



[Pagina iniziale](#) > [Formulario di ricerca](#) > [Elenco dei risultati](#) > **Documenti**



[Avvia la stampa](#)

Lingua del documento :

ECLI:EU:C:2025:935

JUDGMENT OF THE COURT (Grand Chamber)

2 December 2025 (*)

(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 4(7) – Concept of ‘controller’ – Responsibility of the operator of an online marketplace for the publication of personal data contained in advertisements placed on its online marketplace by user advertisers – Article 5(2) – Principle of accountability – Article 26 – Joint control with user advertisers – Article 9(1) and (2)(a) – Advertisements containing sensitive data – Lawfulness of processing – Consent – Articles 24, 25 and 32 – Obligations of the controller – Prior identification of the advertisements containing such data – Prior identification of the identity of the user advertiser – Refusal of publication of unlawful advertisements – Security measures such as to prevent the copying of advertisements and their publication on other websites – Electronic commerce – Directive 2000/31/EC – Articles 12 to 15 – Possibility for such an operator, with regard to an infringement of those obligations, to rely on the exemption from liability of an intermediary information society service provider)

In Case C492/23,

REQUEST for a preliminary ruling under Article 267 TFEU from the Curtea de Apel Cluj (Court of Appeal, Cluj, Romania), made by decision of 15 June 2023, received at the Court on 3 August 2023, in the proceedings

X

v

Russmedia Digital SRL,

Inform Media Press SRL,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, T. von Danwitz, Vice-President, F. Biltgen, K. Jürimäe (Rapporteur), C. Lycourgos, I. Jarukaitis, M.L. Arastey Sahún, I. Ziemele, J. Passer, Presidents of Chambers, S. Rodin, E. Regan, N. Jääskinen and D. Gratsias, Judges,

Advocate General: M. Szpunar,

Registrar: R. Șereș, Administrator,

having regard to the written procedure and further to the hearing on 2 July 2024,

after considering the observations submitted on behalf of:

- X, by I. Kis, avocată,
- the Romanian Government, by E. Gane, L. Ghiță and R.I. Hațieganu, acting as Agents,
- the European Commission, by L. Armati, H. Kranenborg, P.J. Loewenthal and L. Nicolae, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 6 February 2025,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Articles 12 to 15 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), and of Article 2(4), Article 4(7) and (11), Article 5(1)(b) and (f), Article 6(1)(a) and Articles 7, 24 and 25 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 between a natural person, X, on the one hand, and Russmedia Digital SRL and Inform Media Press SRL (together, 'Russmedia'), on the other, concerning an action for compensation for the non-material damage allegedly sustained by the applicant in the main proceedings as a result of the unlawful processing of her personal data and the infringement of her right of personal portrayal, right to honour and right to privacy.

Legal context

European Union law

Directive 2000/31

3 Recitals 14, 42, 46 and 52 of Directive 2000/31 state:

'(14) The protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [(OJ 1995 L 281, p. 31)] and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [(OJ 1998 L 24, p. 1)] which are fully applicable to information society services; ... the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet.

...

(42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a

communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

...

(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.

...

(52) ... damage which may arise in connection with information society services is characterised both by its rapidity and by its geographical extent; in view of this specific character and the need to ensure that national authorities do not endanger the mutual confidence which they should have in one another, this Directive requests Member States to ensure that appropriate court actions are available; ...'

4 Article 1 of Directive 2000/31, entitled 'Objective and scope', provides:

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

...

5. This Directive shall not apply to:

...

(b) questions relating to information society services covered by Directives [95/46] and [97/66];

...'

5 Section 4 of Chapter II of Directive 2000/31, entitled 'Liability of intermediary service providers', included, in the version applicable to the main proceedings, Articles 12 to 15 of that directive. Articles 12 and 13 of Directive 2000/31 concerned, in accordance with their respective titles, 'Mere conduit' and 'Caching'.

6 Article 14 of that directive, entitled 'Hosting', provided:

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

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

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

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

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

7 Article 15 of Directive 2000/31, entitled 'No general obligation to monitor', provided, in paragraphs 1 and 2:

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

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

The GDPR

8 Recitals 4, 10, 39, 51, 74, 75, 78 and 85 of the GDPR state:

'(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, home and communications, 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, and cultural, religious and linguistic diversity.

...

(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. ...

...

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned

and their right to obtain confirmation and communication of personal data concerning them which are being processed. ...

...

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. ... Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation ... In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

...

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to ... identity theft or fraud ... damage to the reputation ... where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; ...

...

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. ...

...

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, ... damage to reputation ...'

9 Article 1 of that regulation, 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.'

10 Article 2 of the GDPR, entitled 'Material scope', provides, in paragraph 4 thereof:

'This Regulation shall be without prejudice to the application of Directive [2000/31], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.'

11 Article 4 of that regulation, entitled 'Definitions', reads as follows:

'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;

...'

12 Chapter II of the GDPR, entitled 'Principles', comprises, inter alia, Articles 5 to 9 of that regulation.

13 Article 5 of that regulation, entitled 'Principles relating to processing of personal data', provides:

'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");

...

(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");

...

(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").

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability").'

14 Article 6 of that regulation, entitled 'Lawfulness of processing', provides, in the first subparagraph of paragraph 1 thereof:

'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.'

15 Article 7 of the GDPR, entitled 'Conditions for consent', provides, in paragraph 1 thereof:

'Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.'

16 Article 9 of the GDPR, entitled 'Processing of special categories of personal data', provides:

'1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

- (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

...'

17 Article 13 of the GDPR, entitled 'Information to be provided where personal data are collected from the data subject', provides, in paragraph 1(a) thereof:

'Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative'.

18 Article 14 of that regulation, entitled 'Information to be provided where personal data have not been obtained from the data subject', provides in paragraph 1(a) thereof:

'Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative'.

19 In Chapter III of the GDPR, entitled 'Rights of the data subject', Article 17 of that regulation, itself entitled 'Right to erasure ("right to be forgotten")', provides in paragraphs 1 and 2 thereof:

'1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

...

(d) the personal data have been unlawfully processed;

...

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.'

20 Chapter IV of the GDPR, entitled 'Controller and processor', includes, in Section 1, itself entitled 'General obligations', inter alia, Articles 24 to 26 thereof.

21 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.'

22 Article 25 of that regulation, entitled 'Data protection by design and by default' provides, in paragraphs 1 and 2 thereof:

'1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.'

23 Article 26 of the GDPR, 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. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.'

24 Under Article 32 of the GDPR, entitled 'Security of processing':

'1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.'

25 Article 82 of that regulation, entitled 'Right to compensation and liability', states, in paragraphs 1 to 3 thereof:

'1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.'

26 Article 94 of the GDPR provides:

- ‘1. Directive [95/46] is repealed with effect from 25 May 2018.
2. References to the repealed Directive shall be construed as references to this Regulation. ...’

