ECLI:EU:C:2016:779

JUDGMENT OF THE COURT (Second Chamber)

19 October 2016 (*)

(Reference for a preliminary ruling — Processing of personal data — Directive 95/46/EC — Article 2(a) — Article 7(f) — Definition of 'personal data' — Internet protocol addresses — Storage of data by an online media services provider — National legislation not permitting the legitimate interest pursued by the controller to be taken into account)

In Case C-582/14,

REQUEST for a preliminary ruling under Article 267 TFEU, from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 28 October 2014, received at the Court on 17 December 2014, in the proceedings

Patrick Breyer

v

Bundesrepublik Deutschland,

THE COURT (Second Chamber),

composed of M. Ilešič, President of the Chamber, A. Prechal, A. Rosas (Rapporteur), C. Toader and E. Jarašiūnas, Judges,

Advocate General: M. Campos Sánchez-Bordona,

Registrar: V. Giacobbo-Peyronnel, Administrator,

having regard to the written procedure and further to the hearing on 25 February 2016,

after considering the observations submitted on behalf of:

– Mr Breyer, by M. Starostik, Rechtsanwalt,

– the German Government, by A. Lippstreu and T. Henze, acting as Agents,

– the Austrian Government, by G. Eberhard, acting as Agent,

– the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,

– the European Commission, by P.J.O. Van Nuffel and H. Krämer, and P. Costa de Oliveira and J. Vondung, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 12 May 2016,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 2(a) and 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 request has been made in proceedings between Mr Patrick Breyer and the Bundesrepublik Deutschland (Federal Republic of Germany) concerning the registration and storage by the latter of the internet protocol address ('IP address') allocated to Mr Breyer when he accessed several internet sites run by German Federal institutions.

Legal context

EU law

3 Recital 26 of Directive 95/46 reads as follows:

'Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.'

4 Article 1 of that directive provides:

‘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 2 of the same directive provides:

‘For the purpose 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;

…

(f) “third party” shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;

…’

6 Article 3 of Directive 95/46, entitled ‘Scope’, provides:

‘1. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

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

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

…'

7 Article 5 of that directive reads 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.'

8 Article 7 of the directive is worded as follows:

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

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

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

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

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

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

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

9 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 measures to safeguard:

…

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

…'

German law

10 Paragraph 12 of the Telemediengesetz (Law on telemedia) of 26 February 2007 (BGBl. 2007 I, p. 179, 'TMG'), provides:

'(1) A service provider may collect and use personal data to make telemedia available only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.

(2) Where personal data have been supplied in order for telemedia to be made available, a service provider may use them for other purposes only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.

(3) Except as otherwise provided, the provisions concerning the protection of personal data which are applicable in the case in question shall apply even if the data are not processed automatically.'

11 Paragraph 15 of the TMG provides:

'(1) A service provider may collect and use the personal data of a user only to the extent necessary in order to facilitate, and charge for, the use of telemedia (data concerning use). Data concerning use include, in particular:

1. particulars for the identification of the user,

2. information about the beginning, end and extent of the particular use, and

3. information about the telemedia used by the user.

(2) A service provider may combine the data concerning use of a user relating to the use of different telemedia to the extent that this is necessary for purposes of charging the user.

…

(4) A service provider may use data concerning use after the end of the use to the extent that they are required for purposes of charging the user (invoicing data). The service provider may block the data in order to comply with existing limits on storage periods laid down by law, statutes or contract.'

12 Under Paragraph 3(1) of the Bundesdatenschutzgesetz (Federal Data Protection Law) of 20 December 1990 (BGBl. 1990 I, p. 2954, 'personal data are individual indications concerning the personal or factual circumstances of an identified or identifiable natural person (data subject). …'.

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

13 Mr Breyer has accessed several websites operated by German Federal institutions. On the websites, which are accessible to the public, those institutions provide topical information.

14 With the aim of preventing attacks and making it possible to prosecute 'pirates', most of those websites store information on all access operations in logfiles. The information retained in the logfiles after those sites have been accessed include the name of the web page or file to which access was sought, the terms entered in the search fields, the time of access, the quantity of data transferred, an indication of whether access was successful, and the IP address of the computer from which access was sought.

15 IP addresses are series of digits assigned to networked computers to facilitate their communication over the internet. When a website is accessed, the IP address of the computer seeking access is communicated to the server on which the website consulted is stored. That connection is necessary so that the data accessed maybe transferred to the correct recipient.

16 Furthermore, it is clear from the order for the reference and the documents before the Court that internet service providers allocate to the computers of internet users either a 'static' IP address or a 'dynamic' IP address, that is to say an IP address which changes each time there is a new connection to the internet. Unlike static IP addresses, dynamic IP addresses do not enable a link to be established, through files accessible to the public, between a given computer and the physical connection to the network used by the internet service provider.

