JUDGMENT OF THE COURT (Fourth Chamber)

7 March 2024 (*)

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Standard-setting sectoral organisation proposing to its members rules on the processing of users' consent – Article 4(1) – Concept of 'personal data' – String of letters and characters capturing, in a structured and machine-readable manner, the preferences of an internet user relating to the consent of that user to the processing of his or her personal data – Article 4(7) – Concept of 'controller' – Article 26(1) – Concept of 'joint controllers' – Organisation which does not itself have access to the personal data processed by its members – Responsibility of the organisation extending to the subsequent processing of data carried out by third parties)

In Case C-604/22,

REQUEST for a preliminary ruling under Article 267 TFEU from the hof van beroep te Brussel (Court of Appeal, Brussels, Belgium), made by decision of 7 September 2022, received at the Court on 19 September 2022, in the proceedings

IAB Europe

v

Gegevensbeschermingsautoriteit,

interveners:

Jef Ausloos,

Pierre Dewitte,

Johnny Ryan,

Fundacja Panoptykon,

Stichting Bits of Freedom,

Ligue des Droits Humains VZW,

THE COURT (Fourth Chamber),

composed of C. Lycourgos, President of the Chamber, O. Spineanu-Matei, J.-C. Bonichot, S. Rodin and L.S. Rossi (Rapporteur), Judges,

Advocate General: T. Ćapeta,

Registrar: A. Lamote, Administrator,

having regard to the written procedure and further to the hearing on 21 September 2023,

after considering the observations submitted on behalf of:

– IAB Europe, by P. Craddock, avocat, and K. Van Quathem, advocaat,

– the Gegevensbeschermingsautoriteit, by E. Cloots, J. Roets and T. Roes, advocaten,

– Jef Ausloos, Pierre Dewitte, Johnny Ryan, Fundacja Panoptykon, Stichting Bits of Freedom and Ligue des Droits Humains VZW, by F. Debusseré and R. Roex, advocaten,

– the Austrian Government, by J. Schmoll and C. Gabauer, acting as Agents,

– the European Commission, by A. Bouchagiar and H. Kranenborg, acting as Agents,

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

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 4(1) and (7) and Article 24(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; 'the GDPR'), read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

2 The request has been made in proceedings between IAB Europe and the Gegevensbeschermingsautoriteit (Data Protection Authority, Belgium; 'the DPA') concerning a decision of the Litigation Chamber of the DPA adopted against IAB Europe with regard to the alleged infringement of several provisions of the GDPR.

Legal context

European Union law

3 Recitals 1, 10, 26 and 30 of the GDPR are worded as follows:

'(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the [Charter] and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.

…

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …

…

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by

the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

…

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.'

4 Article 1 of the GDPR, entitled 'Subject matter and objectives', provides, in paragraph 2 thereof:

'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.'

5 Article 4 of that regulation provides:

'For the purposes of this Regulation:

(1) "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

…

(7) "controller" means the natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

…

(11) "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

…'

6 Article 6 of the GDPR, entitled 'Lawfulness of processing', is worded as follows:

‘1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

…

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

…’

7 Article 24 of that regulation, entitled ‘Responsibility of the controller’, provides, in paragraph 1 thereof:

‘Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.’

8 Article 26 of that regulation, entitled ‘Joint controllers’, states, in paragraph 1 thereof:

‘Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. …’

9 Chapter VI of the GDPR, relating to ‘Independent supervisory authorities’, comprises Articles 51 to 59 of that regulation.

10 Article 51 of that regulation, entitled ‘Supervisory authority’, provides, in paragraphs 1 and 2 thereof:

‘1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union …

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the [European] Commission in accordance with Chapter VII.’

11 According to Article 55(1) and (2) of the GDPR, entitled ‘Competence’:

‘1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.’

12 Article 56 of that regulation, entitled ‘Competence of the lead supervisory authority’, states, in paragraph 1 thereof:

‘Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.’

