Reports of Cases

OPINION OF ADVOCATE GENERAL
SPIELMANN
delivered on 6 February 2025 [1]

Case C-413/23 P

European Data Protection Supervisor
v

Single Resolution Board

(Appeal – Processing of personal data – Procedure for granting compensation to creditors and shareholders following the resolution of a bank – Obligation to provide information – Article 15(1)(d) of Regulation (EU) 2018/1725 – Failure to inform those creditors and shareholders as regards the recipient of the personal data – Decision of the European Data Protection Supervisor finding an infringement of Regulation 2018/1725 in relation to the processing of pseudonymised personal data)

I. Introduction

1. By his appeal, the European Data Protection Supervisor (EDPS) seeks to have set aside the judgment of the General Court of the European Union of 26 April 2023, *SRB* v *EDPS* (T-557/20, 'the judgment under appeal', EU:T:2023:219), by which the General Court annulled the revised decision of the EDPS of 24 November 2020 ('the decision at issue') concerning five complaints submitted by shareholders and creditors affected by the resolution of Banco Popular Español SA ('Banco Popular') complaining that they had not been informed of the transfer of their personal data.

2. The present case gives the Court of Justice the opportunity to clarify, in the context of pseudonymised data, the concept of 'personal data' and the obligations arising therefrom for the purpose of complying with the obligations of fair and transparent processing of data.

II. Legal framework

3. The main provisions of Regulation (EU) 2018/1725 [2] that are relevant to the present appeal are the following.

[1] Original language: French.

[2] Regulation of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ 2018 L 295, p. 39).

4. Recitals 16 and 17 of that regulation read as follows:

‘(16) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(17) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. The explicit introduction of “pseudonymisation” in this Regulation is not intended to preclude any other measures of data protection.’

5. Article 3 of Regulation 2018/1725, entitled ‘Definitions’, provides, in points 1 and 6 thereof:

‘For the purposes of this Regulation, the following definitions apply:

(1) “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

…

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

6. Article 4 of that regulation, entitled ‘Principles relating to processing of personal data’, provides, in paragraphs 1(a) and 2 thereof:

‘1. Personal data shall be:

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

…

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

7. Article 15 of Regulation 2018/1725, entitled 'Information to be provided where personal data are collected from the data subject', provides, in paragraph 1(d) thereof:

'Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

…

(d) the recipients or categories of recipients of the personal data, if any'.

III. Background to the dispute

8. On 7 June 2017, the Single Resolution Board (SRB) adopted a resolution scheme in respect of Banco Popular on the basis of Regulation (EU) No 806/2014 of the European Parliament and of the Council of 15 July 2014 establishing uniform rules and a uniform procedure for the resolution of credit institutions and certain investment firms in the framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No 1093/2010,[3] approved on the same day by decision of the European Commission,[4] which means in practice that the bank's capital instruments were written down or converted and disposed of by way of a transfer of shares.

9. In accordance with Article 20(16) to (18) of Regulation No 806/2014, the SRB entrusted Deloitte, as an 'independent person',[5] with the task of carrying out a valuation of difference in treatment in order to determine whether the shareholders and creditors, thus affected by the resolution action, would have received better treatment if that institution had entered into normal insolvency proceedings.

10. On 14 June 2018, Deloitte sent that valuation of difference in treatment ('Valuation 3') to the SRB. By a preliminary decision, the SRB stated that, in order for it to be able to take its final decision on whether the shareholders and creditors affected by the resolution of Banco Popular should be granted compensation under Article 76(1)(e) of Regulation No 806/2014, it was launching the right to be heard process, including an initial registration phase, in order to verify the eligibility of the parties expressing an interest, and a subsequent consultation phase, in the context of which the affected shareholders and creditors submitted their comments on the SRB's preliminary decision, to which Valuation 3 was annexed.

11. The data collected during the registration phase, that is to say, proof of the participants' identity and of the ownership of capital instruments of Banco Popular that were written down or converted and transferred, were accessible to a limited number of SRB staff tasked with processing those data in order to determine the participants' eligibility. Those data were not visible to the SRB

[3] OJ 2014 L 225, p. 1.

[4] Commission Decision (EU) 2017/1246 of 7 June 2017 endorsing the resolution scheme for Banco Popular Español S.A. (OJ 2017 L 178, p. 15).

[5] Article 20(1) of Regulation No 806/2014 provides that that person is to be 'independent from any public authority, including the [SRB] and the national resolution authority, and from the entity concerned'. Article 20(16) of that regulation refers to Article 20(1) thereof in respect of that concept of 'independent person'.

staff tasked with processing the comments received in the consultation phase, during which those staff members only received comments identified by reference to an alphanumeric code [6] allocated to each individual comment submitted using the form.

12. Following the aggregation, automatic filtering and categorisation of the comments, the SRB sent to Deloitte [7] the filtered, categorised and aggregated comments relating to Valuation 3. The comments transferred to Deloitte were solely those that were received during the consultation phase and that bore an alphanumeric code, developed for audit purposes to enable the SRB to verify, and if necessary to demonstrate subsequently, that each comment had been handled and duly considered. On account of that code, only the SRB could link the comments to the data received in the registration phase. Deloitte had, and still has, no access to the database of data collected during the registration phase.

13. Affected shareholders and creditors ('the complainants') submitted five complaints under Regulation 2018/1725 to the EDPS on the ground that the privacy statement published by the SRB concerning the processing of personal data did not mention the transmission to Deloitte of the data collected using the form. They alleged that the SRB had infringed its obligation to provide information relating to the processing of personal data under that regulation, laid down in Article 15(1)(d) thereof.

14. The EDPS adopted an initial decision on 24 June 2020, which was annulled following a request for review from the SRB and replaced, on 24 November 2020, by the decision at issue, which is worded as follows:

'1. The EDPS finds that the data the SRB shared with Deloitte were pseudonymous data, both because the comments in [the consultation phase] were personal data and because the SRB shared the alphanumeric code that allows linking the replies given in [the registration phase] with the ones given in [the consultation phase] – notwithstanding the fact that the data provided by the participants to identify themselves in [the registration phase] were not disclosed to Deloitte.