Romanian law

27 Article 11 of Legea nr. 365/2002 privind comerțul electronic (Law No 365/2002 on electronic commerce) of 7 June 2002 (*Monitorul Oficial al României*, Part I, No 483 of 5 July 2002), as amended by Legea nr. 121/2006 pentru modificarea și completarea Legii nr. 365/2002 privind comerțul electronic (Law No 121/2006 amending and supplementing Law No 365/2002 on electronic commerce) of 4 May 2006 (*Monitorul Oficial al României*, Part I, No 403 of 10 May 2006) (‘Law No 365/2002’), provides:

- ‘1. Service providers shall be subject to the legal provisions governing civil and criminal liability and liability for administrative offences, unless otherwise provided for in this law.
2. Service providers shall be liable for information supplied by them or on their behalf.
3. Service providers shall not be liable for information transmitted or stored or to which they provide access under the conditions laid down in Articles 12 to 15.’

28 Article 14 of Law No 365/2002, entitled ‘Permanent storage of information, hosting’, provides:

‘1. Where an information society service consists of the storage of information provided by a recipient of that service, the provider of that service shall not be liable for the information stored at the request of a recipient if either of the following conditions is met:

- (a) the service provider is not aware of the illegal nature of the activity or of the information stored and, as regards claims for damages, is not aware of facts or circumstances from which it would follow that the activity or information in question could infringe the rights of a third party;
- (b) if the service provider becomes aware of the illegal nature of the activity or information concerned or of facts or circumstances from which it would follow that the activity or information in question could infringe the rights of a third party, the service provider acts expeditiously to remove it or to block access to it.

2. The provisions of paragraph 1 shall not apply where the recipient is acting under the authority or the control of the service provider.

3. The provisions of this article shall not affect the right of a judicial or administrative authority to require that the service provider terminate or prevent a data breach, and shall not affect the right to establish government procedures to restrict or terminate access to information.’

29 The Normele metodologice pentru aplicarea Legii nr. 365/2002 privind comerțul electronic (implementing rules for Law No 365/2002 on electronic commerce), approved by Hotărârea Guvernului nr. 1.308 privind aprobarea Normelor metodologice pentru aplicarea Legii nr. 365/2002 privind comerțul electronic (Government Decision No 1.308 approving the implementing rules for Law No 365/2002 on electronic commerce) of 20 November 2002 (*Monitorul Oficial al României*, Part I, No 877 of 5 December 2002), provide, in Article 11(1) thereof:

‘Information society service providers that offer the services referred to in Articles 12 to 15 of Law [No 365/2002] are not required to monitor the information which they transmit or store, nor are they required actively to seek data on activities or information having the appearance of unlawful activity in the sector of the information society services that they supply.’

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

30 Russmedia Digital, a company incorporated under Romanian law, is the owner of the website www.publi24.ro, an online marketplace on which advertisements for, inter alia, the sale of goods or the provision of services in Romania can be published either free of charge or for a fee.

31 The applicant in the main proceedings claims that, on 1 August 2018, an unidentified third party published on that website an untrue and harmful advertisement presenting her as offering sexual services. That advertisement contained photographs of that applicant, which had been used without her consent, along with her telephone number. The advertisement was subsequently reproduced identically on other websites containing advertising content, where it was posted online with the indication of the original source. When contacted by the applicant in the main proceedings, Russmedia Digital removed the advertisement from its website less than one hour after receiving that request. The same advertisement nevertheless remains available on other websites which have reproduced it.

32 Taking the view that the advertisement at issue in the main proceedings infringed her right of personal portrayal, and rights to honour, reputation and privacy, as well as the rules relating to the processing of personal data, the applicant in the main proceedings brought an action against Russmedia before the Judecătoria Cluj-Napoca (Court of First Instance, Cluj-Napoca, Romania). That court ordered Russmedia to pay her damages in the amount of EUR 7 000 in respect of the non-material damage caused by the infringement of the right of personal portrayal and the rights to honour and reputation, as well as by the infringement of the right to respect for her private life and the unlawful processing of her personal data.

33 Russmedia appealed against that judgment. The Tribunalul Specializat Cluj (Specialised Court, Cluj, Romania) upheld that appeal, holding that the action brought by the applicant in the main proceedings was unfounded, since the advertisement at issue in the main proceedings did not originate from Russmedia, which merely provided a hosting service for that advertisement, without being actively involved in its content. Accordingly, the exemption from liability provided for in Article 14(1)(b) of Law No 365/2002 would be applicable to it. As regards the processing of personal data, that court held that an information society services provider was not required to check the information which it transmits or actively to seek data relating to apparently unlawful activities or information. In that regard, it held that Russmedia could not be criticised for failing to take measures to prevent the online distribution of the defamatory advertisement at issue in the main proceedings, given that it had rapidly removed that advertisement at the request of the applicant in the main proceedings.

34 That applicant brought an appeal against that judgment before the Curtea de Apel Cluj (Court of Appeal, Cluj, Romania), arguing that the Tribunalul Specializat Cluj (Specialised Court, Cluj) had relied on a misinterpretation of Law No 365/2002. She submits, inter alia, that since that law was not *lex specialis* in relation to the GDPR, the specialised court ought to have examined the applicability of that regulation in the present case. Furthermore, Russmedia's role was not limited to providing its customers with the specific technical means of accessing the hosting server. She submits that it also played a management role, intervening in terms of content in order to ensure good information management. That company, as operator of the website at issue in the main proceedings, stored and processed the information content. The storage of data and making them available to the public in a certain form involves an analysis of the data and information contained in the advertisements. That evidence demonstrates that Russmedia was directly involved in the management and dissemination of the content of the advertisements. Consequently, the provisions of Article 14 of Law No 365/2002 are not applicable.

35 Furthermore, the applicant in the main proceedings submits that the exemption from liability of such a provider does not apply if liability is established under other regulatory acts, such as the GDPR. In her view, Russmedia published her personal data without her consent and, through the operation of its

website, allows anyone to post any kind of advertisement, in particular advertisements which do not ensure the security of personal data, making it impossible permanently to erase data published online.

36 Russmedia contends, for its part, that the solution adopted by the Tribunalul Specializat Cluj (Specialised Court, Cluj) is correct. In Russmedia's view, the applicant in the main proceedings has not shown how the GDPR constituted a special rule which prevents the application of the relevant provisions of Law No 365/2002.

37 The Curtea de Apel Cluj (Court of Appeal, Cluj), which is the referring court and rules in the present case as an appellate court whose decision is final, considers it necessary to determine, in particular, the limits of the exemption from liability of an information society services provider, such as Russmedia, under Directive 2000/31.

