Provisional text

JUDGMENT OF THE COURT (Grand Chamber)

5 December 2023 (*)

(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 4(2) and (7) – Concepts of 'processing' and 'controller' – Development of a mobile IT application – Article 26 – Joint control – Article 83 – Imposition of administrative fines – Conditions – Requirement that the infringement be intentional or negligent – Responsibility and liability of the controller for the processing of personal data carried out by a processor)

In Case C-683/21,

REQUEST for a preliminary ruling under Article 267 TFEU from the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius, Lithuania), made by decision of 22 October 2021, received at the Court on 12 November 2021, in the proceedings

**Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos**

v

**Valstybinė duomenų apsaugos inspekcija,**

interveners:

**UAB 'IT sprendimai sėkmei',**

**Lietuvos Respublikos sveikatos apsaugos ministerija,**

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Arabadjiev, C. Lycourgos, E. Regan, T. von Danwitz, Z. Csehi, O. Spineanu-Matei, Presidents of Chambers, M. Ilešič, J.-C. Bonichot, L.S. Rossi, A. Kumin, N. Jääskinen (Rapporteur), N. Wahl and M. Gavalec, Judges,

Advocate General: N. Emiliou,

Registrar: C. Strömholm, Administrator,

having regard to the written procedure and further to the hearing on 17 January 2023,

after considering the observations submitted on behalf of:

– the Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, by G. Aleksienė,

– the Valstybinė duomenų apsaugos inspekcija, by R. Andrijauskas,

– the Lithuanian Government, by V. Kazlauskaitė-Švenčionienė, acting as Agent,

– the Netherlands Government, by C.S. Schillemans, acting as Agent,

– the Council of the European Union, by R. Liudvinavičiūtė and K. Pleśniak, acting as Agents,

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

after hearing the Opinion of the Advocate General at the sitting on 4 May 2023,

gives the following

## Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 4(2) and (7), Article 26(1) and Article 83(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; 'the GDPR').

2 The request has been made in proceedings between the Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (National Public Health Centre under the Ministry of Health, Lithuania; 'the NVSC') and the Valstybinė duomenų apsaugos inspekcija (State Data Protection Inspectorate, Lithuania; 'the VDAI') concerning a decision by which the VDAI imposed an administrative fine on the NVSC pursuant to Article 83 of the GDPR for infringement of Articles 5, 13, 24, 32 and 35 of that regulation.

### Legal context

#### *European Union law*

3 Recitals 9, 10, 11, 13, 26, 74, 79, 129 and 148 of the GDPR state:

'(9) … Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the [European] Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. …

(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 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. …

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

…

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with

the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. …

…

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information[,] should be considered to be information on an identifiable natural person. … The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

…

(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.

…

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors … requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

…

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions … The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular[,] each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

…

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of[,] appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the [Charter of Fundamental Rights of the European Union], including effective judicial protection and due process.'

4 According to Article 4 of that regulation:

'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;

…

(5) "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

…

(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;

(8) "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

…'

5 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.'

6 Article 28 of that regulation, entitled 'Processor', provides, in paragraph 10 thereof:

'Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.'

7 Article 58 of the GDPR, entitled 'Powers', provides, in paragraph 2 thereof:

'Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

…

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

…

(f) to impose a temporary or definitive limitation including a ban on processing;

…

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of[,] measures referred to in this paragraph, depending on the circumstances of each individual case;

…'

8 Article 83 of that regulation, entitled 'General conditions for imposing administrative fines', is worded as follows:

'1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine[,] in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature[,] scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to [EUR 10 000 000], or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

…

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to [EUR 20 000 000], or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

…

(d) any obligations pursuant to Member State law adopted under Chapter IX;

…

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to [EUR 20 000 000], or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

…'

9 Article 84 of the GDPR, entitled 'Penalties', provides, in paragraph 1 thereof:

'Member States shall lay down the rules on other penalties applicable to infringements of this Regulation[,] in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.'

***Lithuanian law***

10 Article 29(3) of the Viešųjų pirkimų įstatymas (Law on Public Procurement) refers to certain circumstances in which the contracting authority has the right or the obligation to terminate the procurement or design contest procedures at its own discretion and at any time prior to the award of a public contract (or framework agreement) or to the determination of the successful candidate in a design contest.

