Reports of Cases

OPINION OF ADVOCATE GENERAL
PITRUZZELLA
delivered on 27 April 2023 [1]

Case C-340/21

VB

v

Natsionalna agentsia za prihodite

(Request for a preliminary ruling from the Varhoven administrativen sad (Supreme Administrative Court, Bulgaria))

(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Responsibility of the controller – Security of processing – Breach of security of the processing of personal data – Non-material damage suffered as a result of the controller's inaction – Action for damages)

Can the unlawful dissemination of personal data held by a public agency, as a result of a hacking attack, give rise to compensation for non-material damage in favour of a data subject merely because the latter fears a possible misuse of his or her data in the future? What are the criteria for attributing responsibility to the controller? How are the evidentiary burdens of proof allocated in the proceedings? What is the extent of the court's review?

I. Legal framework

1. Article 4, entitled 'Definitions', of Regulation 2016/679 [2] ('the Regulation') provides that:

'For the purposes of this Regulation:

…

(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

…'.

[1] Original language: Italian.

[2] 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).

2. Article 5, entitled 'Principles relating to processing of personal data', states that:

'1. Personal data shall be:

…

(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").'

3. Article 24 of that regulation, entitled 'Responsibility of the controller', provides that:

'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'.

4. Article 32, entitled 'Security of processing', provides that:

'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:

…

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.

…'.

5. Article 82 of that regulation, entitled 'Right to compensation and liability', provides that:

'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.'

II. Facts, main proceedings and questions referred for a preliminary ruling

6. On 15 July 2019, the Bulgarian media spread the news that there had been unauthorised access to the information system of the Natsionalna agentsia za prihodite (National Revenue Agency, Bulgaria; 'the NAP') [3] and that various tax and social security information of millions of persons, both Bulgarian nationals and foreign nationals, had been published on the internet.

7. Many persons, including VB, the appellant in the main proceedings, therefore brought proceedings against the NAP for compensation for non-material damage.

8. In the present case, the appellant in the main proceedings brought an action before the Administratibven sad Sofia-grad (Administrative Court, Sofia City, Bulgaria; 'the ASSG'), arguing that the NAP had infringed national rules, as well as the obligation to process personal data as controller in a manner that 'ensures appropriate security' by implementing appropriate technical and organisational measures, in accordance with Articles 24 and 32 of Regulation 679/2016. In addition, she claimed that she had suffered non-material damage in the form of the worry and fear that her personal data would be misused in the future.

9. The opposing party, for its part, pointed out that it had not received any request from the appellant in the main proceedings seeking an indication of exactly which personal data had been accessed. Moreover, following the news of the intrusion, it had convened meetings with experts to protect the rights and interests of citizens. According to the NAP, there was also no causal link between the cyberattack and the alleged damage, since the agency had implemented all process management and information security systems, in accordance with the applicable international standards.

10. The court of first instance, the ASSG, dismissed the application, taking the view that the dissemination of the data was not attributable to the agency, that the burden of proof as to whether the measures implemented were appropriate was on the applicant, and, lastly, that non-material damage was not eligible for compensation.

[3] The NAP is a controller within the meaning of point 7 of Article 4 of the Regulation. Under national law, it is an administrative body with specific competence, subordinate to the Minister for Finance, and responsible for the assessment, safeguarding and recovery of public finances, and the assessment, safeguarding and recovery of both public and private amounts owed to the State, as determined by law. It processes personal data in the exercise of the official authority conferred on it.

11. The judgment at first instance was then appealed before the Varhoven administrativen sad (Supreme Administrative Court, Bulgaria). Among its submissions, the appellant in the main proceedings pointed out that the court of first instance had erred in its allocation of the burden of proof in relation to the failure to implement security measures. It also argued that the non-material damage should not be subject to the burden of proof, since it is actual and not merely potential non-material damage.

12. The NAP, for its part, reiterated that it had implemented the necessary technical and organisational measures as controller and disputed that there was proof of actual non-material damage. It argued that worry and fears are emotional states for which compensation cannot be claimed.

13. The referring court observed that there had been differing outcomes with regard to the individual proceedings that injured parties had brought separately against the NAP for compensation for non-material damage.

14. In those circumstances, the referring court stayed the proceedings and referred the following questions to the Court of Justice for a preliminary ruling:

‘(1) Are 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)] 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?'

III. Legal analysis

A. Preliminary observations

15. The present case concerns interesting and, in part, novel issues on the interpretation of several provisions of the Regulation. [4]

16. The five questions referred for a preliminary ruling all revolve around the same issue: the conditions under which compensation for non-material damage may be awarded to a person whose personal data, held by a public agency, was published on the internet following a hacking attack.

17. For ease of reference, I will propose brief separate answers to all the questions referred for a preliminary ruling in the order for reference, although I am aware that there are some conceptual overlaps, since the first four are all aimed at identifying the conditions under which the infringement of the provisions of the Regulation may be attributed to the controller [5] and the fifth concerns, more specifically, the concept of non-material damage for the purposes of compensation. [6]

18. I would point out that several cases on Article 82 of the Regulation are currently pending before the Court and I will take into account in the present analysis the Advocate General's Opinion that has already been delivered in one of those cases. [7]

19. Before examining the questions referred, I consider it appropriate to make some preliminary remarks on the principles and aims of the Regulation, which will prove useful for answering each of the questions referred for a preliminary ruling.