2. The EDPS finds that Deloitte was a recipient of the complainants' personal data under Article 3(13) of [Regulation 2018/1725]. The fact that Deloitte was not mentioned in SRB's [privacy statement] as a potential recipient of the personal data collected and processed by the SRB as the controller in the context of the [right to be heard] process constitutes an infringement of the information obligations laid down in Article 15(1)(d) [of Regulation 2018/1725].

3. In light of all the technical and organisational measures set up by the SRB to mitigate the risks for the individuals' right to data protection in the context of the [right to be heard] process, the EDPS decides not to exercise any of his corrective powers laid down in Article 58(2) of [Regulation 2018/1725].

[6] This consists of a randomly generated 33-digit globally unique identifier.

[7] It is apparent from the decision at issue that Deloitte assisted the SRB as an independent person in its decision-making process. It is also apparent from that decision that, on 18 March 2020, the SRB decided that no compensation was due to the affected shareholders and creditors and stated that that decision was based on Deloitte's post-resolution valuation as well as on the analysis of comments received in the context of the right to be heard process.

4. The EDPS nevertheless recommends the SRB to ensure that the data protection notice in future [right to be heard] processes covers the processing of personal data in both the registration phase and the consultation phase, and includes all potential recipients of the information collected, in order to fully comply with the obligation to inform data subjects in accordance with Article 15 [of Regulation 2018/1725].'

IV. The judgment under appeal

15. By application lodged at the Registry of the General Court on 1 September 2020 and by a statement of modification lodged on 29 January 2021, the SRB brought an action seeking, first, the annulment of the decision at issue and, second, a declaration that the original decision of the EDPS of 24 June 2020 is illegal.

16. The SRB relied on two pleas in law in support of the first head of claim.[8] The first plea alleged infringement of Article 3(1) of Regulation 2018/1725 in so far as the information transmitted to Deloitte did not constitute personal data and the second plea alleged infringement of the right to good administration enshrined in Article 41 of the Charter of Fundamental Rights of the European Union.

17. By the judgment under appeal, the General Court declared that head of claim admissible. As to the substance, it upheld the first plea of the action and annulled the decision at issue without examining the second plea in law.

18. As regards the first plea, the General Court held, first, that the EDPS had considered that the information transmitted to Deloitte 'related' to a natural person within the meaning of Article 3(1) of Regulation 2018/1725 on the basis of a presumption, without examining the content, the purpose or the effect of the information transmitted to Deloitte,[9] in breach of the judgment in *Nowak*.[10]

19. Second, with regard to the condition laid down in Article 3(1) of Regulation 2018/1725 that the information must relate to an 'identified or identifiable' natural person, the General Court held that, in the present case, it was for the EDPS to examine whether the comments transmitted to Deloitte constituted personal data for Deloitte. According to the judgment under appeal, the EDPS merely examined whether it was possible to re-identify the authors of the comments from the SRB's perspective and not from Deloitte's. Therefore, since the EDPS did not investigate whether Deloitte had legal means available to it which could in practice enable it to access the

[8] The second head of claim requested that the original decision be declared illegal. By the judgment under appeal, the General Court rejected that second head of claim for lack of jurisdiction, on the ground that the SRB was, in this way, seeking to obtain a declaratory judgment and not the annulment of an act.

[9] See paragraphs 64, 73 and 74 of the judgment under appeal.

[10] Judgment of 20 December 2017 (C-434/16, 'the judgment in *Nowak*', EU:C:2017:994). In this Opinion, reference will be made, by analogy, to the judgments applying Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) and 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'). As is apparent from recitals 4 and 5 of Regulation 2018/1725 and from Article 2(3) and Article 98 of the GDPR, the EU legislature intended to establish a regime for the protection of personal data by the Union institutions, bodies, offices and agencies which is equivalent to that of the GDPR in order to ensure uniform and consistent protection of natural persons with regard to the processing of their personal data within the European Union (see judgment of 7 March 2024, *OC* v *Commission*, C-479/22 P, EU:C:2024:215, paragraph 43).

additional information necessary to re-identify the authors of the comments, the EDPS could not conclude that the information transmitted to Deloitte constituted information relating to an 'identifiable natural person' within the meaning of Article 3(1) of Regulation 2018/1725. [11]

V. Procedure before the Court of Justice and forms of order sought

20. By document lodged at the Registry of the Court of Justice on 5 July 2023, the EDPS brought an appeal against the judgment under appeal. By order of the President of the Court of 29 November 2023, [12] the European Data Protection Board was granted leave to intervene in support of the form of order sought by the EDPS and, by decision of 20 October 2023, the European Commission was granted leave to intervene in support of the SRB.

21. The EDPS claims that the Court should:

– set aside the judgment under appeal;

– give final judgment in the matter;

– order the SRB to pay the costs of the appeal proceedings and of the proceedings before the General Court.

22. The European Data Protection Board, in support of the EDPS, submits that the Court should:

– set aside the judgment under appeal;

– give final judgment in the matter by confirming the decision at issue.

23. The SRB contends that the Court should:

– dismiss the appeal;

– in the alternative, annul the decision at issue;

– in the further alternative, refer the case back to the General Court, and

– order the EDPS to pay the costs of the appeal proceedings and of the proceedings before the General Court.

24. The European Commission, in support of the SRB, contends that the Court should:

– dismiss the appeal;

– order the EDPS to pay the costs.

[11] See paragraphs 100, 103 and 105 of the judgment under appeal.

[12] C-413/23 P, EU:C:2023:1036.

VI. The appeal

25. In support of its appeal, the EDPS, supported by the European Data Protection Board, puts forward two grounds of appeal. The first seeks to challenge the General Court's interpretation of the concept of 'personal data' within the meaning of Article 3(1) and (6) of Regulation 2018/1725, as interpreted by the case-law of the Court of Justice. The second ground of appeal alleges breach of the principle of accountability laid down in Article 4(2) and Article 26(1) of that regulation.

