Case C-340/21

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

Date lodged:

2 June 2021

Referring court:

Varhoven administrativen sad (Bulgaria)

Date of the decision to refer:

14 May 2021

Appellant in cassation:

VB

Respondent in cassation:

Natsionalna agentsia za prihodite (Bulgaria)

Subject matter of the main proceedings

Appeal against a judgment dismissing as unfounded an action for compensation for non-material damage suffered as a result of the unlawful failure of the respondent in cassation, in its capacity as a data controller, to comply to a sufficient extent with its obligations under the Zakon za zashtita na lichnite danni (Law on the protection of personal data; 'Law on data protection') and Regulation 2016/679.

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

Request for a preliminary ruling under Article 267 TFEU on the interpretation of recitals 74, 85 and 146, point 12 of Article 4 and Articles 5(2), 24, 32 and 82 of Regulation 2016/679.

Questions referred for a preliminary ruling

1. Are Articles 24 and 32 of Regulation (EU) 2016/679 to be interpreted as meaning that unauthorised disclosure of, or access to, personal data within the meaning of point 12 of Article 4 of Regulation (EU) 2016/679 by persons who are not employees of the controller's administration and are not subject to its control is sufficient for the presumption that the technical and organisational measures implemented are not appropriate?

2. If the first question is answered in the negative, what should be the subject matter and scope of the judicial review of legality in the examination as to whether the technical and organisational measures implemented by the controller are appropriate pursuant to Article 32 of Regulation (EU) 2016/679?

3. If the first question is answered in the negative, is the principle of accountability under Article 5(2) and Article 24 of Regulation (EU) 2016/679, read in conjunction with recital 74 thereof, to be interpreted as meaning that, in legal proceedings under Article 82(1) of Regulation (EU) 2016/679, the controller bears the burden of proving that the technical and organisational measures implemented are appropriate pursuant to Article 32 of that regulation? Can the obtaining of an expert's report be regarded as a necessary and sufficient means of proof to establish whether the technical and organisational measures implemented by the controller were appropriate in a case such as the present one, where the unauthorised access to, and disclosure of, personal data are the result of a 'hacking attack'?

4. Is Article 82(3) of Regulation (EU) 2016/679 to be interpreted as meaning that unauthorised disclosure of, or access to, personal data within the meaning of point 12 of Article 4 of Regulation (EU) 2016/679 by means of, as in the present case, a 'hacking attack' by persons who are not employees of the controller's administration and are not subject to its control constitutes an event for which the controller is not in any way responsible and which entitles it to exemption from liability?

5. Is Article 82(1) and (2) of Regulation (EU) 2016/679, read in conjunction with recitals 85 and 146 thereof, to be interpreted as meaning that, in a case such as the present one, involving a personal data breach consisting in unauthorised access to, and dissemination of, personal data by means of a 'hacking attack', the worries, fears and anxieties suffered by the data subject with regard to a possible misuse of personal data in the future fall per se within the concept of non-material damage, which is to be interpreted broadly, and entitle him or her to compensation for damage where such misuse has not been established and/or the data subject has not suffered any further harm?

EU legislation and case-law relied on

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; 'the Regulation'): recitals 1, 4, 6, 74, 75, 76, 77, 83, 85 and 146, points 2, 7 and 12 of Article 4, and Articles 5, 24, 32, 33, 79 and 82.

Judgment of the Court of 30 May 2013, *Worten* (C-342/12, EU:C:2013:355, paragraphs 24 and 26).

Provisions of national law

Administrativnoprotsesualen kodeks (Code of Administrative Procedure) – Articles 144(1), 203 and 208.

Grazhdanski protsesualen kodeks (Code of Civil Procedure) – Article 154.

Zakon za otgovornostta na darzhavata i obshtinite za vredi (Law on the liability of the State and municipalities for damage) – Article 1.

Zakon za zashtita na lichnite danni (Law on the protection of personal data) – Article 39(1) and (2), Article 59(1).

Succinct presentation of the facts and procedure in the main proceedings

1 The Natsionalna agentsia za prihodite (National Revenue Agency, Bulgaria; 'the NAP') is a controller within the meaning of point 7 of Article 4 of the Regulation. Under national law, it is a specialist authority that is subordinate to the Minister for Finance, and is responsible for the establishment, securing and recovery of claims of the State under public law and claims of the State under private law which are established by law. It processes personal data in the exercise of the public powers conferred on it.