17 Mr Breyer brought an action before the German administrative courts seeking an order restraining the Federal Republic of Germany from storing, or arranging for third parties to store, after consultation of the websites accessible to the public run by the German Federal institutions' online media services, the IP address of the applicant's host system except in so far as its storage is unnecessary in order to restore the availability of those media in the event of a fault occurring.

18 Since Mr Breyer's action at first instance was dismissed, he brought an appeal against that decision.

19 The court of appeal varied that decision in part. It ordered the Federal Republic of Germany to refrain from storing or arranging for third parties to store, at the end of each consultation period, the IP address of the host system from which Mr Breyer sought

access, which was transmitted when he consulted publicly accessible websites of the German Federal institutions' online media, where that address is stored together with the date of the consultation period to which it relates and where Mr Breyer has revealed his identity during that use, including in the form of an electronic address mentioning his identity, except in so far as that storage is not necessary in order to restore the dissemination of those media in the event of a fault occurring.

20 According to the court of appeal, a dynamic IP address, together with the date on which the website was accessed to which that address relates constitutes, if the user of the website concerned has revealed his identity during that consultation period, personal data, because the operator of that website is able to identify the user by linking his name to his computer's IP address.

21 However, the court of appeal held that Mr Breyer's action could not be upheld in other situations. If Mr Breyer does not reveal his identity during a consultation period, only the internet service provider could connect the IP address to an identified subscriber. However, in the hands of the Federal Republic of Germany, in its capacity as provider of online media services, the IP address is not personal data, even in combination with the date of the consultation period to which it relates, because the user of the websites concerned is not identifiable by that Member State.

22 Mr Breyer and the Federal Republic of Germany each brought an appeal on a point of law before the Bundesgerichtshof (Federal Court of Justice, Germany) against the decision of the appeal court. Mr Breyer sought to have his application for an injunction upheld in its entirety. The Federal Republic of Germany sought to have it dismissed.

23 The referring court states that the dynamic IP addresses of Mr Breyer's computer stored by the Federal Republic of Germany, acting in its capacity as an online media services provider, are, at least in the context of other data stored in daily files, specific data on Mr Breyer's factual circumstances, given that they provide information relating to his use of certain websites or certain internet files on certain dates.

24 Nevertheless, the data stored does not enable Mr Breyer to be directly identified. The operators of the websites at issue in the main proceedings can identify Mr Breyer only if the information relating to his identity is communicated to them by his internet service provider. The classification of those data as 'personal data' thus depends on whether Mr Breyer is identifiable.

25 The Bundesgerichtshof (Federal Court of Justice) refers to the academic disagreement relating to whether, in order to determine whether someone is identifiable, an 'objective' or 'relative' criterion must be used. The application of an 'objective' criterion would have the consequence that data such as the IP addresses at issue in the main proceedings may be regarded, at the end of the period of use of the websites at issue, as being personal data even if only a third party is able to determine the identity of the data subject, that third party being, in the present case, Mr Breyer's internet service provider, which stored the additional data enabling his identification by means of those IP

addresses. According to a ‘relative’ criterion, such data may be regarded as personal data in relation to an entity such as Mr Breyer’s internet service provider because they allow the user to be precisely identified (see, in that connection, judgment of 24 November 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771, paragraph 51), but not being regarded as such with respect to another entity, since that operator does not have, if Mr Breyer has not disclosed his identity during the consultation of those websites, the information necessary to identify him without disproportionate effort.

26 If the dynamic IP addresses of Mr Breyer’s computer, together with the date of the relevant consultation period, were to be considered as constituting personal data, the referring court asks whether the storage of those IP addresses at the end of that consultation period is authorised by Article 7(f) of that directive.

27 In that connection, the Bundesgerichtshof (Federal Court of Justice) states, first, that under Paragraph 15(1) of the TMG, online media services providers may collect and use the personal data of a user only to the extent that that is necessary to facilitate and charge for the use of those media. Second, the referring court states that, according to the Federal Republic of Germany, storage of those data is necessary to guarantee the security and continued proper functioning of the online media services that it makes accessible to the public, in particular, enabling cyber attacks known as ‘denial-of-service’ attacks, which aim to paralyse the functioning of the sites by the targeted and coordinated saturation of certain web servers with huge numbers of requests, to be identified and combated.

28 According to the referring court, if and to the extent it is necessary for the online media services provider to take measures to combat such attacks, those measures may be regarded as necessary to ‘facilitate … the use of telemedia’ pursuant to Paragraph 15 of the TMG. However, academic opinion mostly supports the view, first, that the collection and use of personal data relating to the user of a website is authorised only in order to facilitate the specific use of that website and, second, that those data must be deleted at the end of period of consultation concerned if they are not data required for billing purposes. Such a restrictive reading of Paragraph 15(1) of the TMG would prevent the storage of IP addresses from being authorised in order to guarantee in a general manner the security and continued proper functioning of online media.