13 Article 57 of the GDPR, entitled ‘Tasks’, provides, in paragraph 1 thereof:

‘Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

…

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

…’

14 Section 1, entitled ‘Cooperation’, of Chapter VII of the GDPR, entitled ‘Cooperation and consistency’, comprises Articles 60 to 62 of that regulation. Article 60, relating to ‘Cooperation between the lead supervisory authority and the other supervisory authorities concerned’, provides, in paragraph 1 thereof:

‘The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.’

15 Article 61 of the GDPR, entitled ‘Mutual assistance’, states, in paragraph 1 thereof:

‘Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.’

16 Article 62 of that regulation, entitled ‘Joint operations of supervisory authorities’, provides, in paragraphs 1 and 2 thereof:

‘1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. …’

17 Section 2, entitled ‘Consistency’, of Chapter VII of the GDPR comprises Articles 63 to 67 of that regulation. Article 63, entitled ‘Consistency mechanism’, is worded as follows:

‘In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.’

Belgian law

18 The wet tot oprichting van de Gegevensbeschermingsautoriteit (Law establishing the Data Protection Authority), of 3 December 2017 (*Belgisch Staatsblad*, 10 January 2018, p. 989; 'the LDPA'), provides, in point 9° of Article 100(1) thereof:

'The Litigation Chamber shall have the power to:

…

9° order that the processing be brought into conformity'.

19 Article 101 of the LDPA provides:

'The Litigation Chamber may decide to impose an administrative fine on the parties against whom proceedings are brought in accordance with the general principles referred to in Article 83 of [the GDPR].'

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

20 IAB Europe is a non-profit association established in Belgium which represents undertakings in the digital advertising and marketing sector at European level. The members of IAB Europe are undertakings in that sector, such as publishers, e-commerce and marketing undertakings and intermediaries, as well as national associations, including national IAB (Interactive Advertising Bureau) branches, which, in turn, have undertakings in that sector as members. The members of IAB Europe include, inter alia, undertakings which generate significant income through the sale of advertising space on websites or applications.

21 IAB Europe has drawn up the Transparency & Consent Framework ('the TCF'), which is a framework of rules consisting of guidelines, instructions, technical specifications, protocols and contractual obligations that enable both the provider of a website or application and data brokers or indeed advertising platforms to process lawfully the personal data of a user of a website or application.

22 The TCF is aimed, inter alia, at promoting compliance with the GDPR when those operators use the OpenRTB protocol, one of the most widely used protocols for Real Time Bidding, which is an instant and automated online auction system of user profiles for the purpose of selling and purchasing advertising space on the internet ('RTB'). In the light of certain practices implemented by members of IAB Europe in the context of that mass personal data exchange system relating to user profiles, the TCF was presented by IAB Europe as a solution capable of bringing that auction system into conformity with the GDPR.

23 In particular, as is apparent from the file submitted to the Court, from a technical point of view, when a user consults a website or application containing advertising space, advertising technology companies – particularly data brokers and advertising platforms, which represent thousands of advertisers – can bid in real time, behind the scenes, to acquire that advertising space by means of an automated auction system using algorithms, in order to display in that space targeted advertisements specifically tailored to the profile of such a user.

24 However, before displaying such targeted advertisements, the prior consent of that user must be obtained. Thus, when he or she consults a website or application for the first time, a Consent Management Platform ('CMP') appears in a pop-up window enabling that user, first, to give his or her consent to the provider of the website or application for the collection and processing of his or her personal data for pre-defined purposes, such as, inter alia, marketing or advertising, or with a view to sharing those data with certain providers, and, second, to object to various types of data processing or to the sharing of those data, based on legitimate interests claimed by providers, within the meaning of Article 6(1)(f) of the GDPR. Those personal data relate, inter alia, to the user's location, age and search and recent purchase history.

