BUSINESSEUROPE

COMMENTS

14 March 2025

High-level feedback to the European Data Protection Board's Public Consultation on Guidelines on Pseudonymisation

BusinessEurope appreciates the opportunity to react to the European Data Protection Board's (EDPB) Guidelines 01/2025 on pseudonymisation. We are supportive of the EDPB's initiative to provide further clarity on critical aspects of the General Data Protection Regulation (GDPR). Regrettably, the Guidelines in question raise a lot of questions than they answer.

Given the insufficient time to respond to the Guidelines consultation, we limit our contribution to a few essential elements from the draft document, which require more consideration in order to render the guidelines fit for future application. We note that effective and clear pseudonymisation guidelines must be the objective as these could help, for example, GDPR compliant training of AI models; boost the pooling of data across sectors to advance EU initiatives like different data spaces; help more effective pseudonymisation in the e-commerce domain, etc.

Pseudonymised data and personal data, pseudonymisation domain modalities

- There is a confusion in the reader related to the statement in the Guidelines that pseudonymised data is always personal data as concluded by the EDPB. It is unclear if the EDPB had considered this conclusion's relativity to the AG Opinion to *Case C-413/23 P*, which states that pseudonymised data "under certain conditions would fall outside the scope of the concept "personal data".
    - We invite the EDPB to deliberate further on the available and expected jurisprudence and seek advice[1] and opinion by a broad pool of (technical) experts in order to provide further clarity on this matter in the updated guidelines.

- Actors in the "pseudonymisation domain" should not be able to attribute data to a data subject. From the GDPR, it follows that the "additional information" (e.g. pseudonyms) that renders the data subject identifiable, is generated by the pseudonymising controller, and this is the "additional information" that must be kept separate when processing pseudonymised data.
    - It is unclear why the Guidelines are asking the pseudonymising controller to take into account additional information that is not in the "immediate control of the pseudonymising controller or processor" (§21), and what is the legal basis for such extension[2] of obligations.

- There's confusion as to the pseudonymisation and anonymisation efforts by the controllers, especially if the Guidelines continue to follow its restrictive approach. For example, paragraph 22 suggests that pseudonymised data can become

[1] This invitation to seek advice is not to be understood in conflict with Article 69, GDPR. It should not amount to an instruction.
[2] Recitals 26 and 29 of GDPR do not expressly put the controller in that position.

anonymised data, if the conditions for anonymity are met (i.e. the data subject is no longer identified or identifiable, Recital 26 GDPR). But if the parties in the pseudonymisation domain must not be able to attribute the data to a data subject because the pseudonymising controller had addressed the risks to prevent such attribution, hence it follows that the data is anonymous relatively to those parties participating in the domain, and would this be then a pseudonymisation domain?
    - The updated guidelines need to address clearly this confusion, in order to facilitate the controllers when assessing whether the GDPR is applicable or not.

- The EDPB suggests that the pseudonymising controller could *on purpose* identify and allow non-legitimate data recipients to be part of this pseudonymisation domain (§37), so it is possible for the pseudonymising controller to mitigate the adverse effects of an unauthorized access by those recipients. Paragraph 42 even mentions that "relevant third parties" could be not only cyber-crime actors, but also employees with ill-intent, etc. Opening the pseudonymisation domain to such *relevant third parties*, essentially invites for a data breach.
    - We invite the EDPB to seriously re-consider this idea, and its relativity to increasing trust between controllers and data subjects whose data will be pseudonymised.

- Additionally, even if one assumes that the pseudonymising controller does decide voluntarily to include non-legitimate data recipients (e.g. "white hats") for the sake of mitigation measures identification and application, the controller is still not able to identify or mitigate "all" possible unauthorized access by all possible non-legitimate actors (not to mention that it is impossible to include "all" of them in the domain - §42). Therefore, §43 ("all means available […] to be considered") goes beyond the GDPR legal basis ("all the means reasonably likely") and is inconsistent with wordings earlier in the same guidelines, aligning with the main legal text on this specific matter.
    - We trust that it is not the EDPB's intention to add disproportionate obligations to the pseudonymising controller, which would inhibit the use of pseudonymisation as a technique all together.

In conclusion, lack of clarity and mismatches between the main legal basis and some of the conclusions in EDPB guidelines would have more detrimental effect on innovation impetus of businesses in Europe and add burden to the already overly complicated regulatory landscape in the digital domain.

We therefore take the opportunity to invite the European Data Protection Board to further reflect on its role of ensuring the consistent application of the General Data Protection Regulation (especially via the tool of guidelines) and its main objective of balance between fundamental rights protection and rules relating to free movement of personal data.