38 Making reference to the relevant case-law of the Court of Justice, the referring court states that although, in accordance with that case-law, there is no obligation for operators of online marketplaces to carry out prior verification of the information or advertisements posted by user advertisers, the fact remains that the exemption from liability of those operators is conditional. Thus, in accordance with the judgment of 12 July 2011, *L'Oréal and Others* (C324/09, EU:C:2011:474), an operator of online services cannot rely on the exemption from liability provided for in Article 14(1) of Directive 2000/31 if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously in accordance with Article 14(1)(b) of that directive. Similarly, it is apparent from the judgment of 11 September 2014, *Papasavvas* (C291/13, EU:C:2014:2209), that the limitations of civil liability specified in Articles 12 to 14 of Directive 2000/31 do not apply to the case of a company which operates a website on which the online version of a newspaper is posted, since that company, which is remunerated by commercial advertisements posted on that website, has knowledge of the information posted and exercises control over that information.

39 The referring court emphasises, however, that that case-law refers only to offers posted on a website that were held to be illegal because of an analysis of facts and circumstances explicitly communicated to the data controller after the advertisement in question had been published. Thus, the Court has not yet had occasion to examine a situation, such as that in the main proceedings, in which the content of the advertisement published was manifestly unlawful and deeply harmful to the data subject.

40 The referring court raises the question, in that context, of whether it is necessary for a platform to receive a notification in order to be obliged to erase manifestly unlawful and seriously harmful content. In the present case, the advertisement at issue in the main proceedings was published without verification of the identity of the user advertiser and clearly without the consent of the applicant in the main proceedings having been obtained.

41 Moreover, although the advertisement at issue in the main proceedings was deleted from the original website following a notification from the applicant, the content of that advertisement, including her contact details and photographs, was, it is stated, reproduced in its entirety on numerous other websites, indicating the original source. The damage suffered by the applicant has, therefore, it is claimed, become permanent and is still continuing. The referring court notes in that regard that the sexual services allegedly offered may be associated with serious offences, punishable under the Codul Penal (Criminal Code), such as procuring and human trafficking.

42 The referring court states that, in view of the general terms and conditions of use of the online marketplace operated by Russmedia, although that company does not claim any right of ownership over the content of the advertisements published, it nevertheless retains the right to use that content, including

the right to copy it, distribute it, transmit it, publish it, reproduce it, modify it, translate it, transfer it to partners and remove it at any time, without the need for any valid reason for doing so.

43 In those circumstances the Curtea de Apel Cluj (Court of Appeal, Cluj) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

‘(1) Do Articles 12 to 14 of Directive [2000/31] also apply to a storage and hosting information [society] service provider that makes available to users a website on which free or paid advertisements may be published, which claims that its role in publishing users’ advertisements is purely technical (making the platform available), but which, through the general terms and conditions of use of the website, indicates that it does not claim ownership over the content that is provided, published, uploaded or transmitted, yet retains the right to use the content, including by means of copying it, distributing it, transmitting it, publishing it, reproducing it, modifying it, translating it, transferring it to partners and removing it at any time, without the need for any reason for doing so?’

(2) Must Article 2(4), Article 4(7) and (11), Article 5(1)(f), Article 6(1)(a), Articles 7, 24 and 25 of [the GDPR] and Article 15 of Directive [2000/31] be interpreted as requiring such a storage and hosting information [society] service provider, which is the personal data controller, to verify before publishing an advertisement whether the person publishing the advertisement and the owner of the personal data referred to in the advertisement are the same person?

(3) Must Article 2(4), Article 4(7) and (11), Article 5(1)(f), Article 6(1)(a), Articles 7, 24 and 25 of [the GDPR] and Article 15 of Directive [2000/31] be interpreted as requiring such a storage and hosting information [society] service provider, which is the personal data controller, to verify in advance the content of advertisements published by users, in order to exclude advertisements which are potentially unlawful in nature or likely to infringe a person’s private and family life?

(4) Must Article 5(1)(b) and (f), Articles 24 and 25 of [the GDPR] and Article 15 of Directive [2000/31] be interpreted as requiring such a storage and hosting information [society] service provider, which is the personal data controller, to apply safeguards which prevent or limit the reproduction and redistribution of the content of the advertisements published through it?’

Consideration of the questions referred

44 According to settled case-law, in the procedure laid down by Article 267 TFEU providing for cooperation between national courts and the Court of Justice, it is for the latter to provide the national court with an answer which will be of use to it and enable it to determine the case before it. To that end, the Court should, where necessary, reformulate the questions referred to it. It is for the Court to extract from all the information provided by the national court, in particular from the grounds of the order for reference, the points of EU law which require interpretation, having regard to the subject matter of the dispute (see, to that effect, judgments of 29 November 1978, *Redmond*, 83/78, EU:C:1978:214; paragraph 26; of 28 November 2000, *Roquette Frères*, C88/99, EU:C:2000:652, paragraph 18; and of 30 April 2024, *M.N. (EncroChat)*, C670/22, EU:C:2024:372, paragraph 78).

45 The referring court’s questions seek, together, to determine, first, whether the operator of an online marketplace, such as Russmedia, which allows its users to place advertisements anonymously on its online marketplace free of charge or for a fee, has failed to fulfil its obligations under the GDPR, where an advertisement published on its online marketplace contains personal data, in particular sensitive personal data, in breach of that regulation, and, second, whether Articles 12 to 15 of Directive 2000/31 relating to the liability of intermediary service providers are applicable to such an operator.

46 In order to provide a useful answer to those questions, it is appropriate to examine, first of all, the second to fourth questions referred for a preliminary ruling – which seek to determine the obligations

incumbent under the GDPR on an operator of an online marketplace in a situation such as that at issue in the main proceedings – by reformulating those questions in such a way that they relate solely to the interpretation of that regulation. Subsequently, it will be examined whether such an operator may rely on Articles 12 to 15 of Directive 2000/31, which is, in essence, the subject matter of the first question.

The second to fourth questions, concerning the interpretation of the GDPR

Preliminary remarks

47 As a preliminary point, it should be noted, in the first place, that it is apparent from the request for a preliminary ruling that the advertisement at issue presented the applicant in the main proceedings as offering sexual services, and that that advertisement contained, in particular, photographs of her, used without her consent, as well as her telephone number.

48 It is common ground that such information constitutes personal data, within the meaning of Article 4(1) of the GDPR, which defines such data as ‘any information relating to an identified or identifiable natural person,’ specifying 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’.

49 According to settled case-law, the use of the expression ‘any information’ in the definition of the concept of ‘personal data’ in Article 4(1) of the GDPR 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. 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 3 April 2025, *Ministerstvo zdravotníctví (Data concerning the representative of a legal person)*, C710/23, EU:C:2025:231, paragraph 21 and the case-law cited).

50 In addition, among those personal data, Article 9(1) of the GDPR provides for a special protection regime for special categories of data, including data concerning a natural person’s sex life or sexual orientation.