A. The first ground of appeal

26. The first ground of appeal is divided into two parts. The first part concerns the condition that the information at issue must 'relate' to a natural person and the second concerns the condition that that person must be 'identified or identifiable'.

1. The first part, concerning the question whether the information 'relates' to a natural person

(a) Arguments of the parties

27. The EDPS, supported by the European Data Protection Board, submits that the General Court erred in holding that the EDPS had relied on a presumption concerning the interpretation of the condition that the information transmitted to Deloitte related to a natural person, within the meaning of Article 3(1) of Regulation 2018/1725. In his submission, in the circumstances of the present case, further examination by him was not required.

28. The SRB contends, for its part, that, as the General Court held, the EDPS merely stated that the comments at issue, produced by the complainants during the consultation phase of the right to be heard process, reflected their opinions or views whereas he should have examined whether the information transmitted to Deloitte was linked to a particular person by its content, purpose or effect, as required by the judgment in *Nowak*.

(b) Assessment

29. It should be recalled that the Court has repeatedly held that the use of the expression 'any information' in the definition of the concept of 'personal data' reflects the aim of the EU legislature to assign a wide scope to that concept, which potentially encompasses all kinds of information,[13] not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject.

30. In that regard, information relates to an identified or identifiable natural person where, by reason of its content, purpose or effect, it is 'linked' to a particular person.[14]

[13] See, inter alia, the non-exhaustive list in point 36 of the Opinion of Advocate General Pitruzzella in *Österreichische Datenschutzbehörde and CRIF* (C-487/21, EU:C:2022:1000).

[14] See the judgment in *Nowak*, paragraphs 34 and 35. See, in addition, judgments of 4 May 2023, *Österreichische Datenschutzbehörde and CRIF* (C-487/21, EU:C:2023:369, paragraphs 23 and 24); of 22 June 2023, *Pankki S* (C-579/21, EU:C:2023:501, paragraphs 42 and 43); of 7 March 2024, *OC* v *Commission* (C-479/22 P, EU:C:2024:215, paragraph 45); and of 7 March 2024, *IAB Europe* (C-604/22, EU:C:2024:214, paragraphs 36 and 37).

31. With regard to opinions or assessments, such as the complainants' comments at issue in the present case, it seems to me that a distinction should be drawn according to whether consideration is given to whether those opinions or assessments 'relate' to a person or persons referred to in the text of the opinion or assessment, or whether, as in the present case, it is a matter of determining whether they relate to their author. In the first case, in order to conclude that there is information relating to the person who is the subject of the assessment, it is necessary to analyse whether the content, purpose or effect of the assessment relates to that person. In the second case, by contrast, in order to determine whether the assessment relates to the person who issued it, it seems to me that it could be presumed that this is the case and that an opinion or assessment necessarily relates to its author.

32. Thus, in the judgment in *Nowak*, it was essentially a question of assessing the information contained in an examination script. There were therefore two data subjects: the candidate and the examiner. It is true that the Court examined the content, purpose and effect of the candidate's answers and concluded that they related to him. That said, with regard more specifically to the examiner's comments, which reflect his opinion or assessment,[15] while the Court examined the content, purpose and effect of the information contained in the script in order to conclude that those assessments related to the candidate, it did not carry out such an examination in order to find that they constituted information relating to the examiner who was the author of those assessments.[16] In my view, it cannot therefore be entirely ruled out that a (mere) presumption may apply when assessing whether an opinion or assessment or, as in the present case, a comment, 'relates' to its author.

33. I conclude that, in the absence of proof to the contrary, the comments at issue in the present case, since they emanated from the complainants and showed 'their logic and reasoning', thus reflecting the expression of their 'subjective opinion', necessarily 'related' to those complainants, irrespective of the purpose or effect of their comments.

34. In any event, even in the absence of such a presumption in the present case, I am of the opinion that the comments at issue 'relate' to the complainants by reason of their content, purpose and effect.

35. In that regard, the SRB contends that the arguments based on the purpose and context of the comments at issue are ineffective since they were not examined in the decision at issue, are inadmissible since they contain a new factual allegation and, in any event, are incorrect.

36. I am not convinced by that line of argument. Both the examination carried out by the EDPS in the decision at issue and the General Court's assessment form part of a legal context which was taken into account and which clearly mentions the purpose and effect of the comments at issue, made in the context of the right to be heard process. Those arguments relating to the purpose and effect of the comments at issue are therefore effective and admissible.

37. Moreover, as regards the substance, it is clear from the applicable legal framework that the purpose of the right to be heard process, in the context of which the comments at issue were submitted, was to enable the affected shareholders and creditors to contribute to the process, in particular to enable the SRB to have all the information necessary to take a final decision on whether the shareholders and creditors affected by the resolution of Banco Popular should be granted compensation in accordance with the principle that no creditor should be worse off than

[15] The judgment in *Nowak*, paragraph 43.

[16] The judgment in *Nowak*, paragraph 44 *in fine*.

in the event of liquidation under normal insolvency proceedings.[17] Furthermore, those comments, once taken into account by the SRB, were liable to have an effect on the complainants' interests and rights regarding financial compensation.

38. I conclude on that basis that the comments at issue relate to the data subjects in the present case, including by reason of their purpose and effect.

39. I would add that it is true that the comments at issue, as transferred to Deloitte, were 'filtered, categorised and aggregated', with the result that, as is clear from the facts established by the General Court,[18] individual comments could not be distinguished within a single theme; however, it may be accepted that, even when aggregated, those collective comments, in terms of their content, reflect personal views regarding Valuation 3. They constitute a sum of opinions which, as such, constitute information relating to the persons who expressed them. Their filtering, categorisation and aggregation do not alter that finding, otherwise it would be sufficient, in order to avoid the requirement of information 'relating' to a natural person, to aggregate several points of view. The fact that it is not possible, within that sum of comments, to distinguish the various individual opinions seems to me to fall more within the scope of the second cumulative condition, relating to the identifiability of the data subjects, examined in the context of the second part of the present ground of appeal, than within the scope of the condition requiring the comment to be 'linked' to a natural person.

