Reports of Cases

JUDGMENT OF THE COURT (Third Chamber)

14 December 2023 *

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 5 – Principles relating to that processing – Article 24 – Accountability of the controller – Article 32 – Measures implemented to ensure security of processing – Assessment of the appropriateness of such measures – Scope of judicial review – Taking of evidence – Article 82 – Right to compensation and liability – Possible exemption from liability of the controller in the event of infringement by third parties – Claim for compensation for non-material damage based on fear of potential misuse of personal data)

In Case C-340/21,

REQUEST for a preliminary ruling under Article 267 TFEU from the Varhoven administrativen sad (Supreme Administrative Court, Bulgaria), made by decision of 14 May 2021, received at the Court on 2 June 2021, in the proceedings

VB

v

Natsionalna agentsia za prihodite,

THE COURT (Third Chamber),

composed of K. Jürimäe, President of the Chamber, N. Piçarra, M. Safjan, N. Jääskinen (Rapporteur) and M. Gavalec, Judges,

Advocate General: G. Pitruzzella,

Registrar: A. Calot Escobar,

having regard to the written procedure,

after considering the observations submitted on behalf of:

– the Natsionalna agentsia za prihodite, by R. Spetsov,

– the Bulgarian Government, by M. Georgieva and L. Zaharieva, acting as Agents,

* Language of the case: Bulgarian.

– the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,

– Ireland, by M. Browne, Chief State Solicitor, A. Joyce, J. Quaney and M. Tierney, acting as Agents, and by D. Fennelly, Barrister-at-Law,

– the Italian Government, by G. Palmieri, acting as Agent, and by E. De Bonis, avvocato dello Stato,

– the Portuguese Government, by P. Barros da Costa, A. Pimenta, M.J. Ramos and C. Vieira Guerra, acting as Agents,

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

after hearing the Opinion of the Advocate General at the sitting on 27 April 2023,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 5(2), Articles 24 and 32 and Article 82(1) to (3) 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 VB, a natural person, and the Natsionalna agentsia za prihodite (National Revenue Agency, Bulgaria) ('the NAP') concerning compensation for non-material damage that that person claims to have suffered as a result of an alleged failure by that authority to fulfil its legal obligations as a controller of personal data.

Legal context

3 Recitals 4, 10, 11, 74, 76, 83, 85 and 146 of the GDPR are worded as follows:

'(4) … This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the [Charter of Fundamental Rights of the European Union] as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, … the right to an effective remedy and to a fair trial …

…

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous

application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the [European] Union. …

(11) Effective protection of personal data throughout the [European] 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, …

…

(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.

…

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

…

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

…

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay …

…

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in [EU] or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. …'

4 Article 4 of that regulation, entitled 'Definitions', provides:

'For the purposes of this Regulation:

(1) "personal data" means any information relating to an identified or identifiable natural person ("data subject"); …

(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 …

…

(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; …

…

(10) "third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

…

(12) "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

…'

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

'1. Personal data shall be:

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

…

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

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

6 Under Article 24 of that regulation, entitled 'Responsibility of the controller':

'1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.'

7 Article 32 of the GDPR, entitled 'Security of processing', provides:

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

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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

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

…'

8 Article 79 of that regulation, entitled 'Right to an effective judicial remedy against a controller or processor', states in paragraph 1 thereof:

'Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.'

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

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

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. …

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

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

10 The NAP is an authority attached to the Bulgarian Minister for Finance. As part of its tasks, consisting, inter alia, of identifying, securing and recovering public debts, it is a controller of personal data, within the meaning of Article 4(7) of the GDPR.

11 On 15 July 2019, the media revealed that unauthorised access to the NAP IT system had taken place and that, following that cyberattack, personal data contained in that system had been published on the internet.

12 More than 6 million natural persons, of Bulgarian and foreign nationality, were affected by those events. Several hundred of them, including the appellant in the main proceedings, brought actions against the NAP for compensation for non-material damage allegedly resulting from the disclosure of their personal data.

