DIGITALEUROPE

13 MARCH

Pseudonymisation: a recognised tool to protect data processing

Executive summary

We welcome the European Data Protection Board's (EDPB) draft guidelines on pseudonymisation, and their stated objective to 'help controllers to choose effective techniques.' Today, pseudonymisation is widely used to minimise privacy and security risks around data sharing, notably to develop artificial intelligence (AI) tools or for research and innovation in different sectors. However, the EDPB risks missing the mark on daily operational complexities for controllers, for example where pseudonymised and anonymised data intersect.

It is key to recognise pseudonymisation as a practical and effective tool to apply privacy by design and by default principles, all the more so given upcoming proposals by the Commission to increase the availability of high-quality data.[1] We therefore recommend that the final guidelines:

- Introduce more flexibility in newly proposed definitions such as 'domains' or 'additional information,' and map references in legislation adopted since the GDPR;
- In line with case law from the Court of Justice of the European Union (CJEU), clarify the conditions for pseudonymised data to be considered to have been anonymised;
- Re-affirm the key role of pseudonymisation in international data transfers, and remove any additional obligations to Chapter V GDPR;[2] and
- Recognise and promote the role of privacy enhancing technologies (PETs) in facilitating effective pseudonymisation.

[1] Notably, the upcoming Data Union Strategy. See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14541-European-Data-Union-Strategy_en.

[2] See DIGITALEUROPE *Data transfers in the data strategy: Understanding myth and reality*, available at https://cdn.digitaleurope.org/uploads/2022/06/DIGITALEUROPE_Data-transfers-in-the-datastrategy_Understanding-myth-and-reality.pdf .

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

One of several technical and organisational safeguards

Whist guidance on pseudonymisation has been issued by several data protection authorities and by ENISA,[3] the proposed EDPB guidelines will help provide a harmonised view and increase legal certainty. We recommend that the final guidelines also build upon references to pseudonymisation made in recent legislation.

Risk assessments

We welcome the EDPB's acknowledgement that pseudonymisation is a technical and organisational measure that helps mitigate risks, similarly to other legislative frameworks that recognise pseudonymisation as a valid solution.[4] However, the draft guidelines also describe pseudonymisation as insufficient if not complemented by further additional measures.[5] On top of this, the appropriateness of all measures would have to be assessed by the controller.[6]

Under the GDPR, several technical and organisational measures can be taken but Art. 32 states they should be 'appropriate to the risk.' Similarly, Art. 25 GDPR refers to 'risks of varying likelihood and severity.' Additional burdens on using pseudonymisation should therefore be removed, particularly for low-risk processing, such as where pseudonymised data is breached but not the additional information required to re-identify it.[7] A reasonableness test or a risk assessment methodology that can be included in data protection impact assessments should be clearly delineated within the guidelines, instead of implying the need for separate pseudonymisation assessments or clauses.[8] Similarly, obligations for additional documentation around defining the objectives of pseudonymisation in section 2.2 should be simplified.

Definitions and legislative environment

As noted in the draft guidelines, the GDPR was the first regulation to mention pseudonymisation. Since then, a number of new laws (at both EU and Member State level) have referred to, and thus encouraged, the use of pseudonymisation, however, these are not taken into account in the draft guidelines. The draft guidelines present new definitions such as 'transformation', 'domains' or 'additional information' and terms such as

[3] See for example 'Deploying Pseudonymisation Techniques', issued in 2022.

[4] Such as Arts 17(g) and 18(4) Regulation (EU) 2023/2854 (Data Act).

[5] Point 5 of the draft guidelines.

[6] Point 44, ibid.

[7] Point 62, ibid.

[8] Point 114, ibid.

'secrets' that will impact the application of the GDPR as well as other laws. The final guidelines should leverage references in new legislation and mitigate the impact of new definitions, to allow sufficient flexibility, and map new legislation to facilitate the use of pseudonymised data where cited in law.

We recommend specifying in point 6 that over time, the understanding of 'pseudonymisation' has evolved to match the broader definition of the GDPR. Various techniques can employ encryption or certain PETs. Accordingly, the term 'common understanding' should be rephrased as 'initial understanding'.

Under point 8, we recommend replacing 'provides for the retention of additional information' with 'refers to the retention of additional information,' to clarify that the GDPR does not add a separate obligation for retention. Points 7 and 8 could in fact be replaced with the GDPR's definition of pseudonymisation rather than paraphrasing Art. 4(5) GDPR.