51 The Court has clarified that the purpose of Article 9(1) of that regulation is to ensure enhanced protection as regards processing which, because of the particular sensitivity of the data processed, is 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 (judgment of 21 December 2023, *Krankenversicherung Nordrhein*, C667/21, EU:C:2023:1022, paragraph 41 and the case-law cited).

52 Such enhanced protection necessarily calls for a broad definition of such ‘sensitive data’. Thus, the Court has held that Article 9(1) of the GDPR applies to processing not only of inherently sensitive data to which that provision relates, but also of data revealing information of that nature indirectly, following an intellectual operation involving deduction or cross-referencing (judgment of 5 June 2023, *Commission v Poland (Independence and private life of judges)*, C204/21, EU:C:2023:442, paragraph 344 and the case-law cited).

53 In the context of that broad definition, the untrue and harmful nature of data concerning a natural person’s sex life or sexual orientation cannot mean that such data ceases to be classified as ‘sensitive data’ in terms of Article 9(1) of the GDPR.

54 In the second place, it should be noted that the processing at issue in the main proceedings consists in the publication of the advertisement in question and, therefore, of those data on Russmedia’s online

marketplace. Indeed, the operation of loading personal data on a webpage constitutes processing, within the meaning of Article 4(2) of the GDPR (judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, C184/20, EU:C:2022:601, paragraph 65 and the case-law cited).

55 In the third place, it should be noted that the second to fourth questions refer to the fact that the operator of the online marketplace at issue in the main proceedings is a personal data controller. However, it appears that the personal data, the publication of which is the subject of the dispute in the main proceedings, were inserted in the advertisement in question by an anonymous user advertiser, without the operator having had any actual influence on the content of that advertisement and without it having been aware of its untrue and harmful nature. In those circumstances, it is necessary to clarify the concepts of ‘controller’ and ‘joint controllers’, within the meaning of Article 4(7) and Article 26 of the GDPR, respectively.

56 Article 4(7) of the GDPR defines the concept of ‘controller’ broadly as meaning 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.

57 The objective of that broad definition consists, in accordance with the objective pursued by the GDPR, in ensuring effective protection of the fundamental rights and freedoms of natural persons and in ensuring a high level of protection of the right of every person to the protection of personal data concerning him or her (judgment of 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C683/21, EU:C:2023:949, paragraph 29 and the case-law cited).

58 Thus, any natural or legal person who exerts influence over the processing of such data, for his or her 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 in respect of such processing (judgment of 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C683/21, EU:C:2023:949, paragraph 30 and the case-law cited).

59 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, to that effect, judgment of 29 July 2019, *Fashion ID*, C40/17, EU:C:2019:629, paragraph 67 and the case-law cited).

60 Article 26 of the GDPR, which forms part of the framework for defining the ‘controller’ referred to in Article 4(7) of that regulation, provides, in essence, that, where two or more controllers jointly determine the purposes and means of the processing, they must be classified as ‘joint controllers’ of that processing.

61 Such joint responsibility does not necessarily require the existence of common decisions as to the determination of the purposes and means of the processing of the personal data concerned. Indeed, the Court has held that 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 together by two or more entities or from converging decisions which 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 (see, to that effect, judgment of 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C683/21, EU:C:2023:949, paragraph 43).

62 In that regard, the joint responsibility of several actors for the same processing, under Article 4(7) of the GDPR, does not require each of them to have access to the personal data concerned (judgments of 29 July 2019, *Fashion ID*, C40/17, EU:C:2019:629, paragraph 69 and the case-law cited, and of 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C683/21, EU:C:2023:949, paragraph 42).

63 In the same vein, the Court has made clear that the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case (see, to that effect, judgments of 10 July 2018, *Jehovan todistajat*, C25/17, EU:C:2018:551, paragraph 66 and the case-law cited, and of 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C683/21, EU:C:2023:949, paragraph 42).

64 In the present case, it is common ground that the user advertiser, who placed the untrue and harmful advertisement containing personal data of the applicant in the main proceedings on the online marketplace operated by Russmedia, must be regarded as having principally determined the purposes and means of the processing of those data and therefore falls within the concept of ‘controller’ within the meaning of Article 4(7) of the GDPR.

65 That said, it is established that that advertisement was published on the internet and thus made accessible to internet users only as a result of the online marketplace operated by Russmedia.

66 Although it is apparent from the case-law cited in paragraph 58 above that a person may be classified as a ‘controller’ of personal data only if he or she exerts influence over the processing of such data, for his or her own purposes, it should nonetheless be noted that that may be the case, inter alia, where the operator of an online marketplace publishes the personal data concerned for commercial or advertising purposes which go beyond the mere provision of a service which he or she provides to the user advertiser.

67 In the present case, it is apparent from the order for reference that Russmedia publishes advertisements on its online marketplace for its own commercial purposes. In that regard, the general terms and conditions of use of that marketplace give Russmedia considerable freedom to exploit the information published on that marketplace. In particular, according to the information provided by the referring court, Russmedia reserves the right to use published content, distribute it, transmit it, reproduce it, modify it, translate it, transfer it to partners and remove it at any time, without the need for any ‘valid’ reason for so doing. Russmedia therefore publishes the personal data contained in the advertisements not on behalf of the user advertisers, or not solely on their behalf, but processes and can exploit those data for its own advertising and commercial purposes.

68 Consequently, it must be held that Russmedia exerted influence, for its own purposes, over the publication on the internet of the personal data of the applicant in the main proceedings and therefore participated in the determination of the purposes of that publication and thus of the processing at issue.

69 That finding is not called into question by the fact that Russmedia clearly did not participate in the determination of the untrue and harmful purpose pursued by the user advertiser through the publication of the advertisement at issue in the main proceedings. Indeed, Russmedia participated in the determination of the purpose of the processing that consisted in making the personal data contained in the advertisement at issue in the main proceedings accessible to internet users in order to put such publications to effective use. In addition, by allowing advertisements to be placed anonymously on its online marketplace, Russmedia facilitated the publication of such data without the data subject’s consent.

70 Furthermore, by having made its online marketplace, which was used to publish the advertisement at issue in the main proceedings, available to the user advertiser, Russmedia participated in the determination of the means of that publication.

71 Indeed, the Court has already held, in essence, that a natural or legal person who exerts a decisive influence over the collection and transmission of personal data, or even a person who has an influence, by means of his or her activity of defining parameters – depending on his or her objectives of managing and

promoting his or her activities – on the processing of such data, participates in the determination of the means of processing (see, to that effect, judgments of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C210/16, EU:C:2018:388, paragraph 36, and of 29 July 2019, *Fashion ID*, C40/17, EU:C:2019:629, paragraph 78). The same is true in the case of a search engine, where its activity plays a decisive role in the overall dissemination of personal data in that that activity renders those data publicly accessible online in an organised and aggregated manner (see, to that effect, judgment of 8 December 2022, *Google (De-referencing of allegedly inaccurate content)*, C460/20, EU:C:2022:962, paragraph 50 and the case-law cited).

