Pseudonymisation

When you need more than consent for lawful data processing

Anonos state-of-the-art Pseudonymisation technology enables lawful repurposing of data while preserving up to 100% accuracy to maximise data utility by expanding opportunities to ethically process, share and combine data in compliance with evolving data privacy regulations.

Anonos®

BigPrivacy® Unlocks Data

A Comparison to ENISA Guidance on Pseudonymisation

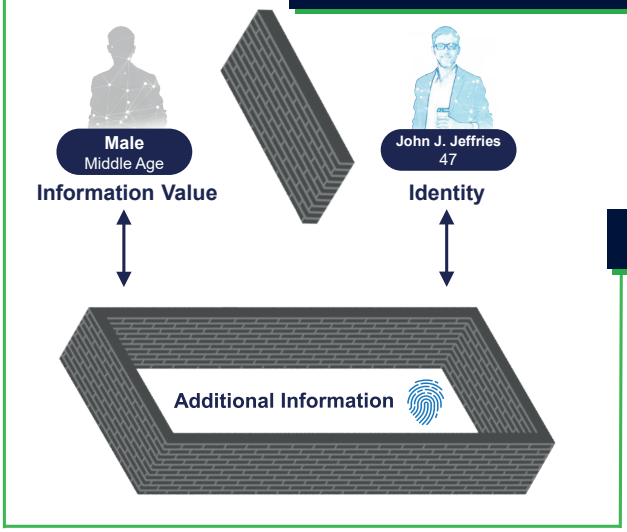
March 2020

www.pseudonymisation.com

Overview

PSEUDONYMISATION = TECHNICAL / ORGANISATIONAL SAFEGUARDS

GDPR DEFINITION OF PSEUDONYMISATION

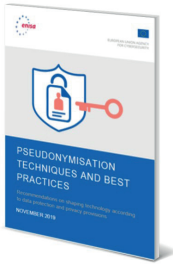


1) Information Value cannot be re-linkable to Identity of data subject without the use of Additional Information that is kept separately, subject to technical and organisational measures.

2) Access to and use of Additional information must be limited to authorized lawful processing only.

ENISA GUIDANCE ON PSEUDONYMISATION

November 2018



November 2019

PSEUDONYMISATION AND DATA PROTECTION BY DESIGN AND BY DEFAULT

The combination of GDPR compliant Pseudonymisation and Data Protection by Design and by Default principles help to satisfy the balancing of interest test requirements for Legitimate Interest processing. This allows ethical and lawful data analytics, machine learning, AI, and data sharing and combining, by creating sustainable data assets that:

1. **Deliver the Resistance to Re-Identification** of "Anonymised" Data
   a) For "locally protected" internal use
   b) For "globally protected" data sharing and combining
2. **Retain the Lawful Controlled Re-linkability** of Pseudonymised Data
3. **Preserve 100% of the Accuracy and the Full Utility** of Source Data
4. **Activate Express Statutory Benefits** of GDPR Pseudonymisation
5. **Enable Lawful Secondary Processing**

Section 1

BACKGROUND

In today's data driven world, new technical measures are required to help balance data innovation and protection of individual privacy rights when consent is no longer effective. The limitations of consent are well articulated in the following quote:

> "The free and informed consent that today's privacy regime imagines simply cannot be achieved. Collection and processing practices are too complicated. No company can reasonably tell a consumer what is really happening to his or her data. No consumer can reasonably understand it. And if companies can continue to have their way with user data as long as they tell users first, consumers will continue to accept the unacceptable: If they want to reap the benefits of these products, this is the price they will have to pay.
>
> Companies should be expected and required to act reasonably to prevent harm to their clients. They should exercise a duty of care. The burden no longer should rest with the user to avoid getting stepped on by a giant. Instead, the giants should have to watch where they're walking."1 (emphasis added)

"The free and informed consent that today's privacy regime imagines simply cannot achieved"

GDPR regulators agree; issued guidance recognises the inadequacy of consent as used in the past. Moreover, the use of consent as a basis for processing is severely restricted, particularly when it comes to secondary uses of personal data such as analytics, machine learning, and AI. Only new technical safeguards can replace consent as the new bulwark of individual privacy while enabling innovation.

BENEFITS OF PSEUDONYMISATION

The GDPR highlights pseudonymisation as an effective technological solution for protecting privacy. Pseudonymisation is legally defined for the first time at the EU level in the GDPR, with

a heightened standard relative to past practice. It is repeatedly mentioned in the GDPR as a technique that can be used in pursuit of both Data Protection by Design and by Default (Article 25) and Security of Processing (Article 32). In more than a dozen places, the GDPR links pseudonymisation to express statutory benefits.