13 It was against that background that the appellant in the main proceedings brought an action before the Administrativen sad Sofia-grad (Administrative Court, Sofia, Bulgaria) seeking an order that the NAP pay her the sum of 1 000 leva (BGN) (approximately EUR 510) by way of damages, on the basis of Article 82 of the GDPR and provisions of Bulgarian law. In support of that request, she claimed that she had suffered non-material damage as a result of a personal data breach, within the meaning of Article 4(12) of the GDPR, more specifically, a breach of security caused by the NAP's failure to fulfil its obligations under, inter alia, Article 5(1)(f) and Articles 24

and 32 of that regulation. Her non-material damage consists in the fear that her personal data, having been published without her consent, might be misused in the future, or that she herself might be blackmailed, assaulted or even kidnapped.

14 In its defence, the NAP, first of all, claimed that the appellant in the main proceedings had not asked it for information concerning the precise data that had been disclosed. Next, the NAP produced documents intended to prove that it had taken all necessary measures, in advance, to prevent the breach of the personal data contained in its IT system and, subsequently, to limit the effects of that breach and to reassure citizens. Furthermore, according to the NAP, there was no causal link between the alleged non-material damage and that breach. Lastly, it argued that, since it had suffered a malicious attack by persons who were not its employees, it could not be held liable for the harmful consequences of that attack.

15 By decision of 27 November 2020, the Administrativen sad Sofia-grad (Administrative Court, Sofia) dismissed the action brought by the appellant in the main proceedings. That court held, first, that unauthorised access to the NAP's database was the result of software piracy committed by third parties and, secondly, that the appellant in the main proceedings had not proved that the NAP had failed to act as regards the adoption of security measures. In addition, it found that the appellant had not suffered any non-material damage giving rise to a right to compensation.

16 The appellant in the main proceedings brought an appeal on a point of law against that decision before the Varhoven administrativen sad (Supreme Administrative Court, Bulgaria), which is the referring court in the present case. In support of her appeal, she submits that the court of first instance erred in law in its allocation of the burden of proof in relation to the security measures taken by the NAP and that the NAP has not demonstrated that it did not fail to act in that regard. In addition, the appellant in the main proceedings claims that the fear of possible misuse of her personal data in the future constitutes actual, and not hypothetical, non-material damage. In its defence, the NAP disputes each of those arguments.

17 First of all, the referring court considers the possibility that the fact that a personal data breach has occurred may, on its own, lead to the conclusion that the measures implemented by the data controller were not 'appropriate' within the meaning of Articles 24 and 32 of the GDPR.

18 However, in the event that that finding is insufficient to reach such a conclusion, it raises the question, first, of the scope of the review that the national courts must carry out in order to assess the appropriateness of the measures concerned and, secondly, of the rules on the taking of evidence that must apply in that context, both as regards the burden of proof and the evidence, in particular where those courts are seised of an action for damages under Article 82 of that regulation.

19 Next, that court wishes to know whether, in the light of Article 82(3) of that regulation, the fact that the personal data breach is a result of an act committed by third parties, in this case a cyberattack, constitutes a factor that systematically exempts the controller of those data from liability for the damage caused to the data subject.

20 Lastly, that court asks whether a person's fear that his or her personal data might be misused in the future, in the present case following unauthorised access to those data and their disclosure by cybercriminals, is capable, in itself, of constituting 'non-material damage', within the meaning of

Article 82(1) of the GDPR. If so, that person would not have to establish that, prior to his or her claim for compensation, third parties made unlawful use of those data, such as misuse of his or her identity.

21 In those circumstances, the Varhoven administrativen sad (Supreme Administrative Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Are Articles 24 and 32 of [the GDPR] to be interpreted as meaning that unauthorised disclosure of, or access to, personal data within the meaning of point 12 of Article 4 of [the GDPR] 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 [the GDPR]?

