Case Note

The Case Notes section will identify and analyse important judgments that shape the interpretation and application of the EU law in the field of privacy and data protection. If you are interested in contributing, please contact the Case Note Editor Maria Tzanou at m.tzanou@sheffield.ac.uk

The Court of Justice Upholds a Relative Approach to EU Data Protection Law

Case C-413/23 P SRB v EDPS, Judgment of the Court (First Chamber) of 4 September 2025

*Pier Giorgio Chiara**

This case note analyses the judgment of the First Chamber of the EU Court of Justice rendered in an appeal, whereby the European Data Protection Supervisor (EDPS) asked the Court to 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). In the earlier judgment, the General Court annulled the revised decision of the EDPS of 24 November 2020, adopted following the request from the Single Resolution Board (SRB) for review of an EDPS decision concerning five complaints from several complainants. The note discusses the background of the dispute and the findings of the CJEU. It particularly focuses on two key points: first, the 'relative approach' confirmed by the CJEU for determining whether data is considered 'personal'; and second, the practical implications of this approach. It finally sheds light on legislative efforts (ie, Digital Omnibus proposal) to codify recent CJEU case law, particularly with regard to SRB, on the definition of personal data.

I. Facts and Background to the Dispute

On 7 June 2017, the Single Resolution Board (SRB)[1] adopted Decision SRB/EES/2017/08 and placed Banco Popular Español S.A. under resolution, endorsed by the European Commission,[2] provided that the conditions set out by Article 18 Regulation (EU) No 806/2014 (Single Resolution Mechanism Regulation)[3] were satisfied. Following the resolution, the SRB commissioned the advisory firm Deloitte to evaluate the difference in treatment, as provided under Article 20(16) to (18) of the SRM Regulation. This assessment, known as 'Valuation 3', was intended to determine whether Banco Popular's shareholders and creditors would have received better treatment under normal insolvency proceedings than the adopted resolution measures. Deloitte submitted this valuation to the SRB on 14 June 2018. On 6 August 2018, the SRB issued a Notice regarding its preliminary decision on whether compensation should be granted to Banco Popular's former shareholders and creditors, as well as a non-confidential version of Valuation 3. Before adopting a final decision on compensation,

DOI: 10.21552/edpl/2025/4/21

* Pier Giorgio Chiara is Junior Assistant Professor at the Department of Legal Studies and CIRSFID ALMA-AI Research Centre, University of Bologna, Italy. For correspondence: <piergiorgio.chiara2@unibo.it>. This work was supported by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU.

1 The SRB is the EU Agency responsible for the resolution of certain credit institutions.

2 Decision (EU) 2017/1246 endorsing the resolution scheme for Banco Popular Español S.A. (OJ 2017 L 178).

3 Regulation (EU) 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.

SRB invited affected shareholders and creditors to express their interest in exercising the right to be heard.

The right to be heard process had two phases: the 'registration phase', where affected shareholders and creditors provided the SRB with supporting documentation, including proof of identity and proof of ownership of one or more Banco Popular's capital instruments, and the 'consultation phase', where eligible participants – whose status of affected shareholders and creditors had been verified by the SRB following the first phase - submit their comments on the preliminary decision.

On 6 November 2018, SRB sent the participants a unique personal link to an online form, which comprised seven questions on the preliminary decision and the non-confidential version of Valuation 3. The SRB examined the relevant comments on the preliminary decision and asked Deloitte to assess the comments relating to Valuation 3 and to examine whether such valuation was still valid in the light of those comments.

The members of the SRB staff handling consultation comments had no access to the data collected during the registration phase, nor to the individual alphanumeric codes linking comments to identities. Each of the 23,822 comments received from 2,855 participants was assigned a unique 33-digit globally unique identifier randomly generated when the answers were received, enabling comments to be filtered and duplicates removed, leaving 3,730 relevant submissions. These were divided into comments on the preliminary decision, examined by the SRB, and those on Valuation 3, reviewed by Deloitte.

The 1,104 Valuation 3-related comments were securely transferred to Deloitte on 17 June 2019 via a secure SRB-dedicated virtual data server, accessible only to a limited number of Deloitte staff directly involved. Deloitte received filtered, categorised and aggregated comments, with duplicates consolidated so that repeated responses could not be traced to the number of participants making the same comment. Importantly, Deloitte only accessed 'consultation phase' comments with alphanumeric codes, while SRB alone was able to link, via these codes, the comments to the identification data. At no stage did Deloitte have access to participants' personal identification data, including by the time of the appeal judgment.