2 On 15 July 2019, the Bulgarian media made it known to the general public that there had been unauthorised access to the NAP's information system and that information from its databases containing personal data and tax and social security information had been published on the internet. 4 057 328 Bulgarian nationals were affected, while the total number of natural persons affected, including both Bulgarian and foreign nationals, amounted to 6 074 140. VB is among those affected.

3 To date, there has been no final criminal conviction of the individuals [allegedly] responsible for the unauthorised access, referred to in the media as a 'hacking attack'.

4 After the data had been accessed, hundreds of citizens brought actions against the NAP seeking compensation for non-material damage.

5 On 16 September 2019, VB brought an action against the NAP before the Administrativen sad Sofia-grad (Administrative Court, Sofia City; 'the ASSG') seeking payment of compensation in the amount of 1 000 leva (BGN) (approximately EUR 511) on the basis of Article 82(1) of the Regulation, Article 1(1) of the Law on the liability of the State and municipalities for damage and Article 39(1) of the Law on the protection of personal data.

6 In the action at first instance, VB claimed that the NAP had 'not fulfilled in the best possible way' its obligation 'to ensure its cybersecurity in a flawless manner' and 'to ensure, to the highest degree, the security of the personal data of the citizens of the Republic of Bulgaria in an effective manner'. She submitted that, as a result, there was a personal data breach within the meaning of point 12 of Article 4 of the Regulation and personal data were unlawfully disclosed.

7 VB took the view that 'the lack of diligence and the failure to implement effective data protection measures' is to be regarded as a failure by the NAP to fulfil its obligations to protect the data of citizens and that this constitutes an infringement of Articles 24 and 32 of the Regulation. She stated that, as controller, the NAP is obliged to process personal data in a manner that 'ensures appropriate security' by implementing appropriate technical and organisational measures.

8 VB claimed that the NAP's breach of duty caused her non-material damage in the form of the worry and fear that her personal data would be misused in the future, for example by way of expropriation of her assets, misuse of her bank accounts, conclusion of loans in her name, change of her civil status or theft of her identity. She is appalled by the 'major breach of the NAP's information system' and feels that she is not protected by the State. She fears that she will be blackmailed, attacked or kidnapped.

9 The NAP contended that the action was unfounded. It submitted that VB had not asked the NAP for information regarding precisely which personal data had been accessed.

10 After the data had been accessed, the NAP immediately took measures to protect the rights and interests of citizens. Meetings were held with representatives and experts of the security services, the Notarialna kamara (Chamber of Notaries), the Agentsia po vpisvaniata (Registry Agency), the Asotsiatsia na targovskite banki (Association of Commercial Banks) and the like in order to coordinate measures to limit the consequences of the access. Special sections on the cyberattack were created on the NAP website, where up-to-date information was published.

11 According to the NAP, there is no causal link between the alleged non-material damage and the unauthorised access to personal data. The NAP was the victim of a malicious attack by third parties who are not its employees. It is therefore not responsible for the damage caused.

12 The NAP submitted that it took numerous measures. Specifically, it implemented process management systems and information security management systems, approved procedures complying with international quality standards ISO 9000 and ISO 9001, and applied information security management policies, rules, procedures, instructions and methods.

13 The NAP relied on evidence, namely various internal documents from the period from January 2013 to May 2019 concerning the content of the databases and the procedure for creating, maintaining and accessing them; the implementation of information security management systems; prevention procedures; internal rules on network and information security; instructions for handling information; personal data protection policies; measures and means for protecting personal data; risk assessment methods and procedure.

14 By judgment of 27 November 2020, the ASSG dismissed VB's action as unfounded.

15 The ASSG stated that the unauthorised access to the NAP database had taken place by means of a 'hacking attack' by persons in respect of whom a preliminary investigation had been opened, which had not yet been concluded.

16 According to that court, the unlawful outcome does not allow the presumption that the controller failed to comply with its obligations to implement appropriate technical and organisational measures to ensure the protection of the database in such a way that no one could have access to it in any way or by any means whatsoever.

17 The ASSG considered that the applicant is required to show which (technical) steps the NAP should actually have taken, but failed to do so or did so poorly, thereby giving rise to or contributing to the outcome of unauthorised access to, and disclosure of, personal data.