(3) If the first question is answered in the negative, is the principle of accountability under Article 5(2) and Article 24 of [the GDPR], read in conjunction with recital 74 thereof, to be interpreted as meaning that, in legal proceedings under Article 82(1) of [that regulation], 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 [the GDPR] to be interpreted as meaning that unauthorised disclosure of, or access to, personal data within the meaning of point 12 of Article 4 of [the GDPR] 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 [the GDPR], 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?'

Consideration of the questions referred

The first question

22 By its first question, the referring court asks, in essence, whether Articles 24 and 32 of the GDPR must be interpreted as meaning that unauthorised disclosure of personal data or unauthorised access to those data by a 'third party', within the meaning of Article 4(10) of that regulation, are sufficient, in themselves, for it to be held that the technical and organisational measures implemented by the controller in question were not 'appropriate', within the meaning of Articles 24 and 32.

23 As a preliminary point, it should be recalled that, according to settled case-law, the terms of a provision of EU law, such as Articles 24 and 32 of the GDPR, which makes no express reference to the law of the Member States for the purposes of determining its meaning and scope must normally be given an autonomous and uniform interpretation throughout the European Union, having regard, inter alia, to the wording of the provision concerned, to the objectives pursued by that provision and to its context (see, to that effect, judgments of 18 January 1984, *Ekro*, 327/82, EU:C:1984:11, paragraph 11; of 1 October 2019, *Planet49*, C-673/17, EU:C:2019:801, paragraphs 47 and 48; and of 4 May 2023, *Österreichische Post (Non-material damage in connection with the processing of personal data)*, C-300/21, EU:C:2023:370, paragraph 29).

24 In the first place, as regards the wording of the relevant provisions, it should be noted that Article 24 of the GDPR lays down a general obligation, on the part of the controller of personal data, to implement appropriate technical and organisational measures to ensure that that processing is performed in accordance with that regulation and to be able to demonstrate this.

25 To that end, Article 24(1) lists a number of criteria to be taken into account in assessing the appropriateness of such measures, namely, the nature, scope, context and purpose of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. That provision adds that those measures are to be reviewed and updated where necessary.

26 From that point of view, Article 32 of the GDPR sets out the obligations of the controller and a possible processor as regards the security of that processing. Thus, paragraph 1 of that article provides that the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks mentioned in the previous paragraph of this judgment, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing concerned.

27 Similarly, paragraph 2 of that article states that, in assessing the appropriate level of security, account is to be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

28 Furthermore, both Article 24(3) and Article 32(3) of that regulation state that the controller or processor may demonstrate that it has complied with the requirements of the respective paragraphs 1 of those articles by relying on the fact that it adheres to approved codes of conduct or approved certification mechanisms, as referred to in Articles 40 and 42 of that regulation.

29 The reference in Article 32(1) and (2) of the GDPR to 'a level of security appropriate to the risk' and to an 'appropriate level of security' shows that that regulation establishes a risk management system and that it in no way purports to eliminate the risks of personal data breaches.

30 Thus, it is apparent from the wording of Articles 24 and 32 of the GDPR that those provisions merely require the controller to adopt technical and organisational measures intended to avoid, in so far as it is at all possible, any personal data breach. The appropriateness of such measures must be assessed in a concrete manner, by assessing whether those measures were implemented by that controller taking into account the various criteria referred to in those articles and the data protection needs specifically inherent in the processing concerned and the risks arising from the latter.

31 Therefore, Articles 24 and 32 of the GDPR cannot be understood as meaning that unauthorised disclosure of personal data or unauthorised access to such data by a third party are sufficient to conclude that the measures adopted by the controller concerned were not appropriate, within the meaning of those provisions, without even allowing that controller to adduce evidence to the contrary.

32 Such an interpretation is all the more necessary since Article 24 of the GDPR expressly provides that the controller must be able to demonstrate that the measures it implemented comply with that regulation, a possibility which it would be deprived of if an irrebuttable presumption were accepted.

33 In the second place, contextual and teleological elements support that interpretation of Articles 24 and 32 of the GDPR.