[4] Article 5(2) (on the principle of accountability of any controller of personal data), Article 24 (on the measures that that person responsible for the processing is required to implement to ensure that processing is in accordance with the Regulation), Article 32 (on that obligation specifically as regards security of processing) and Article 82(1) to (3) (on compensation for damage resulting from an infringement of the Regulation and on the possibility for the controller to implement measures to ensure compliance with the Regulation), as well as recitals 74, 85 and 146 which are related to those articles.

[5] (a) The first aims at answering the question of whether it can be inferred from the mere breach of the systems that the measures put in place are inappropriate; (b) the second concerns the scope of judicial review of the appropriateness of those measures; (c) the third refers to the burden of proof as regards that appropriateness and to certain technical methods for gathering evidence; (d) the fourth relates to the significance for the purposes of the exemption from liability of the fact that the attack on the system comes from outside.

[6] As regards the provisions of the Regulation referred to, the first three questions concern the aspects of the controller's responsibility in relation to the appropriateness of the measures to be implemented (Articles 5, 24 and 32); the fourth and fifth concern the conditions for exemption from liability and the concept of non-material damage for which compensation can be awarded (Article 82).

[7] See Opinion of Advocate General Campos Sánchez-Bordona in *Österreichische Post (Non-material damage resulting from unlawful processing of data)*, (C-300/21, EU:C:2022:756).

20. Article 24 of the Regulation lays down, in general terms, the obligation on the controller to implement appropriate technical and organisational measures to ensure that processing of personal data is performed in accordance with the Regulation and to be able to demonstrate as such, while Article 32 lays down more specifically the same obligation as regards security of processing. Articles 24 and 32 set out more specifically what is already provided for in Article 5(2), which introduces, specifically among the 'principles relating to processing of personal data', the '[principle of] accountability'. That principle follows logically from and is complementary to the '[principle of] integrity and confidentiality' laid down in Article 5(1)(f), and both should be read in the light of the risk-based approach underpinning the Regulation.

21. The principle of accountability is one of the cornerstones of the Regulation and one of its most significant innovations. It places on the controller the responsibility to take proactive steps to ensure compliance with the Regulation and to be ready to demonstrate that compliance. [8]

22. Legal writers have referred to a genuine cultural change as an effect of the 'overall scope of the requirement of accountability'. [9] It is not so much the formal compliance with the legal obligation or the one-off measure as the whole business strategy adopted that exempts the controller from liability on the ground that it is compliant with the data protection legislation.

23. The technical and organisational measures required by the principle of accountability must be 'appropriate' taking into account the factors specified in Article 24: the nature, scope, context and purposes of processing as well as the likelihood and severity of the risks for the rights and freedoms of natural persons.

24. Article 24 therefore requires that measures be appropriate in order to be able to demonstrate that processing is carried out in accordance with the principles and provisions of the Regulation.

25. Article 32, for its part, applies the principle of accountability to the specific measures to be implemented to ensure 'a level of security appropriate to the risk'. In doing so, it adds, to the factors already stipulated as having to be taken into account in the preparation of technical and organisational measures, the state of the art and the costs of implementation.

26. The concept of appropriateness requires that the solutions implemented to protect IT systems reach a level of acceptability, both in technical terms (relevance of measures) and qualitative terms (effectiveness of protection). In order to ensure compliance with the principles of necessity, relevance and proportionality, the processing must not only be suitable but also satisfactory with regard to the purposes to be pursued. Following that logic, the principle of minimisation plays a decisive role, according to which all stages of data processing must constantly strive to minimise security risks. [10]

8 Docksey, C., 'Article 24. Responsibility of the controller', in Kuner, C., Bygrave, L.A., Docksey, C., and Drechsler, L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, p. 561. The principles and obligations of data protection rules should permeate the cultural fabric of organisations, at all levels, rather than being regarded as a set of legal requirements to be ticked off by the legal department.

9 Belisario, E., Riccio, G., and Scorza, G., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 301.

10 Belisario, E., Riccio, G., and Scorza, G., *GDPR*, op. cit., p. 380.

27. The entire Regulation is guided by risk prevention and accountability of the controller and, therefore, by a purposive approach aimed at the best possible outcome in terms of effectiveness, which is far removed from a formalistic approach linked to the mere obligation to fulfil specific procedures in order to no longer be liable. [11]

28. Article 24 does not contain an exhaustive list of 'appropriate' measures: an assessment on a case-by-case basis will have to be carried out. That is in line with the philosophy of the Regulation, which explains how it was preferred that the procedures to be adopted are chosen on the basis of a careful assessment of the specific situation in order to be as effective as possible. [12]

B. The first question referred for a preliminary ruling

29. By its first question, the referring court asks, in essence, whether Articles 24 and 32 of the Regulation must be interpreted as meaning that the occurrence of a 'personal data breach', as defined in point 12 of Article 4, is sufficient in itself to conclude that the technical and organisational measures implemented by the controller were not 'appropriate' to ensure data protection.

30. It follows from the wording of Articles 24 and 32 of the Regulation that the controller, when choosing the technical and organisational measures which it is required to implement in order to ensure compliance with the Regulation, must take into account a number of assessment factors, which are listed in those articles and have been recalled above.