Privacy Enhancing Technologies

The guidelines on pseudonymisation will not be developed in a vacuum. For example, the latest version of the Commission FAQs on the Data Act notes that pseudonymisation plays an important role in the implementation of the Data Act.[9] PETs are recognised in the FAQs as valid pseudonymisation tools, which do not prevent data sharing as they would not be considered as additional investments into assigning values or insights from the data under the Data Act.[10]

Another example is the Clinical Trials Regulation, which requires certain personal data to be pseudonymised.[11] Another is the draft revision of the EU's legal framework for population statistics, which refers to the usage of PETs.[12]

Although certain PETs, such as data obfuscation tools, can be classified as pseudonymisation techniques, some go beyond preventing attribution and bring further protections to personal data. Relevant PETs exist and should be further recognised in the final guidelines as solutions for valuable data to be used, strengthening the single market and boosting research and innovation, whilst protecting privacy and GDPR rights.

Legal basis

We welcome the clarification that pseudonymisation can be considered a technical or organisational measure under Art. 25 GDPR which does not need

[9] See https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act.

[10] See https://commission.europa.eu/law/law-making-process/better-regulation/simplification-and-implementation_en.

[11] Regulation (EU) No 536/2014.

[12] COM(2023) 31 final.

a separate or additional legal basis, with Art. 6(1)(c) explicitly mentioned.[13] A direct reference to Art. 32 GDPR would provide clarity regarding Union law requiring such pseudonymisation activity, and point 23 should be clarified to state that the legal basis used to process data, including consent, can apply to processing operations to pseudonymise that same data.

Unauthorised parties

The draft guidelines note that controllers may have to not only identify unauthorised third parties from domains,[14] but also consider actions in good faith or with criminal intent, that could be taken for attribution. However, in practice the controller will not always be able to identify all persons that may attempt to gain access. This will especially be difficult for large datasets or where such an analysis could cause more risks for instance if a list of unauthorised third parties and actions they might take for attribution, were disclosed.15

The final guidelines should ensure that for external processing, the burden of proof on recipients consists of demonstrating that pseudonymised data be disclosed only to the intended parties, rather than demonstrating that it is not disclosed to all possible other parties.[16] The guidelines should not place the burden solely on the controller, as the latter will not necessarily have the means to identify all the persons in the domain.

The link with anonymisation

The draft guidelines are intended to cover pseudonymisation rather than anonymisation, but in fact impose restrictions on the latter. The final guidelines should recognise the link between pseudonymisation and anonymisation, also taking into consideration all relevant CJEU case law and technological advancements.

‘Additional information’ under the GDPR

Whilst the notion of ‘additional information’ is not defined under the GDPR, its scope in the draft guidelines is overly broad. The draft requires that controllers include different kinds of information that may exist, for instance on social media, in their assessment, which is not reflected in the Art. 4 GDPR’s language.

---

[13] Points 23, 45 and 106 of the draft guidelines.

[14] Section 42, ibid., mentions cyber-crime actors and employees.

[15] Points 37 and 42, ibid.

[16] Point 51, ibid.

In practice, it may be impossible for a controller to be aware of all 'additional information' that may exist on social media, online forums, and publicly available sources. Public information also tends to evolve constantly. The final guidelines should refer to 'means reasonably likely to be used' under point 43, under point 22. Moreover, the final guidelines should recognise that controllers may not always have access to all 'additional information' that may exist, and that they are not liable for it.

We also recommend that contractual agreements and other 'reasonable means' to access or not additional information be taken into account in the guidelines.[17]

The draft guidelines also seem to imply that the mere existence of additional information, whether in the hands of the controller with the pseudonymised data or not, must be considered personal data. Following this logic, even if all additional information (including from social media, publicly available sources, or online forums) were erased, data would still not automatically be considered anonymised. This restrictive interpretation fails to recognise anonymisation as a valid tool and deviates from CJEU case law.

Pseudonymised and anonymised data

Whist the EDPB seems to have split the anonymisation and pseudonymisation guidelines into two separate workstreams, we strongly recommend that the link that exists in practice between pseudonymised and anonymised data be effectively addressed.

CJEU case law is especially relevant to the issue at hand and should be taken into account in the analysis of the final guidelines:

First, in Case C-582/14, the CJEU found that a dynamic IP address held by a website operator was personal data only if the website operator had legal means reasonably likely to be used to obtain additional identifying information (e.g. from an internet service provider). By taking this case into account, the final guidelines should recognise that there are cases where without access to additional information, data cannot be re-identified and is therefore anonymous. This is of particular relevance with the Data Act's upcoming entry into application, which may set legal obligations to share pseudonymised data. The recent FAQs published by the Commission encourage the use of encryption in some cases.[18]

Second, in Case T-557/20 for which the appeal before the CJEU is expected after the EDPB's public consultation on the draft guidelines, the General Court

[17] See section below on 'Pseudonymised and anonymised data.'