In late 2019, several affected participants filed five complaints with the European Data Protection Supervisor (EDPS)[4] under Regulation 2018/1725,[5] alleging that the SRB failed to inform them, in the privacy statement, that their data would be transmitted to third parties, such as Deloitte. After examining the case, the EDPS issued an initial decision on 24 June 2020, finding that the SRB had infringed Article 15 of Regulation 2018/1725 by not mentioning Deloitte as a recipient of personal data. Consequently, the SRB was formally reprimanded under Article 58(2)(b).

On 22 July 2020, the SRB requested a review of this decision, contending *inter alia* that the information shared with Deloitte did not constitute personal data. Upon reconsideration, the EDPS revised the initial decision on 24 November 2020. The EDPS concluded that the data transferred to Deloitte were pseudonymous. Deloitte was therefore deemed a recipient of personal data. The omission of this fact from the SRB's privacy statement constituted an infringement of Article 15(1)(d). However, given the safeguards the SRB had in place, the EDPS chose not to impose corrective measures, instead recommending that future privacy notices explicitly cover all stages of data processing and clearly list potential recipients to ensure compliance with EU data protection law.

On 1 September 2020, the SRB brought an action before the General Court seeking annulment of the EDPS's revised decision and a declaration that the initial decision was unlawful. The SRB argued, first, that the data transmitted to Deloitte did not constitute personal data within the meaning of Article 3(1) of Regulation 2018/1725, and second, alleging infringement of the right to good administration under Article 41 of the Charter. The General Court dismissed the second head of claim for lack of jurisdiction, as SRB sought a declaratory judgment rather than annulment. However, it admitted the first head of claim and upheld the SRB's first plea, annulling the contested decision.

In particular, the General Court held that two cumulative conditions must be met for data to be considered personal data: 'first, that information 'relates'

4 The EDPS is the supervisory authority competent with regard to the processing of personal data by EU Institutions, Bodies Offices and Agencies under Regulation 2018/1725.

5 Regulation (EU) 2018/1725 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 ('Regulation 2018/1725').

to a natural person and, second, that that person is 'identified or identifiable''.[6] According to the Court, the EDPS did not examine the content, the purpose or the effect of the information transmitted to Deloitte, in line with *Nowak,*[7] thus he could not conclude that such information could relate to natural persons.[8] With regard to the second condition, the Court held that the EDPS could not conclude that the data received by Deloitte constituted information relating to an 'identifiable natural person', since he did not investigate whether Deloitte had available means to access the additional information necessary to re-identify the authors of the comments.[9] Importantly, the Court clarified that the EDPS would have considered Deloitte's perspective, instead of examining whether re-identification was possible from the SRB's viewpoint.[10]

The EDPS appealed the judgment of the General Court before the Court of Justice. The EDPS, backed by the EDPB, asked the Court of Justice to set aside the General Court's judgment, issue a final ruling, and order the SRB to cover costs. The SRB, supported by the Commission, requested dismissal of the appeal and, alternatively, annulment of the decision or referral back to the General Court, with the EDPS bearing the costs of both proceedings.

II. Judgment

The EDPS raised two grounds of appeal. With the first, the EDPS submitted that the General Court did not interpret Article 3(1) and (6) of Regulation 2018/1725 correctly.[11] This ground is further divided into two parts: the first concerns the condition that the information 'relates' to a natural person, and the second regards the condition relating to the 'identifiable' nature of that person.

The Court upheld the first part of the first ground of appeal. The EDPS contended that Data Protection Authorities cannot be required in every case to analyse the *content, purpose, or effect* of information to determine if it relates to a natural person. In particular, in the present case, the EDPS submitted that it was obvious that the comments 'related to' a natural person, since they expressed participants' personal views.[12] On the contrary, the SRB contended that, by doing so, the EDPS disregarded established case-law, notably *Nowak*[13] and *Österreichische Datenschutzbehörde and CRIF.*[14]

The Court noted that the EDPS necessarily examined the content of the comments to find that those comments reflected the opinions or views of the data subjects. Moreover, as referred to in relevant case-law,[15] the use of the conjunction 'or' linking the abovementioned criteria implies that 'an examination of the content of information need not necessarily be supplemented by an analysis of the purpose and effects of that information'.[16] In line with the *Novak* case,[17] the Court concluded that the General Court erred in law in holding that the EDPS should have analysed the content, purpose, or effects of the comments transmitted to Deloitte to conclude whether they were 'related' to the individuals who made those comments. It was widely accepted that these comments reflected the personal opinions or views of their authors.[18]

The second part of the first ground of appeal consists of two separate complaints. The first one is rejected by the Court as unfounded.[19] The Court considered that the application of Article 3(1) of Regulation 2018/1725 'presupposes in principle, an examination of whether the data subject is identified or identifiable by the information in question',[20] whereas the EDPS held that pseudonymised data, such as the comments transmitted to Deloitte, *always* constitute personal data because there exist information enabling the data subject to be identified.