11 Article 72(2) of the Law on Public Procurement lays down the stages of the negotiations which are to be conducted by the contracting authority in the context of a negotiated public procurement procedure without prior publication.

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

12 In the context of the pandemic caused by the COVID-19 virus, the Lietuvos Respublikos sveikatos apsaugos ministras (Minister for Health of the Republic of Lithuania), by an initial decision of 24 March 2020, instructed the Director of the NVSC to organise the immediate acquisition of an IT system for the registration and monitoring of the data of persons exposed to that virus, for the purposes of epidemiological follow-up.

13 By email of 27 March 2020, a person claiming to be a representative of the NVSC ('A.S.') informed the company UAB 'IT sprendimai sėkmei' ('the company ITSS') that the NVSC had selected it to create a mobile application for that purpose. A.S. subsequently sent emails to the company ITSS relating to various aspects of the creation of that application, and a copy of those emails was sent to the Director of the NVSC.

14 In the course of the negotiations between the company ITSS and the NVSC, in addition to A.S., other employees of the NVSC also sent emails to that company concerning the drafting of the questions asked in the mobile application at issue.

15 During the creation of that mobile application, a confidentiality policy was drawn up, in which the company ITSS and the NVSC were designated as controllers.

16 The mobile application at issue, which referred to the company ITSS and the NVSC, was available for download in the online shop Google Play Store as from 4 April 2020 and in the online shop Apple App Store as from 6 April 2020. It was operational until 26 May 2020.

17 From 4 April 2020 to 26 May 2020, 3 802 persons used that application and provided data relating to them as requested by the application, such as their ID number, geographical coordinates (latitude and longitude), country, city, municipality, postcode, street name, building number, surname, first name, personal identification number, telephone number and address.

18 By a further decision of 10 April 2020, the Minister for Health of the Republic of Lithuania decided to entrust the Director of the NVSC with the task of organising the acquisition of the mobile application at issue from the company ITSS and, for that purpose, it was envisaged that recourse would be had to Article 72(2) of the Law on Public Procurement. However, no public contract for the official acquisition of that application by the NVSC was awarded to that company.

19 On 15 May 2020, the NVSC asked the company ITSS not to make any reference whatsoever to the NVSC in the mobile application at issue. Furthermore, by letter of 4 June 2020, the NVSC informed that company that, due to a lack of funding for the acquisition of that application, it had, in accordance with Article 29(3) of the Law on Public Procurement, terminated the procedure relating to such acquisition.

20 In the context of an investigation relating to the processing of personal data, initiated on 18 May 2020, the VDAI established that personal data had been collected using the mobile application at issue. Moreover, it was found that the users who had chosen that application as a means of monitoring the isolation made mandatory on account of the COVID-19 pandemic had replied to questions involving the processing of personal data. Those data had allegedly been provided in the replies to the questions asked by the abovementioned application and related, inter alia, to the health status of the data subject and to his or her compliance with the conditions of isolation.

21 By decision of 24 February 2021, the VDAI imposed an administrative fine of EUR 12 000 on the NVSC pursuant to Article 83 of the GDPR, in view of the infringement by the NVSC of Articles 5, 13, 24, 32 and 35 of that regulation. By that decision, an administrative fine of EUR 3 000 was also imposed on the company ITSS as joint controller.

22 The NVSC has challenged that decision before the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius, Lithuania), which is the referring court, maintaining that it is the company ITSS which must be regarded as the sole controller, within the meaning of Article 4(7) of the GDPR. The company ITSS, for its part, contends that it acted in the capacity of processor, within the meaning of Article 4(8) of the GDPR, on the instruction of the NVSC which, according to that company, is the sole controller.

23 The referring court notes that the company ITSS created the mobile application at issue and that the NVSC provided that company with advice regarding the content of the questions asked by that application. It observes that there is, however, no public contract between the NVSC and the company ITSS. In addition, it notes that the NVSC neither consented to nor authorised that application being made available through various online shops.

24 The referring court states that the creation of the mobile application at issue was intended to implement the objective assigned by the NVSC, namely the management of the COVID-19 pandemic through the creation of an IT tool, and that the processing of personal data was envisaged for that purpose. As regards the role of the company ITSS, it notes that it was not envisaged that that company would pursue objectives other than that of receiving remuneration for the IT product created.