> Only new tehnical safeguards can replace consent as new bulwark of individualprivacy while enabling innovation

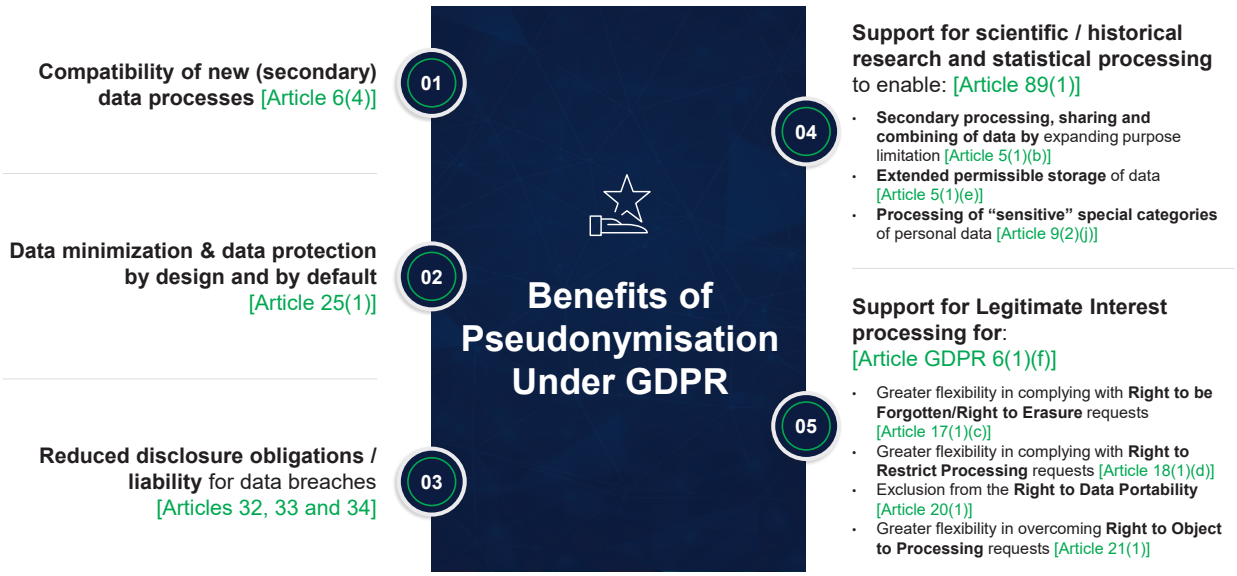


Image 1: GDPR Benefits of Pseudonymisation

The European Union Agency for Cybersecurity (previously, the European Union Agency for Network and Information Security, ENISA)[2] publication titled Recommendations on Shaping Technology According to GDPR Provisions: An Overview on Data Pseudonymisation[3] highlights the following benefits from GDPR compliant pseudonymization:

1. Pseudonymisation serves as a vehicle to "relax" certain data controller obligations, including:

a) Lawful repurposing (further processing) in compliance with purpose limitation principles;
b) Archiving of data for statistical processing, public interest, scientific or historical research; and
c) Reduced notification obligations in the event of a data breach.

2. Pseudonymisation supports a more favourable (broader) interpretation of data minimisation.
3. Pseudonymisation goes beyond protecting "real-world personal identities" by protecting indirect identifiers.
4. Pseudonymisation provides unlinkability, furthering the fundamental data protection principles of necessity and data minimisation.
5. Pseudonymisation decouples privacy and accuracy enabling Data Protection by Design and by Default while at the same time allowing data about individuals to remain more accurate.

While pseudonymisation has many benefits, using it effectively requires significant expertise. The same ENISA report recognises that effective data pseudonymisation is highly context-dependent and "requires a high level of competence" to prevent attacks while maintaining data utility.

> Pseudonymisation provides:
> - Data minimisation
> - Help with requirement relaxation
> - Unlinkability
> - Decoupled privacy

Section 2

INTRODUCTION TO ANONOS® BIGPRIVACY

Anonos BigPrivacy is a privacy engineering solution that transforms identifiable source data into privacy-respectful data assets. The resulting data assets are known as Variant Twins®. Privacy policies are embedded via digital controls at the data element level, satisfying statutory and contractual requirements for lawful data use.

BigPrivacy enables a privacy engineer to create Privacy Actions via a graphical user interface (GUI). Privacy Actions are specifically tailored to selected subsets of data fields/columns in a

data source and integrate a combination of privacy engineering tools:

1. Classic anonymisation techniques;

2. GDPR compliant pseudonymisation of data; and

3. Anonos' patented Controlled Relinkable Dynamic De-Identifiers.

BigPrivacy bundles Privacy Actions to automatically transform the source data in a highly scalable manner on a record by record basis. This transformed data is filtered using k-anonymity, a re-identification risk management technique that prevents an adversary from defeating privacy protections via singling out.