---

6 Case T-557/20 *SRB v EDPS* [2023] EU:T:2023:219, 59. For a detailed analysis on the case, see *ex multis* G Bonetto, 'Will the Court of Justice Confirm the Relativity of Data Protection Law?' (2025) 11 EDPL 1.

7 Case C-434/16 *Nowak* [2017] EU:C:2017:994.

8 T-557/20 *SRB v EDPS* (n 7), 74.

9 Ibid, 105.

10 Ibid, 103.

11 Preliminarily, the Court notes, in para 52, that the concept of 'personal data' set out in art 3(1) of Regulation 2018/1725 is essentially identical to that in art 4(1) of the GDPR, and therefore must be interpreted in the same way.

12 Case C-413/23 *P SRB v EDPS* [2025] EU:C:2023:986, 45.

13 C-434/16 *Nowak* (n 8), 34 and 35

14 Case C-487/21 *Österreichische Datenschutzbehörde and CRIF* [2023] EU:C:2023:369, 23 and 24.

15 C-434/16 *Nowak* (n 8), 35; Case C-479/22 *P OC v Commission* [2024] EU:C:2024:215, 45; Case C-604/22 *IAB Europe* [2024] EU:C:2024:214, 37.

16 C-413/23 *P SRB v EDPS* (n 13), 56.

17 C-434/16 *Nowak* (n 8), 42-44.

18 C-413/23 *P SRB v EDPS* (n 13), 60.

19 Ibid, 90.

20 Ibid, 69.

In particular regarding the concept of pseudonymised data, as noted by the Advocate General,[21] the Court held that pseudonymisation (i) is not part of the definition of 'personal data'; (ii) presupposes the existence of information enabling the data subject to be identified; and, (iii) aims to prevent the data subject from being identified solely by means of pseudonymised data.[22] This follows from the reading of Article 3(6) of that regulation, as the identifying information must be kept separately and subject to technical and organisational measures (TOMs) 'to ensure that the personal data are not attributed to an identified or identifiable natural person'. Accordingly, provided that the TOMs adopted by the controller are such as to prevent the data from being attributed to the data subject, with the effect that the data subject is not or is no longer identifiable, pseudonymisation may have an impact on whether or not those data are personal.[23]

Moreover, the clarifications set out in recital 16 of Regulation 2018/1725, as to the assessment of whether or not the data subject is identifiable[24], 'would be deprived of any practical effect if pseudonymised data were to be regarded as constituting, in all cases and for every person, personal data'.[25] The Court confirmed such conclusion – that is, pseudonymised data must *not* be regarded as constituting, *in all cases and for every person*, personal data – even where there exists additional information enabling the data subject to be identified, but 'the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice'.[26]

As a consequence, the EDPS erred when he submitted that, considering non-personal data the personal data transmitted to an entity outside the controller would unduly remove such data from the scope of EU law: if it cannot be ruled out that those third parties have means reasonably allowing them to attribute pseudonymised data to the data subject, the data subject must be regarded as identifiable.[27]

Therefore, depending on the circumstances of the case, 'pseudonymisation may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable'.[28] Importantly, the Court clarified that 'another person' referred to in recital 16 refers only to persons who have or may have access to the means reasonably likely to be used for the purposes of identifying the data subject.[29]

The second complaint in the second part of the first ground of appeal concerned the alleged disregard by the General Court of the case-law arising from the *Breyer* case. Thus, according to the General Court, the EDPS should have examined whether the comments transmitted to Deloitte constituted personal data from the recipient's viewpoint. However, according to the EDPS, in line with *Breyer,* 'the mere existence of legal channels potentially enabling identification of the data subject is sufficient to conclude that that data subject is identifiable'.[30] Furthermore, the EDPS contended that, in *Breyer,* the Court assessed whether or not the data subject was identifiable from the controller's perspective.[31]