25 The referring court also observes that, during the VDAI investigation, it was established that the Lithuanian company Juvare Lithuania, which manages the IT system for monitoring and controlling transmissible diseases that pose a risk of contagion, had to receive copies of the personal data collected by the mobile application at issue. Furthermore, for the purpose of testing that application, fictitious data were used, with the exception of the telephone numbers of that company’s employees.

26 In those circumstances, the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

‘(1) Can the concept of “controller” set out in Article 4(7) of the GDPR be interpreted as meaning that a person who is planning to acquire a data collection tool (mobile application) by way of public procurement, irrespective of the fact that a public procurement contract has not been concluded and that the created product (mobile application), for the acquisition of which a public procurement procedure had been used, has not been transferred, is also to be regarded as a controller?

(2) Can the concept of “controller” set out in Article 4(7) of the GDPR be interpreted as meaning that a contracting authority which has not acquired the right of ownership of the created IT product and has not taken possession of it, but where the final version of the created application provides links or interfaces to that public entity and/or [where] the confidentiality policy, which was not officially approved or recognised by the public entity in question, specified that public entity itself as a controller, is also to be regarded as a controller?

(3) Can the concept of “controller” set out in Article 4(7) of the GDPR be interpreted as meaning that a person who has not performed any actual data processing operations as defined in Article 4(2) of the GDPR and/or has not provided clear permission/consent to the performance of such operations is also to be regarded as a controller? Is the fact that the IT product used for the processing of personal data was created in accordance with the assignment formulated by the contracting authority significant for the interpretation of the concept of “controller”?

(4) If the determination of actual data processing operations is relevant for the interpretation of the concept of “controller”, is the definition of “processing” of personal data under Article 4(2) of the GDPR to be interpreted as also covering situations in which copies of personal data have been used for the testing of IT systems in the process for the acquisition of a mobile application?

(5) Can joint control of data in accordance with Article 4(7) and Article 26(1) of the GDPR be interpreted exclusively as involving deliberately coordinated actions in respect of the determination of the purpose and means of data processing, or can that concept also be interpreted as meaning that joint control also covers situations in which there is no clear “arrangement” in respect of the purpose and means of data processing and/or actions are not coordinated between the entities? Are the circumstance relating to the stage in the creation of the means of personal data processing (IT application) at which personal data were processed and the purpose of the creation of the application legally significant for the interpretation of the concept of joint control of data? Can an “arrangement” between joint controllers be understood exclusively as a clear and defined establishment of terms governing the joint control of data?

(6) Is the provision in Article 83(1) of the GDPR to the effect that “administrative fines … shall … be effective, proportionate and dissuasive” to be interpreted as also covering cases of imposition of liability on the “controller” when, in the process of the creation of an IT product, the developer also performs personal data processing actions, and do the improper personal data processing actions carried out by the processor always give rise automatically to legal liability on the part of the controller? Is that provision to be interpreted as also covering cases of no-fault liability on the part of the controller?’

## Consideration of the questions referred

### *The first, second and third questions*

27 By its first, second and third questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 4(7) of the GDPR is to be interpreted as meaning that an entity which has

entrusted an undertaking with the development of a mobile IT application may be regarded as a controller, within the meaning of that provision, although that entity has not itself performed any personal data processing operations, has not expressly agreed to the performance of specific operations for such processing or to that mobile application being made available to the public, and has not acquired the abovementioned mobile application.

28 Article 4(7) of the GDPR defines the concept of 'controller' broadly as the natural or legal person, public authority, agency or any other body which, alone or jointly with others, 'determines the purposes and means of the processing' of personal data.

29 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 particular, in ensuring a high level of protection of the right of every person to the protection of personal data concerning him or her (see, to that effect, judgments of 29 July 2019, *Fashion ID*, C-40/17, EU:C:2019:629, paragraph 66, and of 28 April 2022, *Meta Platforms Ireland*, C-319/20, EU:C:2022:322, paragraph 73 and the case-law cited).

30 The Court has already held that any natural or legal person who exerts influence over the processing of such data, for his, her or its own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller in respect of such processing. In that regard, it is not necessary that the purposes and means of processing be determined by the use of written guidelines or instructions from the controller (see, to that effect, judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraphs 67 and 68); nor is it necessary for that controller to have been formally designated as such.