40. In those circumstances, I am of the view that the General Court's assessment may be regarded as vitiated by an error of law in that regard, inasmuch as it considered that the EDPS had not complied with the examination required by the judgment in *Nowak* in order to conclude that the comments at issue 'related' to natural persons, within the meaning of Article 3(1) of Regulation 2018/1725.

41. If the Court were to decide to reject that first part and were to hold that the pseudonymised comments at issue do not relate to their authors, examination of the second part of the ground of appeal would be superfluous, since, under Article 3(1) of Regulation 2018/1725, that is a necessary condition for the existence of personal data, which is cumulative with the condition that data subjects are identifiable, examined below.

2. The second part, relating to the condition that data subjects are identifiable

42. The EDPS and the European Data Protection Board submit, in essence, that the General Court made two errors, the first concerning the concept of 'pseudonymisation' and the second concerning the interpretation of the judgment in *Breyer*,[19] assertions which the SRB and the Commission dispute.

(a) The first complaint, alleging an error concerning the effects of pseudonymisation

43. This complaint illustrates the existence of two very different approaches to the scope of data protection rules. Should pseudonymised data be included within that scope automatically on the sole ground that the data subjects remain identifiable, irrespective of the accessibility of the

[17] See, to that effect, paragraphs 5 to 7 of the judgment under appeal and point 9 of this Opinion.

[18] See paragraph 23 of the judgment under appeal.

[19] Judgment of 19 October 2016, *Breyer* (C-582/14, 'the judgment in *Breyer*', EU:C:2016:779).

additional identification data, or should it be considered that, following the pseudonymisation process, the data are personal data only for those persons who can reasonably identify the data subjects?

(1) Arguments of the parties

44. The EDPS and the European Data Protection Board submit, in essence, that the pseudonymised data are still personal data for the sole reason that the data subjects remain identifiable since the information enabling them to be identified continues to exist. It is argued that the General Court's approach is incorrect in that it allows pseudonymised data to be regarded as anonymised data vis-à-vis the recipient, which poses a risk to the protection of data subjects and creates confusion between pseudonymisation and anonymisation. Such an approach, which is contrary to the wording and purpose of Regulation 2018/1725, would allow the controller unduly to remove personal data from the scope of EU law relating to the protection of such data.

45. The SRB and the Commission contend, for their part, that pseudonymised data remain personal data for the controller who pseudonymised them, however, for the recipients, it is necessary to examine whether the data subjects are identifiable. Moreover, it is argued that, even though Article 3(1) of Regulation 2018/1725 does not specify who must be able to identify the data subject, in the light of recital 16 of that regulation and in the context of Article 15(1)(d) thereof, which are at issue here, it is the recipient's point of view that matters. According to them, if that recipient does not receive personal data, the data subjects have no interest in being informed about the transfer of data because their rights are not affected.

(2) Assessment

46. At the outset, it is worth recalling that pseudonymisation is processing applied to personal data in order, in accordance with recital 17 of Regulation 2018/1725, to 'reduce the risks' of a data set being correlated with the identity of a data subject and to 'help controllers and processors to meet their data protection obligations'.

47. Article 3(6) of Regulation 2018/1725 thus defines pseudonymisation as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, [which] is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'. [20]

48. Pseudonymisation is therefore not part of the definition of personal data, which are defined by Article 3(1) of Regulation 2018/1725, in the light of the concept of the 'identifiability' of the data subject. Moreover, as the Commission indicated in its statement in intervention, that regulation defines the concept of 'pseudonymisation', thus referring to the process for putting in place a safeguard or technical and organisational measure, but not the concept of 'pseudonymised data'.

[20] See also, in that regard, the opinion on the concept of personal data (Article 29 Working Party, Opinion 4/2007, 20 June 2007, WP 136) and the opinion dealing expressly with anonymisation and pseudonymisation techniques (Article 29 Working Party, Opinion 05/2014, 10 April 2014, WP 216). That process of pseudonymisation is therefore particularly important inter alia in the context of research and statistics.

49. That interpretation is confirmed by a combined reading of Article 3(6) and recital 16 of the abovementioned regulation, the first sentence of the latter provision stating that 'the principles of data protection should apply to any information concerning an identified or identifiable natural person.'

50. Furthermore, recital 16 of Regulation 2018/1725 merits a more detailed analysis.[21] It contains a second sentence stating that 'personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person'. This is followed by the third and fourth sentences, which specify the content of that identifiability requirement.

51. I infer from the wording of those provisions that pseudonymisation leaves open the possibility that the data subjects may not be identifiable, otherwise the wording of recital 16 of that regulation would be pointless. I would add that the final sentences of that recital concerning anonymisation confirm this interpretation: they exclude anonymised data (or data rendered anonymous) from the scope of Regulation 2018/1725,[22] but exclude pseudonymised data from it only in so far as the data subjects are not identifiable. If it is impossible to identify those data subjects, they are therefore legally considered to be sufficiently protected by the pseudonymisation process, notwithstanding the fact that the additional identification data have not been completely erased.

52. In other words, it is not a matter of automatically excluding pseudonymised data from the scope of that regulation.[23] However, in the light of recital 16 thereof, it cannot be ruled out that such data may, under certain conditions, fall outside the scope of the concept of 'personal data'.

53. Contrary to what the EDPS maintains, such an approach does not appear to me to be contrary to the objective of ensuring a high level of protection of personal data, in particular in the light of the identifiability requirements laid down by the applicable provisions, on the one hand, and in the light of their interpretation by the case-law, on the other.

54. First, recital 16 of Regulation 2018/1725 refers to identifiability by the controller 'or by another person': that broad, albeit not unlimited,[24] concept forms part of a protective approach to personal data.