25 In that context, the TCF provides a framework for large-scale processing of personal data and facilitates the recording of users' preferences by means of the CMP. Those preferences are subsequently encoded and

stored in a string composed of a combination of letters and characters referred to by IAB Europe as the Transparency and Consent String ('the TC String'), which is shared with personal data brokers and advertising platforms participating in the OpenRTB protocol, so that they know to what the user has consented or objected. The CMP also places a cookie (euconsent-v2) on the user's device. When they are combined, the TC String and the euconsent-v2 cookie can be linked to that user's IP address.

26 The TCF thus plays a role in the operation of the OpenRTB protocol, since it makes it possible to transcribe the user's preferences with a view to communicating them to potential sellers and achieving various processing objectives, including the offering of tailored advertising. The TCF aims, inter alia, to guarantee to personal data brokers and advertising platforms, by means of the TC String, compliance with the GDPR.

27 Since 2019, the DPA has received a number of complaints against IAB Europe, originating both from Belgium and from third countries, concerning the compliance of the TCF with the GDPR. After having examined those complaints, the DPA, in its capacity as lead supervisory authority within the meaning of Article 56(1) of the GDPR, triggered the cooperation and consistency mechanism, in accordance with Articles 60 to 63 of that regulation, in order to reach a common decision approved jointly by all 21 national supervisory authorities involved in that mechanism. Thus, by its decision of 2 February 2022 ('the decision of 2 February 2022'), the Litigation Chamber of the DPA held that IAB Europe was acting as personal data controller as regards the recording of the consent signal, objections and preferences of individual users by means of a TC String, which, according to the Litigation Chamber of the DPA, is associated with an identifiable user. In addition, in that decision, the Litigation Chamber of the DPA ordered IAB Europe, in accordance with point 9° of Article 100(1) of the LDPA, to bring into conformity with the provisions of the GDPR the processing of personal data carried out in the context of the TCF and imposed on it a number of corrective measures as well as an administrative fine.

28 IAB Europe brought an action against that decision before the referring court, the hof van beroep te Brussel (Court of Appeal, Brussels, Belgium). IAB Europe requests that court to annul the decision of 2 February 2022. It challenges, inter alia, the fact that it was considered to have acted as controller. It also submits that, in so far as the decision finds that the TC String is personal data within the meaning of Article 4(1) of the GDPR, that decision is insufficiently qualified and reasoned and that, in any event, it is incorrect. In particular, IAB Europe argues that only the other participants in the TCF could combine the TC String with an IP address to convert it into an item of personal data, that the TC String is not specific to a user and that IAB Europe does not have the possibility to access the data processed in that context by its members.

29 The DPA, supported in the national proceedings by Mr Jef Ausloos, Mr Pierre Dewitte, Mr Johnny Ryan, Fundacja Panoptykon, Stichting Bits of Freedom and Ligue des Droits Humains VZW, contends, inter alia, that TC Strings do constitute personal data, in so far as CMPs can link TC Strings to IP addresses, that, moreover, participants in the TCF can also identify users on the basis of other data, that IAB Europe has access to the information needed to do that, and that such identification of the user is precisely the purpose of the TC String, which is intended to facilitate the sale of targeted advertising. In addition, the DPA maintains, inter alia, that the fact that IAB Europe must be regarded as a controller within the meaning of the GDPR is apparent from its decisive role in the processing of TC Strings. The DPA adds that IAB Europe determines, respectively, the purposes and means of the processing, how TC Strings are generated, modified and read, how and where the necessary cookies are stored, who receives the personal data and on the basis of which criteria the storage periods for TC Strings may be established.

30 The referring court has doubts as to whether a TC String, be it combined with an IP address or not, constitutes personal data and, if so, whether IAB Europe must be classified as a personal data controller in the context of the TCF, in particular with regard to the processing of the TC String. In that respect, the referring court states that, while it is true that the decision of 2 February 2022 reflects the common position adopted jointly by the various national supervisory authorities involved in the present case, the Court of Justice has not yet had the opportunity to rule on that new and far-reaching technology which the TC String represents.