> BigPrivacy:
> - The tools to create Privacy Actions
> - GDPR compliant pseudonymisation of data

OVERVIEW OF K-ANONYMITY

The following overview of k-anonymity is derived from a description provided by the U.S. Department of Health & Human Services (HHS)[4]

When using the k-anonymity technique, "k" refers to the number of people to which each disclosed record must correspond. In practice, this correspondence is assessed using the features that could be reasonably applied by a recipient to identify an individual data subject.

Table 2 below illustrates an application of generalisation and suppression methods to achieve a k-anonymity value of "2" (2-anonymity) with respect to the Age, Gender, and ZIP Code columns in the fictitious protected health information included in Table 1. All rows correspond to fictitious patient records with the same combination of generalized and suppressed values for Age, Gender, and ZIP Code. Notice that Gender has been suppressed completely.

Table 1
Protected Health Information (PHI)

Age (Years)	Gender	ZIP Code	Diagnosis
15	Male	00000	Diabetes
21	Female	00001	Influenza
36	Male	10000	Broken Arm
91	Female	10001	Acid Reflux

Table 2
K-Anonymity Level of "2"

Age (Years)	Gender	ZIP Code	Diagnosis
Under 30		0000	Diabetes
Under 30		0000	Influenza
Over 30		1000	Broken Arm
Over 30		1000	Acid Reflux

K-ANONYMITY AND VARIANT TWINS

The combined set of Privacy Actions and the selected level of k-anonymity comprise what is called a Privacy Transformer, which is specific to a particular source data set. The result of applying the Privacy Transformer to that data set is a Variant Twin® – a version of the source data transformed by the Privacy Actions and filtered for re-identification risk to suppress records that do not meet the required k-anonymity threshold.

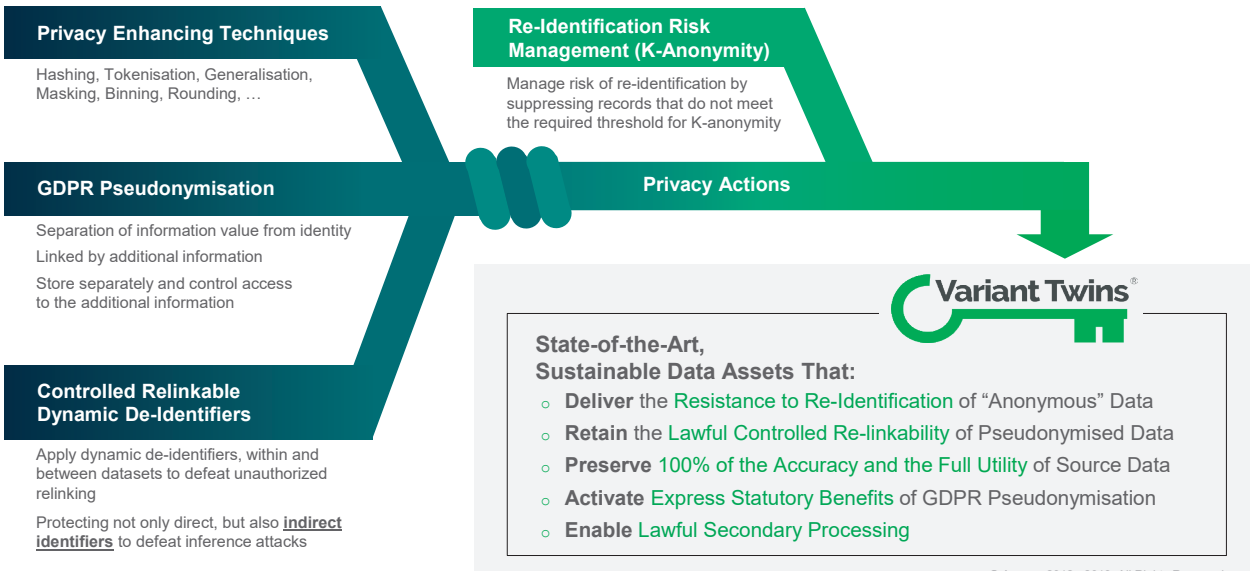


Image 2: State-of-the-art Variant Twins

This combination of Privacy Actions and re-identification risk management provides tailored protection against:

- Unauthorized combining of data with other data sources; and
- Re-identification of data subjects; whilst,
- Preserving full data utility that enables compliant secondary uses of data for analytics, AI, and marketing.