34 As regards, first, the context of those two articles, it should be noted that it is apparent from Article 5(2) of the GDPR that the controller must be able to demonstrate that it has complied with the principles relating to processing of personal data set out in paragraph 1 of that article. That obligation is reproduced and clarified in Article 24(1) and (3) and in Article 32(3) of that regulation, as regards the obligation to implement technical and organisational measures to protect such data during the processing carried out by that controller. Such an obligation to demonstrate the appropriateness of those measures would make no sense if that controller were obliged to prevent all breaches of those data.

35 In addition, recital 74 of the GDPR highlights the importance of the controller being obliged to implement appropriate and effective measures and being able to demonstrate the compliance of processing activities with that regulation, including the effectiveness of the measures, which should take into account the criteria, associated with the characteristics of the processing concerned and with the risk presented by it, which are also set out in Articles 24 and 32 of that regulation.

36 Similarly, according to recital 76 of that regulation, the likelihood and severity of the risk depend on the specific features of the processing in question and that risk should be subject to an objective assessment.

37 Furthermore, it follows from Article 82(2) and (3) of the GDPR that, although a controller is liable for the damage caused by processing which infringes that regulation, it is nevertheless exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

38 Secondly, the interpretation given in paragraph 31 above is also supported by recital 83 of the GDPR, which states, in its first sentence, that 'in order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks'. In so doing, the EU legislature expressed its intention to 'mitigate' the risks of personal data breaches, without claiming that it would be possible to eliminate them.

39 In the light of the foregoing, the answer to the first question is that Articles 24 and 32 of the GDPR must be interpreted as meaning that unauthorised disclosure of personal data or unauthorised access to those data by a 'third party', within the meaning of Article 4(10) of that regulation, are not sufficient, in themselves, for it to be held that the technical and organisational measures implemented by the controller in question were not 'appropriate', within the meaning of Articles 24 and 32.

The second question

40 By its second question, the referring court asks, in essence, whether Article 32 of the GDPR must be interpreted as meaning that the appropriateness of the technical and organisational measures implemented by the controller, under that article, must be assessed by the national courts in a concrete manner, in particular by taking into account the risks associated with the processing concerned.

41 In that regard, it should be recalled that, as was pointed out in the context of the answer to the first question, Article 32 of the GDPR requires the controller and the processor, as appropriate, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the assessment criteria set out in paragraph 1 thereof. In addition, paragraph 2 of that article lists, in a non-exhaustive manner, a number of factors that are relevant for assessing the level of safety appropriate to the risks posed by the processing concerned.

42 It is apparent from Article 32(1) and (2) that the appropriateness of such organisational and technical measures must be assessed in two stages. First, it is necessary to identify the risks of a personal data breach caused by the processing concerned and their possible consequences for the rights and freedoms of natural persons. That assessment must be carried out in a concrete manner, taking into account the likelihood of the risks identified and their severity. Secondly, it is necessary to ascertain whether the measures implemented by the controller are appropriate to those risks, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of that processing.

43 It is true that the controller has some discretion in determining the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as required by Article 32(1) of the GDPR. The fact remains that a national court must be able to evaluate the complex assessment carried out by the controller and, in so doing, make sure that the measures adopted by the controller are appropriate for the purposes of ensuring such a level of security.

44 Such an interpretation is, moreover, capable of ensuring, first, the effectiveness of the protection of personal data highlighted in recitals 11 and 74 of that regulation and, secondly, the right to an effective judicial remedy against a controller, as protected by Article 79(1) of that regulation, read in conjunction with recital 4 thereof.

45 Therefore, in order to review the appropriateness of the technical and organisational measures implemented under Article 32 of the GDPR, a national court must not confine itself to finding how the controller concerned intended to fulfil its obligations under that article, but must carry out an examination of the substance of those measures, in the light of all the criteria referred to in that article, the particular circumstances of the case and the evidence available to that court in that regard.

46 Such an examination requires a concrete analysis of both the nature and the content of the measures implemented by the controller, the manner in which those measures were applied and their practical effects on the level of security that the controller was required to guarantee, having regard to the risks inherent in that processing.

