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

Wool Street House
Gog Magog Hills Estate
Babraham
Cambridge CB22 3AE
United Kingdom
Email: douwe@korff.co.uk

TO: The European Data Protection Board
Brussels
Belgium

DATE: 27 October 2026

RE: Comments on the EDPB Guidelines on anonymisation

Dear Members of the Board –

On 8 July this year, you issued new guidelines on anonymisation.[1]

I recently addressed these guidelines with some critical comments in a wider paper, commissioned by the Swedish law firm **LawGent**.[2] In that paper, I linked the question of what constitutes "personal data" and when data can be regarded "anonymous" to the wider context of AI and in particular the taking of automated decisions based on "profiles". I presented the paper at an initial webinar on 23 October to a selected audience. I attach it and hope the Board will consider it, and more specifically my critical comments on the guidelines, in the consultation. They are contained in section 3, more specifically sub-section 3.2, yet more specifically under the heading "*critical comments*" on pp. 57 – 59. But I hope you will also look at the broader discussion in the paper.

The **LawGent** paper expanded on several earlier papers written by me on the concepts of "personal data", "pseudonymous data" and "anonymous data", in particular:

- 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://ssrn.com/abstract=5734864
- Douwe Korff, 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, 9 December 2025, available at SSRN: https://ssrn.com/abstract=5891404

I also attach these two papers.

---

[1] EDPB, Guidelines 02/2026 on Anonymisation, v.1 for consultation, available at: https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf
The consultation is open until 30 October 2026, see: https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en#no-back

[2] https://lawgent.se/

The main issues addressed in the LawGent paper:

As noted on p. 57 of the **LawGent** paper, my main overall criticism of the guidelines is that they largely fail to relate the proposed criteria for (re-)identifiability – No Record Isolation; No Linkage; and No Inference – to the context of artificial intelligence.

As explained further there, with reference to recent (and earlier) research, it is increasingly recognised that it is becoming well-nigh impossible to avoid re-identification (including especially by inference) from Large Data sets. I hope the Board will address this in its revised guidelines.

I add on p. 58 that, in my opinion:

> The failure of the EDPB guidelines to acknowledge this "death of anonymity" is aggravated by a failure to link their approach to the GDPR requirements relating to automated decision-making (as discussed in section 2.1.v [of the paper]).
>
> In particular, the guidelines suggest (or at least will certainly be read by Big Tech and EU- and state proponents of AI) that if a dataset can be classified as "anonymous" on the basis of the three criteria, that dataset is not subject to the GDPR (or its sister instruments). That is fundamentally wrong.
>
> Rather, if data in a dataset are used to underpin automated decisions on individuals (or to create "scores" that are decisively relied on to take decisions), the data and the algorithms used – the "logic" to use the GDPR terminology – are subject to important data protection rules and safeguards. In particular, the data- and decision subject is entitled to be informed of the fact that this is happening and of meaningful information on the logic used, whereby "meaningful" information must be read as sufficient information to allow for human review of the decision or score and for an effective challenge to the decision (or to the score if it is decisively relied on): see the sub-sections (ea) – (ed) in section 2.1.v(e) [in the paper].
>
> This must be spelled out, with the consequences, in the revised version of the guidelines (to be produced after the consultation on them).

I discuss this further with reference to the example given in the guidelines to the denial of a bank loan by a bank, on the remainder of p. 59.

One further issue: "lawful means"

As the EDPB notes:[3]

> The CJEU has stated that means do not need to be considered if, in reality, the likelihood of their use is insignificant because they are prohibited by law.

This was in fact one of my main points of criticism of the Court's *dicta* in this regard in my November 2025 paper:[4]

> [T]he suggestion that the "means reasonably likely to be used" by someone obtaining access to pseudonymised data do not cover unlawful means must be seen as specific to the *Breyer* case, which concerned the transmission of identifying data by an internet service provider to online media services – which was allowed only under special legal rules. In my opinion,

[3] *Idem*, para. 32, on p. 13, with reference to the CJEU cases C-582/14 *Breyer v Bundesrepublik Deutschland*, para 46, C-479/22 P *OC v European Commission*, para 51 and C-413/23 P *EDPS v SRB*, para 82.

[4] My November paper (referenced in the text, above, on p. 1), p. 9.

