08 P, EU:C:2010:378, that those regulations have different objectives and that, in contrast to Regulation No 1049/2001, Regulation No 45/2001 is not designed to ensure the greatest possible transparency of the decision-making process of the public authorities and to promote good administrative practices by facilitating the exercise of the right of access to documents. That finding applies equally to Directive 95/46, which, in essence, has the same objective as Regulation No 45/2001.

48 It follows from all the foregoing considerations that the answer to the first and second questions in Case C-141/12 and the fifth question in Case C-372/12 is that Article 2(a) of Directive 95/46 must be interpreted as meaning that the data relating to the applicant for a residence permit contained in the minute and, where relevant, the data in the legal analysis contained in the minute are 'personal data' within the meaning of that provision, whereas, by contrast, that analysis cannot in itself be so classified.

The sixth question in Case C-372/12, concerning the possibility of limiting the right of access

49 In the light of the answer given to the first and second questions in Case C-141/12 and to the fifth question in Case C-372/12, and since the referring court specified that the sixth question raised in Case C-372/12 requires an answer only if the legal analysis in the minute must be classified as personal data, there is no need to answer that sixth question.

The third and fifth questions in Case C-141/12 and the first and second questions in Case C-372/12, concerning the scope of the right of access

50 By the third and fifth questions in Case C-141/12 and by the first and second questions in Case C-372/12, which it is appropriate to examine together, the referring courts ask, in essence, whether Article 12(a) of Directive 95/46 and Article 8(2) of the Charter must be interpreted as meaning that the applicant for a residence permit has a right of access to data concerning him which are in the minute and, if so, whether that right to access implies that the competent authorities must provide him with a copy of that minute or whether it is sufficient for them to send him a full summary of those data in an intelligible form.

51 All the parties to the proceedings before the Court agree that Article 12(a) of Directive 95/46 grants an applicant for a residence permit a right of access to all the personal data contained in the minute, although their views as regards the actual extent of that right differ according to their interpretation of the concept of 'personal data'.

52 As regards the form that that access must take, YS, M and S and the Greek Government consider that the applicant has the right to obtain a copy of the minute. They maintain that only such a copy would allow him to ensure that he is in possession of all the personal data which concern him in the minute.

53 By contrast, according to the Netherlands, Czech, French and Portuguese Governments and the Commission, neither Article 12(a) of Directive 95/46 nor Article 8(2) of the Charter requires Member States to provide a copy of the minute to the applicant for a residence permit. Thus, there are other possible ways of disclosing, in an intelligible form, the personal data contained in such a document, inter alia by providing him with a full and comprehensible summary of those data.

54 As a preliminary point, it should be noted that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law of the Court, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter (see, inter alia, the judgments in *Connolly* v *Commission*, C-274/99 P, EU:C:2001:127, paragraph 37; *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; and *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 68).

55 Article 8 of the Charter, which guarantees the right to the protection of personal data, provides in paragraph 2, inter alia, that everyone has the right of access to data which have been collected concerning him or her. That requirement is implemented by Article 12(a) of Directive 95/46 (see, to that effect, the judgment in *Google Spain and Google*, EU:C:2014:317, paragraph 69).

56 That provision of Directive 95/46 provides that Member States are to guarantee every data subject the right to obtain from the controller, without constraint at reasonable intervals and without excessive delay or expense, communication to him in an intelligible form of the data undergoing processing and of any available information as to their source.

57 Although Directive 95/46 requires Member States to ensure that every data subject can obtain from the controller of personal data communication of all such data processed by the controller relating to the data subject, it leaves it to the Member States to determine the actual material form that that communication must take, as long as it is 'intelligible', in other words it allows the data subject to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that that person may, where relevant, exercise the rights conferred on him by Articles 12(b) and (c), 14, 22 and 23 of the directive (see, to that effect, the judgment in *Rijkeboer*, EU:C:2009:293, paragraphs 51 and 52).

58 Therefore, in so far as the objective pursued by that right of access may be fully satisfied by another form of communication, the data subject cannot derive from either Article 12(a) of Directive 95/46 or Article 8(2) of the Charter the right to obtain a copy of the document or the original file in which those data appear. In order to avoid giving the data subject access to information other than the personal data relating to him, he may obtain a copy of the document or the original file in which that other information has been redacted.

59 In situations such as those in the main proceedings, it follows from the answer given in paragraph 48 above that only the data relating to the applicant for a residence permit contained in the minute and, where relevant, the data in the legal analysis contained in the minute are 'personal data' within the meaning of Article 2(a) of Directive 95/46. Consequently the right of access which that applicant may

rely on under Article 12(a) of Directive 95/46 and Article 8(2) of the Charter relates solely to those data. For that right of access to be complied with, it is sufficient for the applicant for a residence permit to be provided with a full summary of all of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him by Articles 12(b) and (c), 14, 22 and 23 of that directive.