47 Consequently, the answer to the second question is that Article 32 of the GDPR must be interpreted as meaning that the appropriateness of the technical and organisational measures implemented by the controller under that article must be assessed by the national courts in a concrete manner, by taking into account the risks associated with the processing concerned and by assessing whether the nature, content and implementation of those measures are appropriate to those risks.

The third question

The first part of the third question

48 By the first part of its third question, the referring court asks, in essence, whether the principle of accountability of the controller, set out in Article 5(2) of the GDPR and given expression in Article 24 thereof, must be interpreted as meaning that, in an action for damages under Article 82 of that regulation, the controller in question bears the burden of proving that the security measures implemented by it are appropriate under Article 32 of that regulation.

49 In that regard, in the first place, it should be recalled that Article 5(2) of the GDPR establishes a principle of accountability, under which the controller is responsible for compliance with the principles relating to the processing of personal data set out in paragraph 1 of that article, and provides that that controller must be able to demonstrate compliance with those principles.

50 In particular, the controller must, in accordance with the principle of integrity and confidentiality of personal data laid down in Article 5(1)(f) of that regulation, make sure that such data are processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, and must be able to demonstrate compliance with that principle.

51 It should also be noted that both Article 24(1) of the GDPR, read in the light of recital 74 thereof, and Article 32(1) of that regulation require the controller, in respect of any processing of personal data carried out by it or on its behalf, to implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is carried out in accordance with that regulation.

52 It is clear from the wording of Article 5(2), Article 24(1) and Article 32(1) of the GDPR that the controller concerned bears the burden of proving that the personal data are processed in such a way as to ensure appropriate security of those data, within the meaning of Article 5(1)(f) and Article 32 of that regulation (see, by analogy, judgments of 4 May 2023, *Bundesrepublik Deutschland (Court electronic mailbox)*, C-60/22, EU:C:2023:373, paragraphs 52 and 53, and of 4 July 2023, *Meta Platforms and Others (General terms of use of a social network)*, C-252/21, EU:C:2023:537, paragraph 95).

53 Those three articles thus set out a rule of general application, which, in the absence of any indication to the contrary in the GDPR, must also be applied in the context of an action for damages based on Article 82 of that regulation.

54 In the second place, it must be held that the foregoing literal interpretation is supported by consideration of the objectives pursued by the GDPR.

55 First, since the level of protection provided for by the GDPR is dependent on the security measures adopted by controllers of personal data, those controllers must be encouraged to do everything in their power to prevent the occurrence of processing operations that do not comply with that regulation, given that they bear the burden of demonstrating the appropriateness of those measures.

56 Secondly, if it were to be held that the burden of proof concerning the appropriateness of those measures lies with the data subjects, as defined in Article 4(1) of the GDPR, it would follow that the right to compensation provided for in Article 82(1) thereof would be deprived of much of its effectiveness, even though the EU legislature intended to strengthen both the rights of those data subjects and the obligations of controllers, as compared with the provisions predating that regulation, as stated in recital 11 thereof.

57 The answer to the first part of the third question is therefore that the principle of accountability of the controller, set out in Article 5(2) of the GDPR and given expression in Article 24 thereof, must be interpreted as meaning that, in an action for damages under Article 82 of that regulation, the controller in question bears the burden of proving that the security measures implemented by it are appropriate pursuant to Article 32 of that regulation.

The second part of the third question

58 By the second part of its third question, the referring court seeks to ascertain, in essence, whether Article 32 of the GDPR and the principle of effectiveness of EU law must be interpreted as meaning that, in order to assess the appropriateness of the security measures implemented by the controller under that article, an expert's report constitutes a necessary and sufficient means of proof.