> the uncritical and unqualified repeating of that phrase in *OC* and *SRB* is wrong: as Chris Pounder pointed out in relation to a UK case, *DSG Retail*, in which credit card details were stolen, but without the names and details of the card holders, it would be absurd to hold that the hacker would not be "reasonably likely" to also use unlawful means to obtain the card holders' details (typically, from the "dark web") and thus re-identify the data (and carry out fraud).[5]

I am pleased that the Board recognised this too (albeit it in less strident terms). It said (with reference to the above-mentioned cases of *Breyer*, *OC* and *SRB*):[6]

> It should be noted that these cases involved actors who were properly limited by the rule of law, so that the law effectively prevented the use of the means in question. Indeed, we can generally assume that people will follow the law. However, there may also be cases where illegality does not provide any meaningful barrier to identification, because the entities involved will not actually be restricted by this prohibition.
>
> The general assumption that people will follow the law can, therefore, be rebutted if there is sufficient evidence of a concrete risk that unlawful means are nevertheless reasonably likely to be used. The assessment of this risk should consider, in particular, evidence that the prohibition in question is not respected by the entities involved. Relevant factors may include, but are not limited to:
>
> - evidence that the legal prohibition is not effectively monitored, enforced and sufficiently dissuasive;
> - evidence that the gains from breaking the legal prohibition might outweigh costs, effort and potential risks of doing so;
> - evidence of a situation where data relevant for re-identification (i.e. both the given and, potentially, the additional data useful for re-identification) is especially vulnerable to illegal access using the prohibited means, due to a lack of protection; and
> - evidence that the prohibition has previously been breached or circumvented in comparable situations.

The Board gives as an example a media company that has out-of-date network security and where there is therefore a risk that sensitive data held by the company may be intercepted or hacked by "unintended receivers of the data" that can include "entities located outside the scope of applicable Union and Member State law, not effectively bound by such laws prohibiting unauthorised access"[7] (in my view, clearly a reference to US and other third countries' intelligence agencies). It concludes that:

> Since the media company's out-of-date security measures mean that those third parties could also likely hack into the media company's servers, these unintended receivers of the data would be able to access the privileged information and therefore re-identify the individuals through means reasonably likely to be used. The shared information would not, therefore, be considered anonymous from their perspective.

---

[5] See Chris Pounder's blog at https://amberhawk.typepad.com/ for 23/10/2024, "*Upper Tribunal undermines data breach reporting under the UK_GDPR?*". [original footnote]

[6] EDPB, Guidelines 02/2026 on Anonymisation, v.1 (footnote 1, above), paras 32 – 33, on p. 13.

[7] *Idem*, Example 8 in para. 33, on p. 14.

I am pleased that the Board has confirmed that from the point of view of EU law, data illegally obtained by hackers who can (equally illegally) identify or re-identify the data subjects *are* personal data and the hackers are subject to the GDPR: just because the obtaining of the data is prohibited by law – and contrary to the suggestion in the Court's *dicta* – it does not mean that the data are outside the GDPR and the hackers can act with impunity.

But again, I feel that the guidelines do not yet sufficiently recognise that at a time when AI can be used to identify "zero-day" vulnerabilities – as worryingly demonstrated in the PHP case – the likelihood of unlawful access to data is massively increased.

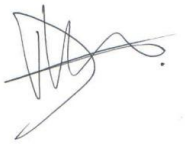
Moreover, criminal- and foreign intelligence service hackers will also often have the means to re-identify individuals from supposedly anonymised data – either by inference or by linking the stolen data to other stolen data.

This is yet another reason why "anonymisation" should not become a means for controllers – and especially developers of Large Data AI models – to evade European data protection law.

In my opinion, the first version of the guidelines does not sufficiently recognise the above problems (both as discussed in my **LawGent** paper and as discussed above).

I hope this will be rectified in the revised version of the guidelines.

Yours sincerely –



Douwe Korff (Prof.)

Attached:

Douwe Korff, The (ab)use of personal and supposedly anonymised data to train AI models including General-Purpose AI (GPAI) models: A warning, paper produced for the Swedish lawfirm **LawGent**, October 2026.

As well as the two papers I produced in, respectively, November and December last year, referenced on p. 1, above.