To The European Data Protection Board

DANSKE
UNIVERSITETER
UNIVERSITIES DENMARK

FIOLSTRÆDE 44, 1. TH
1171 KØBENHAVN K
TLF. +45 33 36 98 00
WWW.DKUNI.DK

Public consultation reference: 01/2025
Comments to "Guidelines 01/2025 on Pseudonymisation Adopted on 16 January 2025"

Universities Denmark hereby send our comments to the proposed "*Guidelines 01/2025 on Pseudonymisation*" adopted on 16 January 2025 (hereinafter referred to as the "Guidelines").

Universities Denmark have keenly anticipated the publication of these Guidelines, and we would like to express our appreciation for the effort undertaken by EDPB in formulating the Guidelines. We trust that the comprehensive approach will help address many of the challenges related to pseudonymisation.

By way of introduction, Universities Denmark is an organization of the eight Danish universities, which work to enhance their cooperation, visibility and impact. Universities Denmark has established a General Data Protection Regulation working group (hereinafter referred to as the "GDPR Working Group") as a subcommittee, which is tasked with providing the basis for universities to ensure data protection in research, education programs and day-to-day administration. This includes influencing the universities' current agendas within the EU General Data Protection Regulation[1] and related areas.

The following comments on the Guidelines have been drafted by the GDPR Working Group.

Considerations of actions with a criminal intent in the pseudonymisation process

The Guidelines' clause 2.3, paragraphs 35-43 discuss the concept of the "pseudonymisation domain," which we understand as the context in which pseudonymised

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter referred to as the "GDPR").

data cannot be attributed to specific data subjects. Controllers can define this domain based on a risk analysis, ensuring that additional information enabling attribution is kept separate. The pseudonymisation domain may include legitimate recipients of the data, as well as those who may attempt unauthorized access. Controllers and processors should implement technical and organizational measures to ensure that pseudonymised data remains within the domain and cannot be reversed. Measures should also address the risk of attribution by unauthorized third parties, including employees or service providers. Pseudonymisation may be performed before transmitting data to ensure appropriate security levels for the risk involved.

We acknowledge that proper and effective pseudonymisation should prevent unauthorised use and attribution of data and that such considerations are necessary. In research collaborations the parties will often – and it can be compulsory in Denmark according to national legislation – enter into a written collaboration agreement containing both the practical and the legal framework for the research collaboration. Such agreements include analysis of the parties' roles from a data protection perspective and a suiting "Personal Data"-clause or something similar also to ensure unathorised use etc.

If, for example, the collaboration includes two separate data controllers, and the research project involves transfer of personal data from one of the controllers to the other data controller, the typical "Personal Data"-clause of the collaboration agreement will often contain the terms and conditions for the transferring as well as the receiving party's processing of the personal data. Typically, in such cases, it is stated that the receiving party obliges not to try and reverse/link the transferred pseudonymised data, and that both parties ensure the proper handling, safety, and technical and organizational measures for processing the data, including proper instructions to the involved personnel, for the stated purposes of the research collaboration. So, on top of an effective pseudonymisation, there is also a contractual framework alongside the ethical guidelines related to the research governing the processing of the data, which is subject to the enforcement provisions of the agreement.

Thus, in our view, such contractual obligations between the parties may generally provide a necessary guarantee for an appropriate level of security, since the data controller has conducted a general risk assessment, including the recipient, and assessed that:

- data shall be shared in pseudonymised form using a suitable pseudonymisation method,
- the 'key' to the pseudonymised data will not be shared with the recipient,
- the recipient declares through the contractual obligations that they will not attempt to identify the data subjects,
- other necessary measures pursuant to the GDPR article 32-assessment are imposed on the recipient through the contract.

It is stated in paragraph 42 of the Guidelines that the pseudonymisation domain can include "*unauthorised third parties*" and that the "*means they are reasonably*

likely to use for attribution" should be assessed. It also follows that such relevant third parties include both cyber-crime actors, employees or maintenance service providers acting in their own interest rather than on instructions from the controller and/or with a criminal intent.

By entering into the above-described contracts, the transferring data controller already ensures a sufficient guarantee that the proper safety and technical framework is in in place, and through that the recipient acknowledges that it has the sufficient means to handle those events that are most reasonably likely to occur, including criminal acts of its employees or its employees or service providers acting in their own interests. If not, it will be a breach of contract, which is subject to further legal actions.