The Court noted that Article 3(1) of Regulation 2018/1725 does not expressly specify the relevant perspective for assessing the identifiable nature of the data subject, and all the information enabling the identification of the data subject need *not necessarily* be in the hands of one person.[32] Importantly, 'the relevant perspective for assessing whether the data subject is identifiable depends, in essence, on the circumstances of the processing of the data in each individual case'.[33]

In the present case, the Courts held that, to assess whether or not SRB failed to comply with the obligation to provide information to data subjects as per Article 15(1)(d) of Regulation 2018/1725, in particular, regarding potential recipients of the personal da-

21 Case C-413/23 P *EDPS v SRB* [2025] EU:C:2025:59, Opinion of AG Spielmann, 46 and 48.

22 C-413/23 P *EDPS v SRB* (n 13), 71-74.

23 Ibid, 75.

24 […] 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.

25 C-413/23 P *EDPS v SRB* (n 13), 80.

26 Ibid, 82.

27 Ibid, 85.

28 Ibid, 86.

29 Ibid, 87.

30 Ibid, 92.

31 Ibid, 93.

32 Ibid, 99.

33 Ibid, 100.

ta (such as Deloitte), the identifiable nature of the data subject must be assessed at the time of collection of the data, that is, before any potential transfer to a third party,[34] and from the point of view of the controller, irrespective of whether or not those data were personal data.[35] Accordingly, the General Court erred in law in holding that EDPS should have examined whether the comments transmitted to Deloitte constituted, from Deloitte's point of view, personal data to assess whether the SRB had complied with Article 15(1)(d).[36] The Court upheld the second complaint in the second part of the first ground of appeal.

Finally, the Court decided not to examine the second ground of appeal because the first part and the second complaint of the second part of the first ground of appeal were well-founded. Accordingly, the Court set aside the judgment under appeal.[37] However, the Court of Justice gave final judgment as regards the first plea in law raised by the SRB, in particular, by finding that (i) EDPS did not err in law when he found that the comments transmitted to Deloitte constituted information relating to natural persons; and, (ii) as regards the application of the obligation to provide information set out in Article 15(1)(d) of Regulation 2018/1725, the identifiable nature of the data subject must be assessed by putting oneself in the controller's position.[38] The second plea in law cannot be judged by the Court, as it involves factual assessments that were not made by the General Court. The case was then referred back to the General Court so that it could examine that plea.

III. Commentary

This case is of utmost relevance. While it does not depart from existing case-law, it sheds further light on the very core of EU data protection law, that is, what is personal data. In particular, the Court explicitly confirms the relative nature of personal data. Pseudonymised data can be non-personal, for a given recipient, provided that several conditions are met, notwithstanding the opposing views of the EDPS and the EDPB, for which the judgment turned out to be a Pyrrhic victory. Yes, the Court set aside the judgment under appeal and found two complaints of the EDPS well-founded. However, it rebutted EDPS's claim that pseudonymised data always constitute personal data due to the existence of additional information that enables them to be attributed to a particular person[39].

By upholding a relative approach to the notion of personal data, the Court implicitly dismisses the so-called 'absolutist' stance, which essentially considers data to be personal in nature if at least *one party* is able to (re-)identify a natural person from that data.[40] An absolutist approach would thus deprive the test set out in recital 16 of Regulation 2018/1725 and, by extension, that of recital 26 GDPR, of any practical effect if pseudonymised data were to be considered as personal data in all cases and for everyone, as recalled inter alia by the AG.[41]

Unsurprisingly, the mere existence of information enabling identification precludes pseudonymised data from being considered 'in all cases, anonymous'.[42] At the same time, pseudonymised data do not constitute 'in all cases and for every person, personal data'.[43] Pseudonymisation can, 'depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable'.[44]

It follows that pseudonymised data can be considered non-personal by a recipient provided that: (i) the controller adopts TOMs so that the data in question cannot be attributed to the data subject, who is no longer identifiable[45]; (ii) the recipient cannot lift those TOMs, (iii) cannot re-identify the data subject by recourse to other means of identification[46] and (iv) does not puts the pseudonymised data (or 'impersonal', in the wording of the Court) at the dispos-

34 Ibid, 110; Opinion of AG Spielmann (n 22), 69.

35 Ibid, 111-112.

36 Ibid, 115.

37 Ibid, 117-118.

38 Ibid, 120.

39 Ibid, 63.

40 On the 'relative and absolutist debate' in EU data protection law, see M Finck and F Pallas, 'They who must not be identified—distinguishing personal from non-personal data under the GDPR' (2020) 10 International Data Privacy Law 1; G Spindler and P Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 JIPITEC 163; K Hon et al, 'The Problem of "Personal Data" in Cloud Computing: What Information Is Regulated? - The Cloud of Unknowing' (2011) 1 International Data Privacy Law 211.