31 Therefore, in order to establish whether an entity such as the NVSC may be regarded as a controller within the meaning of Article 4(7) of the GDPR, it is necessary to examine whether that entity actually exerted influence, for its own purposes, over the determination of the purposes and means of the processing in question.

32 In the present case, subject to matters to be determined by the referring court, it is apparent from the file before the Court of Justice that the creation of the mobile application at issue was commissioned by the NVSC and was intended to implement the objective assigned by that entity, namely the management of the COVID-19 pandemic by means of an IT tool for registering and monitoring the data of persons exposed to the COVID-19 virus. For that purpose, the NVSC had envisaged that the personal data of users of the mobile application at issue would be processed. Furthermore, it is apparent from the order for reference that the parameters of that application, such as the questions asked and their wording, were adapted to the needs of the NVSC and that that entity played an active role in their determination.

33 In those circumstances, it must, in principle, be considered that the NVSC actually participated in the determination of the purposes and means of the processing.

34 By contrast, the mere fact that the NVSC was referred to as a controller in the confidentiality policy of the mobile application at issue and that links to that entity were included in that application could be regarded as relevant only if it were established that the NVSC consented, either expressly or implicitly, to such reference or links.

35 Moreover, the circumstances stated by the referring court in the considerations provided in support of its first three questions referred for a preliminary ruling – namely that the NVSC did not itself process any personal data, that there was no contract between the NVSC and the company ITSS, that the NVSC did not acquire the mobile application at issue and that the dissemination of that application through online shops was not authorised by the NVSC – do not preclude the NVSC from being classified as a 'controller' within the meaning of Article 4(7) of the GDPR.

36 Indeed, it is apparent from that provision, read in the light of recital 74 of the GDPR, that an entity, provided that it satisfies the condition laid down by Article 4(7) of that regulation, is responsible and liable not only for any processing of personal data which it itself carries out, but also for any such processing carried out on its behalf.

37 In that respect, however, it must be stated that the NVSC cannot be regarded as the controller of personal data processing resulting from the mobile application at issue being made available to the public if, prior to that application being made available, the NVSC expressly objected to such making available, which is a matter for the referring court to ascertain. In such a situation, it cannot be considered that the processing in question was carried out on behalf of the NVSC.

38 In the light of the foregoing, the answer to the first, second and third questions is that Article 4(7) of the GDPR must be interpreted as meaning that an entity which has entrusted an undertaking with the development of a mobile IT application and which has, in that context, participated in the determination of the purposes and means of the processing of personal data carried out through that application may be regarded as a controller, within the meaning of that provision, even if that entity has not itself performed any processing operations in respect of such data, has not expressly agreed to the performance of specific operations for such processing or to that mobile application being made available to the public, and has not acquired the abovementioned mobile application, unless, prior to that application being made available to the public, that entity expressly objected to such making available and to the resulting processing of personal data.

***The fifth question***

39 By its fifth question, which it is appropriate to examine in the second place, the referring court asks, in essence, whether Article 4(7) and Article 26(1) of the GDPR are to be interpreted as meaning that the classification of two entities as joint controllers requires that there be an arrangement between those entities regarding the determination of the purposes and means of the processing of personal data in question or that there be an arrangement laying down the terms of the joint control.

40 Under Article 26(1) of the GDPR, 'joint controllers' exist where two or more controllers jointly determine the purposes and means of processing.

41 As the Court has held, in order to be regarded as a joint controller, a natural or legal person therefore must independently meet the definition of 'controller' laid down in Article 4(7) of the GDPR (see, to that effect, judgment of 29 July 2019, *Fashion ID*, C-40/17, EU:C:2019:629, paragraph 74).

42 However, 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 of personal data 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 (judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, paragraph 43). Furthermore, the joint responsibility of several actors for the same processing does not require each of them to have access to the personal data concerned (judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 69 and the case-law cited).

43 As the Advocate General observed in point 38 of his Opinion, participation in the determination of the purposes and means of processing can take different forms, since such participation can result from a common decision taken by two or more entities or from converging decisions of those entities. However, where the latter is the case, those decisions must complement each other in such a manner that they each have a tangible impact on the determination of the purposes and means of the processing.