[18] The Commission's FAQ document mentions that: 'Anonymisation or pseudonymisation can be relevant, for instance, when the data holder must respond to a request under Article 4 or 5, and the requesting user is not the data subject, or there are several data subjects who may all be users of the same connected product (e.g. a rented car).'

held that pseudonymised data that has been transmitted to a data recipient is not personal data if the data recipient does not have the means to re-identify the data subjects. Once again, the means and legal means to re-identify data subjects were part of the Court's assessment. In light of this, point 22 of the draft guidelines should be amended. The Advocate General has already issued an Opinion to guide the case, where it is clarified that an entity that cannot reasonably identify a data subject should not have to comply with GDPR obligations:

> *The fact that the rules stemming from Regulation 2018/1725 do not apply to data relating to non-identifiable persons would not preclude entities that are at the origin of misconduct from incurring legal liability where appropriate, for example in the event of disclosure of data resulting in harm. On the other hand,* ***it seems to me disproportionate to impose on an entity, which could not reasonably identify the data subjects, obligations arising from Regulation 2018/1725, obligations which that entity could not, in theory, comply with or which would specifically require it to attempt to identify the data subjects.***

Additionally, Recital 26 GDPR itself specifies that the means reasonably likely to be used to make the information identifiable should be taken into account. We recommend at least clarifying that pseudonymised data may be considered 'anonymous' for third parties outside the domain, without access to the additional information.

Last, the OECD also defines pseudonymisation as a weaker form of de-identification than anonymisation, suggesting that if de-identification is strengthened, data can become anonymised.[19] The final guidelines should recognise this link between pseudonymisation and anonymisation.

Use cases and medical data

Practical guidance can support practitioners across industries, including along the healthcare value chain, for a classification framework.[20] Whilst use cases pertaining to the health sector are very pertinent, we recommend that the EDPB put forward examples from a variety of sectors, for instance finance.

The draft guidelines make the use of pseudonymisation conditional in certain cases on recipients not being able to single out data subjects, which could be difficult to apply in practice. For instance, for clinical trials, data will be

[19] OECD DIGITAL ECONOMY PAPERS March 2023 No. 351, see https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html .

[20] See https://www.digitaleurope.org/resources/digitaleuropes-recommendations-for-the-european-health-data-space/ .

pseudonymised pursuant to the Clinical Trials Regulation and good clinical practice from the European Medicines Agency because individuals need to be easily singled out in the case of adverse events.[21] We recommend that the final guidelines elaborate on the meaning of 'directly identifiable', rather than setting criteria based on singling out which is only referred to as an example in Recital 26.

Additionally, we would welcome a new separate line in the use cases section on possible legal bases that can be relevant, including legitimate interest for example. The final guidelines could include the different possible legal bases to process health data for scientific research, when it has been pseudonymised.[22] In practice, public interest has been accepted as a legal basis and not only consent, however the analysis of this varies from Member State to Member State. Practical examples of how Art. 6(1) and Art. 6(4) apply would be welcome.

Finally, the requirement to replace or modify pseudonyms a second time before sharing them with third parties may be unnecessarily complex, depending on the level of risk. The examples should note that this technique is one amongst others, and give counter-examples where this approach is not necessary.

International data transfers

We welcome the draft guideline's recognition that pseudonymisation can constitute an additional safeguard regarding data transfers. However, the conditions proposed in points 64-68 add new obligations that go beyond Chapter V GDPR. The draft guidelines seem to indicate that third-country authorities should not have access to pseudonymised data, going beyond the supplementary measures under the GDPR. The second bullet-point of point 64 should not refer to adequacy decisions, as supplementary measures are not relevant when adequacy decisions are in place.

Additionally, point 65 seems to require that controllers assess or find out which information third-country public authorities can possess even infringing the legal framework of their own country. We recommend that this section be replaced with a direct reference to Recommendations 01/2020, as companies cannot be expected to investigate third-country authorities.

Data subject rights

We recommend deleting or clarifying point 79 of the draft guidelines, as it seems to encourage additional information to be shared and oblige controllers to help data subjects find their pseudonym. Requiring re-identification based

[21] See https://www.ema.europa.eu/en/ich-e6-good-clinical-practice-scientific-guideline.

[22] For a more in-depth analysis, see DIGITALEUROPE, *Making the most of the GDPR to advance health research*, available at https://cdn.digitaleurope.org/uploads/2021/06/Making-the-most-of-the-GDPR-to-advance-health-research_DIGITALEUROPE.pdf.

on pseudonyms provided to the data subject may introduce security risks and would go beyond the GDPR requirements. Art.11(1) GDPR states that if the purposes for data processing no longer require identification of the data subject, the controller shall not be obliged to maintain, acquire or process additional information. The guidelines should not impose new information obligations on the controller, who might not have direct access to the original identifying information, that would go beyond the GDPR.

FOR MORE INFORMATION, PLEASE CONTACT:

Beatrice Ericson

Policy Manager

beatrice.ericson@digitaleurope.org / +32 490 44 35 66

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 108 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.