[21] Although they have no binding legal force and cannot form the basis of an interpretation which would be contrary to the objectives pursued by Regulation 2018/1725, the Court has frequently resorted to recitals in interpreting provisions of an EU legal act (see, inter alia, Opinions of Advocate General Szpunar in *Planet49*, C-673/17, EU:C:2019:246, point 71, and of Advocate General Kokott in *Commission* v *CK Telecoms UK Investments*, C-376/20 P, EU:C:2022:817).

[22] Moreover, from a strictly technical point of view, anonymisation does not exclude the possibility of re-identification, which is why controllers implementing anonymisation techniques must regularly analyse the inherent risk of re-identification by assessing the seriousness and likelihood of that risk on a case-by-case basis (see, in that regard, O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant 2020, paragraph 68 and the references cited in that regard, in particular in footnote 162).

[23] While the initial intention of introducing the concept of 'pseudonymisation' into the GDPR was to provide flexibility to reduce data protection obligations (see, in that regard, Kuner, C., Bygrave, L.A. and Docksey, C., 'Background and evolution of the EU General Data Protection Regulation (GDPR)', in Kuner, C., Bygrave, L.A., Docksey, C. and Drechsler, L. (eds), *The EU General Data Protection Regulation (GDPR) - A Commentary*, Oxford University Press, Oxford, 2020, pp. 1 to 47), that intention was not followed by the Council in recital 26 of the GDPR, the wording of which was reproduced in recital 16 of Regulation 2018/1725.

[24] As Advocate General Campos Sánchez-Bordona stated in points 64 to 67 of his Opinion in *Breyer* (C-582/14, EU:C:2016:339), 'it would never be possible to rule out, with absolute certainty, the possibility that there is no third party in possession of additional data which may be combined with that information and are, therefore, capable of revealing a person's identity. … However, I think that that concern – which, moreover, is quite legitimate – must not result in a failure to take account of the terms in which the legislature has formulated its intentions and that a systematic interpretation of recital [16 of Regulation 2018/1725] would be "the means likely reasonably to be used" *by certain third parties*'.

55. Similarly, recital 16 of that regulation states that account should be taken of the means reasonably likely to be used to identify, directly or indirectly, a natural person, taking into account all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments, which constitutes a broad and protective definition of personal data.

56. Second, the interpretation in the case-law of that concept of 'identifiability', which focuses on the risk of re-identification of data subjects, also allows for a broad application of the concept of 'personal data'. Thus, the Court has consistently classified as 'personal data' data which, although dissociated from the identification data held by someone else, could, in the situation in question, give rise to a risk that the data subjects would be re-identified. [25]

57. Thus, it is only where the risk of identification is non-existent or insignificant [26] that data can legally escape classification as 'personal data'.

58. I am not convinced by the arguments of the EDPS and of the European Data Protection Board concerning the dangers arising from an overly strict interpretation of personal data. The fact that the rules stemming from Regulation 2018/1725 do not apply to data relating to non-identifiable persons would not preclude entities that are at the origin of misconduct from incurring legal liability where appropriate, for example in the event of disclosure of data resulting in harm. On the other hand, it seems to me disproportionate to impose on an entity, which could not reasonably identify the data subjects, obligations arising from Regulation 2018/1725, [27] obligations which that entity could not, in theory, comply with or which would specifically require it to attempt to identify the data subjects.

59. In the light of those considerations, if the dispute is analysed with regard to the data as transferred to Deloitte, I am of the opinion that, contrary to what the EDPS maintains, it was necessary to determine whether the pseudonymisation of the data at issue was sufficiently robust to conclude that the complainants, who were the authors of the information transmitted to Deloitte, were not reasonably identifiable. In other words, in that context, if Deloitte had reasonable means to identify those complainants, it could be considered to be processing personal data.

[25] For example, in the judgment in *Breyer*, a dynamic IP address in the hands of an online media services provider, although dissociated from the identification data held by the internet service provider, is classified as 'personal data', since the online media services provider had the means which may likely reasonably be used in order to identify the data subject of that IP address. Similarly, the judgment of 9 November 2023, *Gesamtverband Autoteile-Handel (Access to vehicle information)* (C-319/22, EU:C:2023:837), concerned the VIN of a vehicle, defined as the alphanumeric code assigned to a vehicle by its manufacturer in order to ensure proper identification of that vehicle. Although it is not in itself personal data, that VIN becomes personal as regards someone who reasonably has means enabling that datum to be associated with a specific person (paragraph 46) and thus to be linked to an identified or identifiable natural person (paragraph 49). Again in the same vein, a press release of the European Anti-Fraud Office (OLAF) containing identifiers allowing the appellant to be identified, either on the basis of a simple, objective reading of that press release or by means 'reasonably likely to be used' by one of its readers, constitutes personal data (judgment of 7 March 2024, *OC* v *Commission*, C-479/22 P, EU:C:2024:215). Similarly, in the judgment of 7 March 2024, *IAB Europe* (C-604/22, EU:C:2024:214), the association IAB, which represents undertakings in the digital advertising and marketing sector, had set up a framework for recording the preferences of website users, encoded by means of a 'TC String' (a combination of letters and characters). That TC String was regarded as personal data since, when associated with an identifier, it allows the internet user concerned to be identified, including for IAB, which did not hold the identifying data but could indirectly have access to it by reasonable means (paragraphs 48 to 50 of the judgment).

[26] It follows from paragraph 46 of the judgment in *Breyer* that that would be the case if the identification of the data subject was prohibited by law or practically impossible, for instance on account of the fact that it requires a disproportionate effort in terms of time, cost and manpower.

[27] Reference may be made to the obligations arising from the right to rectification of personal data provided for in Article 18 of Regulation 2018/1725, for example.

60. The first complaint raised by the EDPS should therefore, in my view, be rejected.

(b) The second complaint, alleging an error in the comparison made with the judgment in Breyer

(1) Arguments of the parties

61. According to the EDPS, supported by the European Data Protection Board, the pseudonymised data at issue are personal data for the SRB and, therefore, the obligation to provide information to the data subjects regarding the recipient was incumbent on the SRB. He submits, in essence, that the General Court misinterpreted the judgment in *Breyer* which concerned a different factual situation.

