



Reports of Cases

JUDGMENT OF THE COURT (Sixth Chamber)

7 March 2024*

(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Articles 2, 4, 6, 10 and 86 – Data held by a court relating to the criminal convictions of a natural person – Oral disclosure of such data to a commercial company on account of a competition organised by that company – Concept of ‘processing of personal data’ – National legislation governing access to those data – Reconciliation between the right of public access to official documents and the protection of personal data)

In Case C-740/22,

REQUEST for a preliminary ruling under Article 267 TFEU from the Itä-Suomen hovioikeus (Court of Appeal, Eastern Finland, Finland), made by decision of 30 November 2022, received at the Court on 2 December 2022, in the proceedings

Endemol Shine Finland Oy

THE COURT (Sixth Chamber),

composed of T. von Danwitz (Rapporteur), President of the Chamber, P.G. Xuereb and I. Ziemele, Judges,

Advocate General: T. Ćapeta,

Registrar: A. Calot Escobar,

having regard to the written procedure,

after considering the observations submitted on behalf of:

- the Finnish Government, by A. Laine and M. Pere, acting as Agents,
- the Portuguese Government, by P. Barros da Costa, J. Ramos and C. Vieira Guerra, acting as Agents,
- the European Commission, by A. Bouchagiar, H. Kranenborg and I. Söderlund, acting as Agents,

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

* Language of the case: Finnish.

gives the following

Judgment

- 1 This request for a preliminary ruling concerns the interpretation of Article 2(1), Article 4(2) and Article 86 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’).
- 2 The request has been made in proceedings concerning the refusal of a national court to communicate data relating to criminal convictions concerning a third party to Endemol Shine Finland Oy.

Legal context

European Union law

- 3 Recitals 4, 10, 11, 15, 19 and 154 of the GDPR are worded as follows:
 - ‘(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter [of Fundamental Rights of the European Union (“the Charter”)] as enshrined in the Treaties, in particular the respect for private and family life, ... the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, ...
- ...
- (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. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing 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)], Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify [their] rules, including

for the processing of special categories of personal data (“sensitive data”). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

- (11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

...

- (15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

...

- (19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89)]. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under

specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

...

- (154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council [of 17 November 2003 on the re-use of public sector information (OJ 2003 L 345, p. 90)] leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.'

4 Article 2 of the GDPR, entitled 'Material scope', provides:

1. This Regulation 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 Regulation does not apply to the processing of personal data:
 - (a) in the course of an activity which falls outside the scope of Union law;
 - (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the [EU Treaty];
 - (c) by a natural person in the course of a purely personal or household activity;
 - (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, 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)] applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application 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)], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.’

5 Article 4 of the GDPR, entitled ‘Definitions’, provides, in points 1, 2, 6 and 7:

‘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;

...

(6) “filing system” means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(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’.

6 Article 5 of that regulation, entitled ‘Principles relating to processing of personal data’, is worded as follows:

‘1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);

- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ... (“purpose limitation”);
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ... (“storage limitation”);
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”);

...’

7 Article 6 of the GDPR, entitled ‘Lawfulness of processing’, provides, in paragraphs 1 to 3:

‘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;
- (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;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (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;
- (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.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other

measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in [points] (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.'

8 Article 10 of the GDPR, entitled 'Processing of personal data relating to criminal convictions and offences', provides:

'Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.'

9 Article 23 of that regulation, entitled 'Restrictions', is worded as follows:

'1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

...

(f) the protection of judicial independence and judicial proceedings;

...'

- 10 Article 85 of the GDPR, entitled ‘Processing and freedom of expression and information’, provides, in paragraph 1:

‘Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.’

- 11 Article 86 of the GDPR, entitled ‘Processing and public access to official documents’, provides:

‘Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.’

Finnish law

Law on the protection of personal data (1050/2018)

- 12 The tietosuojalaki (1050/2018) (Law on the protection of personal data (1050/2018)) provides, in Paragraph 1:

‘This Law clarifies and supplements the [GDPR] and the national application thereof.’

- 13 Paragraph 28 of that law is worded as follows:

‘The provisions on the public nature of public authorities’ activity shall apply to the right to obtain information from a public authority’s register of persons and to any other disclosure of personal data from a public authority’s register of persons.’