72 It must, therefore, be held that where the operator of an online marketplace such as Russmedia sets the parameters for the dissemination of advertisements likely to contain personal data depending on the recipients concerned, determines the presentation and duration of that dissemination or the headings structuring the information published, or even organises the classification which will determine the arrangements for such dissemination, it participates in the determination of the essential elements of the publication of the personal data concerned, thereby exerting a decisive influence on the overall dissemination of those data.

73 In that regard, the content of the general terms and conditions of use of the online marketplace concerned may provide evidence demonstrating that the operator of that marketplace exerts a decisive influence over the processing of personal data concerned and thus determines the means of that processing. That would appear to be the case with the general terms and conditions of use of Russmedia's online marketplace, in which that company reserves in particular the right to distribute, transmit, publish, remove or reproduce the information contained in the advertisements, including the personal data contained therein.

74 In any event, the operator of an online marketplace cannot avoid its liability, as controller of personal data, on the ground that it has not itself determined the content of the advertisement at issue published on that marketplace. Indeed, to exclude such an operator from the definition of 'controller' on that ground alone would be contrary not only to the clear wording, but also the objective, of Article 4(7) of the GDPR, which is to ensure effective and complete protection of data subjects by means of a broad definition of the concept of 'controller'.

75 Accordingly, it must be held that the referring court was fully entitled to base its second to fourth questions on the premiss that, in a situation such as that at issue in the main proceedings, the operator of the online marketplace is a controller of the personal data contained in an advertisement published on that online marketplace, within the meaning of Article 4(7) of the GDPR.

76 It is in the light of all the foregoing preliminary remarks that those questions must be answered.

The second and third questions

77 By its second and third questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 5(2) and Articles 24 to 26 of the GDPR must be interpreted as meaning that the operator of an online marketplace, as controller, within the meaning of Article 4(7) of the GDPR, of the personal data contained in advertisements published on its online marketplace, is required, before the publication of the advertisements, to identify those which contain sensitive data, in terms of Article 9(1) of the GDPR, to ascertain whether the user advertiser preparing to place such an advertisement is the person whose sensitive data are included in that advertisement and, if that is not the case, to refuse publication of the advertisement in the absence of explicit consent from the data subject, inasmuch as such publication would be liable to result in a serious infringement of that subject's rights to respect for private life and to the protection of his or her personal data, guaranteed in Articles 7 and 8 of the Charter.

78 Under Article 1(2) of the GDPR, read in the light of recitals 4 and 10 thereof, that regulation has the objective in particular of ensuring a high level of protection of the fundamental rights and freedoms of natural persons with respect to the processing of personal data; that right to such protection is also recognised in Article 8 of the Charter and is closely connected to the right to respect for private life, enshrined in Article 7 of the Charter (see, to that effect, judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, C184/20, EU:C:2022:601, paragraph 61 and the case-law cited).

79 To that end, first, Chapter II of the GDPR sets out the principles governing the processing of personal data which the controller must observe. In particular, all processing of personal data must comply with the principles relating to processing of data and the conditions governing lawfulness of processing listed in Articles 5 and 6 of that regulation (see, to that effect, judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, C184/20, EU:C:2022:601, paragraph 62 and the case-law cited).

80 In accordance with Article 5(1)(a) of the GDPR, personal data are to be processed lawfully, fairly and in a transparent manner in relation to the data subject. Article 5(1)(d) of the GDPR adds that personal data processed must be accurate and, where necessary, kept up to date. Thus, 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. Article 5(1)(f) of that regulation provides that personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing.

81 As regards the conditions for lawful processing, as the Court has held, the first subparagraph of Article 6(1) of the GDPR sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Processing must thus fall within one of the cases provided for in that provision (see, to that effect, judgment of 9 January 2025, *Mousse*, C394/23, EU:C:2025:2, paragraph 25 and the case-law cited).

82 In particular, under point (a) of the first subparagraph of Article 6(1) of the GDPR, processing of personal data is to be lawful if, and to the extent that, the data subject has given consent thereto for one or more specific purposes. Article 7(1) of that regulation states that, in that case, the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data. In the absence of such consent, or where that consent is not freely given, specific, informed and unambiguous, within the meaning of Article 4(11) of the GDPR, such processing is nevertheless justified where it meets one of the requirements of necessity mentioned in points (b) to (f) of the first subparagraph of Article 6(1) of that regulation (judgment of 9 January 2025, *Mousse*, C394/23, EU:C:2025:2, paragraph 26 and the case-law cited).

83 In addition to those principles and conditions, there are specific requirements for sensitive data as defined in Article 9(1) of the GDPR, the processing of which is, in principle, prohibited (see, to that effect, judgment of 21 December 2023, *Krankenversicherung Nordrhein*, C667/21, EU:C:2023:1022, paragraph 73).

84 That prohibition may be derogated from only if one of the exceptions provided for in Article 9(2)(a) to (j) of that regulation is met. Among those exceptions, which must be interpreted strictly, Article 9(2)(a) of the GDPR provides that the prohibition on processing sensitive data is not to apply if the data subject has given his or her explicit consent to the processing of his or her sensitive personal data for one or more specified purposes, except where EU or Member State law provide that that prohibition may not be lifted by the data subject.

85 Second, Chapter IV of the GDPR clarifies the scope of the obligations incumbent on the controller of personal data, in accordance with the principle of accountability set out in Article 5(2) of the GDPR.

86 Under Article 5(2) of the GDPR, the controller is responsible for compliance with paragraph 1 of that article and must be able to demonstrate its compliance with each of the principles set out in paragraph 1 of that article, the burden of such proof thus being placed on it (judgment of 4 May 2023, *Bundesrepublik Deutschland (Court electronic mailbox)*, C60/22, EU:C:2023:373, paragraph 53 and the case-law cited).

87 That principle of accountability of the controller is given expression in particular in Article 24 of the GDPR (see, to that effect, judgment of 25 January 2024, *MediaMarktSaturn*, C687/21, EU:C:2024:72, paragraph 43 and the case-law cited). That article requires that, 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 in respect of that processing must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing has been performed in accordance with that regulation.

88 Thus, Article 5(2) and Article 24 of the GDPR impose general accountability and compliance requirements upon the controller of personal data. They require that controller to take appropriate steps to prevent any infringements of the rules laid down in the GDPR in order to ensure the right to the protection of data (see, to that effect, judgment of 27 October 2022, *Proximus (Public electronic directories)*, C129/21, EU:C:2022:833, paragraph 81).