31 In those circumstances, the hof van beroep te Brussel (Court of Appeal, Brussels) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

‘(1) (a) Must Article 4(1) of [the GDPR], read in combination with Articles 7 and 8 of the [Charter], be interpreted as meaning that a character string that captures the preferences of an [internet] user in connection with the processing of his or her personal data in a structured and machine-readable manner constitutes personal data within the meaning of [that] provision in respect of [(i)] a sectoral organisation which makes available to its members a standard whereby it prescribes to them how that string should be generated, stored and/or distributed practically and technically, and [(ii)] the parties that have implemented that standard on their websites or in their apps and thus have access to that string?

(b) Does it make a difference in that regard if the implementation of the standard means that [that] string is available together with an IP address?

(c) Does the answer to questions 1(a) and 1(b) lead to a different conclusion if [that] standard-setting sectoral organisation does not itself have legal access to the personal data that are processed within [that] standard by its members?

(2) (a) Must [Article] 4(7) and [Article] 24(1) of [the GDPR], read in combination with Articles 7 and 8 of the [Charter], be interpreted as meaning that a standard-setting sectoral organisation must be classified as a controller if it offers its members a standard for managing consent which contains, in addition to a binding technical framework, rules setting out in detail how those consent data – which constitute personal data – must be stored and disseminated?

(b) Does the answer to question 2(a) lead to a different conclusion if [that] sectoral organisation … does not itself have legal access to the personal data that are processed within [that] standard by its members?

(c) If the standard-setting sectoral organisation must be designated as a controller or a joint controller for the processing of [internet] users’ preferences, does that (joint) responsibility of the standard-setting sectoral organisation therefore automatically extend to the subsequent processing by third parties for which the [internet] users’ preferences were obtained, such as targeted online advertising by publishers and vendors?’

The first question

32 By its first question, the referring court asks, in essence, whether Article 4(1) of the GDPR must be interpreted as meaning that a string composed of a combination of letters and characters, such as the TC String, containing the preferences of a user of the internet or of an application relating to that user’s consent to the processing of personal data concerning him or her by website or application providers as well as by brokers of such data and by advertising platforms, constitutes personal data within the meaning of that provision, where a sectoral organisation has established the framework of rules under which that string must be generated, stored or disseminated and the members of such an organisation have implemented such rules and thus have access to that string. That court also wishes to ascertain whether, for the purpose of answering that question, it is important, in the first place, for that string to be associated with an identifier, such as, inter alia, the IP address of that user’s device, allowing the data subject to be identified, and, in the second place, for such a sectoral organisation to have the right to access directly the personal data which are processed by its members under the framework of rules that it has established.

33 As a preliminary point, it should be recalled that, since the GDPR repealed and replaced 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 the relevant provisions of that regulation have essentially the same scope as that of the

relevant provisions of that directive, the Court's case-law on that directive is also applicable, in principle, to that regulation (judgment of 17 June 2021, *M.I.C.M.*, C-597/19, EU:C:2021:492, paragraph 107).

34 It should also be borne in mind that, according to settled case-law, the interpretation of a provision of EU law requires that account be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms part (judgment of 22 June 2023, *Pankki S*, C-579/21, EU:C:2023:501, paragraph 38 and the case-law cited).

35 In that regard, it should be noted that Article 4(1) of the GDPR states that personal data is 'any information relating to an identified or identifiable natural person', and specifies that 'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

36 The use of the expression 'any information' in the definition of the concept of 'personal data' in that provision reflects the aim of the EU legislature to assign a wide scope to that concept, which potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates to' the data subject (judgment of 4 May 2023, *Österreichische Datenschutzbehörde and CRIF*, C-487/21, EU:C:2023:369, paragraph 23 and the case-law cited).