60 It follows from the foregoing considerations that the answer to the third and fifth questions in Case C-141/12 and the first and second questions in Case C-372/12 is that Article 12(a) of Directive 95/46 and Article 8(2) of the Charter must be interpreted as meaning that an applicant for a residence permit has a right of access to all personal data concerning him which are processed by the national administrative authorities within the meaning of Article 2(b) of that directive. For that right to be complied with, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him by that directive.

The fourth question in Case C-141/12 and the third and fourth questions in Case C-372/12, concerning Article 41 of the Charter

61 By the fourth question in Case C-141/12 and the third and fourth questions in Case C-372/12, which it is appropriate to examine together, the referring courts ask, in essence, whether Article 41(2)(b) of the Charter must be interpreted as meaning that the applicant for a residence permit may rely against national authorities on the right of access to the file provided for in that provision and, if so, what is the scope of the phrase 'while respecting the legitimate interests of confidentiality' in decision-making within the meaning of that provision.

62 The Commission considers that those questions are inadmissible on account of their hypothetical and obscure wording.

63 It should be borne in mind that, according to settled case-law of the Court, questions on the interpretation of EU law referred by a national court in the factual and legislative context which that court is responsible for defining, and the accuracy of which is not a matter for the Court to determine, enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (see, inter alia, the judgment in *Márquez Samohano*, C-190/13, EU:C:2014:146, paragraph 35 and the case-law cited).

64 However, that is not so in the present case. In the light of the factual context outlined by the referring courts, it does not appear that the question of whether the applicants in the main proceedings may, pursuant to Article 41(2)(b) of the Charter, rely on a right of access to the file concerning their applications for a residence permit is of a purely hypothetical nature. The wording of the questions and the information concerning them in the orders for reference are, furthermore, sufficiently clear to determine the scope of those questions and to enable, first, the Court to answer them and, secondly, the interested parties to submit their observations pursuant to Article 23 of the Statute of the Court of Justice of the European Union.

65 On the substance of the questions referred, YS, M and S as well as the Greek Government consider that the applicant for a resident permit may take Article 41(2)(b) of the Charter as a basis for a right of access to the file, given that, in the context of the procedure for granting such a permit, the national authorities apply the asylum directives. By contrast, the Netherlands, Czech, French, Austrian

and Portuguese Governments and the Commission consider that Article 41 of the Charter is directed exclusively at the EU institutions and cannot, therefore, establish a right of access to a file in the context of a national procedure.

66 It should be noted from the outset that Article 41 of the Charter, 'Right to good administration', states in paragraph 1 that every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the European Union. Article 41(2) specifies that that right includes the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy.

67 It is clear from the wording of Article 41 of the Charter that it is addressed not to the Member States but solely to the institutions, bodies, offices and agencies of the European Union (see, to that effect, the judgment in *Cicala*, C-482/10, EU:C:2011:868, paragraph 28). Consequently, an applicant for a resident permit cannot derive from Article 41(2)(b) of the Charter a right to access the national file relating to his application.

68 It is true that the right to good administration, enshrined in that provision, reflects a general principle of EU law (judgment in *HN*, C-604/12, EU:C:2014:302, paragraph 49). However, by their questions in the present cases, the referring courts are not seeking an interpretation of that general principle, but ask whether Article 41 of the Charter may, in itself, apply to the Member States of the European Union.

69 Consequently, the answer to the fourth question in Case C-141/12 and the third and fourth questions in Case C-372/12 is that Article 41(2)(b) of the Charter must be interpreted as meaning that the applicant for a residence permit cannot rely on that provision against the national authorities.

Costs

70 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Third Chamber) hereby rules:

1. **Article 2(a) 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 must be interpreted as meaning that the data relating to an applicant for a residence permit contained in an administrative document, such as the 'minute' at issue in the main proceedings, setting out the grounds that the case officer puts forward in support of the draft decision which he is responsible for drawing up in the context of the procedure prior to the adoption of a decision concerning the application for such a permit and, where relevant, the data in the legal analysis contained in that document, are 'personal data' within the meaning of that provision, whereas, by contrast, that analysis cannot in itself be so classified.**

2. **Article 12(a) of Directive 95/46 and Article 8(2) of the Charter of Fundamental Rights of the European Union must be interpreted as meaning that an applicant for a residence permit has a right of access to all personal data concerning him which are processed by the national administrative authorities within the meaning of Article 2(b) of that directive. For that right to be complied with, it is sufficient that the applicant be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that**

applicant to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him by that directive.

3. **Article 41(2)(b) of the Charter of Fundamental Rights of the European Union must be interpreted as meaning that the applicant for a residence permit cannot rely on that provision against the national authorities.**

[Signatures]