31. The controller has a certain margin of discretion in determining the most appropriate measures in the light of its specific situation, but that choice is nevertheless subject to possible judicial review of the compliance of the measures applied with all the obligations and aims of the Regulation.

32. In particular, as regards security measures, Article 32(1) requires the controller to take into account the 'state of the art'. That implies that the technological level of measures to be implemented is limited to what is reasonably possible at the time the measures are implemented: the suitability of the measure to prevent the risk must therefore be proportionate to the solutions that the state of the art in science, technique, technology and research offers at the time, also taking into account, as will be seen, the implementation costs.

33. Measures may be 'appropriate' at a given time and, despite that, be circumvented by cybercriminals using highly sophisticated tools that are capable of breaching even security measures that are in accordance with the state of the art.

[11] That is why, as we shall see, the first and fourth questions referred for a preliminary ruling can only be answered in the negative. No automatic mechanism can be inferred from the provisions of the Regulation: nor is the mere fact that personal data has been disclosed sufficient to find that the technical and organisational measures implemented are inappropriate and nor is the circumstance that that disclosure took place through the involvement of persons external to the controller's organisation and outside its scope of control sufficient to exempt it from liability.

[12] Bolognini, L., and Pelino, E., *Codice della disciplina privacy*, Giuffrè, 2019, p. 201. The European legislator therefore goes beyond the concept of security of processing based on the existence of predetermined security measures and adopts a methodology specific to international standards on the risk-based management of information systems: it provides for the identification of risk mitigation measures that set aside preconfigured and generically applicable checklists. International guidelines and standards should therefore be used. The outcome of that risk assessment therefore becomes binding when the organisation adopts decisions in order to mitigate the identified risks, making it accountable.

34. On the other hand, it seems illogical to assume that the intention of the EU legislator was to impose on the controller the obligation to prevent any personal data breach irrespective of the diligence in the preparation of security measures. [13]

35. As mentioned above, the Regulation moves away from an automatic approach, and requires a high level of accountability on the part of the controller, which cannot, however, make it impossible for the controller to demonstrate that it has correctly fulfilled the obligations imposed on it.

36. In addition, Article 32(1) provides for the 'costs of implementation' of the technical and organisational measures concerned to be taken into account, as mentioned above. It follows that the assessment of the appropriateness of those measures must be based on a balancing exercise between the interests of the data subject, which generally tend towards a higher level of protection, and the economic interests and technological capacity of the controller, which sometimes tend towards a lower level of protection. That balancing exercise must comply with the requirements of the general principle of proportionality.

37. It should be added to that, with a view to a systematic interpretation, that the legislator contemplates the possibility of breaches of systems occurring; Article 32(1)(c) includes among the suggested measures the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. Providing, among the security measures that ensure a level of security appropriate to the risk, for that ability would be pointless if it were considered that the breach of systems alone constitutes in itself proof of the inappropriateness of those measures.

C. The second question referred for a preliminary ruling

38. By its second question, the referring court asks, in essence, what the subject matter and scope of the judicial review should be when assessing whether the technical and organisational measures implemented by the controller of personal data are appropriate pursuant to Article 32 of the Regulation.

39. Given the variability of situations which may arise in practice, the Regulation, as mentioned above, does not lay down binding provisions for determining the technical and organisational measures that the controller must implement to comply with the requirements of the Regulation itself. The appropriateness of the measures implemented will therefore have to be assessed *in concreto*, by verifying whether the specific measures were suitable to reasonably prevent the risk and minimise the negative effects of the breach.

40. While it is undoubtedly true that the choice and implementation of those measures falls within the subjective assessment of the controller, since the measures mentioned in the Regulation are only examples, the court's review cannot be limited to monitoring compliance by the controller with the obligations arising from Articles 24 and 32, that is to say, to having (formally) provided for certain technical and organisational measures. It must carry out a specific analysis of the content of those measures, the manner in which they were applied and their practical effects, on the basis of the evidence before it and the circumstances of the specific case.

[13] The concept of appropriateness unequivocally shows the intention not to accord relevance to all theoretically possible technical and organisational measures. See, to that effect, Gambini, M., 'Responsabilità e risarcimento nel trattamento dei dati personali', in Cuffaro, V., D'Orazio, R., and Ricciuto, V., *I dati personali nel diritto europeo*, Giappichelli, 2019, p. 1059.

As the Portuguese Government has effectively observed, 'the manner in which it has fulfilled its obligations appears to be inseparable from the content of the measures adopted, for the purpose of demonstrating that, taking into account the specific data processing (its nature, scope, context and purposes), the state of the art of the available technologies and their costs, as well as the risks for the rights and freedoms of citizens, the controller has implemented all necessary and appropriate measures to ensure a level of security appropriate to the underlying risk'. [14]

41. Judicial review must therefore take into account all the factors set out in Articles 24 and 32, which, as mentioned above, list a number of criteria for assessing appropriateness and provide examples of measures which may be considered appropriate. Moreover, as the Commission and all the Member States that submitted observations on the second question have pointed out, Article 32(1) to (3) emphasises the need to 'ensure a level of security appropriate to the risk', indicating other relevant factors in that regard, such as the possible adoption by the controller of an approved code of conduct or an approved certification system, as provided for in Articles 40 and 42 of the Regulation respectively.

