Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

DIGITAL OMNIBUS:
PROPOSED CHANGES TO THE DEFINITION OF PERSONAL DATA IN THE EU GDPR
ANALYSED IN THE LIGHT OF THE *SRB* AND EARLIER CJEU JUDGMENTS

1. Introduction

On 19 November, the European Commission issued its Proposal [for] Digital Omnibus Regulation.[1] Among various other matters, this includes proposed changes to the definition of "personal data" in the EU General Data Protection Regulation (GDPR) (and to the same concept in the other EU data protection rules including Regulation 2018/1725).[2] The Commission also issued with these proposals a "Staff Working Document" that explains the thinking behind the proposals.

This brief note sets out the proposed text with the explanation in the Staff Working Document, analyses the relevant case-law, and sets out my (critical) conclusions.

2. The proposed changes

Staff Working Document:

Sub-section 1.2.2.1.: **The definition of personal data**

"*Taking into account the recent case-law of the Court of Justice of the European Union, the proposal clarifies that information is not to be considered personal data for a given entity where that entity does not have the means reasonably likely to be used to identify the natural person to whom the information relates. The proposal further clarifies that an entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679, for the processing of that data.*"

Textual proposals: **Article 4 Definitions, para. 1:** (proposed new text in green)

> For the purposes of this Regulation:
>
> '[P]ersonal 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; **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.**

---

1 https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

2 See the Proposal for a Regulation of the European Parliament and of the Council amending 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 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus). The proposed changes to the definition of "personal data" are set out in Article 3 of this proposal, on p. 54.

3. Analysis

3.1 The case-law

As I have explained in a recent paper (in fact, a slightly edited section from a handbook on the GDPR that I am writing) on the concepts of "data subject", "personal data", "pseudonymous data" and "anonymised data",[3] recital 26 to the GDPR makes clear that a person must be regarded as "identified" or "identifiable", and the data on that person must therefore be regarded and treated as "personal data", not just if the person can be identified from the data by name, but also if she or he can be "**singled out**" from a larger dataset in some way. For instance, the datum 'the man wearing a black suit' "may identify someone out of the passers-by standing at a traffic light".[4] However, in the articles relating to pseudonymisation, including in the very definition of that concept in Article 4(5), the GDPR text refers to "*attribut[ing] [personal data] to a specific data subject*" in a different way, effectively as **identifying a person by name**.

In its recent judgment in the case of *EDPS v. SRB*, the Court of Justice of the EU (CJEU) said in that regard that:[5]

> "[P]seudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of [the GDPR], in so far as pseudonymisation may, 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."

It is not clear whether the Court here refers to "identification" in the recital 26 ("singling out") or Article 4(5) ("identify" by name) sense. But it is important to note that the data at stake in that case were not typical pseudonymised data – that are normally specifically intended to allow linking of different records on the same individual without revealing the full identity of the person (by name).

For instance, in longitudinal medical research, patient data that are (often rather flimsily) pseudonymised are analysed to see if a specific patient (only "identified" in the data set with a patient number) who underwent certain treatment later developed medical issues or complications that could be attributed to the earlier treatment. If the data on the earlier treatment and on the later issues are correlated (which is the whole point), that patient is undoubtedly "singled out" from the other patients in the data set – and should therefore, under the general approach indicated in recital 26, be regarded as "identified".

---

[3] Douwe Korff, The concepts of "data subject", "personal data", "pseudonymous data" and "anonymous data" in the EU GDPR, 11 November 2025, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5734864 (hereafter: "my earlier paper")

[4] The example is taken from Article 29 Working Party, Opinion 4/2007 on the concept of personal data (WP136), adopted on 20 June 2007, p. 13, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
The European Data Protection Board appeared to also endorse this view in its Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, para. 16, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en

[5] CJEU, judgment of 4 September 2025 in Case C-413/23, *European Data Protection Supervisor (EDPS) v. Single Resolutions Board (SRB)*, ECLI:EU:C:2025:645, para. 86.