29 The referring court asks whether that interpretation, which is the interpretation advocated by the court of appeal, is in accordance with Article 7(f) of Directive 95/46, having regard, in particular with the criteria laid down by the Court in paragraph 29 et seq. of the judgment of 24 November 2011, *ASNEF and FECEMD* (C-468/10 and C-469/10, EU:C:2011:777).

30 In those circumstances the Bundesgerichtshof (Federal Court of Justice) decided to stay the proceedings before it and to refer the following questions to the Court for a preliminary ruling:

‘(1) Must Article 2(a) of Directive 95/46 … be interpreted as meaning that an internet protocol address (IP address) which an [online media] service provider stores when his website is accessed already constitutes personal data for the service provider if a third party (an access provider) has the additional knowledge required in order to identify the data subject?

(2) Does Article 7(f) of [that directive] preclude a provision in national law under which a service provider may collect and use a user’s personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of the telemedium by the user concerned, and under which the purpose of ensuring the general operability of the telemedium cannot justify use of the data beyond the end of the particular use of the telemedium?’

Consideration of the questions referred for a preliminary ruling

The first question

31 By its first question, the referring court asks essentially whether Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that that provider makes accessible to the public constitutes, with regard to that service provider, personal data within the meaning of that provision, where, only a third party, in the present case the internet service provider, has the additional data necessary to identify him.

32 According to that provision, ‘personal data’ ‘mean any information relating to an identified or identifiable natural person (“data subject”)’. Pursuant to that provision, 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.

33 As a preliminary point, it must be noted that, in paragraph 51 of the judgment of 24 November 2011, *Scarlet Extended* (C-70/10, EU:C:2011:771), which concerned inter alia the interpretation of the same directive, the Court held essentially that the IP addresses of internet users were protected personal data because they allow users to be precisely identified.

34 However, that finding by the Court related to the situation in which the collection and identification of the IP addresses of internet users is carried out by internet service providers.

35 In the present case, the first question concerns the situation in which it is the online media services provider, namely the Federal Republic of Germany, which registers IP addresses of the users of a website that it makes accessible to the public, without having the additional data necessary in order to identify those users.

36 Furthermore, it is common ground that the IP addresses to which the national court refers are ‘dynamic’ IP addresses, that is to say provisional addresses which are assigned for each internet connection and replaced when subsequent connections are made, and not ‘static’ IP addresses, which are invariable and allow continuous identification of the device connected to the network.

37 The referring court’s first question is based therefore on the premiss, first, that data consisting in a dynamic IP address and the date and time that a website was accessed from that IP address registered by an online media services provider do not, without more, give the service provider the possibility to identify the user who consulted that website during that period of use and, second, the internet services provider has additional data which, if combined with the IP address would enable the user to be identified.

38 In that connection, it must be noted, first of all, that it is common ground that a dynamic IP address does not constitute information relating to an ‘identified natural person’, since such an address does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer.

39 Next, in order to determine whether, in the situation described in paragraph 37 of the present judgment, a dynamic IP address constitutes personal data within the meaning of Article 2(a) of Directive 96/45 in relation to an online media services provider, it must be ascertained whether such an IP address, registered by such a provider, may be treated as data relating to an ‘identifiable natural person’ where the additional data necessary in order to identify the user of a website that the services provider makes accessible to the public are held by that user’s internet service provider.

40 In that connection, it is clear from the wording of Article 2(a) of Directive 95/46 that an identifiable person is one who can be identified, directly or indirectly.

41 The use by the EU legislature of the word ‘indirectly’ suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified.

42 Furthermore, recital 26 of Directive 95/46 states that, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.

43 In so far as that recital refers to the means likely reasonably to be used by both the controller and by ‘any other person’, its wording suggests that, for information to be treated as ‘personal data’ within the meaning of Article 2(a) of that directive, it is not required that all the information enabling the identification of the data subject must be in the hands of one person.

44 The fact that the additional data necessary to identify the user of a website are held not by the online media services provider, but by that user's internet service provider does not appear to be such as to exclude that dynamic IP addresses registered by the online media services provider constitute personal data within the meaning of Article 2(a) of Directive 95/46.

45 However, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject.

46 Thus, as the Advocate General stated essentially in point 68 of his Opinion, that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.

47 Although the referring court states in its order for reference that German law does not allow the internet service provider to transmit directly to the online media services provider the additional data necessary for the identification of the data subject, it seems however, subject to verifications to be made in that regard by the referring court that, in particular, in the event of cyber attacks legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings.

48 Thus, it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored.

49 Having regard to all the foregoing considerations, the answer to the first question is that Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.