37 In that regard, the Court has held that information relates to an identified or identifiable natural person where, by reason of its content, purpose or effect, it is linked to an identifiable person (judgment of 4 May 2023, *Österreichische Datenschutzbehörde and CRIF*, C-487/21, EU:C:2023:369, paragraph 24 and the case-law cited).

38 As regards the 'identifiable' nature of a person, it is clear from the wording of Article 4(1) of the GDPR that an identifiable person is one who can be identified not only directly, but also indirectly.

39 As the Court has already held, 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 (see, by analogy, judgment of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 41). On the contrary, it follows from Article 4(5) of the GDPR, read in conjunction with recital 26 of that regulation, that personal data which could be attributed to a natural person by the use of additional information must be considered to be information on an identifiable natural person (judgment of 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C-683/21, EU:C:2023:949, paragraph 58).

40 Furthermore, that recital 26 states that, in order to determine whether a person is 'identifiable', account should be taken of 'all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly'. That wording suggests that, for information to be treated as 'personal data' within the meaning of Article 4(1) of that regulation, it is not required that all the information enabling the identification of the data subject must be in the hands of one person (see, by analogy, judgment of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 43).

41 Therefore, the concept of 'personal data' covers not only data collected and stored by the controller, but also includes all information resulting from the processing of personal data relating to an identified or identifiable person (judgment of 22 June 2023, *Pankki S*, C-579/21, EU:C:2023:501, paragraph 45).

42 In the present case, it should be noted that a string composed of a combination of letters and characters, such as the TC String, contains the preferences of a user of the internet or of an application relating to that user's consent to the processing by third parties of personal data concerning him or her or relating to any objection by him or her to the processing of such data based on an alleged legitimate interest under Article 6(1)(f) of the GDPR.

43 Even if a TC String did not itself contain factors allowing the data subject to be identified directly, it would still be the case, in the first place, that it contained the individual preferences of a specific user regarding his or her consent to the processing of personal data concerning him or her, that information 'relating to [a] … natural person' within the meaning of Article 4(1) of the GDPR.

44 In the second place, it is also common ground that, where the information contained in a TC String is associated with an identifier, such as, inter alia, the IP address of the device of such a user, that information may make it possible to create a profile of that user and actually identify the person specifically concerned by such information.

45 In so far as associating a string composed of a combination of letters and characters, such as the TC String, with additional data, inter alia with the IP address of a user's device or with other identifiers, allows that user to be identified, it must be considered that the TC String contains information concerning an identifiable user and therefore constitutes personal data within the meaning of Article 4(1) of the GDPR, a conclusion which is supported by recital 30 of the GDPR, which expressly refers to such a case.

46 That interpretation cannot be called into question by the mere fact that IAB Europe cannot itself combine the TC String with the IP address of a user's device and does not have the possibility of directly accessing the data processed by its members in the context of the TCF.

47 As is apparent from the case-law referred to in paragraph 40 above, such a fact does not preclude a TC String from being classified as 'personal data' within the meaning of Article 4(1) of the GDPR.

48 Moreover, it is apparent from the documents before the Court, and in particular from the decision of 2 February 2022, that the members of IAB Europe are required to provide that organisation, at its request, with all the information allowing it to identify the users whose data are the subject of a TC String.

49 It therefore appears, subject to the verifications which are for the referring court to carry out in that regard, that IAB Europe has, in accordance with what is stated in recital 26 of the GDPR, reasonable means allowing it to identify a particular natural person from a TC String, on the basis of the information which its members and other organisations participating in the TCF are required to provide to it.

50 It follows from the foregoing that a TC String constitutes personal data within the meaning of Article 4(1) of the GDPR. It is irrelevant in that regard that, without an external contribution which it is entitled to require, such a sectoral organisation can neither access the data that are processed by its members under the rules which it has established nor combine the TC String with other identifiers, such as, inter alia, the IP address of a user's device.