Law on the public nature of public authorities’ activity (621/1999)

- 14 The laki viranomaisten toiminnan julkisuudesta (621/1999) (Law on the public nature of public authorities’ activity (621/1999)) provides, in Paragraph 13:

‘A request for information on the content of an official document must be sufficiently specific to enable the public authority to identify the document to which the request relates. The public authority must assist the person requesting information in identifying the document from which he or she is requesting the information by means of a log and other directories. The person requesting information need not identify him or herself or state reasons for his or her request, save where this is necessary to enable the authority to exercise its discretion or to determine whether the applicant has a right to obtain information on the content of the document.

When requesting information from a confidential document, a public authority’s register of persons or another document from which information may be provided only under certain conditions, the person requesting information must, unless otherwise expressly provided for, state the purpose for which the information is to be used, set out any other circumstances required to clarify the conditions for disclosure of the information and, where necessary, indicate how the information is to be protected.’

15 Paragraph 16 of that law provides:

‘Information on the content of a document held by a public authority shall be provided orally or by making the document available to be inspected, copied or listened to at the public authority’s premises or by providing a copy or printout thereof. Information on the public content of a document shall be provided in the manner requested, unless this would entail unreasonable interference in official activities on account of the large number of documents or the difficulty of copying a document or for other comparable reasons.

...

Personal data from a public authority’s register of persons may, unless otherwise expressly provided for in law, be provided in the form of a copy, printout or in electronic form where the recipient has the right to store and use such personal data under the provisions on the protection of personal data. However, personal data may only be provided for direct marketing and opinion or market research if this is expressly provided for or if the data subject has given his or her consent.

...’

Law on the public nature of proceedings before ordinary courts (370/2007)

16 Under Paragraph 1 of the laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa (370/2007) (Law on the public nature of proceedings before ordinary courts (370/2007)):

‘Court proceedings and procedural documents are public, unless otherwise provided for in this Law or any other law.’

Law on the processing of personal data in criminal matters and in connection with the maintenance of national security (1054/2018)

17 Paragraph 1 of the laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018) (Law on the processing of personal data in criminal matters and in connection with the maintenance of national security (1054/2018)) provides, in the first subparagraph, that that law is to apply to the processing of personal data by competent authorities where, inter alia, criminal proceedings before a court are concerned. Under the fourth subparagraph of that paragraph, that law is to apply only to such processing of personal data within the meaning of the first subparagraph as is wholly or partly automated or where the data to be processed form or are intended to form a register or part of a register.

18 Under the second subparagraph of Paragraph 2 of that law:

‘The provisions on the public nature of public authorities’ activity shall apply to the right to obtain information from a public authority’s register of persons and to any other disclosure of personal data from a public authority’s register of persons.’

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

- 19 Endemol Shine Finland, the appellant in the main proceedings, made an oral request to the Etelä-Savon käräjäoikeus (District Court, South Savo, Finland) for information on possible ongoing or completed criminal proceedings concerning a natural person involved in a competition organised by that company for the purpose of clarifying the criminal record of that person.
- 20 The Etelä-Savon käräjäoikeus (District Court, South Savo) refused the request of the appellant in the main proceedings while taking the view that that request related to public decisions or information for the purpose of the Law on the public nature of proceedings before ordinary courts. According to that court, the reason stated by the appellant in the main proceedings was not a reason for processing criminal convictions or offences, referred to in Paragraph 7 of the Law on the protection of personal data. A search of that court's information systems would also have constituted processing of personal data, which is why the requested information could also not have been disclosed orally.
- 21 The appellant in the main proceedings brought an appeal against that judgment before the Itä-Suomen hovioikeus (Court of Appeal, Eastern Finland, Finland), which is the referring court, contending that the oral disclosure of the information that it seeks does not constitute processing of personal data within the meaning of Article 4(2) of the GDPR.
- 22 The referring court is uncertain whether Article 2(1) and Article 4(2) of the GDPR are to be interpreted as meaning that the oral disclosure of information on possible ongoing or completed criminal proceedings to which a natural person has been subject constitutes processing of personal data within the meaning of that regulation. In that regard, that court notes that the processing of personal data by Finnish public authorities is governed by the Law on the protection of personal data. However, the restrictions usually associated with processing such data do not apply on account of the public nature of the data held by those authorities, but also of Paragraph 28 of that law and of the second subparagraph of Paragraph 2 of the Law on the processing of personal data in criminal matters and in connection with the maintenance of national security (1054/2018).
- 23 The court notes that, in order to reconcile the protection of personal data with the right of public access to information, Paragraph 16 of the Law on the public nature of public authorities' activity (621/1999) restricts the disclosure of personal data in the form of a copy, printout or in electronic form from a public authority's register of persons. However, since that paragraph does not apply to an oral disclosure of personal data contained in a public authority's register of persons, it is appropriate to consider how such reconciliation is to be ensured and how important aspects related to the protection of personal data are to be taken into account where such data contained in a public authority's register of persons are disclosed orally.
- 24 In those circumstances, the Itä-Suomen hovioikeus (Court of Appeal, Eastern Finland) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:
 - '(1) Does an oral transfer of personal data constitute processing of personal data within the meaning of Article 2(1) and Article 4(2) of the [GDPR]?