62. According to the SRB, supported by the Commission, by contrast, the comparison with the judgment in *Breyer* is relevant and leads to the conclusion that the obligation to provide information applies only if the data transferred are personal data from the point of view of the recipient, in this case Deloitte, which, they argue, as the General Court correctly held, has not been demonstrated in the present case.

(2) Assessment

63. I am of the opinion that the obligation to provide information, laid down in Article 15(1)(d) of Regulation 2018/1725, and the parallel with the judgment in *Breyer* lead, in the present case, to a solution different from that reached by the General Court, which I will set out in the context of the analysis of the present complaint.

64. Article 4(1)(a) of Regulation 2018/1725 lays down the requirement of lawful, fair and transparent processing of data in relation to the data subject.

65. In particular, Article 15(1)(d) of that regulation provides that, where personal data relating to a data subject are collected from the data subject, the controller is to inform the data subjects, 'at the time when personal data are obtained', of the possible recipients of those data. It thus appears that that information must be provided by the controller immediately, namely at the time when the data are collected. [28]

66. The importance of compliance with such an obligation to provide information is also confirmed by recital 35 of Regulation 2018/1725 which states that the principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes, it being emphasised that the controller should provide any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed. [29]

[28] See, by analogy, judgment of 29 July 2019, *Fashion ID* (C-40/17, EU:C:2019:629, paragraph 104 and the case-law cited). See, also, Opinion of Advocate General Szpunar in *Association Mousse* (C-394/23, EU:C:2024:610, point 58).

[29] See, by analogy, judgments of 1 October 2015, *Bara and Others* (C-201/14, EU:C:2015:638, paragraph 34); of 1 October 2019, *Planet49* (C-673/17, EU:C:2019:801, paragraph 77); and of 11 July 2024, *Meta Platforms Ireland (Representative action)* (C-757/22, EU:C:2024:598, paragraph 57). Recital 36 of Regulation 2018/1725 further states that, 'where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient'. In other words, if a new factor comes to light, it must be brought to the attention of the data subjects prior to that 'further processing' (see, to that effect and by analogy, judgment of 27 April 2022, *Roos and Others* v *Parliament*, T-710/21, T-722/21 and T-723/21, EU:T:2022:262, paragraph 171).

67. Such an obligation to provide information is all the more important since the validity of the consent given by the data subject depends, inter alia, on whether that person has previously obtained the information to which he or she was entitled in the light of all the circumstances surrounding the processing of the data in question, under Articles 14 and 15 of Regulation 2018/1725, and which allows him or her to give consent in full knowledge of the facts. [30]

68. I would add that the only exception to that obligation to provide information, laid down in Article 15(4) of Regulation 2018/1725, concerns the situation in which the data subject already has the information in question.

69. On that basis I conclude that, in the present case, that obligation to provide information is part of the legal relationship between the data subjects, in this case the complainants, on the one hand, and the SRB as controller, on the other, and not part of the relationship between the SRB and the recipient, namely Deloitte. The obligation to provide information therefore concerns the data as held by the SRB before the transfer to Deloitte. It is not disputed that the data in question are personal data, since the SRB holds the comments and the database for identifying the persons who made them.

70. Such an approach from the 'relevant perspective' [31] thus leads me to a different solution from that reached by the General Court, even if I make the comparison with the judgment in *Breyer*.

71. I would point out that, in the dispute which gave rise to the question referred for a preliminary ruling in that judgment, Mr Breyer sought to prohibit the controller (the Federal Republic of Germany) from storing his dynamic IP address. The additional data enabling him to be identified through the IP address attached to his computer was in the hands not of the controller, but of the internet service provider. The question was therefore whether the dynamic IP address held by the controller could be classified as 'personal data' and, accordingly, in the context of the legal relationship between Mr Breyer and that controller, trigger obligations for the latter in terms of storage, even though the data identifying Mr Breyer were in the hands of a person other than the controller. It was held, in essence, that the controller, although not in possession of the additional identifying data, could reasonably have access to it and the dynamic IP address was therefore classified as 'personal data'.

72. In the present case, as recalled above, [32] the obligation to provide information is part of the relationship between the data subjects (the complainants) and the controller (the SRB): it is when the data in question are collected by the SRB and, in particular as regards the information about the recipient, at the latest when that recipient is known, that the obligation to provide information arises. At that particular moment, the data in question are personal data in the SRB's possession, which holds the additional identification data. In the light of the obligation to provide information

[30] See, by analogy, judgment of 11 July 2024, *Meta Platforms Ireland (Representative action)* (C-757/22, EU:C:2024:598, paragraph 60) and point 47 of the Opinion of Advocate General Richard de la Tour in the same case (EU:C:2024:88). See, also, Article 14(1) of Regulation 2018/1725, according to which 'the controller shall take appropriate measures to provide any information referred to in Articles 15 and 16 … relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language'.

[31] In so far as it appears that that approach was not addressed in that way in the written pleadings, I would point out that, apart from the fact that it was raised at the hearing before the Court, that approach falls within the scope of the present dispute in so far as it seeks to determine the relevant perspective with regard to the obligation to provide information at issue in the present case. In that context, although the Court must rule only on the heads of claim put forward by the parties, whose role it is to define the framework of the dispute, the Court cannot confine itself to the arguments put forward by the parties in support of their claims, or it might be forced, in some circumstances, to base its decisions on erroneous legal considerations (see judgment of 21 September 2010, *Sweden and Others* v *API and Commission*, C-514/07 P, C-528/07 P and C-532/07 P, EU:C:2010:541, paragraph 65 and the case-law cited).

[32] See point 69 of this Opinion.

at issue and having regard to the specific point in time at which it arises, the data at issue therefore constituted personal data, irrespective of their identifiability by Deloitte, which is not concerned either by the legal relationship between the complainants and the SRB – the only relationship that is relevant – or by that obligation to provide information incumbent on the SRB.