18 The ASSG took the view that, taking into account the evidence submitted, no omission on the part of the controller could be established. The court stated that VB did not suffer any non-material damage for which compensation can be awarded. The psychological distress experienced, triggered by the news of the unauthorised access to the NAP's information databases, is normal but does not constitute actual damage in the legal sense. VB did not show any interest in precisely which of her personal data had been accessed. That behaviour does not reveal any severe emotional distress.

19 The ASSG found that the public disclosure of the unlawful access to the NAP's database that had taken place did not affect VB's life in terms of her self-confidence, self-esteem, work, relationships and state of health. There is no causal link with the negative emotions experienced, as they are not the result of the NAP's conduct.

20 VB contested the judgment of the ASSG before the referring court, the Varhoven administrativen sad (Supreme Administrative Court; 'the VAS').

Essential arguments of the parties in the main proceedings

21 In the appeal in cassation, VB claims that the ASSG incorrectly allocated the burden of proof with regard to the proving of a negative fact, namely the failure of the controller to implement appropriate technical and organisational measures.

22 VB takes the view that the application of effective measures is a matter at the discretion of the NAP, with the result that it is not possible to show what specific obligations the employees of the NAP should have discharged but failed to do so. She submits that the evidence submitted by the NAP did not demonstrate that the technical and organisational measures implemented were appropriate.

23 VB argues that the concerns about a possible future misuse of the personal data constitute not hypothetical but actual non-material damage that must be compensated. It is not necessary to provide evidence of ordinary non-material damage.

24 The NAP submits that the ASSG rightly considered that the NAP had not failed to act in its capacity as controller, but had implemented numerous technical and organisational measures to afford protection in the processing of personal data. The actual occurrence of damage has not been proved. Worries and fear in respect of future events are not compensable.

Succinct presentation of the reasoning in the request for a preliminary ruling

25 Similar court proceedings against the NAP ended at first instance with contradictory results. The actions were either dismissed as unfounded or upheld in whole or in part. The legislation was interpreted and applied inconsistently in relation to all elements of the controller's liability.

26 The VAS takes the view that the elements constituting liability under Article 82 of the Regulation include: (i) an infringement of the Regulation by the controller; (ii) material or non-material damage suffered by the data subject; and (iii) a causal link between the damage suffered and that specific infringement.

First question

27 According to Article 24(1) of the Regulation, the controller is to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation. Those measures are to be reviewed and updated where necessary.

28 Article 32 of the Regulation provides for obligations on the part of the controller in relation to the security of processing, which are relevant to and trigger its responsibility under Article 24, setting out the criteria according to which the appropriate technical and organisational measures must be applied to ensure a level of security appropriate to the risk. These include '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'.

29 The Regulation does not define 'appropriate technical and organisational measures'. Recital 74 states that the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with the Regulation, including the effectiveness of the measures.

30 The foregoing leads to the conclusion that the controller must carry out a risk assessment according to the criteria laid down in Article 32 of the Regulation, on the basis of which it must implement technical and organisational measures that are appropriate with regard to the level of security of personal data that is required and appropriate to the risk. By implementing appropriate technical and organisational measures, the controller ensures that it processes personal data in compliance with the Regulation.

31 It follows from that legislation that the choice of appropriate technical and organisational measures is a matter of expediency. However, the controller's assessment of expediency is not subject to judicial review, since the court conducts a review of legality. At the same time, the processing of personal data where there is discretion as to the choice of technical and organisational measures must be carried out within the framework of the Regulation and in compliance with the objective of safeguarding the fundamental right to the protection of personal data of natural persons.

32 In the light of the foregoing, the VAS seeks clarification as to whether Articles 24 and 32 of the Regulation are to be interpreted as meaning that the mere occurrence of an unlawful result in the form of unauthorised disclosure of, or access to, personal data within the meaning of point 12 of Article 4 of the Regulation proves that the technical and organisational measures implemented by the controller were not appropriate.

Second question (if the first question is answered in the negative)

33 Since the choice and application of technical and organisational measures are left to the subjective assessment of the controller and fall within its discretion, the question that arises for the VAS is what should be the subject matter and scope of the judicial review of legality in the examination as to whether the technical and organisational measures implemented by the controller are appropriate and comply with Articles 24 and 32 of the Regulation.

34 The VAS has doubts as to whether it is sufficient for the court to establish in what way the controller has complied with the obligations arising from the abovementioned provisions, or whether it must examine the substance of the technical and organisational measures taken and implemented, which, however, are listed merely by way of example in the Regulation and are implemented as appropriate.