42. The adoption of codes of conduct or certification systems may constitute a relevant criterion of assessment, for the purposes of discharging the burden of proof and the related judicial review. However, it must be pointed out that it is not sufficient for the controller to adhere to a code of conduct; the controller has the burden of proving that it actually implemented the measures which that code provides for, in accordance with the principle of accountability. Certification, on the other hand, constitutes 'in itself proof that the processing is carried out in compliance with the Regulation even if it is liable to be disproved in practice'. [15]

43. Lastly, it should be noted that those measures must be reviewed and updated where necessary, pursuant to Article 24(1). That will also be subject to assessment by the national court. Indeed, Article 32(1) of the Regulation [16] imposes on the controller an onus of constant control and monitoring, prior to and subsequent to the processing activities, and also of maintenance and possible updating of the measures adopted, for the purpose of both preventing breaches and, if need be, limiting their effects.

44. I am, however, inclined to argue that it would not be appropriate for the forthcoming judgment to include a list of substantive elements, such as that suggested by the Portuguese Government. [17] That could provide room for conflicting interpretations as the list can obviously never be exhaustive.

[14] Written observations, point 31.

[15] Gambini, M., 'Responsabilità', op. cit., p. 1067. Having certification therefore results in a reversal of the burden of proof in favour of the controller which is facilitated in proving that it acted in compliance with the obligations laid down by the Regulation.

[16] By expressly providing, in point (d), that the assessment of appropriateness extends to the effectiveness of the measures implemented, which must be regularly tested, assessed and evaluated, both at the initial stage and at regular intervals, in order to ensure the effective security of all types of processing, whatever their level of risk; and, again, by explicitly providing, in point (c), that the technical and organisational measures implemented must have the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. See Gambini, M., 'Responsabilità', op. cit., pp. 1064-1065.

[17] Point 30 of the written observations: 'it is for the controllers to demonstrate how it has assessed all the factors and circumstances relating to the processing in question, and in particular the result of the risk analysis carried out, the risks identified, the specific measures found to mitigate those risks, the justification of the options chosen in the light of the technological solutions available on the market, the effectiveness of the measures, the correlation between the technical and organisational measures, the training of the staff processing the data, the existence of outsourcing of data processing operations, including the development and maintenance of the information technology, and the existence of supervision by the controller and of precise instructions given to the processors, pursuant to Article 28 of the GDPR, on the processing of personal data by the latter; how the infrastructure supporting the communication and information systems has been assessed and how the level of risk for the rights and freedoms of data subjects has been classified'.

D. The third question referred for a preliminary ruling

45. By the first part of its third question, the referring court essentially asks the Court to determine whether, having regard to the principle of accountability under Article 5(2) and Article 24 of the Regulation, read in conjunction with recital 74 thereof,[18] in the context of an action for damages under Article 82 of that regulation, the burden of proving that the technical and organisational measures are appropriate pursuant to Article 32 of the Regulation rests on the controller of the personal data.

46. The foregoing considerations enable me to reply briefly that it does.

47. Indeed, the letter of the law, the context and the aims of the Regulation point unequivocally towards the burden of proof being on the controller.

48. It follows from the wording of several provisions of the Regulation that the controller must be 'able' to or 'capable' of 'demonstrating' compliance with the obligations laid down in the Regulation and, in particular, that it has implemented appropriate measures to that end, as indicated in recital 74, Article 5(2) and Article 24(1). As the Portuguese Government points out, recital 74 states that the burden of proof thus placed on the controller must include proof of the 'effectiveness of the measures' in question.

49. That literal interpretation seems to me to be supported by the following practical and purposive considerations.

50. As regards the allocation of the burden of proof, in the context of an action for damages based on Article 82, the data subject who has brought the action against the controller must prove, first, that there has been an infringement of the Regulation, second, that he or she has suffered damage and, third, that there is a causal link between the two preceding elements, as was noted in all the written observations on the fifth question referred for a preliminary ruling. Those three conditions are cumulative, as is also apparent from the settled case-law of the Court of Justice and the General Court in the context of non-contractual liability in the European Union.[19]

51. However, I consider that the applicant's obligation to demonstrate the existence of an infringement of the Regulation cannot go so far as to require him or her to demonstrate how the technical and organisational measures implemented by the controller are not appropriate, for the purposes of Articles 24 and 32.

52. As the Commission points out, the submission of such evidence is often virtually impossible in practice, since data subjects generally do not have sufficient knowledge to be able to analyse those measures, and do not have access to all the information in the possession of the controller

[18] According to Recital 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'.

[19] See, inter alia, judgments of the Court of Justice of 5 September 2019, *European Union* v *Guardian Europe* and *Guardian Europe* v *European Union* (C-447/17 P and C-479/17 P, EU:C:2019:672, paragraph 147), and of 28 October 2021, *Vialto Consulting* v *Commission* (C-650/19 P, EU:C:2021:879, paragraph 138), as well as the judgments of the General Court of 13 January 2021, *Helbert* v *EUIPO* (T-548/18, EU:T:2021:4, paragraph 116), and of 29 September 2021, *Kočner* v *Europol* (T-528/20, not published, EU:T:2021:631, paragraph 61), in which it is recalled that three conditions must be fulfilled, namely 'the unlawfulness of the conduct alleged against the EU institution, the fact of damage and the existence of a causal link between the conduct of that institution and the damage complained of'.

responsible for the processing at issue, in particular as regards the methods applied to ensure the security of that processing. Moreover, the controller could sometimes argue that its refusal to disclose those facts to data subjects is based on the legitimate ground of not making public its internal affairs, or information covered by professional secrecy, in particular for reasons of security.

