SHOOSMITHS

Draft response the European Data Protection Board (EDPB) on the draft Guidelines 01/2025 on Pseudonymisation, adopted on 16 January 2025.

We are greatly appreciative of the work carried out by the European Data Protection Board (EDPB) in its draft Guidelines 01/2025 on Pseudonymisation adopted on 16 January 2025 (“Guidelines”). As the first dedicated draft guidance on pseudonymisation, it offers some valuable new concepts and insights into the benefits and risks of pseudonymisation techniques, many of which are being actively explored by our clients across different sectors.

While many of the concepts and examples are useful and will certainly help inform advice on practical approaches to project design, there are in our view four important areas where further clarification would be appreciated. These are set out below.

(Throughout, *italics* have been added by us for emphasis and are not part of the Guidelines.)

The role of legitimate interests in pseudonymisation

Under paragraph 55 of the Guidelines, the EDPB notes: “In the case of processing based on the legitimate interest provision in Art. 6(1)(f) GDPR, controllers other than public authorities in the performance of their tasks may consider the reduction of the risks to the rights and freedoms of the data subjects achieved by pseudonymisation (as by any other effective safeguard). This may be the case when assessing whether their legitimate interests are overridden by the interests of the fundamental rights and freedoms of data subjects. The use of pseudonymisation for this purpose is illustrated in Example 7 in the Annex.”

This is not necessarily a position on which all would agree, and is not well established as a principle. The note to this paragraph cites WP opinion 06/2014 in support, which unfortunately is no longer available on the EDPB website. It is also notable that pseudonymisation is cited in the GDPR as a mitigating factor in relation to purpose compatibility (Art 6(4)) but not in relation to legitimate interests (Art. 6(1)).

Pseudonymisation is also not discussed in the recently issued draft EDPB Guidelines 1/2024 on processing based on legitimate interests. These, however, note that: “mitigating measures can, for instance, not consist of measures meant to ensure compliance with the controllers’ information obligations, security obligations, obligations to comply with the principle of data minimisation, or the fulfilment of data subject rights under the GDPR, and must go beyond what is already necessary to comply with these legal obligations under the GDPR.” Pseudonymisation techniques would seem to fall naturally within these prohibited categories. It is also notable that the positive examples of mitigating measures given are all related to extension of data subject rights, not to techniques for ensuring the security of data.

It is especially important to weigh the possible effects of treating pseudonymisation as part of a legitimate interests balancing test when pseudonymisation techniques may pose a risk as well as a benefit, given the risks of unauthorised linking through consistent identifiers.

We suggest that an approach more consistent with existing law and guidance would be to limit possible uses of pseudonymisation to Article 6(4) (purpose limitation), Article 25 (data protection by design) and Article 32 (security of processing), and to remove the reference to Article 6(1)(f) in this section, except in the context of national laws, as per paragraph 54.

Assessment of lawful basis in the use of pseudonymisation

Paragraph 23 of the Guidelines say: ”Pseudonymisation is a technical and organisational measure that allows controllers and processors to reduce the risks to data subjects and meet their data-protection obligations, for example under Art. 25 or 32 GDPR. Therefore, if a controller processes personal data and applies pseudonymisation in the process, then the legal basis for the processing of the personal data extends to all processing operations needed to apply the pseudonymising transformation.”

This rather general proposition is difficult to reconcile with paragraph 34, which says “all processing operations mentioned in this section (including data set linkage) will need to be executed in compliance with the GDPR, in particular observing all data protection principles according to Art. 5 GDPR, and,

+44 (0) 3700 863 000 | www.shoosmiths.com

Shoosmiths is a trading name of Shoosmiths LLP, a limited liability partnership registered in England and Wales (registered number OC 374987). Shoosmiths LLP is authorised and regulated by the Solicitors Regulation Authority (SRA ID 569065). We use the word partner to refer to a member of Shoosmiths LLP, or an employee or consultant who is a lawyer with equivalent standing and qualifications or a non lawyer who has met the firm’s stringent promotion criteria. A list of members’ names together with a list of non members who are designated as partners, is available for inspection at our registered office at 100 Avebury Boulevard, Milton Keynes. MK9 1FH.