The second question

50 By its second question, the referring court asks essentially whether Article 7(f) of Directive 95/46 must be interpreted as precluding the legislation of a Member State under which an online media services provider may collect and use a user's personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of those services by the user concerned, and under which the purpose of

ensuring the general operability of those services cannot justify use of the data beyond the end of the particular use of them.

51 Before answering that question, it must be determined whether the processing of personal data at issue in the main proceedings, that is dynamic IP addresses of users of certain websites of the German Federal institutions, is excluded from the scope of Directive 95/46 under Article 3(2), first indent thereof, pursuant to which that directive does not apply to personal data processing operations concerning, in particular, the activities of the State in areas of criminal law.

52 In that connection, it must be recalled that the activities mentioned by way of examples by that provision are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals (see 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).

53 In the present case, subject to verifications to be made in that regard by the referring court, it appears that the German Federal institutions, which provide the online media services and which are responsible for the processing of dynamic IP addresses act, in spite of their status as public authorities, as individuals and outside the activities of the State in the area of criminal law.

54 Therefore, it must be determined whether the legislation of a Member State, such as that at issue in the main proceedings, is compatible with Article 7(f) of Directive 95/46.

55 To that end, it is important to recall that the national legislation at issue in the main proceedings, as interpreted in the restrictive sense described by the referring court, authorises the collection and use of personal data relating to a user of those services, without his consent, only to the extent that is necessary to facilitate and charge for the specific use of online media by the user concerned, even though the objective aiming to ensure the general capacity relating to the functioning of the online media may justify the use of those data at the end of that period of use of such media.

56 Pursuant to Article 7(f) of Directive 95/46, personal data may be processed if ‘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)’ of the Directive.

57 The Court has held 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 and that the Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article (see, to that

effect, judgment of 24 November 2011, *ASNEF and FECEMD*, C-468/10 and C-469/10, EU:C:2011:777, paragraphs 30 and 32).

58 Article 5 of Directive 95/46 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, the margin of discretion which Member States have pursuant to Article 5 can therefore be used only in accordance with the objective pursued by that directive of maintaining a balance between the free movement of personal data and the protection of private life. 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 (see, to that effect, judgment of 24 November 2011, *ASNEF and FECEMD*, C-468/10 and C-469/10, EU:C:2011:777, paragraphs 33, 34 and 36).

59 In the present case, it appears that Paragraph 15 of the TMG, if it were interpreted in the strict manner mentioned in paragraph 55 of the present judgment, has a more restrictive scope than that of the principle laid down in Article 7(f) of Directive 95/46.

60 Whereas Article 7(f) of that directive refers, in a general manner, to 'the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed', Paragraph 15 of the TMG authorises the service provider to collect and use personal data of a user only in so far as that is necessary in order to facilitate, and charge for, the particular use of electronic media. Therefore, Paragraph 15 of the TMG precludes the storage of personal data, after the consultation of online media, in a general manner in order to guarantee the use of those media. The German Federal institutions, which provide online media services, may also have a legitimate interest in ensuring, in addition to the specific use of their publicly accessible websites, the continued functioning of those websites.

61 Thus, as the Advocate General pointed out, in points 100 and 101 of his Opinion, such national legislation goes further than defining the notion of 'legitimate interests' in Article 7(f) of Directive 95/46, in accordance with Article 5 of Directive 95/46.

62 Article 7(f) of that directive precludes Member States from excluding, categorically and in general, 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. Thus, Member States cannot definitively prescribe, for certain categories of personal data, 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 (see, to that effect, judgment of 24 November 2011, *ASNEF and FECEMD*, C-468/10 and C-469/10, EU:C:2011:777, paragraphs 47 and 48).

63 As regards the processing of personal data of the users of online media websites, legislation, such as that at issue in the main proceedings, reduces the scope of the principle laid down in Article 7(f) of Directive 95/46 by excluding the possibility to

balance the objective of ensuring the general operability of the online media against the interests or fundamental rights and freedoms of those users which, in accordance with that provision, calls for protection under Article 1(1) of that directive.

64 It follows from all of the foregoing considerations that the answer to the second question is that Article 7(f) of Directive 95/46 must be interpreted as meaning that it precludes the legislation of a Member State under which an online media services provider may collect and use personal data relating to a user of those service, without his consent, only in so far as the collection and use of that information are necessary to facilitate and charge for the specific use of those services by that user, even though the objective aiming to ensure the general operability of those services may justify the use of those data after consultation of those websites.

Costs

65 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 (Second 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 a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.**

2. **Article 7(f) of Directive 95/46 must be interpreted as precluding the legislation of a Member State, pursuant to which an online media services provider may collect and use personal data relating to a user of those services, without his consent, only in so far as that the collection and use of that data are necessary to facilitate and charge for the specific use of those services by that user, even though the objective aiming to ensure the general operability of those services may justify the use of those data after a consultation period of those websites.**

[Signatures]

---

* Language of the case: German.