89 From that point of view, Article 25(1) of the GDPR requires that the controller must, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures that are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of that regulation and protect the rights of data subjects. In addition, Article 25(2) on data protection by default provides, inter alia, that the appropriate technical and organisational measures which the controller must implement to that effect are to ensure that, by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

90 Where the personal data that are processed are sensitive data, in terms of Article 9(1) of the GDPR, the controller must, inter alia, in order to determine what measures are appropriate within the meaning of Articles 24 and 25 of that regulation, take account of the fact that an infringement of the principles set out in Chapter II of that regulation with regard to the processing of such data may constitute a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data guaranteed in Articles 7 and 8 of the Charter.

91 It is in the light of all those clarifications that the second and third questions, as reformulated in paragraph 77 above, must be examined.

92 As regards, in the first place, the question whether the operator of an online marketplace must identify the advertisements that contain sensitive data, in terms of Article 9(1) of the GDPR, before publishing them, it must be recalled, as is apparent from paragraphs 64 and 75 above, that that operator and the user advertiser who has placed such an advertisement on that online marketplace must be considered joint controllers, within the meaning of Article 26 of that regulation, when the advertisement concerned is published there.

93 It follows that both that operator and that user advertiser are required to ensure compliance with the obligations arising from Article 5(2) and Articles 24 and 25 of the GDPR. In particular, they must be able to demonstrate that the personal data contained in the advertisement concerned are lawfully published, that is to say, that the data subject has consented to such publication, unless they can rely on another condition laid down in Article 6(1) of the GDPR. Where the personal data concerned are sensitive data, in terms of Article 9(1) of the GDPR, consent to such publication must, as is apparent from paragraph 84 above, be

explicit. Similarly, according to the principle of accuracy set out in Article 5(1)(d) of the GDPR, controllers must be able to demonstrate that the personal data concerned are accurate.

94 In order to determine specifically the appropriate technical and organisational measures that the operator of an online marketplace, as joint controller of personal data, is required to implement, pursuant to Articles 24 and 25 of the GDPR, in order to ensure and be able to demonstrate that the publication of sensitive data contained in an advertisement is made in accordance with that regulation, it is apparent from those provisions that the appropriateness of such measures must be assessed in a concrete manner, taking into account the nature, scope, context and purposes of the processing in question and the likelihood and severity of the risks for the rights and freedoms of the data subject which are specific to it (see, to that effect, judgment of 21 December 2023, *Krankenversicherung Nordrhein*, C667/21, EU:C:2023:1022, paragraph 96).

95 In that regard, it should be noted that the publication of personal data on an online marketplace entails significant risks to the rights and freedoms of the data subject, since it makes those data accessible in principle to any internet user. In addition, once published on an online marketplace, those data may be copied and reproduced on other websites, with the result that it may prove difficult, if not impossible, for the data subject to obtain their actual erasure from the internet.

96 The risks associated with such publication are all the more serious in the case of sensitive data in terms of Article 9(1) of the GDPR. As expressly stated in recital 51 of the GDPR, personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to those fundamental rights and freedoms (see, to that effect, judgment of 4 October 2024, *Lindenapotheke*, C21/23, EU:C:2024:846, paragraph 75). The processing of such data may, as noted in paragraph 90 above, constitute a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data guaranteed in Articles 7 and 8 of the Charter. In addition, the likelihood of an infringement of those rights by the publication of an advertisement containing sensitive data is very high where the user advertiser is not himself or herself the data subject and where the online marketplace allows such advertisements to be placed anonymously.

97 Accordingly, inasmuch as the operator of an online marketplace, such as the marketplace at issue in the main proceedings, knows or ought to know that, generally, advertisements containing sensitive data in terms of Article 9(1) of the GDPR, are liable to be published by user advertisers on its online marketplace, that operator, as controller in respect of that processing, is obliged, as soon as its service is designed, to implement appropriate technical and organisational measures in order to identify such advertisements before their publication and thus to be in a position to verify whether the sensitive data that they contain are published in compliance with the principles set out in Chapter II of that regulation. Indeed, as is apparent in particular from Article 25(1) of that regulation, the obligation to implement such measures is incumbent on it not only at the time of the processing, but already at the time of the determination of the means of processing and, therefore, even before sensitive data are published on its online marketplace in breach of those principles, that obligation being specifically intended to prevent such breaches.

98 As regards, in the second place, the question whether the operator of an online marketplace, as controller of the sensitive data contained in advertisements published on its website, jointly with the user advertiser, must verify the identity of that user advertiser before the publication, it should be recalled that it follows from a combined reading of Article 9(1) and Article 9(2)(a) of the GDPR that the publication of such data is prohibited, unless the data subject has given his or her explicit consent to the data in question being published on that online marketplace or one of the other exceptions laid down in Article 9(2)(b) to (j) is satisfied, which does not, however, appear to be the case here.

99 On that basis, while the placing by a data subject of an advertisement containing his or her sensitive data on an online marketplace may constitute explicit consent, within the meaning of Article 9(2)(a) of the GDPR, such consent is lacking where that advertisement is placed by a third party, unless that party can demonstrate that the data subject has given his or her explicit consent to the publication of that advertisement on the online marketplace in question. Consequently, in order to be able to ensure, and to be able to demonstrate, that the requirements laid down in Article 9(2)(a) of the GDPR are complied with, the operator of the marketplace is required to verify, prior to the publication of such an advertisement, whether the user advertiser preparing to place the advertisement is the person whose sensitive data appear in that advertisement, which presupposes that the identity of that user advertiser is collected.

100 In addition, it is apparent from Article 13(1)(a) and Article 14(1)(a) of the GDPR that controllers of personal data must, in any event, provide their identities and contact details to the data subject.

101 Lastly, it must be observed that Article 26 of the GDPR requires joint controllers of personal data processing to determine, in a transparent manner, their respective responsibilities for compliance with the obligations under that regulation. However, such an obligation would prove impossible if one of the controllers of that processing could remain anonymous in relation to the other.

102 It follows from the foregoing that the operator of an online marketplace, as a party responsible for publishing the sensitive data contained in an advertisement published on its online marketplace, jointly with the user advertiser, is obliged to collect the identity of that user advertiser and to verify whether that user advertiser is the person whose sensitive data appear in that advertisement.

103 In that regard, as the Advocate General observed, in essence, in point 132 of his Opinion, it is apparent from recital 75 of the GDPR that, in particular in the case of identity theft, the processing of personal data may entail risks to the rights and freedoms of data subjects which could, as a result, be prevented from exercising control over their personal data. In general, an identity is stolen with the aim of carrying out fraudulent actions to the detriment of the data subject or third parties.

104 In those circumstances and having regard also to the considerations set out in paragraphs 95 and 96 above, in order to be able to ensure and to demonstrate that the sensitive data contained in advertisements are processed in accordance with the requirements of the GDPR, the operator of an online marketplace must provide, pursuant to Articles 24 and 25 of that regulation, for appropriate technical and organisational measures enabling it not only to collect, but also to verify, the identity of the user advertisers before the publication of those advertisements, in particular in order to be able to determine whether that user advertiser is the person whose sensitive data appear in those advertisements. As the Advocate General observed in point 134 of his Opinion, such measures must in particular make it possible to limit the risk of unlawful processing of the personal data of data subjects and to combat unfair use of such an online marketplace, by limiting the feeling of impunity and thus encouraging user advertisers to comply with the requirements of the GDPR when they publish advertisements containing personal data.

