Case C-683/21

Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice

Date of receipt:

12 November 2021

Referring court:

Vilniaus apygardos administracinis teismas (Lithuania)

Date of the decision to refer:

22 October 2021

Applicant:

Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos

Defendant:

Valstybinė duomenų apsaugos inspekcija

Subject matter of the action in the main proceedings

In the main proceedings, a dispute has arisen as to the content of the concept of 'controller', recognition of a person as a controller and/or as a joint controller (hereinafter 'joint controller') and determination of the entity liable in respect of infringements of Regulation (EU) 2016/679.

Subject matter and legal background of the request for a preliminary ruling

Interpretation of provisions of Regulation (EU) 2016/679 (the General Data Protection Regulation, hereinafter 'the GDPR'); second paragraph of Article 267 TFEU.

Questions referred

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 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?

Provisions of EU law and case-law of the Court of Justice cited

Recitals 4, 10 and 74, Article 4(2) and (7), Article 26(1) and (2) 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 (the General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C-210/16, EU:C:2018:388, paragraphs 26 and 27).

Judgment of 10 July 2018, *Jehovan todistajat* (C-25/17, EU:C:2018:551, paragraph 66).

Provisions of national law cited

Viešųjų pirkimų įstatymas (Law on Public Procurement) (‘the LPP’):

Article 29(3):

‘At any time prior to the award of a contract of sale (conclusion of a framework agreement) or determination of the successful candidate in a design contest, the contracting authority shall have the right to terminate the procurement or design contest procedures at its own discretion in the event of the occurrence of unforeseeable circumstances and must do so in the event of an infringement of the principles set out in Article 17(1) of this Law and if the situation in question cannot be remedied’.

Article 72(2):

‘The contracting authority shall carry out a negotiated procedure without publication of a contract notice in the following stages:

(1) written invitation to the selected economic operators to submit tenders;

(2) verification as to whether there are any grounds for the exclusion of economic operators as laid down in the procurement documents, and verification as to whether the economic operators fulfil the qualification requirements imposed and, where applicable, meet the required quality assurance standards and/or environmental management standards;

(3) conduct of negotiations with the tenderers in accordance with the procedure established in Article 66 of this Law and the request for them to submit final

tenders. The contracting authority shall not be required to request the submission of a final tender in the case of one economic operator participating in the negotiated procedure without publication of a prior notice;

(4) evaluation of the final tenders and determination of the successful candidate'.

Civil Code

Article 2.133(9):

'If an agent has exceeded the scope of his or her rights but in such a manner that a third party had serious reasons for taking the view that he or she has entered into a transaction with a duly authorised agent, the transaction shall be binding upon the principal, except for cases in which the other party to the transaction knew, or ought to have known, that the agent was exceeding the scope of his or her rights'.

Article 2.136(1):

'A transaction which is being concluded on behalf of another person by a person who does not have the right to conclude the transaction or by a person exceeding the rights granted to that person shall create, change or abolish rights and obligations for the principal only in cases where the principal subsequently approves the whole of that transaction or the part thereof which exceeds those rights'.

Brief description of the facts and procedure in the main proceedings

1 In order to manage effectively the situation resulting from the spread of COVID-19, the Minister for Health of the Republic of Lithuania, by Decision No V-519 of 24 March 2020, instructed the Director of the Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (the National Public Health Centre under the Ministry of Health) (hereinafter 'the NVSC') to organise the acquisition of an information platform (system) (hereinafter 'the KARANTINAS mobile application' or 'the application') intended for the registration and monitoring of data relating to persons who have been in contact with carriers of the COVID-19 infection.

2 On 27 March 2020, A. S., a person claiming to be an agent representing the NVSC, informed the company 'IT sprendimai sėkmei' UAB (hereinafter also 'the company') by email that the NVSC had selected that company to be the developer of the KARANTINAS mobile application. A. S. had no employment contract or other contract with the NVSC. A. S., claiming to be an agent representing the NVSC, subsequently sent numerous emails to that company (with copies to the Director of the NVSC) regarding various aspects of the development of the mobile application. Emails related to the application were also sent to the company by a number of NVSC employees.

3 A confidentiality policy was drawn up at the application development stage, specifying 'IT sprendimai sėkmei' UAB and the NVSC as controllers. The application was made available for downloading from the online shop Google Play Store as from 4 April 2020 and from the sales platform Apple App Store as from 6 April 2020. The application provided links to 'IT sprendimai sėkmei' UAB and to the NVSC. On 15 May 2020, the NVSC requested the company not to use any details of the NVSC or other links with the NVSC in the application.

4 The KARANTINAS mobile application collected various items of information relating to its users: identity number, latitude and longitude coordinates, country, city, municipality, residential address, forename, surname, personal identification number, telephone number, whether the person must self-isolate, whether he/she has registered, and so forth. Data were collected not only in Lithuania but also abroad.

