PSEUDONYMISATION UNDER THE GDPR

Anonos®

BigPrivacy® Unlocks Data

BACKGROUND

What is Pseudonymised Data Under the GDPR?

Pseudonymised data remains within the scope of the EU General Data Protection Regulation (GDPR) as personal data, however, **it provides substantial benefits as the state of the art in Data Protection by Design and by Default.** The European Union Agency for Network and Information Security (ENISA)[1] publication entitled *Recommendations on Shaping Technology According to GDPR Provisions: An Overview on Data Pseudonymisation*[2] highlights the following benefits:

1. **Pseudonymisation serves as a vehicle to "relax" certain data controller obligations**, including:
    - Lawful repurposing (further processing) in compliance with purpose limitation principles;
    - Archiving of data for statistical processing, public interest, scientific or historical research; and
    - Reduced notification obligations in the event of a data breach.
2. **Pseudonymisation supports more favorable (broader) interpretation of data minimisation**.
3. **Pseudonymisation goes beyond protecting "real-world personal identities' by protecting indirect identifiers**.
4. The unlinkability enabled by **Pseudonymisation furthers the fundamental data protection principles of necessity and data minimisation.**
5. The decoupling aspect of **Pseudonymisation enables Data Protection by Design and by Default** while at the same time improving accuracy since the integrity of the original dataset (which can only be reconstructed on the basis of the two outputs of the pseudonymisation process) cannot be contested - further **advancing the data protection principle of accuracy.**

According to GDPR Article 4(5) definitional requirements, data is Pseudonymised if it cannot be attributed to a specific data subject without the use of separately kept "additional information." Pseudonymised data embodies the state of the art in Data Protection by Design and by Default because it requires protection of both direct and indirect identifiers (not just direct). The shortcomings of prior approaches to data protection (e.g., failed attempts at anonymisation) are highlighted by two well-known historical examples of unauthorized re-identification of individuals using AOL[3] and Netflix[4] data. These examples of unauthorized re-identification did not require access to separately kept "additional information" that was under the control of the data controller as is now required for GDPR compliant Pseudonymisation.

GDPR Data Protection by Design and by Default principles as embodied in Pseudonymisation require protection of both direct and indirect identifiers so that personal data is not cross-referenceable (or re-identifiable) without access to "additional information" that is kept separately by the controller. Because access to separately kept "additional information" is required for re-identification, attribution of data to a specific data subject can be limited by the controller to support lawful purposes only.

GDPR Article 25(1) identifies Pseudonymisation as an *"appropriate technical and organizational measure"* and Article 25(2) requires controllers to:

> *"…implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."*

PSEUDONYMISATION

Characteristics & Benefits of Pseudonymised Data

The importance of protecting both direct and indirect identifiers is highlighted in Article 29 Working Party Opinion 05/2014,[5] written in anticipation of the GDPR, which states:

> *It is still possible to single out individuals' records if the individual is still identified by a unique attribute which is the result of the pseudonymisation function [i.e., a static attribute that does not change, in contrast to a dynamic attribute which does change]…*
>
> *Linkability will still be trivial between records using the same pseudonymised attribute to refer to the same individual….*
>
> *Inference attacks on the real identity of a data subject are possible within the dataset or across different databases that use the same pseudonymised attribute for an individual, or if pseudonyms are self-explanatory and do not mask the original identity of the data subject properly…*
>
> *Simply altering the ID does not prevent someone from identifying a data subject if quasi-identifiers remain in the dataset, or if the values of other attributes are still capable of identifying an individual.*

State of the art Pseudonymisation not only enables greater privacy-respectful use of data in today's "big data" world of data sharing and combining, but it also enables data controllers and processors to reap explicit benefits under the GDPR for correctly Pseudonymised data. **The benefits of properly Pseudonymised data are highlighted in multiple GDPR Articles, including:**

- **Article 6(4) as a safeguard to help ensure the compatibility of new data processing.**
- Article 25 as a technical and organizational measure to **help enforce data minimisation principles and compliance with data protection by design and by default obligations**.
- Articles 32, 33 and 34 as a security measure helping to make data breaches **"unlikely to result in a risk to the rights and freedoms of natural persons" thereby reducing liability and notification obligations for data breaches.**
- Article 89(1) as a safeguard in connection with processing for archiving purposes in the public interest; scientific or historical research purposes; or statistical purposes; moreover, **the benefits of pseudonymisation under this Article 89(1) also provide greater flexibility under:**
    1. Article 5(1)(b) with regard to purpose limitation;
    2. Article 5(1)(e) with regard to storage limitation; and
    3. Article 9(2)(j) with regard to overcoming the general prohibition on processing Article 9(1) special categories of personal data.
- **In addition, properly Pseudonymised data is recognized** in Article 29 Working Party Opinion 06/2014[6] **as playing "…a role with regard to the evaluation of the potential impact of the processing on the data subject...tipping the balance in favour of the controller" to help support Legitimate Interest processing** as a legal basis under Article GDPR 6(1)(f). Benefits from processing personal data using Legitimate Interest as a legal basis under the GDPR include, without limitation:
    1. Under Article 17(1)(c), if a data controller shows they "have overriding legitimate grounds for processing" supported by technical and organizational measures to satisfy the balancing of interest test, they have greater flexibility in complying with Right to be Forgotten requests.

2. Under Article 18(1)(d), a data controller has flexibility in complying with claims to restrict the processing of personal data if they can show they have technical and organizational measures in place so that the rights of the data controller properly override those of the data subject because the rights of the data subjects are protected.
3. Under Article 20(1), data controllers using Legitimate Interest processing are not subject to the right of portability, which applies only to consent-based processing.
4. Under Article 21(1), a data controller using Legitimate Interest processing may be able to show they have adequate technical and organizational measures in place so that the rights of the data controller properly override those of the data subject because the rights of the data subjects are protected; however, data subjects always have the right under Article 21(3) to not receive direct marketing outreach as a result of such processing.

References

[1] ENISA's mandate is to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU.

[2] https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions

[3] https://techcrunch.com/2006/08/09/first-person-identified-from-aol-data-thelma-arnold/

[2] https://bits.blogs.nytimes.com/2010/03/12/netflix-cancels-contest-plans-and-settles-suit/

[5] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[6] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Anonos
BigPrivacy Unlocks Data

Contact us at:
LearnMore@anonos.com