- (2) Can public access to official documents be reconciled with the right to protection of personal data pursuant to the [GDPR], in the manner referred to by Article 86 of the regulation, by allowing information on criminal convictions or offences of a natural person to be obtained from a court's register of persons without restriction where a request is made to transfer the information orally to the applicant?
- (3) Is it relevant for the answer to Question 2 whether the applicant is a company or a private individual?

Consideration of the questions referred

First question

- 25 By its first question, the referring court asks, in essence, whether Article 2(1) and Article 4(2) of the GDPR must be interpreted as meaning that the oral disclosure of information on possible ongoing or completed criminal proceedings to which a natural person has been subject constitutes processing of personal data within the meaning of Article 4(2) of that regulation and, if so, whether that processing comes within the material scope of that regulation, as defined in Article 2(1) thereof.
- 26 As a preliminary point, first, it should be borne in mind that, in order to interpret those provisions of EU law, it is necessary to take account not only of the wording of those provisions, but also of their context and the objectives pursued by the rules of which they form part (judgment of 12 January 2023, *Österreichische Post (Information regarding the recipients of personal data)*, C-154/21, EU:C:2023:3, paragraph 29).
- 27 Secondly, it should be noted that it is not disputed, in the main proceedings, that the information which the appellant in the main proceedings seeks to obtain constitutes personal data within the meaning of Article 4(1) of the GDPR.
- 28 Article 4(2) of the GDPR defines the concept of 'processing' 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'.
- 29 It is apparent in particular from the expression 'any operation' that the EU legislature intended to give the concept of 'processing' a broad scope, which is corroborated by the non-exhaustive nature, expressed by the phrase 'such as', of the operations listed in that provision (see, to that effect, judgments of 24 February 2022, *Valsts ieņēmumu dienests (Processing of personal data for tax purposes)*, C-175/20, EU:C:2022:124, paragraph 35, and of 22 June 2023, *Pankki S*, C-579/21, EU:C:2023:501, paragraph 46).
- 30 Those operations listed include, inter alia, disclosure by transmission, dissemination or 'otherwise making available', whether or not by automated means. In that regard, Article 4(2) of the GDPR does not lay down any condition as to the form of processing 'other than by automated means'. The concept of 'processing' therefore covers the oral disclosure of personal data.
- 31 That interpretation of the concept of 'processing' is supported by the objective pursued by the GDPR, which seeks, inter alia, as is apparent from Article 1 thereof and recitals 1 and 10 thereof, 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, as enshrined in Article 8(1) of the Charter and Article 16(1) TFEU (see, to that effect, judgment of 4 May 2023, *Bundesrepublik Deutschland (Court electronic mailbox)*, C-60/22, EU:C:2023:373, paragraph 64). The possibility of circumventing the application of that regulation by disclosing personal data orally rather than in writing would be manifestly incompatible with that objective.

- 32 In those circumstances, the concept of ‘processing’ referred to in Article 4(2) of the GDPR necessarily covers the oral disclosure of personal data.
- 33 Yet, the question still arises as to whether such processing falls within the material scope of the GDPR. Article 2 of that regulation, which determines that scope, provides, in paragraph 1, that that regulation applies to the processing ‘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’.
- 34 In that regard, it is clear from the wording of that provision and from recital 15 of the GDPR that that regulation applies both to automatic processing of personal data and to the manual processing of such data, so that the scope of the protection that that regulation confers on data subjects does not depend on the techniques used and avoids the serious risk of that protection being circumvented. However, it is also clear that that regulation applies to the manual processing of personal data only where the data processed ‘form part of a filing system or are intended to form part of a filing system’ (see, by analogy, judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 53).
- 35 Since the oral disclosure of personal data constitutes, as such, processing other than by automated means, the data that are the subject of that processing must therefore ‘form part’ or be ‘intended to form part of’ a ‘filing system’ in order for that processing to come within the material scope of the GDPR.
- 36 As regards the concept of a ‘filing system’, Article 4(6) of the GDPR provides that it covers ‘any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis’.
- 37 In that regard, the Court has already held that, in accordance with the objective set out in paragraph 34 of the present judgment, that provision broadly defines the concept of ‘filing system’, in particular by referring to ‘any’ structured set of personal data. Furthermore, the requirement that the set of personal data must be ‘structured according to specific criteria’ is simply intended to enable personal data to be easily retrieved. Apart from that requirement, Article 4(6) of the GDPR does not lay down the practical means by which a filing system is structured or the form in which it is to be presented. In particular, it does not follow from that provision, or from any other provision of that regulation, that the personal data at issue must be contained in data sheets or specific lists or in another search method, in order to establish the existence of a filing system within the meaning of that regulation (see, by analogy, judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraphs 56 to 58).
- 38 In the present case, it is clear from the request for a preliminary ruling that the data requested by the appellant in the main proceedings are contained in ‘a court’s register of persons’. It thus appears that those data are contained in a filing system within the meaning of Article 4(6) of the GDPR, which it is, however, for the referring court to verify, it being immaterial whether those data are contained in electronic databases or in physical files or registers.