Third question (if the first question is answered in the negative)

35 In accordance with Article 5(2) of the Regulation, the controller is to be responsible for, and be able to demonstrate compliance with, the principles set out in paragraph 1 of that provision, relating to the processing of personal data. Article 24(1) of the Regulation obliges the controller to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the] Regulation'.

36 Article 82(3) of the Regulation allows the controller or processor to 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'. According to that paragraph 2, the controller is to be liable for the damage caused by processing which infringes the Regulation.

37 Under national law, each party to an action is obliged to prove the circumstances from which it derives its claims or objections. In the similar proceedings, the courts of first instance distributed the burden of proof between the applicant and the defendant differently.

38 In the present case, the relevant question is whether the principle of accountability under Article 5(2) of the Regulation, read in conjunction with recital 74 and Article 24(1) thereof, is to be interpreted as meaning that it reverses the burden of proof and that the controller against whom an action for compensation has been brought for an infringement of the Regulation is obliged, as the defendant, to prove that the technical and organisational measures that it implemented were appropriate.

39 In addition to the question of the subject matter and scope of the judicial review of compliance with the obligations under the Regulation, there is also the issue of how and on the basis of which evidence the courts are to verify whether those obligations were complied with and, in particular, whether all appropriate technical and organisational measures were applied.

40 In the proceedings, the NAP produced evidence regarding the guarantee of protection of the information networks according to the standards specified in the documents, but no forensic technical expert's report was obtained to establish whether the technical and organisational measures were appropriate within the meaning of the Regulation. The VAS is aware that a controller such as the NAP is obliged to apply organisational, technological and technical measures for network

and information security that are proportionate to the threats posed by cybercrime in order to minimise the risk of such threats materialising. However, access to forensic experts in every case that is based on Article 82 of the Regulation could have new adverse consequences for the protection of personal data.

41 Having regard to the state of the art, the existing standards for the protection of information network systems, and the unauthorised access by means of a 'hacking attack' by persons external to the administration of the controller, the VAS raises the question whether the obtaining of a forensic technical expert's report by the court can be regarded as a necessary and sufficient means of proof to establish whether the technical and organisational measures taken and applied were appropriate for the purposes of ensuring the protection of personal data.

Fourth question

42 As a controller involved in processing, the NAP is liable but can be exempted from liability in accordance with Article 82(3) if it proves that it is not in any way responsible for the event giving rise to the damage.

43 It is common ground in the proceedings that the access to personal data took place by means of a 'hacking attack' against the NAP. However, the unauthorised access to, and disclosure of, personal data did not take place in the course of or in connection with the processing of personal data by employees of the NAP.

44 The VAS seeks to establish whether, in the present case, it is possible to assume that there is an event for which the controller is not in any way responsible and that that event accordingly exempts it from liability.

Fifth question

45 The data subject seeks compensation for non-material damage manifesting itself in worry, anxiety, stress, feelings of insecurity and fears in respect of a future misuse of her personal data in various ways described by her. There is no evidence that VB's personal data has been misused.

46 As is clear from recitals 75 and 85 of the Regulation, the list of examples of material or non-material damage takes into account the nature of the personal data and the adverse effects for the data subjects, and not only their subjective perception.

47 Recital 146 of the Regulation defines the limit of liability. It encompasses 'any damage' which a person may suffer as a result of processing that infringes the Regulation.

48 Once accessed, the personal data of the data subject may be subject to a number of cases of misuse of a non-material and material nature, with significant

consequences. Such cases of misuse have become known to the public, and this may give rise to a higher level of concern on the part of the persons affected by the 'hacking attack'. In the present case, due to the lack of evidence of any misuse that has already taken place, a future misuse is merely a presumption, a hypothesis, with a possible but uncertain risk for the rights of the data subject.

49 For the reasons set out above, the question arises as to whether the negative perceptions of the data subject in that context, that is to say, whether the mere fact that a risk of a possible misuse of the personal data in the future has arisen, fall within the concept of non-material damage, which is to be interpreted broadly, and constitute a ground for compensation under Article 82(1) of the Regulation, read in conjunction with recital 146 thereof.

50 However, it is possible that Article 82(1) of the Regulation, read in conjunction with recital 146 thereof, cannot be interpreted as meaning that any negative perception, fear or anxiety on the part of the data subject entitles him or her to compensation for the non-material damage suffered if there has been no prior unlawful use, for example by way of the expropriation of assets, conclusion of loans in the name of the data subject, or identity theft.