BSI UKAS QUALITY MANAGEMENT 003

Certificate No. FS 31466

especially, need to rely on a legal basis according to Art. 6 GDPR." There are further examples of this more qualified approach in the Guidelines, such as note 10, which says that linking "may be lawful only under certain conditions", without further specification.

Given the increasing use of pseudonymisation as a technique to enable linking as well as to reduce the risks of re-identification, the position on lawful basis might benefit from further refinement. In particular, the following clarifications would be helpful:

- clearly distinguishing between pseudonymisation used as a security measure, where indeed it would be helpful to clarify that a controller does not need a further lawful basis for processing (as per paragraph 23) and processing which enables linking, where they presumably do (as per paragraph 34);
- setting out in fuller detail when the placement of consistent identifiers may constitute a separate processing purpose. Paragraph 117 (a partial repeat of 116) goes some way to addressing this: "The use of such pseudonymisation is admissible if and only if the linking of different pieces of pseudonymised data relating to the same person may become necessary and will be lawful in this case. This condition is often fulfilled if there is only one common purpose, or the various purposes are compatible." However, the proposition is not entirely clear and would benefit in our view from further examination;
- discussion of lawful basis when consistent identifiers are placed by a controller for future use by *another* entity within the pseudonymisation domain.

Understanding the breach test in the context of pseudonymisation

Paragraphs 62 and 81 are somewhat inconsistent and it would be helpful to clarify them for practitioners. The test for breach notification for the purposes of Articles 33 and 34 set out in paragraph 81 is characterised as depending on the risks to data subjects posed only as a *result* of reversal (that is, based on the sensitivity of the data), rather than the *likelihood* of reversal (that is, based on the effectiveness of the pseudonymisation process), which is the test set out in paragraph 62. On the assumption that both these tests may be relevant it would be helpful to clarify this and align these two paragraphs.

Any further elucidation of the tests which the EDPB is able to give would be helpful in view of the extreme practical importance of this issue for controllers. This is especially the case since pseudonymisation is only briefly addressed in EDPB Guidelines 9/2022 on personal data breach notification, which notes at paragraph 112 that "pseudonymisation techniques alone cannot be regarded as making the data unintelligible".

Definition and scope of the "pseudonymisation domain"

The concept of the pseudonymisation domain is potentially powerful but we foresee that it may be difficult to apply confidently in practice because of the over-flexible definition.

The domain may be a limited set of people within controller control or purview, for example they may be "recipients bound by a common purpose" (Executive Summary at section 9); or they may be actively selected by the controller as described at paragraph 48: "the pseudonymising controller sets up the pseudonymisation domain".

In other contexts, the domain includes *everyone* outside what might be called the "attribution domain". This approach is suggested for example at paragraph 10: "The guidelines introduce a new concept, called pseudonymisation domain, to capture one aspect of that freedom: to determine *who should be precluded from attributing the pseudonymised data to individuals"* (which presumably is anyone not holding the attribution information and authorised to do so). Another example of this approach is in the glossary: "Environment in which the controller or processor wishes to preclude → attribution of data to specific data subjects".

A third approach is to include in the domain possible unauthorised third parties such as third country controllers subject to legal obligations incompatible with the GDPR.

The flexibility is not only acknowledged in the Guidelines, but choice over the extent of the domain is given to the controller, as discussed at paragraphs 36 to 38. Furthermore, the choice is dependent on "the objective of pseudonymisation and [the controller's] risk assessment". This might be seen as a rather wide discretion, given that the concept of the domain is linked to clear controller obligations. For example at paragraph 40: “Controllers that process pseudonymised data should also put in place such measures to ensure that actors *within the pseudonymisation domain* are not able to reverse the pseudonymisation”. In conclusion, it seems to be up to controllers to determine what the “useful” extent of the domain is, which may encourage over-confident use of pseudonymisation techniques on the assumption that the risk of unauthorised re-identification does not need to be considered.

Further consideration of the definition and scope of the pseudonymisation domain would therefore be welcomed. One possible approach would be to distinguish between (say) the “active pseudonymisation domain” (characterised by a defined set of people within controller control or purview, who should be subject to contractual controls, for example) and the “passive pseudonymisation domain” which would be the world at large, and might include third country recipients and unknown malicious actors. This would give controllers wishing to design compliant projects, and those advising them, greater confidence in their understanding.

Shoosmiths LLP

February 2025