105 Lastly, as regards, in the third place, the question whether the operator of an online marketplace must refuse publication of an advertisement containing sensitive data where it becomes apparent – after such verification of the identity of the user advertiser who is preparing to place that advertisement – that that user is not the person whose sensitive data appear in that advertisement, it should be noted that it follows from paragraphs 98 and 99 above that, in such a situation, it cannot be excluded that that publication may occur in breach of the prohibition on processing such data, laid down in Article 9(1) of the GDPR. Accordingly, unless that user advertiser can demonstrate to the requisite legal standard that the data subject has given his or her explicit consent to the data in question being published on that online marketplace, within the meaning of Article 9(2)(a), or that one of the other exceptions provided for in Article 9(2)(b) to (j) is satisfied, the operator of that online marketplace must refuse publication of the

advertisement in question, which it must ensure by implementing appropriate technical and organisational measures.

106 In the light of all the foregoing reasons, the answer to the second and third questions is that Article 5(2) and Articles 24 to 26 of the GDPR must be interpreted as meaning that the operator of an online marketplace, as controller, within the meaning of Article 4(7) of the GDPR, of the personal data contained in advertisements published on its online marketplace, is required, before the publication of the advertisements and by means of appropriate technical and organisational measures,

- to identify the advertisements that contain sensitive data in terms of Article 9(1) of the GDPR,
- to verify whether the user advertiser preparing to place such an advertisement is the person whose sensitive data appear in that advertisement and, if this is not the case,
- to refuse publication of that advertisement, unless that user advertiser can demonstrate that the data subject has given his or her explicit consent to the data in question being published on that online marketplace, within the meaning of Article 9(2)(a), or that one of the other exceptions provided for in Article 9(2)(b) to (j) is satisfied.

The fourth question

107 The fourth question essentially concerns whether an operator of an online marketplace, as controller, is required to implement security measures such as to prevent or limit the copying and redistribution of advertisements containing sensitive data which have been published on its online marketplace.

108 In the present case, it is apparent from the request for a preliminary ruling that the untrue and harmful advertisement at issue in the main proceedings was reproduced on other websites with advertising content, which published it by indicating the original source; in addition, in the general terms and conditions of use of its online marketplace, Russmedia reserves, inter alia, the right to transmit the content of the advertisements published there and to transfer that content to partners. In that regard, the referring court does not specify whether Russmedia voluntarily transferred the advertisement at issue to those other websites or, at the very least, allowed those publications by means of contracts, or whether, on the contrary, those publications are the result of copies of the original advertisement that were not authorised by Russmedia.

109 If the first part of that alternative were established, that transmission would constitute further processing of personal data for which Russmedia would be controller, within the meaning of Article 4(7) of the GDPR. That processing should be distinguished from the publication by the user advertiser of the untrue and harmful advertisement at issue in the main proceedings on Russmedia's online marketplace.

110 Indeed, a distinction must be drawn between the various personal data processing operations forming part of the same chain of operations, in order to take account of the need to assess individually, for each person capable of being classified as a controller of personal data, the level of responsibility which may be attributed to him or her. That is because, in order to be regarded as a joint controller, a natural or legal person must independently meet the definition of 'controller' laid down in Article 4(7) of the GDPR (judgment of 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C683/21, EU:C:2023:949, paragraph 41 and the case-law cited).

111 It follows that if personal data are subsequently transmitted under distribution contracts between the operator of the online marketplace, on which the personal data in question were initially published, and operators of other websites, that first operator is, in principle, the sole controller in respect of the processing constituted by that transmission. In all events, any controller is required, alone or jointly, to comply with all the obligations arising from the GDPR.

112 Having made those clarifications, the fourth question should be understood as referring to a situation in which Russmedia did not transfer the untrue and harmful advertisement at issue in the main proceedings to other websites with advertising content and did not, therefore, authorise those subsequent publications.

113 Moreover, it should also be observed that the fourth question essentially concerns the scope of the security obligation with which a controller of personal data must comply. As it is, Article 32 of the GDPR specifically concerns the security of processing; it gives concrete form to and specifies a particular aspect of the requirements laid down in Article 24 of the GDPR, which, together with Article 5(2) of that regulation, defines in general terms the responsibility of the controller.

114 In those circumstances, it must be found that, by its fourth question, the referring court asks, in essence, whether Article 32 of the GDPR must be interpreted as meaning that the operator of an online marketplace, as controller, within the meaning of Article 4(7) of that regulation, of the personal data contained in advertisements published on its online marketplace, is required to implement security measures such as to prevent advertisements published there and containing sensitive data, in terms of Article 9(1) of that regulation, from being copied and unlawfully published on other websites.

115 Article 32(1) of the GDPR provides that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

116 Article 32(2) of that regulation provides that, in assessing the appropriate level of security, account must be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, and unauthorised disclosure of, or access to, personal data.

117 The Court has held that the reference in Article 32(1) and (2) of the GDPR to ‘a level of security appropriate to the risk’ and to an ‘appropriate level of security’ shows that that regulation establishes a risk management system and that it in no way purports to eliminate the risks of personal data breaches (judgment of 14 December 2023, *Natsionalna agentsia za prihodite*, C340/21, EU:C:2023:986, paragraph 29).

118 Thus, it is apparent from the wording of Article 32 of the GDPR, read in conjunction with Article 24 of that regulation, that Article 32 merely requires the controller to adopt technical and organisational measures intended to avoid, in so far as it is at all possible, any personal data breach. The appropriateness of such measures must be assessed in a concrete manner, by assessing whether those measures were implemented by that controller taking into account the various criteria referred to in those articles and the data protection needs specifically inherent in the processing concerned and the risks arising from the latter (see, to that effect, judgment of 14 December 2023, *Natsionalna agentsia za prihodite*, C340/21, EU:C:2023:986, paragraph 30).

119 In that regard, in order to determine the specific risk represented by the processing concerned, account must be taken of the possible sensitivity of the personal data processed. As recalled in paragraphs 51 and 90 above, the enhanced protection, provided for in Article 9(1) of the GDPR for certain categories of data, because of their particular sensitivity, is based on the fact that the processing of such data is liable to constitute a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed in Articles 7 and 8 of the Charter (see, to that effect, judgment of 21 December 2023, *Krankenversicherung Nordrhein*, C667/21, EU:C:2023:1022, paragraph 41 and the case-law cited).

120 That said, once an advertisement containing personal data is online and is thus already generally accessible, the dissemination of those data entails, inter alia, the risk of a loss of control over the personal data concerned which, where it happens, deprives of all practical effect the rights and safeguards provided for by the GDPR for the benefit of the data subject, foremost among which is the right to erasure provided for in Article 17 of that regulation.