73. It is in that respect that the parallel with the judgment in *Breyer* must in my view be placed in context in the present case.

74. It follows that the obligation to provide information was incumbent on the SRB as controller and by virtue of its relationship with the complainants, from whom it collected the data at issue, irrespective of whether or not the data as transferred into Deloitte's possession were personal data.

75. The SRB's argument, which was reiterated at the hearing, that the recipient's point of view is relevant because it is important to ascertain whether or not it is a 'recipient of personal data' must, on that basis, be rejected.

76. In that regard, it is true that the wording of Article 15(1)(d) of Regulation 2018/1725, which refers to the 'recipients … of the personal data', may give rise to confusion. However, the effectiveness of that provision requires that the information be transmitted to the data subjects as soon as possible and prior to that transfer of data. [33] In the present case, even though the SRB did not, when initially collecting the comments, intend to seek Deloitte's opinion as to whether those comments changed Valuation 3, it is apparent from the decision that was contested before the General Court that Deloitte assisted the SRB in the context of the right to be heard process. [34] Moreover, the SRB's intention to disclose the pseudonymised data to Deloitte may be considered to have existed at the latest at the time when it was decided to process the comments in question precisely for the purpose of pseudonymising them, [35] otherwise there would be no justification for pseudonymisation.

77. I therefore take the view that to review compliance with the obligation to provide information at the time when the data were transferred by the SRB to Deloitte, by adopting the viewpoint of the recipient in order to classify the data at issue as personal or not, results in the timing of that review being shifted. That review would, as a consequence, be wrongly delayed in that it would be carried out in relation to data already transferred to the recipient, even though the purpose of the obligation to provide information concerns the relationship between the SRB and the complainants and is intended to enable the latter to give their informed consent before the transfer.

[33] With regard to the prior nature of the information in order to enable informed consent, see judgment of 11 July 2024, *Meta Platforms Ireland (Representative action)* (C-757/22, EU:C:2024:598, paragraph 60).

[34] See footnote 7 to point 12 of this Opinion.

[35] See paragraph 13 et seq. of the judgment under appeal. See also the SRB's replies to the questions at the hearing.

78. Moreover, as regards the complainants' consent, their participation in the right to be heard process may admittedly be interpreted as implicit consent to share personal data with the controller with a view to having their comments taken into account. However, that is not sufficient, in my view, to constitute informed consent for the pseudonymisation of the data and their transfer to Deloitte without prior information in that regard from the SRB. [36]

79. It follows that, in my view, the SRB's obligation to provide information applied in the present case prior to the transfer of the data at issue and irrespective of whether or not they were personal data in Deloitte's possession.

80. Therefore, the issue of whether or not pseudonymisation is sufficiently robust and effective, so as to permit a conclusion regarding whether or not the data in Deloitte's possession constitute personal data, ultimately does not seem to me to be *material* with regard to the SRB's obligation to provide information.

81. Consequently, the obligation to provide information, incumbent on the SRB as controller, had to be complied with in the present case and the judgment under appeal must, for that reason, be set aside on the ground of an error of law.

82. Since the point of view of the recipient of the data at issue is not relevant to the obligation to provide information laid down in Article 15(1)(d) of Regulation 2018/1725, the arguments of the parties concerning the possibility for Deloitte to identify, by lawful and practically feasible means, the data subjects are ineffective and there is therefore no need to examine them.

83. If the Court of Justice were not to take that view, I note in the alternative that the EDPS disputes, in that regard, the General Court's finding that Deloitte did not have access to the identification data. He relies, in particular, on the alleged contractual relationship based on controller-processor subcontracting between the SRB and Deloitte. The SRB and the Commission contend that, in so doing, the EDPS raises new factual allegations which are inadmissible at the appeal stage. I agree with that contention. The existence of a contractual relationship between the SRB and Deloitte, which would demonstrate that Deloitte could ask the SRB to identify the complainants, constitutes a new line of argument on which, moreover, the General Court did not in any way rule. It follows that that line of argument should, if necessary, be rejected as inadmissible under the second sentence of Article 170(1) of the Rules of Procedure of the Court of Justice, according to which the subject matter of the proceedings before the General Court may not be changed in the appeal. [37]

[36] With regard to the concise, transparent, intelligible and easily accessible nature of that information, and its formulation using clear and plain language, see Article 14(1) of Regulation 2018/1725. See also the Article 29 Working Party's Guidelines on transparency under Regulation (EU) 2016/679, 11 April 2018, WP 260 rev.01, paragraph 30: 'If the change to the information is indicative of a fundamental change to the nature of the processing (e.g. enlargement of the categories of recipients or introduction of transfers to a third country) or a change which may not be fundamental in terms of the processing operation but which may be relevant to and impact upon the data subject, then that information should be provided to the data subject well in advance of the change actually taking effect and the method used to bring the changes to the data subject's attention should be explicit and effective. This is to ensure the data subject does not "miss" the change and to allow the data subject a reasonable timeframe for them to (a) consider the nature and impact of the change and (b) exercise their rights under the GDPR in relation to the change (e.g. to withdraw consent or to object to the processing).'

[37] See, inter alia, judgment of 29 February 2024, *Euranimi* v *Commission* (C-95/23 P, not published, EU:C:2024:177, paragraph 53).

B. The second ground of appeal, examined in the alternative

84. By his second ground of appeal, alleging breach of the principle of accountability laid down in Article 4(2) and Article 26(1) of Regulation 2018/1725, the EDPS, supported by the European Data Protection Board, submits that the General Court erred in holding that it was for the EDPS to demonstrate that the information transmitted to Deloitte was personal data, in breach of the principle of accountability of the SRB.

85. In the light of the foregoing and in particular points 81 and 82 above, I consider that there is no need to examine the second ground of appeal.

86. I shall therefore address it only briefly and in the alternative.

87. As regards the admissibility, disputed by the SRB, of that ground of appeal, which was not raised as a plea before the General Court, I would point out that an appellant is entitled to lodge an appeal relying on grounds which arise from the judgment under appeal itself and seek to criticise, in law, its correctness. [38] That seems to me to be the case with the present ground of appeal, which is therefore admissible.