41 Opinion of AG Spielmann (n 22), 51; C-413/23 P *EDPS v SRB,* 80-82.

42 Ibid, 73.

43 Ibid, 86.

44 Idem.

45 Ibid, 75.

46 Ibid, 77.

al of other persons who have means reasonably likely to identify the data subject.[47]

Regarding TOMs, as in other cases before the CJEU, notably related to (data) security and cybersecurity,[48] one would be disappointed if they expected the Court to set clear standards on which TOMs enable them to meet the Court's test. Thus, the appropriateness (or inappropriateness) of the TOMs put in place is to be assessed *in concreto*,[49] on a contextual basis and through individual cases before courts and DPAs.

With regard to (iii), the Court confirms its established caselaw, notably *OC v Commission*,[50] where it was held that (re-)identification is *not reasonably likely* as it would be prohibited by the law or impossible in practice, for example, because it would involve a disproportionate effort in terms of time, cost and labour, rendering therefore the risk of (re-)identification insignificant.[51]

The implications of (iv) can be more challenging to navigate. According to both *Gesamtverband Autoteile-Handel* and *SRB,* if a recipient of alleged non-personal data, because all of the above criteria are met, shares the data with a third-party who has the means to (re-)identify the data subject (even though the former recipient does not know it), then that non-personal data becomes personal. It follows that the former recipient *might consider* implementing technical and organisational measures to be able to demonstrate that it tried to avoid (re-)identification by others, paradoxically, even if it shared non-personal data. Stalla-Bourdillon argues to that effect that data protection law 'should impose upon both controllers and anticipated data recipients claiming that the data are anonymised for a closed release model an obligation to protect the data against situationally relevant attackers, while the anticipated recipient should be under an obligation not to attempt re-identification'.[52] Against this backdrop, it is clear from *SRB* that data protection rules do not apply to the recipient holding impersonal data. This example may serve as a counterargument to those who claim that, following this ruling, any information that falls outside the definition of 'personal data' can be freely exploited. Another example can be made out of controllers' transparency obligations. As seen in the judgement, the assessment of the controllers' obligation of providing data subjects with information relating to the potential recipients of pseudonymised data, that can turn out to be non-personal for a given recipient, must be made at the time of collection, prior to the transfer of those data to recipients and, more importantly, irrespective of whether or not those data were personal data.

Against the backdrop of the potential erosion of GDPR safeguards following this judgment, it is worthwhile to discuss the implications of *SRB* on the controller-processor contractual relationship. The issue of Deloitte being a processor was raised by the EDPS only in the appeal. As a new factual allegation, this was inadmissible and, therefore, the Court could not assess this new line of argument.[53] After *SRB,* if a data processor receives pseudonymised data from a data controller, and does not have available legal means to (re-)identify the data subjects, it might in fact hold 'impersonal' data. One might derive, therefore, that Article 28 GDPR obligations would not apply as the processor did not receive personal data. However, a possible interpretation against such a carve-out of processors' obligations relies on the fact that the processor acts *on behalf of* the controller.[54] If the processor processes data on behalf of the controller, it could be argued that the relevant perspective to assess the identifiability of data subjects is that of the controller. In turn, the relativistic approach of *SRB* to the notion of personal data would apply when the recipient can be considered a controller in its own right. At the same time, processors receiving 'impersonal' data might, in theory, reuse that non-personal data for other purposes (eg, algorithmic training) without triggering EU data protection rules, notably Articles 5 and 6 GDPR, provided that the data controller specifies that that data might be reused by the processor as part of its information duties.

47 Ibid, 84. See also Case C-319/22 *Gesamtverband Autoteile-Handel (Access to vehicle information)* [2023] EU:C:2023:837, 46-49.

48 Case C-340/21 *Natsionalna agentsia za prihodite* [2023] EU:C:2023:986. See L A Bygrave, 'The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes' (2025) 56 Computer Law & Security Review.

49 C-340/21 *Natsionalna agentsia za prihodite* (n 49), 47; Case C-687/21 *MediaMarktSaturn* [2024] EU:C:2024:72, 38. See S Nusselder, 'Scrutinising the Interplay between Data Protection and Cybersecurity: A Paradox Shrouded Behind the 'State-of-the-Art'' (2025) 11(2) EDPL 150.