53. Therefore, if the burden of proof were to be considered to lie with the data subject, the practical result would be that the right to bring an action provided for in Article 82(1) would be rendered largely meaningless. In my view, this would not be consistent with the intentions of the EU legislator, which, in adopting the Regulation, sought to strengthen the rights of data subjects and increase the obligations on the persons responsible for processing, by comparison to Directive 95/46 which it replaced. It is therefore more logical, and legally tenable, that the controller is required to prove, in its defence against an action for damages, that it complied with the obligations under Articles 24 and 32 of that regulation by implementing measures which are actually appropriate.

54. By the second part of its third question, the referring court asks the Court, in essence, whether an expert's report can be regarded as necessary and sufficient evidence to assess whether the technical and organisational measures implemented by the controller of personal data were appropriate in a situation in which unauthorised access to and disclosure of personal data are the result of hacking.

55. I consider, as was also stressed (in essence) by the Bulgarian and Italian Governments, Ireland and the Commission, that the answer to those questions must be based on our settled case-law according to which, in accordance with the principle of procedural autonomy, in the absence of EU rules on the matter, it is for the national legal order of each Member State to lay down the detailed procedural rules governing judicial proceedings intended to safeguard the rights of individuals, provided, however, that those rules are not, in situations governed by EU law, less favourable than those governing similar situations subject to domestic law (the principle of equivalence) and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness).

56. In the present case, I note that the Regulation does not contain any provision aimed at determining the admissible methods of proof and their probative value, in particular with regard to the acts of inquiry (such as an expert's report) which the national courts may or must order in order to assess whether a controller of personal data has implemented measures which are appropriate within the meaning of that regulation. I therefore consider that, in the absence of harmonised rules on the matter, it is for the national legal order of each Member State to determine those detailed procedural rules, subject to compliance with the principles of equivalence and effectiveness.

57. The abovementioned 'principle of effectiveness', which means that an independent judge must carry out an impartial assessment, could be undermined if the adjective 'sufficient' were to be understood by the meaning which the referring court seems in my view to attribute to it, that is to say, if it could automatically infer from an expert's report that the measures implemented by the controller are appropriate. [20]

[20] Written observations, point 39.

E. The fourth question referred for a preliminary ruling

58. By its fourth question, the referring court asks, in essence, whether Article 82(3) of the Regulation must be interpreted as meaning that, where there is an infringement of that regulation (consisting, as in the present case, of 'unauthorised disclosure' of or 'unauthorised access' to personal data within the meaning of point 12 of Article 4 by persons who are not employees of the controller of that data and who are not under the latter's control, that constitutes an event for which the controller is not in any way responsible, and is therefore a ground for exemption from its liability, within the meaning of Article 82(3).

59. The answer to the question follows linearly from what has been set out above on the general philosophy of the Regulation: no provision is made for automatism and therefore the mere fact that unauthorised disclosure of or access to personal data has taken place due to persons outside the scope of control of the controller does not exempt the latter from liability.

60. In the first place, in literal terms, it should be noted that neither Article 82(3) nor recital 146 lay down any specific conditions which can be fulfilled in order for the controller to be exempted from liability, except by proving that 'it is not in any way responsible for the event giving rise to the damage'. It follows from that wording, first, that the controller may be exempted from liability only if it proves that it is not responsible for the event giving rise to the damage at issue and, secondly, that the standard of proof required by that provision is high, given the use of the term 'in any way', as the Commission has pointed out. [21]

61. The liability regime provided for in Article 82 and, more generally, in the Regulation as a whole, has been the subject of extensive debate in the legal literature of the various Member States. Indeed, it contains not only traditional elements specific to non-contractual liability but also elements which, in the structure of the provisions, bring it closer to contractual liability, or even to a form of strict liability, on account of the risk inherent in the activity of data processing. This is not the place to give an account of the detailed debate but, in my view, Article 82 does not seem to provide a regime of strict liability. [22]

62. Damage resulting from a personal data breach may be the non-intentional consequence of the failure to implement technical and organisational measures that are reasonable and, in any event, appropriate to prevent it, taking into account the risks for the rights and freedoms of persons related to the processing activity. Those risks make the obligation to prevent and avoid damage stricter, by broadening the duty of care on the controller. Therefore, from a coordinated reading of the obligations of conduct placed on the controllers and of the provision relating to the

[21] In accordance with the settled case-law of the Court, according to which exceptions to a general rule must be interpreted restrictively, any exemption from liability provided for in Article 82(3) must be interpreted restrictively. See, by analogy, judgments of 15 October 2020, *Association française des usagers de banques* (C-778/18, EU:C:2020:831, paragraph 53), and of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258, paragraph 40).