We note that it follows from the Breyer case (Case file no. C-582/14), recitals 45-47:

> "*45. However, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider* ***constitutes a means likely reasonably to be used*** *to identify the data subject.*
>
> *46. Thus, as the Advocate General stated essentially in point 68 of his Opinion,* ***that would not be the case if the identification of the data subject was prohibited by law*** *or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.*" (our emphasis)

Even though the Breyer-case did not involve public authorities, but a private service provider, the CJEU – in our view – still reached the conclusion that unlawful measures to identify a physical person should not be considered as "means reasonably likely to be used" by a data controller.

The Court seemed to conclude in Breyer that it is not a "means reasonably likely to be used" to also consider potential unlawful measures or infringements, which also severely broadens the scope of considerations for EU data controllers.

We encourage EDPB to confirm that the stated in paragraph 42 is covered by using the wide-spread practice in many sectors, where transferring parties enter into contracts governing the transfer and processing of data. If not, we encourage EDPB to specify in further detail what the transferring data controller needs to do in its due diligence of the recipient.

We estimate that taking criminal acts of e.g. an employee into account further than what a sufficient binding contract can ensure as described above, is difficult to enforce between research collaborators.

We ask EDPB to elaborate the stated considerations on taking criminal acts of employees or collaborating partners in general into account in relation to due diligence of the recipient when defining the pseudonymisation domain in relation to securing a proper contractual framework between the transferring and receiving data controllers. Otherwise, we estimate that it will be very difficult to enforce further obligations towards contractual parties in practice, since too broad obligations can be next to impossible to enforce, and the scope for due diligence also becomes too broad.

Pseudonymization in internal processing
Paragraph 47 in the Guidelines sets out the conditions for effective pseudonymization in internal processing. It is highlighted here as a condition that the individuals processing the data "*[must not] be able to reconstitute the original value of the attributes that have been omitted or transformed in the process of pseudonymization*".

In our opinion, there are situations where the same physical person may be responsible for processing data within the pseudonymisation domain, while also – if required for treatment of exceptional cases or for later purposes – being responsible for processing data outside the pseudonymisation domain. This could, for example, be the case if a researcher who normally processes research data within the pseudonymisation domain is also part of the process for handling requests from data subjects.

Naturally, these situations require measures to be in place to prevent identification except for the stated purposes (such as logging access to the supplementary information). But if these measures are in place, such pseudonymisation can be (and frequently is) a measure that contributes to the principles described in the Guidelines.

We therefore encourage the guidance to be clarified, for example by clarifying paragraph 47 to state that "[..]the following conditions hold for the person handling the pseudonymized data*, while acting within the pseudonymization domain*"

Data subject rights in relation to pseudonymised data
Paragraph 76-79 in the Guidelines emphasizes the possibility for the data subject to exercise their rights towards a data controller within the pseudonymisation domain by providing the necessary information for identification themselves. This also raises the question of what significance the receipt of this supplementary information has for the further processing of the pseudonymised data. Since the data controller, by processing the request, has received the supplementary information, they now possess the tools to identify the individual in the future.

In some cases, this can be avoided by deleting the supplementary information once the request has been processed. But in some cases, the data controller may be subject to legal or security requirements that necessitate the retention of the information. It is our assessment that this is a consequence of the right of the data subject to "break" pseudonymisation, and that it therefore does not alter the guarantee

that pseudonymisation provides. Thus, the fact that a subject has exercised their rights under the GDPR does not in itself prevent the data controller from continuing to rely on the pseudonymisation.

However, in our opinion, the Guidelines should encourage the data controller to inform the data subject about the consequences of providing the supplementary information before receiving and processing it.

Pseudonymisation in relation to third-country transfers

Transfer of personal data to third countries is highly relevant to the member universities under Universities Denmark. There are many scientific collaborations between research institutions in the EU and institutions outside of the EU, e.g. the United States. Often, such research collaborations entail the transfer of personal data between the research institutions for analysis and scientific publications in accordance with applicable laws and ethical guidelines.

It follows from the conditions listed in clause 2.4.3, paragraphs 63-64 of the Guidelines that when transferring personal data to a third country (without an adequacy decision), appropriate safeguards must be in place for pseudonymisation to be effective for the pseudonymisation to protect the transferred personal data from government access by public authorities in the recipient country. If the conditions listed in recital 64 are met, we understand it as if pseudonymisation can be an effective safeguard against such unwanted government access to the data.