51 In view of the foregoing, the answer to the first question is that Article 4(1) of the GDPR must be interpreted as meaning that a string composed of a combination of letters and characters, such as the TC String, containing the preferences of a user of the internet or of an application relating to that user's consent to the processing of personal data concerning him or her by website or application providers as well as by brokers of such data and by advertising platforms constitutes personal data within the meaning of that provision in so far as, where those data may, by reasonable means, be associated with an identifier, such as, inter alia, the IP address of that user's device, they allow the data subject to be identified. In such circumstances, the fact that, without an external contribution, a sectoral organisation holding that string can neither access the data that are processed by its members under the rules which that organisation has established nor combine that string with other factors does not preclude that string from constituting personal data within the meaning of that provision.

The second question

52 By its second question, the referring court asks, in essence, whether Article 4(7) of the GDPR must be interpreted as meaning that:

– first, a sectoral organisation, in so far as it proposes to its members a framework of rules that it has established relating to consent to the processing of personal data, which contains not only binding technical rules but also rules setting out in detail the arrangements for storing and disseminating personal data relating to such consent, must be classified as a 'controller' within the meaning of that provision, and whether, for the answer to that question, it is relevant that such a sectoral organisation itself have direct access to the personal data processed by its members under those rules;

– second, any joint controllership of that sectoral organisation extends automatically to the subsequent processing of personal data carried out by third parties, such as website or application providers, with regard to users' preferences for the purposes of targeted online advertising.

53 As a preliminary point, it should be borne in mind that the objective pursued by the GDPR, as is set out in Article 1 thereof and in recitals 1 and 10 thereof, consists, inter alia, in ensuring 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, as enshrined in Article 8(1) of the Charter and Article 16(1) TFEU (judgment of 4 May 2023, *Bundesrepublik Deutschland (Court electronic mailbox),* C-60/22, EU:C:2023:373, paragraph 64).

54 In accordance with that objective, Article 4(7) of the GDPR defines broadly the concept of 'controller' as referring to 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.

55 As the Court has previously held, the objective of that provision is to ensure, through that broad definition of the concept of 'controller', effective and complete protection of data subjects (see, by analogy, judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, paragraph 28).

56 Furthermore, since, as Article 4(7) of the GDPR expressly provides, the concept of 'controller' relates to the entity which 'alone or jointly with others' determines the purposes and means of the processing of personal data, that concept does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data protection provisions (see, by analogy, judgments of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, paragraph 29, and of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 65).

57 The Court has also found that a natural or legal person who exerts influence over the processing of personal data, for his, her or its own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 4(7) of the GDPR (see, by analogy, judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 68). Thus, under Article 26(1) of the GDPR, 'joint controllers' exist where two or more controllers jointly determine the purposes and means of processing (judgment of 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C-683/21, EU:C:2023:949, paragraph 40).

58 In that regard, although each joint controller must independently meet the definition of 'controller' which is set out in Article 4(7) of the GDPR, the existence of joint controllership does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed in the light of all the relevant circumstances of the particular case. In addition, the joint controllership of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned (see, by analogy, judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraphs 66 and 69 and the case-law cited).

59 Participation in the determination of the purposes and means of processing can take different forms, since such participation can result from a common decision taken by two or more entities or from converging decisions of those entities. Where the latter is the case, those decisions must complement each other in

such a manner that they each have a tangible impact on the determination of the purposes and means of the processing. By contrast, it cannot be required that there be a formal arrangement between those controllers as regards the purposes and means of processing (judgment of 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C-683/21, EU:C:2023:949, paragraphs 43 and 44).

60 In the light of the foregoing, the first part of the second question referred must be regarded as seeking to ascertain whether a sectoral organisation, such as IAB Europe, may be regarded as a joint controller for the purposes of Article 4(7) and Article 26(1) of the GDPR.