39 In those circumstances, the answer to the first question is that Article 2(1) and Article 4(2) of the GDPR must be interpreted as meaning that the oral disclosure of information on possible ongoing or completed criminal proceedings to which a natural person has been subject constitutes processing of personal data, within the meaning of Article 4(2) of that regulation, and comes within the material scope of that regulation where that information forms part of a filing system or is intended to form part of a filing system.

Second and third questions

40 By the second and third questions, which it is appropriate to examine together, the referring court asks, in essence, whether the provisions of the GDPR, in particular Article 86 thereof, must be interpreted as precluding data relating to criminal convictions of a natural person contained in a court's filing system from being disclosed orally to any person for the purpose of ensuring public access to official documents, without the person requesting the disclosure of those data having to establish a specific interest in obtaining those data, and whether the answer to that question differs according to whether that person is a commercial company or a private individual.

41 That question arises from the national legislation at issue in the main proceedings inasmuch as that legislation does not require compliance with the national provisions on the protection of personal data where such data are disclosed orally.

42 In that regard, it should be recalled that, under the second paragraph of Article 288 TFEU, a regulation is of general application and directly applicable in all Member States. Accordingly, by virtue of the very nature of regulations and of their function in the system of sources of EU law, the provisions of regulations generally have immediate effect in the national legal systems without it being necessary for the national authorities to adopt implementing measures (judgments of 16 June 2022, *Port de Bruxelles and Région de Bruxelles-Capitale*, C-229/21, EU:C:2022:471, paragraph 47, and of 30 March 2023, *Hauptpersonalrat der Lehrerinnen und Lehrer*, C-34/21, EU:C:2023:270, paragraph 77).

43 Thus, a national court is required to apply the requirements of the GDPR as a whole, even if there is no specific provision in the applicable national law allowing regard to be had to the interests of the persons whose personal data are at issue (see, to that effect, judgment of 2 March 2023, *Norra Stockholm Bygg*, C-268/21, EU:C:2023:145, paragraphs 44 and 59).

44 It follows from the foregoing considerations that the oral disclosure of data relating to criminal convictions of a natural person may take place only if the conditions imposed by the GDPR are satisfied where those data form part of a filing system or are intended to form part of a filing system.

45 In that regard, it is important to note that, in accordance with the settled case-law of the Court, any processing of personal data must, first, comply with the principles relating to the processing of data established in Article 5 of the GDPR and, secondly, in the light, in particular, of the principle of the lawfulness of processing, laid down in Article 5(1)(a), satisfy one of the conditions of the lawfulness of the processing listed in Article 6 of that regulation (see, to that effect, judgments of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 96, and of 7 December 2023, *SCHUFA Holding and Others (Scoring)*, C-634/21, EU:C:2023:957, paragraph 67).