88. As to the substance, it should be recalled that the General Court held that, since the EDPS did not investigate whether Deloitte had legal means available to it which could in practice enable it to access the additional information necessary to re-identify the complainants, the EDPS could not conclude that the information transmitted to Deloitte constituted information relating to an 'identifiable natural person' within the meaning of Article 3(1) of Regulation 2018/1725.

89. The EDPS, supported by the European Data Protection Board, submits, in essence, that the General Court should have verified whether the SRB, the controller, had proved that it had anonymised the data at issue vis-à-vis Deloitte.

90. The SRB disputes that line of argument, contending that the principle of accountability applies only where personal data exist and that, in the present case, the data in Deloitte's possession had been anonymised.

91. The Commission, for its part, contends that, first, the EDPS bears a reasonable burden of proving, on the basis of the available evidence, the existence of personal data. Second, it would be for the controller concerned to rebut that finding by submitting further evidence.

92. I would point out that, under Article 4(1)(a) of Regulation 2018/1725, personal data are to be processed lawfully, fairly and in a transparent manner in relation to the data subject. Article 4(2) of that regulation provides that 'the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1'. It thus follows from the principle of accountability, set down in Article 4(2) and fleshed out in Article 26(1) of Regulation 2018/1725, that the controller must be able to demonstrate its compliance with the principles relating to the processing of personal data laid down in Article 4(1) of that regulation. [39]

[38] See judgment of 25 January 2022, *Commission* v *European Food and Others* (C-638/19 P, EU:C:2022:50, paragraph 77 and the case-law cited).

[39] See inter alia, to that effect, judgment of 4 May 2023, *Bundesrepublik Deutschland (Court electronic mailbox)* (C-60/22, EU:C:2023:373, paragraph 53 and the case-law cited). See also, on the burden of proving consent to the processing of data borne by the controller, judgment of 11 November 2020, *Orange Romania* (C-61/19, EU:C:2020:901, paragraph 52).

93. Where the controller provides sufficient evidence to that effect, it may be regarded as having discharged its burden of proof. [40]

94. In the present case, it seems to me that the SRB has relied on several factual elements (including the processes for filtering, categorisation and aggregation of comments, described in the decision at issue and the judgment under appeal) in order to prove, in accordance with the principle of accountability incumbent on it, that it was impossible for Deloitte to identify the data subjects.

95. Before the General Court, the EDPS took a position of principle in that regard, consisting of putting himself in the SRB's position and not Deloitte's and thus classifying the comments transferred to Deloitte as 'personal data'.

96. If it is accepted, for the purposes of the alternative examination of the present ground of appeal, that Deloitte's point of view was relevant in the present case, [41] it may be considered, as the General Court held, that it was for the EDPS to demonstrate [42] for what reason, legal or technical, the pseudonymisation process implemented by the SRB in the present case was not sufficient and should have led to the conclusion that Deloitte was processing personal data.

97. I would therefore be of the opinion that, if appropriate, the judgment under appeal should be upheld as regards that second ground of appeal.

VII. The action before the General Court

98. In accordance with the first paragraph of Article 61 of the Statute of the Court of Justice of the European Union, if the appeal is well founded the Court of Justice is to quash the decision of the General Court. It may itself give final judgment in the matter, where the state of the proceedings so permits, or refer the case back to the General Court for judgment.

99. The first plea in law raised by the SRB against the decision that was contested before the General Court alleges infringement of Article 3(1) of Regulation 2018/1725. It follows from points 63 to 82 of this Opinion that, since the SRB failed to fulfil its obligation to provide information under Article 15(1)(d) of Regulation 2018/1725, the decision at issue should therefore, in my view, be confirmed.

100. By contrast, the second plea in law, alleging infringement by the EDPS of the right to good administration in the context of the procedure which led to the adoption of the decision at issue, does not appear to me to permit final judgment to be given in the matter.

[40] See, by analogy, in the context of an action for compensation based on the GDPR, judgment of 25 January 2024, *MediaMarktSaturn* (C-687/21, EU:C:2024:72, paragraphs 43 to 45): the controller in question bears the burden of proving that the security measures implemented by it are appropriate and the court hearing the action must take into account all of the evidence that the controller provided to demonstrate that the technical and organisational measures adopted by him or her are appropriate with a view to complying with his or her obligations. However, the fact that the employees of the controller provided to an unauthorised third party in error a document containing personal data is not sufficient, in itself, to consider that the technical and organisational measures implemented by the controller at issue were not 'appropriate'.

[41] See points 59 and 60 of this Opinion.

[42] See, in that regard, the comparison made by the Commission with State aid law in the judgment of 12 October 2023, *Larko* v *Commission* (C-445/22 P, EU:C:2023:773, paragraph 29); just as the classification of a given measure as State aid is the precondition for that measure to fall within the Commission's competence to ensure the implementation of Articles 107 and 108 TFEU, in this case the classification as 'personal data' is the precondition for Regulation 2018/1725 to apply and for the EDPS to have competence (see Article 52(3) of that regulation).

101. The SRB maintains in particular that, in the administrative procedure preceding the adoption of the decision at issue, the EDPS infringed its right of access to the file, its right to be heard and the principle of equality of arms by refusing it access to the file, on the one hand, and by not communicating to it the complainants' observations or the content thereof, on the other.

102. The General Court held that, since the first plea of the action had been upheld, it was not necessary to examine the second plea raised before it. Consequently, the state of the proceedings does not permit final judgment to be given on that second plea, which involves, inter alia, factual assessments. I therefore consider that the case should be referred back to the General Court for judgment in that regard, the costs being reserved.

VIII. Conclusion

103. In the light of the foregoing considerations, I propose that the Court should:

– set aside the judgment of the General Court of the European Union of 26 April 2023, *SRB* v *EDPS* (T-557/20, EU:T:2023:219);

– refer the case back to the General Court for judgment on the second plea in law raised before it;

– reserve the costs.