However, it follows further from clause 2.4.3, paragraphs 64-65 of the Guidelines, that

> "*64. (...)*
>
> *This implies that the public authorities, who would be able to have access to the pseudonymised data based on foreign law or practice, need to be framed within the pseudonymisation domain.*
>
> *65. Thus, any design of a pseudonymisation procedure needs to start from an assessment of which information the public authorities of the recipient country can be expected to possess or to be able to obtain with reasonable means,* ***even if those means may infringe the legal norms in the third country****. This information must then be assumed to be available in the pseudonymisation domain.*" (our emphasis)

According to these guidelines, Danish research institutions transferring data to e.g. the United States in a scientific collaboration in accordance with applicable laws, need to evaluate which information US public authorities are expected to possess or be able to obtain with reasonable means. This includes considering whether these public authorities might breach US legal norms to access the information.

This means that research institutions must ensure that the additional information required to identify pseudonymised data is stored separately and exclusively accessible to them or an independent and trusted entity under a jurisdiction with similar protection as the EU, and that it is considered how to prevent US public authorities gaining access to the information in an illegal fashion.

How does it fit with paragraph 46 of EDPB's "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", version 2.0 adopted on 18 June 2021, where it is stated that "*…sources and information should be relevant, objective, reliable, verifiable* ***and publicly available*** *or otherwise accessible to determine whether your Article 46 transfer tool can be effectively applied and you will have to assess and document that they are*" (our emphasis), if it is not possible to find publicly available information on a third country's potential for infringing legal norms or unlawfully break its laws.

As mentioned above, we note that it follows from the Breyer case (Case file no. C-582/14), recitals 45-47, that – in our view – the CJEU seemed to conclude that it is not a "means reasonably likely to be used" to also consider potential unlawful measures or infringements. Determining what information foreign public authorities in third countries – and not just the receiving processor or controller – might possess or can reasonably obtain also by means of infringing legal norms is very challenging to EU research institutions.

What is EDPB's opinion on this; how does paragraph 65 of the Guidelines align with recital 46 in the Breyer-case?

Pseudonymisation of qualitative data

In our view, the Guidelines emphasize the effectiveness of pseudonymisation primarily for quantitative datasets, where individual data points can be pseudonymised within the broader dataset while still being useful for research. However, within the research sector lot of research activities also involve the use of qualitative data, e.g. interviews, observations, transcriptions, recordings, etc. Pseudonymizing qualitative data presents several concrete challenges.

Firstly, qualitative data is typically rich in context and detail, containing nuanced information that cannot be easily generalized or anonymized. For example, interview transcripts often contain specific personal experiences, locations, and other identifiers that are difficult to remove without losing the essence of the data.

Secondly, the interconnectedness of qualitative data points means that even if direct identifiers are removed or changed, it may still be possible to re-identify individuals based on the remaining information.

Lastly, the process of pseudonymisation itself can be labor-intensive and complex, requiring a thorough understanding of the data and the context in which it was collected.

In light of these challenges, we kindly suggest that the Guidelines be expanded to address the specific issues and suggested methodologies related to the pseudonymisation of qualitative data and by doing so also make research in qualitative data as feasible as in quantitative data.

DANSKE UNIVERSITETER
UNIVERSITIES DENMARK

Pseudonymisation as a guarantee under GDPR Article 89
The concept of pseudonymisation is used in several places in the GDPR as an example of a technical measure that can contribute to processing security.

Pseudonymisation is particularly highlighted as a technical measure in Article 89 of the GDPR:

> "*Processing for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes shall be subject to appropriate safeguards for the rights and freedoms of the data subjects in accordance with this Regulation. These safeguards shall ensure that technical and organizational measures are in place, in particular to ensure compliance with the principle of data minimization.* ***These measures may include pseudonymization, provided that these purposes can be fulfilled in this way****. When these purposes can be fulfilled by further processing that does not allow or no longer allows the identification of data subjects, these purposes shall be fulfilled in this way*" (our emphasis).

Universities Denmark have been informed by the Danish Data Protection Agency that EDPB is planning new guidelines on data protection for the research sector.

We suggest that the new guide concerning research specifically describes situations where pseudonymisation can contribute to – or be sufficient to – meet specific requirements and constitute a guarantee under Article 89 of the GDPR.

Universities Denmark therefore encourages the EDPB to include pseudonymisation as a measure and as a guarantee as part of the new guidance text.

***

Best regards,

Søren Broberg Nielsen
Chairman of the GDPR Working Group, Universities Denmark