121 Thus, where sensitive data are published online, the controller is required, under Article 32 of the GDPR, to take all technical and organisational measures to ensure a level of security apt to effectively prevent the occurrence of a loss of control over those data.

122 To that end, the data controller must consider in particular all technical measures available in the current state of technical knowledge that are apt to block the copying and reproduction of online content.

123 Nevertheless, it should also be stated that Articles 24 and 32 of the GDPR cannot be understood as meaning that the unlawful dissemination of personal data initially published online is sufficient to conclude that the measures adopted by the controller concerned were not appropriate, within the meaning of those provisions, without even allowing that controller to adduce evidence to the contrary (judgment of 14 December 2023, *Natsionalna agentsia za prihodite*, C340/21, EU:C:2023:986, paragraph 31).

124 In the present case, it is apparent from the order for reference that, despite the deletion of the untrue and harmful advertisement at issue in the main proceedings from Russmedia's online marketplace, that advertisement is still accessible online on other websites without the applicant in the main proceedings being able, it appears, to obtain its deletion.

125 However, it appears that that loss of control originated in the unlawful initial publication of the untrue and harmful advertisement at issue in the main proceedings, in breach of the requirements laid down by the GDPR. In any event, Russmedia was required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk under Article 32 of the GDPR and to block as far as possible any copies of that advertisement. It will be for the referring court to ascertain whether that was the case.

126 Having regard to all the foregoing reasons, the answer to the fourth question is that Article 32 of the GDPR must be interpreted as meaning that the operator of an online marketplace, as controller, within the meaning of Article 4(7) of that regulation, of the personal data contained in advertisements published on its online marketplace, is required to implement appropriate technical and organisational security measures in order to prevent advertisements published there and containing sensitive data, in terms of Article 9(1) of that regulation, from being copied and unlawfully published on other websites.

First question, concerning the interpretation of Directive 2000/31

127 As has been noted in paragraphs 45 and 46 above, the referring court also seeks to ascertain whether the operator of an online marketplace, as controller, within the meaning of Article 4(7) of the GDPR, of personal data contained in advertisements published on its online marketplace, may rely, in respect of an infringement of the obligations arising from Article 5(2) and Articles 24 to 26 and 32 of that regulation – such obligations having been determined in paragraphs 106 and 126 of the present judgment – on Articles 12 to 15 of Directive 2000/31 relating to the liability of intermediary service providers.

128 The question therefore arises as to the relationship between those two instruments of EU law. In particular, it is necessary to determine whether Articles 12 to 15 of Directive 2000/31 are liable to interfere with the liability regime laid down by the GDPR.

129 In that regard, it should be noted, first, that Article 1(5)(b) of Directive 2000/31 states that that directive is not to apply to questions relating to information society services covered by Directives 95/46 and 97/66.

130 That provision has been interpreted by the Court as meaning that questions related to the protection of the confidentiality of communications and personal data must be assessed on the basis of the GDPR and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), which replaced, respectively, Directive 95/46 and Directive 97/66; it should also be noted that the protection that Directive 2000/31 is intended to ensure cannot, in any event, undermine the requirements under the GDPR and Directive 2002/58 (judgment of 6 October 2020, *La Quadrature du Net and Others*, C511/18, C512/18 and C520/18, EU:C:2020:791, paragraph 200 and the case-law cited).

131 It follows, in particular, that the possible benefit of the exemption provided for in Article 14(1) of Directive 2000/31, on which the operator of an online marketplace might be able to rely as regards the information hosted on its website, cannot interfere with the GDPR regime which applies to such an operator in the same way as to any other operator falling within the scope of that regulation.

132 The same is true of Article 15 of Directive 2000/31, under which Member States may not impose a general monitoring obligation on providers, when the latter provide the services covered by, inter alia, Article 14 of that directive. Moreover, the obligation on the operator of an online marketplace to comply with the requirements arising from the GDPR cannot, in any event, be classified as such a general monitoring obligation.

133 Second, Article 2(4) of the GDPR provides that that regulation is to be without prejudice to the application of Directive 2000/31, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that directive.

134 Article 2(4) of the GDPR must be understood as meaning that the fact that an operator has obligations laid down by the GDPR does not automatically preclude that operator from being able to rely on Articles 12 to 15 of Directive 2000/31 for matters other than those relating to the protection of personal data.

135 It thus follows from a combined reading of Article 1(5)(b) of Directive 2000/31 and Article 2(4) of the GDPR that the provisions of that directive, in particular Articles 12 to 15 thereof, cannot interfere with the regime under that regulation.

136 Having regard to all the foregoing reasons, the answer to the first question is that Article 1(5)(b) of Directive 2000/31 and Article 2(4) of the GDPR must be interpreted as meaning that the operator of an online marketplace, as controller, within the meaning of Article 4(7) of the GDPR, of the personal data contained in advertisements published on its online marketplace, cannot rely, in respect of an infringement of the obligations arising from Article 5(2) and Articles 24 to 26 and 32 of that regulation, on Articles 12 to 15 of that directive, relating to the liability of intermediary providers.

Costs

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

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

1. Article 5(2) and Articles 24 to 26 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 operator of an online marketplace, as controller, within the meaning of Article 4(7) of that regulation, of the personal data contained in advertisements published on its online marketplace, is required, before the publication of the advertisements and by means of appropriate technical and organisational measures,

- to identify the advertisements that contain sensitive data in terms of Article 9(1) of that regulation,
- to verify whether the user advertiser preparing to place such an advertisement is the person whose sensitive data appear in that advertisement and, if this is not the case,
- to refuse publication of that advertisement, unless that user advertiser can demonstrate that the data subject has given his or her explicit consent to the data in question being published on that online marketplace, within the meaning of Article 9(2)(a), or that one of the other exceptions provided for in Article 9(2)(b) to (j) is satisfied.

2. Article 32 of Regulation 2016/679

must be interpreted as meaning that the operator of an online marketplace, as controller, within the meaning of Article 4(7) of that regulation, of the personal data contained in advertisements published on its online marketplace, is required to implement appropriate technical and organisational security measures in order to prevent advertisements published there and containing sensitive data, in terms of Article 9(1) of that regulation, from being copied and unlawfully published on other websites.

3. Article 1(5)(b) 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'), and Article 2(4) of Regulation 2016/679,

must be interpreted as meaning that the operator of an online marketplace, as controller, within the meaning of Article 4(7) of Regulation 2016/679, of the personal data contained in advertisements published on its online marketplace, cannot rely, in respect of an infringement of the obligations arising from Article 5(2) and Articles 24 to 26 and 32 of that regulation, on Articles 12 to 15 of that directive, relating to the liability of intermediary providers.

[Signatures]

* Language of the case: Romanian