[22] Civil liability tends to be regarded as strict liability whenever the agent in question is required to adopt all theoretically possible measures to avoid the damage, irrespective of the actual knowledge that it had or the economic viability of those measures. On the other hand, where an agent is required to adopt measures normally observable by an operator in the economic sector of reference in order to maintain security and prevent damage which may result from the activity carried out, the attribution of that damage tends to move towards a specific fault-based liability regime. Gambini, M., 'Responsabilità', op. cit., p. 1055.

exonerating evidence as regards the infringing party, it is possible to draw an argument in favour of recognising aggravated liability for presumed fault in the case of liability for the unlawful processing of personal data under Article 82 of the Regulation. [23]

63. That gives rise to the possibility for the controller to provide exonerating evidence (which is not permitted in the case of strict liability). As regards the allocation of the burden of proof, Article 82(3) of the Regulation lays down a regime which is favourable to the injured party, by providing for a form of reversal of the burden of proving the fault of the infringing party, [24] in line with the aforementioned reversal of the burden of proof as regards whether the measures implemented are appropriate. The legislator thus shows that it is aware of the risks inherent in accepting a different allocation of the burden of proof; that, if it were to place on the injured natural person the burden of proving the fault of the infringing party, it would place an excessive burden on him or her and thus compromise, in practice, the effectiveness of the compensation protection, in a context of rules linked to the use of new technologies. Indeed, it could be particularly burdensome for the data subject to reconstruct and have access to the manner in which the damage was caused and, consequently, to prove fault on the part of the controller. By contrast, the controller is in the best position to provide exonerating evidence to demonstrate that it is in no way responsible for the event which gave rise to the damage. [25]

64. The controller must also demonstrate, in accordance with the principle of accountability described above, that it has done everything possible to restore the availability and access to personal data in a timely manner.

65. Returning to the referring court's question, on the basis of the foregoing regarding the nature of the responsibility of the controller, although, as mentioned above, the controller may be exempted from liability by demonstrating that the breach was due to a cause for which it was in no way responsible, the mere fact that the event was caused by a person outside its sphere of control cannot be regarded as such.

66. Where a controller is the victim of an attack by cybercriminals, the event giving rise to the damage could be considered as not attributable to the controller, but it cannot be ruled out that the negligence of the data controller was the cause of the attack in question, by facilitating it due to the absence or inappropriateness of the personal data security measures which the latter is required to implement. Those are assessments of fact, specific to each case, which are left to the national court hearing the action to undertake, in the light of the evidence adduced before it.

67. Furthermore, according to common experience, external attacks on the systems of public or private entities which hold a large amount of personal data are far more frequent than internal attacks. The controller must therefore put in place appropriate measures to deal in particular with external attacks.

68. In the last place, from a purposive point of view, it should be noted that the Regulation pursues the objective of providing a high level of protection. In that regard, the Court has already pointed out that as is clear from Article 1(2) of the Regulation, read together with recitals 10, 11

[23] Gambini, M., 'Responsabilità', op. cit., p. 1059. To the same effect, for the view that the proof that it implemented appropriate measures does not consist of a mere allegation of the greatest due diligence, but in the demonstration of a third event giving rise to the damage, having the characteristics of unpredictability and inevitability inherent in unforeseeable circumstances and *force majeure*, see Sica, S., 'Art. 82', in D'Orazio, R., Finocchiaro, G., Pollicino, O., and Resta, G., *Codice della privacy e data protection*, Giuffrè, 2021.

[24] 'If it proves that it is not in any way responsible for the event giving rise to the damage' (Article 82(3)).

[25] M. Gambini, 'Responsabilità', op. cit., p. 1060.

and 13 thereof, that regulation requires the EU institutions, bodies, offices and agencies, and the competent authorities of the Member States, to ensure a high level of protection of the rights relating to the protection of personal data guaranteed in Article 16 TFEU and Article 8 of the Charter. [26]

69. If the Court were to opt for the interpretation that, where the infringement of the Regulation was committed by a third party, the controller should automatically be exempted from liability under Article 82(3), such an interpretation would have an effect incompatible with the objective of protection pursued by that regulation, as it would weaken the rights of data subjects, in that it would limit that liability to cases in which the infringement was due to persons who are under the authority and/or control of that controller.

F. The fifth question referred for a preliminary ruling

70. By its fifth question, the national court asks the Court, in essence, to interpret the concept of 'non-pecuniary damage' (in the wording of the Regulation, 'non-material') for the purposes of Article 82 of the Regulation. In particular, it asks whether the provisions of Article 82(1) and (2) of the Regulation, read in conjunction with recitals 85 and 146 thereof, [27] must be interpreted as meaning that, in a situation where the infringement of that regulation consisted in unauthorised access to personal data and unauthorised disclosure of that data by cybercriminals, the fact that the data subject fears a potential misuse of his or her personal data in the future may in itself constitute (non-material) damage which gives rise to a right to compensation.

71. Neither Article 82 nor the recitals on compensation for damage provide a clear answer to the question, but some elements useful for the analysis can be derived from them: non-material (or non-pecuniary) damage may be the subject of a claim for compensation in addition to material (or pecuniary) damage; it does not automatically follow that the infringement of the Regulation has 'caused' damage or, more specifically, that the breach of personal data 'may cause' physical, material or non-material damage to natural persons; the concept of damage should be interpreted 'in a broad sense' in the light of the case-law of the Court, in such a way as to fully reflect the objectives of the Regulation; compensation for damage 'suffered' should be 'full and effective'.

72. The wording of the provisions of the Regulation already excludes any possible suggestion of self-evident damages: the primary aim of the civil liability provided for by the Regulation is to give the data subject satisfaction through 'full and effective' compensation for the damage suffered and, therefore, to restore the balance of the legal situation which has been negatively affected by infringement of the right. [28]

[26] See, to that effect, judgment of 15 June 2021, *Facebook Ireland and Others* (C-645/19, EU:C:2021:483, paragraphs 44 and 45).