Similarly, in advertising a flimsy "Mobile Advertising ID" – a unique identifier for the online advertising industry that Google and Apple automatically assign to each phone and that therefore functions as a re-identification code for the supposedly pseudonymised data – allows for the correlation of records including highly revealing location data.[6]

By contrast, the SRB case concerned the collection, by SRB (an EU agency),[7] of comments from shareholders in a bank subject to a preliminary decision by SRB on the effect of that decision on their interests, and the transfer of those comments in aggregated form to the consultancy firm Deloitte for assessment:[8]

> The comments transferred to Deloitte were filtered, categorised and aggregated. Where the comments were duplicates of earlier comments, only one version was transmitted to Deloitte [with an alphanumerical code that related to the comment, rather than to the individual or individuals who submitted the comment]. This meant that individual comments that had been duplicated could not be distinguished within a single theme, and Deloitte was unaware whether a comment had been made by one or more participants in the right to be heard process.

SRB could, via the code and its own database, still link individual comments (including duplicate ones) to individual shareholders who had submitted them. But Deloitte did not have access to that database: **crucially, in the specific circumstances of the SRB case, Deloitte really could not link the data (anonymous comments provided in aggregate only) to any specific individual**.

It is also crucial to note that the Court, in *SRB*, just before the above quoted paragraph, expressly re-affirmed its earlier case-law on identifiability. Specifically, it noted that:

- In its judgment in *OC v. Commission*, it had held that if statements about a person in a press release that did not name the person still "***reasonably enabled*** *the public concerned to* ***identify*** *that person, in particular by combining those statements with information available on the internet*", the information concerned does constitute personal data;[9]

---

[6] See: Ingo Dachwitz & Sebastian Meineck, *Databroker Files: Targeting the EU*, *Netzpolitik*, 4 November 2025, available at: https://netzpolitik.org/2025/databroker-files-targeting-the-eu/
Also: Nicolas Baudoux & Benjamin Verboogen, *Vous n'avez rien à cacher? Tant mieux, car tous vos déplacements sont à vendre en ligne* (*You have nothing to hide? Good, because all your movements are for sale online*), L'Echo, 4 November 2025, available at: https://multimedia.lecho.be/telephone-localisation/ Both articles are based on an investigation carried out by researchers from the Belgian paper, *L'Echo*, the French paper *Le Monde*, German public broadcasters *BR / ARD*, civil society association *Netzpolitik.org*, and Belgian *BNR nieuwsradio*.

[7] See: https://www.srb.europa.eu/en/about On the implications, see the next footnote.

[8] For details, see Part II of the judgment, *Background to the dispute*, paras. 9 – 28. The quote in the text is from para. 27, with the text in square brackets added; that information is taken from para. 28. Since SRB is an EU agency, the case was addressed under Regulation 2018/1725 containing the rules relating to processing of personal data by EU bodies and institutions. However, as the Court rightly noted, Recital 5 to that regulation makes clear that: "*Whenever the provisions of [that] Regulation follow the same principles as the provisions of [the GDPR], those two sets of provisions should, under the case-law of the [Court of Justice], be interpreted homogeneously*". (para. 2). The reasoning of the Court in this case therefore applies equally to the corresponding (often identical) provisions in the GDPR.

[9] CJEU, judgment of 7 March 2024 in Case C-479/22, *OC v Commission*, EU:C:2024:215, paras 52 – 64, summarised in *SRB*, para. 81.

- In that same case, it had also held (with reference to earlier case-law), on the other hand, that the mere existence, somewhere, of information that could be used to identify a person, does not mean that that person is identifiable in the GDPR sense **if** "***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**, for example because it would involve a disproportionate effort in terms of time, cost and labour*";[10]

- In is judgments in *Breyer* and *IAB*, it had held that data that are as such impersonal but that can be linked to a specific individual through information held by a third party should be regarded and treated as personal information ***if the entity that holds the impersonal information has the means to obtain the linking information from the third party in certain circumstances***;[11]

- The Court also recalled, "above all", that it had held in its *Gesamtverband* judgment that "*data which are in themselves impersonal may become 'personal' in nature where the controller puts them at the disposal of other persons who have means reasonably likely to enable the data subject to be identified*." Indeed: "*It is apparent, in particular, from the latter judgment that – where those data are put at their disposal – those data are personal data both for those persons and, indirectly, for the controller.*"[12]