59 In that connection, it should be recalled that it is settled case-law that, in the absence of EU rules on the matter, it is for the national legal order of each Member State to establish procedural rules for actions intended to safeguard the rights of individuals, in accordance with the principle of procedural autonomy, on condition, however, that those rules are not, in situations covered by EU law, less favourable than those governing similar domestic situations (principle of equivalence) and that they do not make it excessively difficult or impossible in practice to exercise the rights

conferred by EU law (principle of effectiveness) (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, paragraph 53 and the case-law cited).

60 In the present case, it should be noted that the GDPR does not lay down rules relating to the admission and probative value of evidence, such as an expert's report, which must be applied by the national courts hearing an action for damages under Article 82 of that regulation and responsible for assessing, in the light of Article 32 thereof, the appropriateness of the security measures implemented by the controller concerned. Therefore, in accordance with what has been stated in the preceding paragraph of the present judgment and in the absence of rules of EU law governing the matter, it is for the legal system of each Member State to prescribe the detailed rules for safeguarding rights which individuals derive from Article 82 and, in particular, the rules relating to the types of evidence that make it possible to assess the appropriateness of such measures in that context, subject to compliance with those principles of equivalence and effectiveness (see, by analogy, judgments of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, paragraph 297, and of 4 May 2023, *Österreichische Post (Non-material damage in connection with the processing of personal data)*, C-300/21, EU:C:2023:370, paragraph 54).

61 In the present proceedings, the Court does not have before it any evidence capable of giving rise to doubt as to compliance with the principle of equivalence. The position is different as regards compliance with the principle of effectiveness, in so far as the very wording of the second part of the third question presents the use of an expert's report as a 'necessary and sufficient means of proof'.

62 In particular, a national procedural rule under which it would be systematically 'necessary' for national courts to order that an expert's report be obtained would be liable to conflict with the principle of effectiveness. The systematic use of such an expert's report may be superfluous in the light of the other evidence held by the court seised, in particular, as the Bulgarian Government stated in its written observations, in the light of the results of a review of compliance with measures to protect personal data carried out by an independent authority, established by law, provided that that review is recent, since those measures must, in accordance with Article 24(1) of the GDPR, be reviewed and updated if necessary.

63 In addition, as the European Commission noted in its written observations, the principle of effectiveness could be infringed if the term 'sufficient' were to be understood as meaning that a national court must infer exclusively or automatically from an expert's report that the security measures implemented by the controller in question are 'appropriate', within the meaning of Article 32 of the GDPR. The protection of rights conferred by that regulation, which the principle of effectiveness seeks to ensure, and in particular the right to an effective judicial remedy against the controller, which is guaranteed by Article 79(1) of that regulation, require an impartial tribunal to carry out an objective assessment of the appropriateness of the measures concerned, instead of confining itself to such a deduction (see, to that effect, judgment of 12 January 2023, *Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-132/21, EU:C:2023:2, paragraph 50).

64 In the light of the foregoing, the answer to the second part of the third question is that Article 32 of the GDPR and the principle of effectiveness of EU law must be interpreted as meaning that, in order to assess the appropriateness of the security measures implemented by the controller under that article, an expert's report cannot constitute a systematically necessary and sufficient means of proof.

The fourth question

65 By its fourth question, the referring court asks, in essence, whether Article 82(3) of the GDPR must be interpreted as meaning that the controller is exempt from its obligation to pay compensation for the damage suffered by a data subject, under Article 82(1) and (2) of that regulation, solely because that damage is a result of unauthorised disclosure of, or access to, personal data by a 'third party', within the meaning of Article 4(10) of that regulation.

66 As a preliminary point, it should be noted that it follows from Article 4(10) of the GDPR that persons other than those who, under the direct authority of the controller or the processor, are authorised to process personal data are considered to be a 'third party'. That definition covers persons who are not employees of the controller and are not subject to its control, such as those mentioned in the question referred.

67 Next, it should be recalled, in the first place, that Article 82(2) of the GDPR provides that 'any controller involved in processing shall be liable for the damage caused by processing which infringes [that] Regulation' and that paragraph 3 of that article provides that a controller, or a processor as the case may be, is exempt from such liability 'if it proves that it is not in any way responsible for the event giving rise to the damage'.