5 By Decision No V-821 of 10 April 2020, the Minister for Health instructed the Director of the NVSC to organise urgently the acquisition of the KARANTINAS mobile application. It was planned to acquire the application from 'IT sprendimai sėkmei' UAB by negotiated procedure without publication of a contract notice. The procurement procedures were initiated but, having failed to receive the necessary funding, the NVSC terminated them in accordance with Article 29(3) of the LPP. No public contract for purchase and sale was concluded.

6 The Valstybinė duomenų apsaugos inspekcija (State Data Protection Inspectorate) (hereinafter 'the Inspectorate') carried out an investigation and, by Decision No 3R-180 of 24 February 2021, imposed administrative fines on the NVSC and on 'IT sprendimai sėkmei' UAB, in their capacity as joint controllers, for breaches of Articles 5, 13, 24, 32 and 35 of Regulation (EU) 2016/679.

7 The Inspectorate found that personal data had been collected using the KARANTINAS mobile application. According to 'IT sprendimai sėkmei' UAB, personal data were provided via the application by 3 802 users.

8 Each day, users who had chosen the application as the method for monitoring their forced isolation were requested to answer the following questions: Did you measure your temperature today? If so, what is your temperature? If not, please measure it now and enter details. Do you experience at least one of the following symptoms: coughing or difficulty in breathing? Do you have any other symptoms? If so, please specify (enter details). Are you complying with the self-isolation requirements (a link to the isolation rules can be added)? Do you require social assistance? If so, please specify which kind (enter details). Do you require psychological assistance?

9 The Inspectorate also found that copies of the data collected in the KARANTINAS mobile application had to be received by another company, 'Juvare Lithuania' UAB, which is the processor of the Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinė sistema

(Information System for the monitoring and control of communicable diseases which may spread and pose a threat) (hereinafter 'ULSKIS'). The NVSC was subsequently appointed as the controller of ULSKIS.

Essential arguments of the parties to the main proceedings

10 The NVSC basically relies on the arguments that the public procurement procedure was not completed through the conclusion of a contract of purchase and sale; therefore, ownership of the mobile application was not transferred and the NVSC cannot be regarded as a controller of the personal data collected through use of the application.

11 'IT sprendimai sėkmei' UAB points out that, as a processor, it technically supervised the operation of the application but that the personal data were processed in the application exclusively for the purposes determined by the NVSC and in accordance with its instructions.

12 The Inspectorate points out that the concept of 'controller' is a functional concept, the purpose of which is to attribute, on the basis of an analysis of the specific facts, liability to the entity which exercises actual influence; being a controller is a consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes. The Inspectorate stresses that a controller determines, rather than legitimises, the purpose and methods of data processing, that joint controllers should complement each other by their decisions and that basically each other's decisions should have a tangible influence on the determination of the purpose and means of data processing. In addition, the objectives sought by the joint controllers of data should be closely linked and should complement each other.

Concise justification of the request for a preliminary ruling

13 The dispute between the parties centres essentially on the question whether the concept of 'controller' set out in the GDPR is to be interpreted broadly, that is to say, as meaning that a person who has merely established the objectives and means of data processing is to be regarded as a controller of personal data, or whether this concept must be interpreted more narrowly, taking into account the procedure governing the organisation of the public procurement and its outcome. It is established in the present case that 'IT sprendimai sėkmei' UAB developed the KARANTINAS mobile application and that the NVSC, as the contracting authority, assisted by providing advice on the content of the information to be collected; however, the NVSC did not conclude a public contract of purchase and sale, no certificate of transfer and acceptance regarding the created IT product was signed, the rights of ownership of the KARANTINAS mobile application were not transferred, and there is nothing to indicate that official consent (permission) was given to make the mobile application available in various online stores (*Google Play Store*, *App Store*).

14 The legal regulation of public procurement and the fact that a public administrative entity which, in accordance with EU law, is subject to one of the essential principles of public administration, namely the principle of legality, has been made accountable for breaches of the GDPR are also relevant in the present case. The body of rules governing public procurement is subject to both national and EU law; however, EU law does not regulate all aspects of public procurement and some of these are left to national law. According to national law, a public procurement procedure is to be regarded as completed when a public contract of purchase and sale has been concluded.

15 The LPP establishes clearly defined preconditions for the negotiated procedure without publication of a contract notice, the point in time at which such a procedure begins and the moment at which the negotiations are to be regarded as having taken place.

16 It is apparent from the correspondence between ‘IT sprendimai sėkmei’ UAB and the NVSC that achievement of the objective set for the NVSC (the creation of an IT solution to manage the pandemic) was sought through development of the application and that the processing of personal data was planned with that objective in mind. There is also information in the case that the technical decisions (questions to be asked, their wording, and suchlike) were changed according to the needs of the contracting authority (the customer). It has not been established that the company sought any objectives other than to receive remuneration for the created product.

17 Since the NVSC has been recognised as a joint controller of personal data, questions also arise as to the interpretation of Article 4(7) and Article 26(1) of the GDPR in relation to the joint control of data.

18 Finally, the referring court also asks how Article 83(1) of the GDPR, which provides that ‘administrative fines … shall … be effective, proportionate and dissuasive’, is to be construed when a decision is taken on the liability of several entities.