44 By contrast, it cannot be required that there be a formal arrangement between those controllers as regards the purposes and means of processing.

45 It is true that, by virtue of Article 26(1) of the GDPR, read in the light of recital 79 of that regulation, joint controllers must, by means of an arrangement between them, determine in a transparent manner their respective responsibilities for compliance with the obligations under that regulation. However, the existence of such an arrangement constitutes not a precondition for two or more entities to be classified as joint controllers, but rather an obligation which Article 26(1) of the GDPR imposes on joint controllers, once they have been classified as such, for the purposes of compliance with their obligations under that regulation. Thus, such classification arises solely from the fact that several entities have participated in the determination of the purposes and means of processing.

46 In the light of the foregoing, the answer to the fifth question is that Article 4(7) and Article 26(1) of the GDPR must be interpreted as meaning that the classification of two entities as joint controllers does not require that there be an arrangement between those entities regarding the determination of the purposes and means of the processing of personal data in question; nor does it require that there be an arrangement laying down the terms of the joint control.

***The fourth question***

47 By its fourth question, the referring court asks, in essence, whether Article 4(2) of the GDPR is to be interpreted as meaning that the use of personal data for the purposes of the IT testing of a mobile application constitutes 'processing' within the meaning of that provision.

48 In the present case, as is apparent from paragraph 25 of the present judgment, the Lithuanian company which manages the IT system for monitoring and controlling transmissible diseases that pose a risk of contagion had to receive copies of the personal data collected by the mobile application at issue. For IT testing purposes, fictitious data were used, with the exception of the telephone numbers of that company's employees.

49 In that regard, in the first place, Article 4(2) of the GDPR defines the concept of 'processing' as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means'. In a non-exhaustive list, beginning with the wording 'such as', that provision refers to the collection, making available and use of personal data as examples of processing.

50 It is therefore apparent from the wording of that provision, and in particular from the expression 'any operation', that the EU legislature intended to confer a broad scope upon the concept of 'processing' (see, to that effect, judgment of 24 February 2022, *Valsts ieņēmumu dienests (Processing of personal data for tax purposes)*, C-175/20, EU:C:2022:124, paragraph 35), and that the reasons for which an operation or set of operations is performed cannot be taken into account for the purpose of determining whether that operation or set of operations constitutes 'processing' within the meaning of Article 4(2) of the GDPR.

51 Consequently, the question whether personal data are used for the purposes of IT testing or for another purpose has no bearing on whether the operation in question is classified as 'processing' within the meaning of that provision.

52 In the second place, however, it should be pointed out that only processing which relates to 'personal data' constitutes 'processing' within the meaning of Article 4(2) of the GDPR.

53 In that regard, Article 4(1) of that regulation states that 'personal data' must be understood as meaning 'any information relating to an identified or identifiable natural person', that is to say, relating to a 'natural person … 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'.

54 The fact, alluded to by the referring court in its fourth question, that 'copies of personal data' are involved does not, in itself, preclude such copies from being classified as personal data within the meaning of

Article 4(1) of the GDPR, provided that those copies actually contain information relating to an identified or identifiable natural person.

55 However, it must be stated that fictitious data, where they relate not to an identified or identifiable natural person but rather to a person who does not actually exist, do not constitute personal data within the meaning of Article 4(1) of the GDPR.

56 The same applies with regard to data used for the purposes of IT testing which are anonymous or have been rendered anonymous.

57 It follows from recital 26 of the GDPR and from the very definition of the concept of 'personal data' provided in Article 4(1) of that regulation that neither 'anonymous information, namely information which does not relate to an identified or identifiable natural person', nor 'personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable', is covered by that concept.

58 By contrast, it follows from Article 4(5) of the GDPR, read in conjunction with recital 26 of that regulation, that personal data which have undergone only pseudonymisation and which could be attributed to a natural person by the use of additional information must be considered to be information on an identifiable natural person, to which the principles of data protection apply.

59 In the light of the foregoing, the answer to the fourth question is that Article 4(2) of the GDPR must be interpreted as meaning that the use of personal data for the purposes of the IT testing of a mobile application constitutes 'processing', within the meaning of that provision, unless such data have been rendered anonymous in such a manner that the subject of those data is not or is no longer identifiable, or unless it involves fictitious data which do not relate to an existing natural person.