[27] According to recital 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 …'. According to recital 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 Union or Member State law. …. Data subjects should receive full and effective compensation for the damage they have suffered. …'.

[28] See Opinion of Advocate General Campos Sánchez-Bordona, cited above, point 29 and footnote 11. In the same Opinion, the Advocate General rightly concludes his analysis by considering the literal, historical, contextual and purposive perspectives, ruling out the 'punitive' nature of the compensation for damage which data subjects may be entitled to under Article 82 (points 27 to 55), pointing out, first, that Member States 'do not have to choose (nor, in reality are they able to) between the mechanisms for guaranteeing data protection laid down in Chapter VIII. In the event of a breach which does not create harm, the data subject is still afforded (as a minimum) the right to make a complaint to a supervisory authority' and, second, that 'the prospect of obtaining compensation independently of any harm would, in all likelihood, encourage civil litigation, with proceedings that are perhaps not always justified, and, to that extent, could discourage data processing' (points 54 and 55).

73. On the other hand, also from a systematic point of view, as in competition law, the Regulation provides for two pillars of protection: one that is public in nature, providing for penalties in the event of infringements of the provisions of the Regulation, and one that is private in nature, providing indeed for civil liability that is non-contractual in nature, which may be categorised as aggravated for presumed fault with the characteristics mentioned above, including with reference to the exonerating evidence. [29]

74. Therefore, a broad interpretation [30] of the concept of (non-material) damage cannot go so far as to lead to the conclusion that the legislator has waived the requirement for there to be genuine 'damage'.

75. The real substantive issue is whether, once the existence of the breach and the causal link has been established, the mere worries, fears and anxieties suffered by the data subject with regard to a possible misuse of personal data in the future entitle him or her to compensation where such misuse has not been established and/or the data subject has not suffered any further harm.

76. In accordance with settled case-law of the Court, the terms of a provision of EU law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope must normally be given an independent and uniform interpretation throughout the European Union, having regard to the wording of the provision in question, the context in which it is set, the objectives pursued by the act of which it forms part and the legislative history of that provision. [31]

77. The Court, as recalled by Advocate General Campos Sánchez-Bordona, [32] has not drawn up a general definition of 'damage' which is applicable without distinction in any sphere. [33] With regard to non-material damage, it can be inferred from the Court's case-law that: where one of the objectives of the provision being interpreted is the protection of individuals or a certain category of individuals, [34] the definition of damage must be broad; in keeping with that rule, compensation covers non-material damage, even where it is not mentioned in the provision interpreted. [35]

[29] Refusal of the right to compensation for vague, fleeting feelings or emotions connected with the infringement of rules on processing would not therefore leave the data subject without any protection at all (see, to that effect, Opinion of Advocate General Campos Sánchez-Bordona, op. cit., point 115).

[30] See recital 146.

[31] See judgments of 15 April 2021, *The North of England P & I Association* (C-786/19, EU:C:2021:276, paragraph 48), and of 10 June 2021, *KRONE – Verlag* (C-65/20, EU:C:2021:471, paragraph 25).

[32] See Opinion of Advocate General Campos Sánchez-Bordona, op. cit., point 104.

[33] Nor has it stated a preferred method of interpretation, whether autonomous or by reference to national legal systems: it depends on the matter under examination. Compare the judgments of 10 May 2001, *Veedfald* (C-203/99, EU:C:2001:258, paragraph 27), on the subject of defective products; of 6 May 2010, *Walz* (C-63/09, EU:C:2010:251, paragraph 21), on the liability of air carriers; and of 10 June 2021, *Van Ameyde España* (C-923/19, EU:C:2021:475, paragraph 37 et seq.), in relation to civil liability applicable to accidents resulting from the use of motor vehicles.

[34] For example, consumers of products or victims of traffic accidents.

[35] In relation to package trips, see judgment of 12 March 2002, *Leitner* (C-168/00, EU:C:2002:163); in connection with civil liability in respect of the use of motor vehicles, judgments of 24 October 2013, *Haasová* (C-22/12, EU:C:2013:692, paragraphs 47 to 50); of 24 October 2013, *Drozdovs* (C-277/12, EU:C:2013:685, paragraph 40); and of 23 January 2014, *Petillo* (C-371/12, EU:C:2014:26, paragraph 35).

78. While the case-law of the Court permits the argument that, in the terms stated, a principle of compensation for non-material damage exists in EU law, I agree with Advocate General Campos Sánchez-Bordona that it is not possible to infer from this a rule pursuant to which *all* non-material damage, regardless of how serious it is, is eligible for compensation. [36]

79. Relevant in that connection is the distinction between non-material damage for which compensation may be awarded and other *inconveniences arising as a result of abuse of the law* which, owing to their insignificance, do not necessarily create the right to compensation. [37]

80. The Court accepts that difference when referring to trouble and inconvenience as a separate category from damage, in areas where it finds that those items should be compensated. [38]

81. Empirically, it can be observed that any breach of a provision governing data protection leads to some negative reaction on the part of the data subject. Compensation payable as a result of a mere feeling of displeasure due to another person's failure to comply with the law could easily be confused with compensation without damage, which, as mentioned above, does not appear to be compatible with Article 82 of the Regulation.