50 Case C-479/22 P *OC* v *Commission* [2024] EU:C:2024:215, 51.

51 C-413/23 P *EDPS v SRB* (n 13), 82.

52 S Stalla-Bourdillon, 'Déjà vu in data protection law: the risks of rewriting what counts as personal data' (2025) 26 Privacy and Data Protection 2, 10.

53 Opinion of AG Spielmann (n 22), 83.

54 Art 4(8) GDPR; art 3(12) EUDPR.

IV. Conclusion

Against the background of an ever-encompassing and overstretched interpretation of personal data,[55] the Court holds that the concept of personal data is not 'unlimited', since the data subject must be identified or identifiable. Despite the EDPS (and the EDPB) claiming that the relative approach to the concept of identification would undermine the high level of protection required by the Charter and implemented by the EU legislature,[56] adopting such an approach is not much about reducing the level of protection of personal data but rather is about acknowledging that EU data protection law must meet some limits.[57] Thus, the GDPR's rigid, non-scalable set of obligations would be an unnecessary burden if (re-)identification is *in concreto* not possible for a given party, say, a recipient of pseudonymous data.[58] Whereas such a 'relative' or 'contextual' view of data protection might be welcome by many actors of the processing (not only data controllers), as it reinforces the 'flexible' nature of the data protection legal instruments, such as the GDPR, at the same time, it is susceptible to creating legal uncertainty. Against this backdrop, an SRB-inspired reformed test of the definition of personal data might find legislative expression, considering the recent Commission's proposal for a Digital Omnibus of 19 November 2025.[59] Thus, an amendment to Article 4 GDPR is proposed with a view to clarifying that

> information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.[60]

Interestingly, the Digital Omnibus proposal explicitly acknowledges that the reason behind amending Article 4(1)(a) follows the CJEU's case law concerning the definition of personal data[61], thus hinting inter alia at *SRB.* Several civil society organisations[62] and scholars[63] critiqued this and other relevant amendments[64] as they would endanger the consistency of the EU data protection legal framework and effectively weaken the level of protection, particularly with regard to the hollowing out of the complex and context-based assessment to determine whether data has been deidentified[65], as the draft proposal seemingly adopts a binary approach to anonymisation, or potential safeguards – in terms of purpose or obligations – to be implemented by third-party recipients to prevent re-identification by other parties, as seen above. Awaiting the outcome of political negotiations on the Digital Omnibus file(s), the challenge ahead for DPAs and courts alike will lie in auditing *in concreto* identifiability claims, thus placing a greater emphasis on enforcement, and sanctioning entities where they do not indeed lack means reasonably likely to be used to identify the person.

55 N Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10 Law, Innovation and Technology 1; see also N Purtova and B Clayton Newell, 'Against Data Fixation: Why 'Data' Fails as a Regulatory Target for Data Protection Law and What to Do About It' (2025) Oxford Journal of Legal Studies.

56 C-413/23 P *EDPS v SRB* (n 13), 66.

57 M R Leiser, 'From the law of everything to a system that works: why recalibrating personal data enables, rather than undermines, digital protection (A response to Professor Nadezhda Purtova)' (2026) 60 Computer Law & Security Review.

58 Bonetto (n 7), 127.

59 To optimise and simplify the application and implementation of EU digital rules, the European Commission published a Digital Omnibus package consisting of two proposals. The first (COM(2025) 837 final) aims to amend Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557, and to repeal Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus). The second (COM (2025) 836 final) regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)'. For a detailed analysis on the latter, see M Gartner, 'The Digital Omnibus on AI: First Analysis of the EU's Policy Pivot on the AI Act' (2025) 2(4) Journal of AI Law and Regulation 376-383.

60 Digital Omnibus Proposal, art 3(1)(a).

61 Digital Omnibus Proposal, recital 27.

62 EDRi, 'When data relate to us: The SRB ruling and the erosion of the right to data protection' (2025) <https://edri.org/wp-content/uploads/2025/12/When-data-relates-to-us.pdf> accessed 10 December 2025; noyb, 'Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the Commission' (2025) <https://noyb.eu/en/digital-omnibus-first-analysis-select-gdpr-and-eprivacy-proposals-commission> accessed 10 December 2025.

63 Stalla-Bourdillon (n 53).

64 A new art 41a in the GDPR would grant the Commission the power to specify via implementing acts whether data resulting from pseudonymisation no longer constitutes personal data for certain entities, potentially overstepping data protection authorities' powers: see Digital Omnibus Proposal, art 3(10).

65 See *ex multis* Finck and Pallas (n 41).