The flexibility of this approach enables a privacy engineer to create Variant Twins for different contexts, uses, and risks. This flexibility opens a range of levels of data protection, from "local protection" for use within a locally controlled enclave or siloed environment to "global protection", enabling lawful and ethical data sharing and combining.

> BigPrivacy® creates privacy-respectful Variant Twins® for different contexts, uses, and risks.

Section 3

BIGPRIVACY'S UNIQUE APPROACH

BigPrivacy's unique approach:

- Provides a powerful tool for organizations to implement GDPR-mandated Data Protection by Design and by Default.
- Supports a risk-based approach to data protection. Delivering the flexibility and control to provide purpose, context, required utility, and desired scalability of intended processing, while addressing the necessary protection of personal data. This is accomplished by empowering privacy engineers to apply finely tuned combinations of anonymisation techniques, pseudonymisation techniques, and both common and novel pseudonymisation policies on a field by field basis.
- Ensures transparency and auditability of privacy-engineering techniques and offers the visibility of the security and data protection levels used to achieve desired accountability.

- Implements ENISA recommendations and best practices for Pseudonymisation.[3 5]
- Introduces multiple new innovations that advance the state-of-the-art to address new challenges presented by Big Data.

THE ADVANTAGES OF CONTROLLED RELINKABLE DYNAMIC DE-IDENTIFIERS

Anonos' patented **Controlled Relinkable Dynamic De-Identifiers[6]** are a significant advance in pseudonymisation. Traditionally, pseudonymisation policy has been one-dimensional: i.e., deterministic pseudonymisation applied to direct identifiers, where a specific identifier is assigned the same pseudonym consistently both within and between databases. While useful as a localised security technique, this approach provides limited protection against unauthorised re-identification because it is vulnerable to so-called linkage attacks and inference attacks.

Two additional policies are enumerated by ENISA[5]:

- **Fully randomised pseudonymisation:** a specific identifier receives a different pseudonym every time it occurs. This maximises protection but significantly reduces data utility.
- **Document-randomised pseudonymisation** (an intermediate policy): In this case, each occurrence of an identifier within a database receives a different pseudonym. However, that set of pseudonyms is used again for the same identifier with each succeeding database.

BigPrivacy®:
- A powerful tool for organisations to implement GDPR-mandated Data Protection by Design and by Default
- Risk-based approach to data protection
- Visibility of the security and data protection levels
- Advances the state-of-the-art

Controlled Relinkable Dynamic De-Identifiers6 provide a practical implementation of pseudonymisation that advances the state-of-the-art in data protection in at least three important ways:

1. Powerful resistance to reidentification by adversaries attempting linkage and inference attacks, while preserving much higher levels of analytical utility than previously obtainable, by enabling easy application of deterministic pseudonymisation to individual indirect identifiers, or combinations of them, and not just to direct identifiers.
2. Granular control over relinking, unlike traditional all-or-nothing relinking of traditional pseudonymisation approaches. This makes it possible to retrieve individual fields from the source data that were not included in the original Variant Twin.
3. Support for not only ENISA-defined5 fully randomised and deterministic pseudonymisation policies, but also for three additional intermediate pseudonymisation policies. Drawing on the ENISA nomenclature, these can be characterised as field, table, and document deterministic pseudonymisation respectively.

    - **Field deterministic pseudonymisation:** Consistency is maintained only within individual fields in a table, with different pseudonyms being used between columns containing the same data (e.g. country of purchaser, and country of vendor within a single table) as well as other tables/databases. This is the default for BigPrivacy, a unique HMAC key is generated for each field within a dataset. This ensures that each occurence of a data value in a field is replaced by the same pseudonym. The same data value in other fields would be replaced by different pseudonyms.
    - **Table deterministic pseudonymisation:** Consistency is maintained within each table. Multiple (or all) fields within the same table or data set use the same HMAC key so that pseudonym values are deterministic within that table, but different pseudonyms are used in other tables/data sets.
    - **Document deterministic pseudonymisation:** All occurrences of a data value within all fields in all tables in one database are assigned the same pseudonym in the resulting Variant Twins; whilst also assigning a new pseudonym in each succeeding database.

BigPrivacy supports this range of pseudonymisation policies by leveraging two recommended ENISA techniques as pseudonymisation functions, both of which are characterized by ENISA5 as providing strong data protection:

- **Cryptographic pseudo-random number generation (CRNG):** BigPrivacy leverages the computer operating system entropy pool to create **Replacement Dynamic De-Identifiers (R-DDIDs)**. This supports the ENISA recommendation for fully randomized pseudonymisation.