82. The fact that, in circumstances such as those in the main proceedings, the misuse of personal data is only potential, and not actual, is sufficient for it to be considered that the data subject may have suffered non-material damage caused by the infringement of the Regulation, provided that the data subject demonstrates that the fear of such misuse has actually and specifically caused him or her actual and certain emotional damage. [39]

83. There is undoubtedly a fine line between mere upset (which is not eligible for compensation) and genuine non-material damage (which is eligible for compensation), but the national courts, which have the task of establishing that line on a case-by-case basis, should carry out a detailed assessment of all the elements provided by the data subject seeking compensation, who will have the burden of producing precise, and not generic, evidence actually capable of establishing the existence of 'non-material damage actually suffered' as a result of the personal data breach, without, however, that damage having to reach a predetermined threshold of particular gravity: what matters is that it is not a mere subjective perception, changeable and dependent also on

[36] See Opinion of Advocate General Campos Sánchez-Bordona, cited above, point 105. The Court, for example, has accepted the compatibility with European rules of national law which, for the purpose of calculating compensation, differentiates between non-material damage linked to physical injury caused by an accident depending on the origin of that accident; see judgment of 23 January 2014, *Petillo* (C-371/12, EU:C:2014:26, operative part): EU law does not preclude 'national legislation … which lays down a specific compensation scheme for non-material damage resulting from minor physical injuries caused by road traffic accidents, limiting the compensation payable for that damage in comparison with the compensation allowed for identical damage arising from causes other than those accidents'.

[37] That distinction is visible in some national legal systems as an inevitable corollary of life in society. Recently, in relation to data protection in Italy, Tribunale di Palermo, sez. I civile, judgment 05/10/2017 No 5261, and Cass Civ., Ord. sez VI, No 17383/2020. In Germany, inter alia, AG Diez, 07.11.2018 – 8 C 130/18; LG Karlsruhe, 02.08.2019 – 8 O 26/19; and AG Frankfurt am Main, 10.07.2020 – 385 C 155/19 (70). In Austria, OGH 6 Ob 56/21k.

[38] See judgment of 23 October 2012, *Nelson and Others* (C-581/10 and C-629/10, EU:C:2012:657, paragraph 51), on the distinction between 'damage' within the meaning of Article 19 of the Convention for the Unification of Certain Rules for International Carriage by Air, concluded in Montreal on 28 May 1999, and 'inconveniences' within the meaning of Regulation No 261/2004, for which compensation is payable under Article 7 thereof, pursuant to the judgment of 19 November 2009, *Sturgeon and Others* (C-402/07 and C-432/07, EU:C:2009:716). In that sector, as in the sector for the transport of passengers by sea and inland waterway, to which Regulation No 1177/2010 relates, the legislator was able to recognise an abstract category as a result of the fact that the factor which creates the trouble and the essence of that trouble are identical for all those affected. I do not believe that that inference is possible in relation to data protection.

[39] According to Ireland, those considerations are particularly important in practice, in the context of cybercrime, because if every person affected by a breach – even those affected only to a very limited extent – were entitled to compensation for non-material damage, this would have a significant impact, in particular on public sector data controllers, which are financed by limited public funds that should instead serve collective interests, including the improvement of personal data security (written observations, paragraph 72).

character and personal elements, but actual inconvenience, even slight but demonstrable, to his or her physical or psychological sphere or to his or her personal relationships; the nature of the personal data involved and its importance in the life of the data subject and perhaps also the perception prevailing in society at a given time regarding that specific inconvenience linked to the data breach. [40]

IV. Conclusion

84. In the light of the above considerations, I propose that the Court answer the questions referred for a preliminary ruling as follows:

Articles 5, 24, 32 and 82 of Regulation 2016/679 must be interpreted as meaning that:

the mere existence of a 'personal data breach', as defined in point 12 of Article 4, is not in itself sufficient to conclude that the technical and organisational measures implemented by the controller were not 'appropriate' to ensure the protection of the data at issue;

when verifying whether the technical and organisational measures implemented by the controller of personal data are appropriate, the national court hearing the action must carry out a review which extends to a specific analysis of both the content of those measures and the manner in which they were applied as well as their practical effects;

in the context of an action for damages under Article 82 of the GDPR, the controller of personal data bears the burden of demonstrating that the measures it has implemented are appropriate pursuant to Article 32 of that regulation;

in accordance with the principle of procedural autonomy, it is for the national legal order of each Member State to determine the admissible methods of proof and their probative value, including the measures of inquiry which national courts may or must order, for the purposes of assessing whether a personal data controller has implemented measures which are appropriate pursuant to that regulation, in compliance with the principles of equivalence and effectiveness laid down by EU law;

the fact that the infringement of that regulation which caused the damage in question was committed by a third party does not in itself constitute a ground for exempting the controller from liability and, in order to benefit from the exemption provided for by that provision, the controller must demonstrate that it is not in any way responsible for the infringement;

detriment consisting in the fear of a potential misuse of his or her personal data in the future, the existence of which the data subject has demonstrated, may constitute non-material damage giving rise to a right to compensation, provided that the data subject demonstrates that he has individually suffered actual and certain emotional damage, which is a matter for the national court hearing the action to verify in each individual case.

[40] See Opinion of Advocate General Campos Sánchez-Bordona, op. cit., point 116.