61 To that end, it is therefore necessary to assess whether, having regard to the particular circumstances of the case at issue, IAB Europe exerts influence over the processing of personal data, such as the TC String, for its own purposes, and determines, jointly with others, the purposes and means of such processing.

62 As regards, in the first place, the purposes of such processing of personal data, subject to the verifications which are for the referring court to carry out, it is apparent from the documents before the Court that, as has been noted in paragraphs 21 and 22 above, the TCF established by IAB Europe constitutes a framework of rules intended to ensure that the processing of personal data of a user of a website or application carried out by certain operators which participate in the online auctioning of advertising space is in compliance with the GDPR.

63 In those circumstances, the TCF aims, in essence, to promote and enable the sale and purchase of advertising space on the internet by such operators.

64 Accordingly, the view may be taken, subject to the verifications which are for the referring court to carry out, that IAB Europe exerts influence over the personal data processing operations at issue in the main proceedings, for its own purposes, and determines, as a result, jointly with its members, the purposes of such operations.

65 In the second place, as regards the means employed for the purposes of such processing of personal data, it is apparent from the documents before the Court, subject to the verifications which are for the referring court to carry out, that the TCF constitutes a framework of rules which the members of IAB Europe are supposed to accept in order to join that association. In particular, as was confirmed by IAB Europe at the hearing before the Court, if one of its members does not comply with the rules of the TCF, IAB Europe may adopt a non-compliance and suspension decision in respect of that member, which may result in the exclusion of that member from the TCF and, consequently, prevent it from relying on the guarantee of GDPR compliance that that system is supposed to provide with regard to the processing of personal data which that member carries out using TC Strings.

66 Furthermore, and from a practical point of view, as has been stated in paragraph 21 above, the TCF established by IAB Europe contains technical specifications relating to the processing of the TC String. In particular, it appears that those specifications describe precisely how CMPs are required to collect users' preferences relating to the processing of personal data concerning those users and how such preferences must be processed in order to generate a TC String. Moreover, precise rules are also laid down as regards the content of the TC String as well as the storage and sharing thereof.

67 It is apparent in particular from the decision of 2 February 2022 that IAB Europe prescribes, as part of those rules, inter alia the standardised manner in which the various parties involved in the TCF may consult the preferences, objections and consents of users contained in the TC Strings.

68 In those circumstances, and subject to the verifications which are for the referring court to carry out, a sectoral organisation such as IAB Europe must be regarded as exerting influence over the personal data processing operations at issue in the main proceedings, for its own purposes, and determines, as a result, jointly with its members, the means behind such operations. It follows that such an organisation must be regarded as a 'joint controller', for the purposes of Article 4(7) and Article 26(1) of the GDPR, in accordance with the case-law referred to in paragraph 57 above.

69 The fact, mentioned by the referring court, that such a sectoral organisation does not itself have direct access to the TC Strings or, therefore, to the personal data processed under the abovementioned rules by its members, with which it jointly determines the purposes and means of the processing of those data, does not, in accordance with the case-law referred to in paragraph 58 above, preclude it from being classified as a 'controller' within the meaning of those provisions.

70 Furthermore, in response to the doubts expressed by that court, it can be ruled out that any joint controllership of that sectoral organisation extends automatically to the subsequent processing of personal data carried out by third parties, such as website or application providers, with regard to users' preferences for the purposes of targeted online advertising.

71 In that regard, it should be noted, first, that Article 4(2) of the GDPR defines the 'processing' of personal data as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

72 It is clear from that definition that the processing of personal data may consist of one or more operations, each relating to a different stage of that processing.

73 Second, as the Court has already held, it follows from Article 4(7) and Article 26(1) of the GDPR that a natural or legal person may be regarded as a joint controller in respect of personal data processing operations only where that person jointly determines the purposes and means of such operations. Therefore, and without prejudice to any civil liability provided for in national law in that respect, such a natural or legal person cannot be regarded as a controller, within the meaning of those provisions, in respect of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means (see, by analogy, judgment of 29 July 2019, *Fashion ID*, C-40/17, EU:C:2019:629, paragraph 74).