68 In addition, recital 146 of the GDPR, which relates specifically to Article 82 thereof, states, in its first and second sentences, that 'the controller or processor should compensate any damage which a person may suffer as a result of processing that infringes that Regulation' and 'should be exempt from liability if it proves that it is not in any way responsible for the damage'.

69 It follows from those provisions, first, that the controller in question must, in principle, make good any damage caused by an infringement of that regulation linked to that processing and, secondly, that it can be exempt from liability only if it proves that it is in no way responsible for the event giving rise to that damage.

70 Thus, as is apparent from the express addition of the words 'in any way' during the legislative process, the circumstances in which the controller may claim to be exempt from civil liability under Article 82 of the GDPR must be strictly limited to those in which the controller is able to demonstrate that the damage is not attributable to it.

71 Where, as in the present case, a personal data breach, within the meaning of Article 4(12) of the GDPR, has been committed by cybercriminals, and therefore by a 'third party', within the meaning of Article 4(10) of that regulation, that infringement cannot be attributed to the controller, unless the controller has made that infringement possible by failing to comply with an obligation laid down in the GDPR, and in particular the data protection obligation to which it is subject under Article 5(1)(f) and Articles 24 and 32 of that regulation.

72 Thus, in the event of a personal data breach by a third party, the controller may be exempt from liability, on the basis of Article 82(3) of the GDPR, by proving that there is no causal link between its possible breach of the data protection obligation and the damage suffered by the natural person.

73 In the second place, the foregoing interpretation of Article 82(3) is also consistent with the GDPR's objective of ensuring a high level of protection of natural persons with regard to the processing of their personal data, set out in recitals 10 and 11 of that regulation.

74 In the light of the foregoing considerations, the answer to the fourth question is that Article 82(3) of the GDPR must be interpreted as meaning that the controller cannot be exempt from its obligation to pay compensation for the damage suffered by a data subject, under Article 82(1) and (2) of that regulation, solely because that damage is a result of unauthorised disclosure of, or access to, personal data by a 'third party', within the meaning of Article 4(10) of that regulation, in which case that controller must then prove that it is in no way responsible for the event that gave rise to the damage concerned.

The fifth question

75 By its fifth question, the referring court asks, in essence, whether Article 82(1) of the GDPR must be interpreted as meaning that the fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of that regulation is capable, in itself, of constituting 'non-material damage' within the meaning of that provision.

76 In the first place, as regards the wording of Article 82(1) of the GDPR, it should be recalled that that paragraph states that 'any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered'.

77 In that regard, the Court has observed that it is clear from the wording of Article 82(1) of the GDPR that the existence of 'damage' which has been 'suffered' constitutes one of the conditions for the right to compensation laid down in that provision, as does the existence of an infringement of that regulation and of a causal link between that damage and that infringement, those three conditions being cumulative (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, paragraph 32).

78 Furthermore, on the basis of considerations of a literal, systematic and teleological nature, the Court interpreted Article 82(1) of the GDPR as precluding a national rule or practice which makes compensation for 'non-material damage', within the meaning of that provision, subject to the condition that the damage suffered by the data subject has reached a certain degree of seriousness (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, paragraph 51).

79 That said, it must be pointed out, in the present case, that Article 82(1) of the GDPR does not distinguish between situations in which, as a result of an established infringement of provisions of that regulation, the 'non-material damage' alleged by the data subject, first, is linked to a misuse of his or her personal data by third parties that has already occurred, at the date of his or her claim for compensation, or, secondly, is linked to that person's fear that such use may occur in the future.

80 Therefore, the wording of Article 82(1) of the GDPR does not rule out the possibility that the concept of 'non-material damage' in that provision encompasses a situation, such as that referred to by the referring court, in which the data subject invokes, in order to obtain compensation on the basis of that provision, the fear that his or her personal data will be misused by third parties as a result of the infringement of that regulation that has taken place.