After referencing these cases, the Court held that:[13]

- "*Consequently, in the light of the case-law referred to in the preceding paragraph, the EDPS is incorrect in so far as he submits that the fact that pseudonymised data are not, as the case may be, personal in nature for persons to whom the controller transfers the pseudonymised data makes it unduly possible to remove those data from the scope of EU law on the protection of personal data. According to [the case-law summarized above], that fact [that data has been transferred by a controller to another entity in pseudonymous format] has no bearing on the assessment of the personal nature of those data in the context, inter alia, of a potential subsequent transfer of those data to third parties. Accordingly, in so far as it cannot be ruled out that those third parties have means reasonably allowing them to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal, the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those third parties. In such circumstances, pseudonymised data should be considered to be personal in nature.*"

---

[10] *Idem*, paragraph 51, with reference to earlier case-law. Summarised in *SRB*, para. 82. On the "prohibited by law" issue, see my second critical comments in section 2.2 in the earlier paper.

[11] CJEU judgments of 19 October 2016 in Case C-582, *Breyer*, EU:C:2016:779, paragraphs 44, 47 and 48, and of 7 March 2024 in Case C-604/22, *IAB Europe*, EU:C:2024:214, paragraphs 43 and 48. Summarised in *SRB*, para. 83.

[12] CJEU, judgment of 9 November 2023 in Case C-319/22, *Gesamtverband Autoteile-Handel (Access to vehicle information)*, EU:C:2023:837, paragraphs 46 and 49, summarised in *SRB*, para.84.

[13] *SRB* judgment (para. 3, above), para. 85.

The statement in paragraph 86 of the judgment, quoted above, that "pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725 [or the GDPR]", should therefore clearly not be read as in any way departing from the previous case-law. On the contrary, the Court makes very clear that it sees its reasoning in *SRB* as being fully in line with that previous case-law. In my opinion:

The view of the Court on the question of "identifiability" and "personal data" in previous cases and the SRB judgment, read together, can be summed up as follows:

- **If a set of personal data is "adapted" or "altered" and passed on to another entity in such a format that the recipient really cannot re-identify the data – i.e., cannot "single out" individuals from the data even if not by name (Recital 26) – as was the case in the atypical SRB situation – then those altered data in principle do not constitute personal data for the recipient (as per *SRB*).**

BUT:

- **If the recipient of the altered data has at its disposal means that allow the altered data to be re-identified ("singled out") – as will be the case for typical pseudonymised data sets and indeed is usually the very purpose – then the data should be regarded as personal data also for the recipient of the altered data, even if re-identification has not [yet] happened (as per *Breyer* and *IAB*);**

AND:

- **If the recipient of the altered data (who cannot link the data to specific individuals, even in the recital 26 sense, passes on the altered data to a third party that has at its disposal means that allow the altered data to be re-identified/data subjects to be "singled out", then the data should be regarded as personal data, not just for the third party but also for the recipient of the altered data who disclosed the altered data to the third party (as per *Gesamtverband*).**

If any confusion has arisen in that regard – or if the Court's jurisprudence is deliberately twisted to suggest less restraint in relation to certain altered data – that is in my opinion due to the regrettably unqualified references to "pseudonymised data" in the SRB judgment.

In that specific case the data consisted of aggregated comments with a code attached that linked to each comment (and not to specific comment-submitters); the recipient of those data, Deloitte, really could not re-identify the data subjects (the people who had sent the comments to SRB). The data in the dataset passed on to Deloitte were not typical pseudonymised data.

3.2 Assessment of the proposed changes to the definition of "personal data" in the light of the Court's case-law

In my opinion, the changes to the definition of the concept of "personal data" in the GDPR (and the other EU data protection instruments) are both unnecessary and in conflict with the case-law of the Court of Justice.

CJEU *SRB* judgment, para. 86:	**EU Commission proposed additional sentences to the definition of personal data in Article 4(1) GDPR:**
"[P]seudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of [the GDPR], in so far as pseudonymisation may, 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."	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.