***The sixth question***

60 By its sixth question, the referring court asks, in essence, whether Article 83 of the GDPR is to be interpreted as meaning that (i) an administrative fine may be imposed pursuant to that provision only where it is established that the controller has intentionally or negligently committed an infringement referred to in paragraphs 4 to 6 of that article, and (ii) such a fine may be imposed on a controller in respect of processing operations performed by a processor on behalf of that controller.

61 As regards, in the first place, the question whether an administrative fine may be imposed pursuant to Article 83 of the GDPR only in so far as it is established that the controller or processor has intentionally or negligently committed an infringement referred to in paragraphs 4 to 6 of that article, it is apparent from paragraph 1 thereof that such fines must be effective, proportionate and dissuasive. On the other hand, Article 83 of the GDPR does not expressly state that such an infringement may not be penalised by means of such a fine unless it was committed intentionally or, at the very least, negligently.

62 The Lithuanian Government and the Council of the European Union infer from this that the EU legislature intended to leave the Member States a certain margin of discretion in the implementation of Article 83 of the GDPR, allowing them to provide for the imposition of administrative fines pursuant to that provision, if necessary, without it being established that the infringement of the GDPR penalised by means of such a fine was committed intentionally or negligently.

63 Such an interpretation of Article 83 of the GDPR cannot be adopted.

64 In that regard, it should be recalled that, pursuant to Article 288 TFEU, the provisions of regulations generally have immediate effect in the national legal systems without it being necessary for the national authorities to adopt measures of application. Nonetheless, some provisions of regulations may necessitate, for their implementation, the adoption of measures of application by the Member States (see, to that effect, judgment of 28 April 2022, *Meta Platforms Ireland*, C-319/20, EU:C:2022:322, paragraph 58 and the case-law cited).

65 That is particularly the case for the GDPR, certain provisions of which make it possible for Member States to lay down additional, stricter or derogating national rules, which leave them a margin of discretion as to the manner in which those provisions may be implemented (judgment of 28 April 2022, *Meta Platforms Ireland*, C-319/20, EU:C:2022:322, paragraph 57).

66 Similarly, in the absence of specific procedural rules in the GDPR, it is for the legal system of each Member State, subject to compliance with the principles of equivalence and effectiveness, to prescribe the detailed rules governing actions for safeguarding rights which individuals derive from the provisions of that regulation (see, to that effect, judgment of 4 May 2023, *Österreichische Post (Non-material damage in connection with the processing of personal data)*, C-300/21, EU:C:2023:370, paragraphs 53 and 54 and the case-law cited).

67 However, there is nothing in the wording of Article 83(1) to (6) of the GDPR to suggest that the EU legislature intended to leave the Member States a margin of discretion as regards the substantive conditions which must be satisfied by a supervisory authority where that authority decides to impose an administrative fine on a controller in respect of an infringement referred to in Article 83(4) to (6) of that regulation.

68 It is true that Article 83(7) of the GDPR provides that each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. Moreover, it is clear from Article 83(8) of that regulation, read in the light of recital 129 thereof, that the exercise by the supervisory authority of its powers under that article is to be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

69 However, the fact that the GDPR thereby grants Member States the possibility to lay down exceptions in relation to public authorities and bodies established in those Member States and requirements concerning the procedure to be followed by supervisory authorities in order to impose an administrative fine in no way means that those States are also authorised to lay down, in addition to such exceptions and procedural requirements, substantive conditions which must be satisfied in order to render the controller liable and impose an administrative fine on it pursuant to Article 83 of that regulation. In addition, the fact that the EU legislature took care to make express provision for that possibility but not the possibility to lay down such substantive conditions confirms that it did not leave the Member States a margin of discretion in that regard.

70 That conclusion is also borne out by a combined reading of Articles 83 and 84 of the GDPR. Article 84(1) of that regulation recognises that Member States retain the power to lay down the rules on ‘other penalties applicable’ to infringements of that regulation, ‘in particular for infringements which are not subject to administrative fines pursuant to Article 83’. It thus follows from such a combined reading of those provisions that the determination of substantive conditions for imposing such administrative fines falls outside the scope of that power. Consequently, such conditions are governed solely by EU law.