74 In the present case, a distinction must be drawn between the processing of personal data carried out by the members of IAB Europe, namely website or application providers and data brokers or advertising platforms, when the consent preferences of the users concerned are recorded in a TC String in accordance with the framework of rules established in the TCF, on the one hand, and the subsequent processing of personal data carried out by those operators and by third parties on the basis of those preferences, such as the transmission of those data to third parties or the offering of personalised advertising to those users, on the other.

75 That subsequent processing, subject to the verifications which are for the referring court to carry out, does not appear to involve the participation of IAB Europe, with the result that automatic responsibility on the part of such an organisation, held jointly with the abovementioned operators and with third parties, must be precluded in respect of the processing of personal data carried out on the basis of data relating to the preferences of the users concerned contained in a TC String.

76 Accordingly, a sectoral organisation, such as IAB Europe, may be regarded as a controller in respect of such subsequent processing only where it is established that that organisation has exerted an influence over the determination of the purposes and means of that processing, which it is for the referring court to ascertain in the light of all the relevant circumstances of the case in the main proceedings.

77 In view of all the foregoing considerations, the answer to the second question is that Article 4(7) and Article 26(1) of the GDPR must be interpreted as meaning that:

– first, a sectoral organisation, in so far as it proposes to its members a framework of rules that it has established relating to consent to the processing of personal data, which contains not only binding technical rules but also rules setting out in detail the arrangements for storing and disseminating personal data relating to such consent, must be classified as a 'joint controller' for the purpose of

those provisions where, in the light of the particular circumstances of the individual case, it exerts influence over the personal data processing at issue, for its own purposes, and determines, as a result, jointly with its members, the purposes and means of such processing. The fact that such a sectoral organisation does not itself have direct access to the personal data processed by its members under those rules does not preclude it from holding the status of joint controller for the purpose of those provisions;

– second, the joint controllership of that sectoral organisation does not extend automatically to the subsequent processing of personal data carried out by third parties, such as website or application providers, with regard to users' preferences for the purposes of targeted online advertising.

Costs

78 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 (Fourth Chamber) hereby rules:

1. **Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**

   must be interpreted as meaning that a string composed of a combination of letters and characters, such as the TC String (Transparency and Consent String), containing the preferences of a user of the internet or of an application relating to that user's consent to the processing of personal data concerning him or her by website or application providers as well as by brokers of such data and by advertising platforms constitutes personal data within the meaning of that provision in so far as, where those data may, by reasonable means, be associated with an identifier, such as, inter alia, the IP address of that user's device, they allow the data subject to be identified. In such circumstances, the fact that, without an external contribution, a sectoral organisation holding that string can neither access the data that are processed by its members under the rules which that organisation has established nor combine that string with other factors does not preclude that string from constituting personal data within the meaning of that provision.

2. **Article 4(7) and Article 26(1) of Regulation 2016/679**

   must be interpreted as meaning that:

   – **first, a sectoral organisation, in so far as it proposes to its members a framework of rules that it has established relating to consent to the processing of personal data, which contains not only binding technical rules but also rules setting out in detail the arrangements for storing and disseminating personal data relating to such consent, must be classified as a 'joint controller' for the purpose of those provisions where, in the light of the particular circumstances of the individual case, it exerts influence over the personal data processing at issue, for its own purposes, and determines, as a result, jointly with its members, the purposes and means of such processing. The fact that such a sectoral organisation does not itself have direct access to the personal data processed by its members under those rules does not preclude it from holding the status of joint controller for the purpose of those provisions;**

– **second, the joint controllership of that sectoral organisation does not extend automatically to the subsequent processing of personal data carried out by third parties, such as website or application providers, with regard to users' preferences for the purposes of targeted online advertising.**

[Signatures]

---

* Language of the case: Dutch.