- 46 In particular, the processing of personal data at issue in the main proceedings – namely the oral disclosure to the public of data relating to criminal convictions – may fall within Article 6(1)(e) of the GDPR, under which processing is lawful if and to the extent that it 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’ (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 99).
- 47 In addition, as regards, more specifically, data relating to criminal convictions and offences, Article 10 of the GDPR makes their processing subject to additional restrictions. Under that provision, processing of those data ‘shall be carried out only under the control of official authority’, unless it is ‘authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects’ (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 100).
- 48 The Court has already held that neither Article 6(1)(e) of the GDPR nor Article 10 of that regulation lays down a general and absolute prohibition preventing a public authority from being empowered, or indeed compelled, to disclose personal data to persons requesting such data (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 103).
- 49 Thus, the GDPR does not preclude personal data from being disclosed to the public where such disclosure is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, within the meaning of Article 6(1)(e) of that regulation. That is so even where the data in question are covered by Article 10 of the GDPR, provided that the legislation authorising the disclosure provides for appropriate safeguards for the rights and freedoms of data subjects (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 104).
- 50 In the present case, it is apparent from the order for reference and from the written observations submitted by the Finnish Government that the national legislation on the public nature of public authorities’ activity and that on the public nature of proceedings before ordinary courts are intended to perform the task in the public interest of enabling public access to official documents to be ensured.
- 51 In those circumstances, the referring court seeks to establish more specifically whether the processing of personal data at issue in the main proceedings may be regarded as lawful in the light of the principle of proportionality, in particular in the light of the weighing up to be carried out of the right of public access to official documents, referred to in Article 86 of the GDPR, on the one hand, and the fundamental rights to respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter, on the other.
- 52 In that latter regard, it should be borne in mind that the fundamental rights to respect for private life and to the protection of personal data are not absolute rights, as stated in recital 4 of the GDPR, but must be considered in relation to their function in society and be weighed against other fundamental rights. Limitations may therefore be imposed, so long as, in accordance with Article 52(1) of the Charter, they are provided for by law, respect the essence of the fundamental rights and observe the principle of proportionality. Under the principle of proportionality, limitations may be made only if they 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. They must apply only in so far as is strictly necessary and the legislation which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 105).

- 53 In order to determine whether public disclosure of personal data relating to criminal convictions is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, within the meaning of Article 6(1)(e) of the GDPR, and whether the legislation authorising such disclosure provides for appropriate safeguards for the rights and freedoms of data subjects, within the meaning of Article 10 of that regulation, it should be ascertained in particular whether, having regard to the seriousness of the interference with the fundamental rights to respect for private life and to the protection of personal data caused by that disclosure, the latter is justified, and in particular proportionate, for the purpose of achieving the objectives pursued (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 106).
- 54 As regards the seriousness of the interference with those rights, the Court has already held that the processing of data relating to criminal convictions and offences or related security measures is, because of the particular sensitivity of those data, liable to constitute a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter. Since such data relate to behaviour that gives rise to social disapproval, the grant of access to those data is liable to stigmatise the data subject and thereby to constitute a serious interference with his or her private or professional life (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraphs 74, 75 and 112).
- 55 Whilst, as follows from recital 154 of the GDPR, public access to official documents – to which the referring court refers – constitutes a public interest capable of justifying the disclosure of personal data contained in such documents, that access must nevertheless be reconciled with the fundamental rights to respect for private life and to the protection of personal data, as Article 86 of the GDPR indeed expressly requires. In the light in particular of the sensitivity of data relating to criminal convictions and of the seriousness of the interference with the fundamental rights of data subjects to respect for private life and to the protection of personal data, which is caused by the disclosure of such data, it must be held that those rights prevail over the public's interest in having access to official documents (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 120).
- 56 For the same reason, the right to freedom of information referred to in Article 85 of the GDPR cannot be interpreted as justifying the disclosure to any person who so requests of personal data relating to criminal convictions (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 121).
- 57 In that regard, it is irrelevant whether the person requesting access to data relating to criminal convictions is a commercial company or a private individual or whether such data are disclosed in writing or orally.
- 58 In the light of the foregoing considerations, the answer to the second and third questions referred is that the provisions of the GDPR, in particular Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding data relating to criminal convictions of a natural person contained in a court's filing system from being disclosed orally to any person for the purpose of ensuring public

access to official documents, without the person requesting the disclosure of those data having to establish a specific interest in obtaining those data, it being irrelevant in that regard whether that person is a commercial company or a private individual.

Costs

- 59 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 (Sixth Chamber) hereby rules:

- 1. Article 2(1) and Article 4(2) 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 the oral disclosure of information on possible ongoing or completed criminal proceedings to which a natural person has been subject constitutes processing of personal data, within the meaning of Article 4(2) of that regulation, and comes within the material scope of that regulation where that information forms part of a filing system or is intended to form part of a filing system.

- 2. The provisions of Regulation 2016/679, in particular Article 6(1)(e) and Article 10 thereof,**

must be interpreted as precluding data relating to criminal convictions of a natural person contained in a court's filing system from being disclosed orally to any person for the purpose of ensuring public access to official documents, without the person requesting the disclosure of those data having to establish a specific interest in obtaining those data, it being irrelevant in that regard whether that person is a commercial company or a private individual.

[Signatures]