71 As regards the abovementioned conditions, it should be noted that Article 83(2) of the GDPR lists the factors in the light of which the supervisory authority may impose an administrative fine on the controller. Those factors include, in point (b) of that provision, ‘the intentional or negligent character of the infringement’. By contrast, none of the factors listed in the abovementioned provision refers to any possibility of rendering the controller liable in the absence of wrongful conduct on its part.

72 Furthermore, paragraph 2 of Article 83 of the GDPR must be read in conjunction with paragraph 3 of that article, the purpose of which is to provide for consequences in cases involving multiple infringements of that regulation and according to which ‘if a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement’.

73 It thus follows from the wording of Article 83(2) of the GDPR that only infringements of the provisions of that regulation which are committed wrongfully by the controller, that is to say, those committed intentionally or negligently, may result in an administrative fine being imposed on that controller pursuant to that article.

74 The general scheme and purpose of the GDPR support such a reading.

75 First, the EU legislature provided for a system of sanctions allowing supervisory authorities to impose the most appropriate penalties depending on the circumstances of each individual case.

76 Article 58 of the GDPR, which determines the powers of supervisory authorities, provides, in paragraph 2(i) thereof, that those authorities may impose administrative fines pursuant to Article 83 of that regulation, 'in addition to, or instead of', the other corrective measures listed in Article 58(2) of the GDPR, such as warnings, reprimands or orders. Similarly, recital 148 of that regulation states, inter alia, that, in a case of a minor infringement or if the administrative fine likely to be imposed would constitute a disproportionate burden to a natural person, supervisory authorities may refrain from imposing an administrative fine and instead issue a reprimand.

77 Second, it is apparent, in particular, from recital 10 of the GDPR that the objectives of the provisions of that regulation are, inter alia, to ensure a consistent and high level of protection of natural persons with regard to the processing of personal data within the Union and, to that end, to ensure 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 such data throughout the Union. In addition, recitals 11 and 129 of the GDPR emphasise the need to ensure, for the purpose of guaranteeing the consistent application of that regulation, that the supervisory authorities have equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and that they can impose equivalent sanctions in the event of infringements of that regulation.

78 The existence of a system of sanctions, which allows an administrative fine to be imposed pursuant to Article 83 of the GDPR where justified by the specific circumstances of each individual case, provides an incentive for controllers and processors to comply with that regulation. Through their dissuasive effect, administrative fines contribute to strengthening the protection of natural persons with regard to the processing of personal data and are therefore a key element in ensuring respect for the rights of those persons, in accordance with the purpose of that regulation, which is to ensure a high level of protection for such persons with regard to the processing of personal data.

79 However, the EU legislature did not deem it necessary, for the purpose of ensuring such a high level of protection, to provide for the imposition of administrative fines in the absence of fault. Having regard to the fact that the GDPR aims to achieve a level of protection which is both equivalent and homogenous, and that, to that end, it must be applied consistently throughout the Union, it would be contrary to that purpose to allow the Member States to lay down such a regime for imposing a fine pursuant to Article 83 of that regulation. Moreover, such freedom of choice would be liable to distort competition between economic operators within the Union, which would run counter to the objectives set out by the EU legislature in, inter alia, recitals 9 and 13 of that regulation.

80 Therefore, it must be found that Article 83 of the GDPR does not allow an administrative fine to be imposed in respect of an infringement referred to in paragraphs 4 to 6 of that article without it being established that such an infringement was committed intentionally or negligently by the controller, and that, accordingly, a wrongful infringement constitutes a condition for imposing such a fine.

81 In that regard, it must also be stated, in relation to the question whether an infringement has been committed intentionally or negligently and is therefore liable to be penalised by way of an administrative fine under Article 83 of the GDPR, that a controller may be penalised for conduct falling within the scope of the GDPR where that controller could not have been unaware of the infringing nature of its conduct, whether or not it was aware that it was infringing the provisions of the GDPR (see, by analogy, judgments

of 18 June 2013, *Schenker & Co. and Others*, C-681/11, EU:C:2013:404, paragraph 37 and the case-law cited; of 25 March 2021, *Lundbeck* v *Commission*, C-591/16 P, EU:C:2021:243, paragraph 156; and of 25 March 2021, *Arrow Group and Arrow Generics* v *Commission*, C-601/16 P, EU:C:2021:244, paragraph 97).