81 In the second place, that interpretation is supported by recital 146 of the GDPR, which relates specifically to the right to compensation provided for in Article 82(1) thereof and which states, in its third sentence, that 'the concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives' of that regulation. An interpretation of the concept of 'non-material damage', within the meaning of Article 82(1), which does not include situations in which the person concerned by an infringement of that regulation relies on the fear that his or her own personal data will be misused in the future, would not be consistent with a broad interpretation of that concept, as intended by the EU legislature (see, by analogy, 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 37 and 46).

82 Furthermore, the first sentence of recital 85 of the GDPR states that 'a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, … or any other significant economic or social disadvantage to the natural person concerned'. It is apparent from that illustrative list of types of 'damage' that may be suffered by the data subjects that the EU legislature intended to include in those concepts, in particular, the mere 'loss of control' over their own data, as a result of an infringement of that regulation, even if there had been no misuse of the data in question to the detriment of those data subjects.

83 In the third and last place, the interpretation set out in paragraph 80 above is supported by the objectives of the GDPR, which must be taken into account in order to define the concept of 'damage', as stated in the third sentence of recital 146 of that regulation. An interpretation of Article 82(1) of the GDPR to the effect that the concept of 'non-material damage', within the meaning of that provision, does not include situations in which a data subject relies solely on the fear that his or her personal data will be misused by third parties, in the future, would not be consistent with the guarantee of a high level of protection of natural persons with regard to the processing of personal data within the European Union, which is the aim of that instrument.

84 However, it must be pointed out that a person concerned by an infringement of the GDPR which had negative consequences for him or her is required to demonstrate that those consequences constitute non-material damage within the meaning of Article 82 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, paragraph 50).

85 In particular, where a person claiming compensation on that basis relies on the fear that his or her personal data will be misused in the future owing to the existence of such an infringement, the national court seised must verify that that fear can be regarded as well founded, in the specific circumstances at issue and with regard to the data subject.

86 In the light of the foregoing reasons, the answer to the fifth question is that Article 82(1) of the GDPR must be interpreted as meaning that the fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of that regulation is capable, in itself, of constituting 'non-material damage' within the meaning of that provision.

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 (Third Chamber) hereby rules:

1. **Articles 24 and 32 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 unauthorised disclosure of personal data or unauthorised access to those data by a 'third party', within the meaning of Article 4(10) of that regulation, are not sufficient, in themselves, for it to be held that the technical and organisational measures implemented by the controller in question were not 'appropriate', within the meaning of Articles 24 and 32.

2. **Article 32 of Regulation 2016/679**

   must be interpreted as meaning that the appropriateness of the technical and organisational measures implemented by the controller under that article must be assessed by the national courts in a concrete manner, by taking into account the risks associated with the processing concerned and by assessing whether the nature, content and implementation of those measures are appropriate to those risks.

3. **The principle of accountability of the controller, set out in Article 5(2) of Regulation 2016/679 and given expression in Article 24 thereof,**

   must be interpreted as meaning that, in an action for damages under Article 82 of that regulation, the controller in question bears the burden of proving that the security measures implemented by it are appropriate pursuant to Article 32 of that regulation.

4. **Article 32 of Regulation 2016/679 and the principle of effectiveness of EU law**

   must be interpreted as meaning that, in order to assess the appropriateness of the security measures implemented by the controller under that article, an expert's report cannot constitute a systematically necessary and sufficient means of proof.

5. **Article 82(3) of Regulation 2016/679**

   must be interpreted as meaning that the controller cannot be exempt from its obligation to pay compensation for the damage suffered by a data subject, under Article 82(1) and (2) of that regulation, solely because that damage is a result of unauthorised disclosure of, or access to, personal data by a 'third party', within the meaning of Article 4(10) of that regulation, in which case that controller must then prove that it is in no way responsible for the event that gave rise to the damage concerned.

6. **Article 82(1) of Regulation 2016/679**

must be interpreted as meaning that the fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of that regulation is capable, in itself, of constituting 'non-material damage' within the meaning of that provision.

[Signatures]