The dictum of the Court is clear: certain altered data (which the Court refers to as "pseudonymised data", but that should here be read as pseudonymised in the rather special SRB-Deloitte situation) may not constitute "personal data" for "persons other than the controller" if those persons (the recipients of the altered data) in the specific circumstances of the case really cannot re-identify the data subjects – which I read in the recital 26 sense, i.e., if those persons/recipients of the altered data are not only not able to identity the data subjects by name, but can also not use the data to link different records to a specific, ("singled out") individual.

Presumably, this is what the first proposed additional sentence seeks to reflect. However, it leaves out the crucial caveat that this only holds true if the recipient of any altered (pseudonymised) data really cannot re-identify the data subjects. **The first proposed additional sentence is therefore misleading by omission.**

The second proposed sentence is even worse: "*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***." The crux is in the latter words (put in bold and underlined). **This directly contradicts the Court's dictum in its *Gesamtverband* judgment, where it held that when even completely impersonal data are put at the disposal of an entity that can link those data to specific individuals, those data do not only become personal data for the recipient but also, "indirectly" for the entity that discloses the data.**

And the third sentence – "*Such information does not become personal for [a receiving] entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates*" – **directly contradicts the Court's ruling in paragraph 85 of its *SRB* judgment (quoted in full in the previous section), read with its other – re-affirmed – earlier case-law**, from which it follows that: If one entity (Entity 1) alters a personal data set (in the way SRB did) and discloses the altered data set to a second

entity (Entity 2) with the alterations being such that Entity 2 really cannot re-identify those data (in my reading: neither in the "re-identify by name" nor in the "singling out" sense) (as was the case for Deloitte in the SRB case), the data do not constitute personal data for that second entity (as they did not for Deloitte in that case). However, if that second entity (Entity 2) passes on the data set to a third entity (Entity 3) and if that third entity does have the means to (re-)identify the data (in my reading: in either sense), then the data clearly become personal data for that third entity, and also, "indirectly" for the second entity.

4. Conclusion

The European Commission believes that:[14]

> **The economic and societal potential of data is enormous**: it can enable new products and services based on novel technologies, make production more efficient, and provide tools for combatting societal challenges. In the area of health, for example, data can contribute to providing better healthcare, improving personalised treatments and helping cure rare or chronic diseases. It is also a powerful engine for innovation and new jobs, and a critical resource for start-ups and SMEs.
>
> **However, this potential is not being realised. Data sharing in the EU remains limited due to a number of obstacles** (including low trust in data sharing, issues related to the reuse of public sector data and data collection for the common good, as well as technical obstacles).
>
> In order to truly capitalise on this enormous potential, it should be easier to share data in a trusted and secure manner.

The "*issues related to the reuse of public sector data and data collection for the common good*" that pose "*obstacles*" to "*the realisation of the [full] potential*" of data clearly (in the view of the Commission) include those pesky EU data protection laws. The proposed amendments to the GDPR are largely aimed precisely at removing those obstacles, including in relation to "research" (which it is proposed should be defined so as to cover purely commercial "research" and "training" of AI models).[15]

The proposed additional "clarifications" of the concept of "personal data" in EU data protection law I discussed above are clearly part of this endeavour. However, as I believe I have shown, although at first glance they appear to be inspired by the recent Court of Justice judgment in *SRB*, in fact they are misleading and in conflict with the overall case-law – and thus in breach of the Charter of Fundamental Rights. They are unacceptable and should be completely withdrawn.

- o – O – o -

[14] European Commission, *Data Governance Act explained*, available at: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained (emphases added)
Although the DGA relates specifically to "protected data" that could not be made available to third parties under the Open Data Directive, including personal data and commercially confidential data, this desire to "open up" the market for the exploitation of data including personal data is clear from the whole raft of digital laws including also the Data Act, the Digital Markets Act, the Digital Services Act and the Artificial Intelligence Act. The Omnibus Proposals make no secret of this aim.

[15] See *nyob's* Mickey Manakas, *Digital Omnibus: major GDPR compliance challenges ahead*, GDPR Today, 27 November 2025, available to subscribers to the GDPR Today Newsletter, accessible here: https://noyb.eu/en/gdprtoday