82 Where the controller is a legal person, it must also be stated that, for Article 83 of the GDPR to apply, it is not necessary for there to have been action by, or even knowledge on the part of, the management body of that legal person (see, by analogy, judgments of 7 June 1983, *Musique diffusion française and Others* v *Commission*, 100/80 to 103/80, EU:C:1983:158, paragraph 97, and of 16 February 2017, *Tudapetrol Mineralölerzeugnisse Nils Hansen* v *Commission*, C-94/15 P, EU:C:2017:124, paragraph 28 and the case-law cited).

83 As regards, in the second place, the question whether an administrative fine may be imposed pursuant to Article 83 of the GDPR on a controller in respect of processing operations performed by a processor, it should be recalled that, according to the definition contained in Article 4(8) of that regulation, a processor is 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

84 Since, as has been stated in paragraph 36 of the present judgment, a controller is responsible and liable not only for any processing of personal data which it itself carries out, but also for any such processing carried out on its behalf, that controller may have an administrative fine imposed on it pursuant to Article 83 of the GDPR in a situation where personal data are unlawfully processed and where it was not such a controller, but rather a processor used by that controller, which carried out the abovementioned processing on behalf of that controller.

85 However, the responsibility and liability of the controller for the conduct of a processor cannot extend to situations where the processor has processed personal data for its own purposes or where that processor has processed such data in a manner incompatible with the framework of, or detailed arrangements for, the processing as determined by the controller, or in such a manner that it cannot reasonably be considered that that controller consented to such processing. In accordance with Article 28(10) of the GDPR, the processor must, in such a situation, be considered to be a controller in respect of such processing.

86 In the light of the foregoing considerations, the answer to the sixth question is that Article 83 of the GDPR must be interpreted as meaning that (i) an administrative fine may be imposed pursuant to that provision only where it is established that the controller has intentionally or negligently committed an infringement referred to in paragraphs 4 to 6 of that article, and (ii) such a fine may be imposed on a controller in respect of personal data processing operations performed by a processor on behalf of that controller, unless, in the context of those operations, that processor has carried out processing for its own purposes or has processed such data in a manner incompatible with the framework of, or detailed arrangements for, the processing as determined by the controller, or in such a manner that it cannot reasonably be considered that that controller consented to such processing.

## Costs

87 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 4(7) 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 an entity which has entrusted an undertaking with the development of a mobile IT application and which has, in that context, participated in the determination of the purposes and means of the processing of personal data carried out through that application may be regarded as a controller, within the meaning of that provision, even if that entity has not itself performed any processing operations in respect of such data, has not expressly agreed to the performance of specific operations for such processing or to that mobile application being made available to the public, and has not acquired the abovementioned mobile application, unless, prior to that application being made available to the public, that entity expressly objected to such making available and to the resulting processing of personal data.**

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

**must be interpreted as meaning that the classification of two entities as joint controllers does not require that there be an arrangement between those entities regarding the determination of the purposes and means of the processing of personal data in question; nor does it require that there be an arrangement laying down the terms of the joint control.**

3. **Article 4(2) of Regulation 2016/679**

**must be interpreted as meaning that the use of personal data for the purposes of the IT testing of a mobile application constitutes 'processing', within the meaning of that provision, unless such data have been rendered anonymous in such a manner that the subject of those data is not or is no longer identifiable, or unless it involves fictitious data which do not relate to an existing natural person.**

4. **Article 83 of Regulation 2016/679**

**must be interpreted as meaning that (i) an administrative fine may be imposed pursuant to that provision only where it is established that the controller has intentionally or negligently committed an infringement referred to in paragraphs 4 to 6 of that article, and (ii) such a fine may be imposed on a controller in respect of personal data processing operations performed by a processor on behalf of that controller, unless, in the context of those operations, that processor has carried out processing for its own purposes or has processed such data in a manner incompatible with the framework of, or detailed arrangements for, the processing as determined by the controller, or in such a manner that it cannot reasonably be considered that that controller consented to such processing.**

[Signatures]

---

* Language of the case: Lithuanian.