- **Hashed Message Authentication Codes (HMAC) with SHA-256:** BigPrivacy uses the operating system entropy pool to generate the pseudonymisation secret (key) to create **Association Dynamic De-Identifiers (A-DDIDs).** This can be configured to support ENISA recommended deterministic pseudonymisation as well as each of the three additional intermediate deterministic pseudonymisation policies noted above (i.e., field, table and document deterministic). As required by this technique; the key is securely stored separately from the generated pseudonym(s).

In both techniques, a recovery function is provided via a securely and separately stored mapping table. This enables reversal of pseudonymisation when authorized. The mapping table is the "information kept separately subject to technical and organisational measures to ensure that the personal data are not attributable to an identified or identifiable natural person" under the GDPR definition of pseudonymisation.

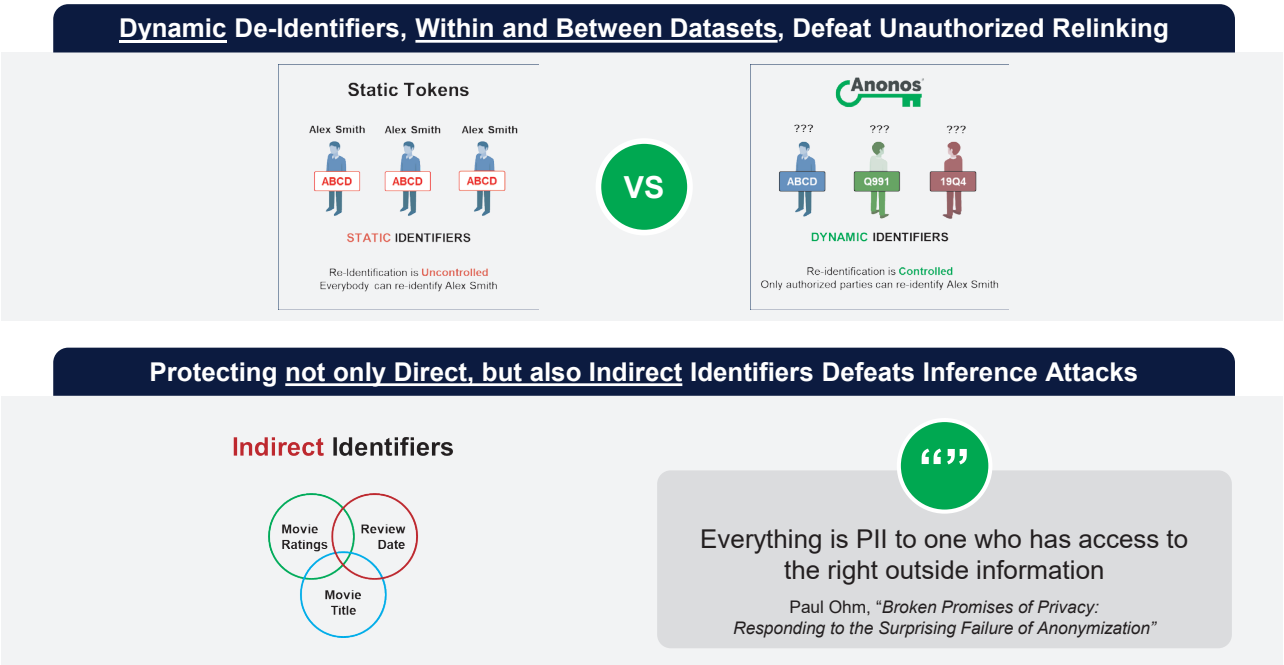


Image 3: Controlled Relinkable Dynamic De-Identifiers

Section 4

CREATING DIGITAL TWINS®

Shown below, is a simplified example of the data elements Variant Twins can include.

The left-hand side shows a Digital Twin, "John J Jeffries", i.e., a digital representation of a specific person. This includes direct identifiers like name and location, as well as indirect or quasi-identifiers like date of birth, zip code, income and loan details. This Digital Twin is the original source data.

A privacy engineer designs "Variant Twin A", to reveal the minimum data necessary to support an authorised use of the source data, while protecting the identity of the data subject.

By selecting different Privacy Actions, different versions of Variant Twins are created to support different use cases and purposes.

For example, you might choose to reveal a town or city instead of an exact address or a binned age, income or loan range instead of identifying amounts. All records included and revealed in Variant Twins must satisfy a specified k-anonymity threshold to ensure there are a minimum number of similar records in each cohort, based on selected fields.

In this example, "Variant Twin B" has a higher likelihood of meeting a higher k-anonymity requirement and getting included in the final output.

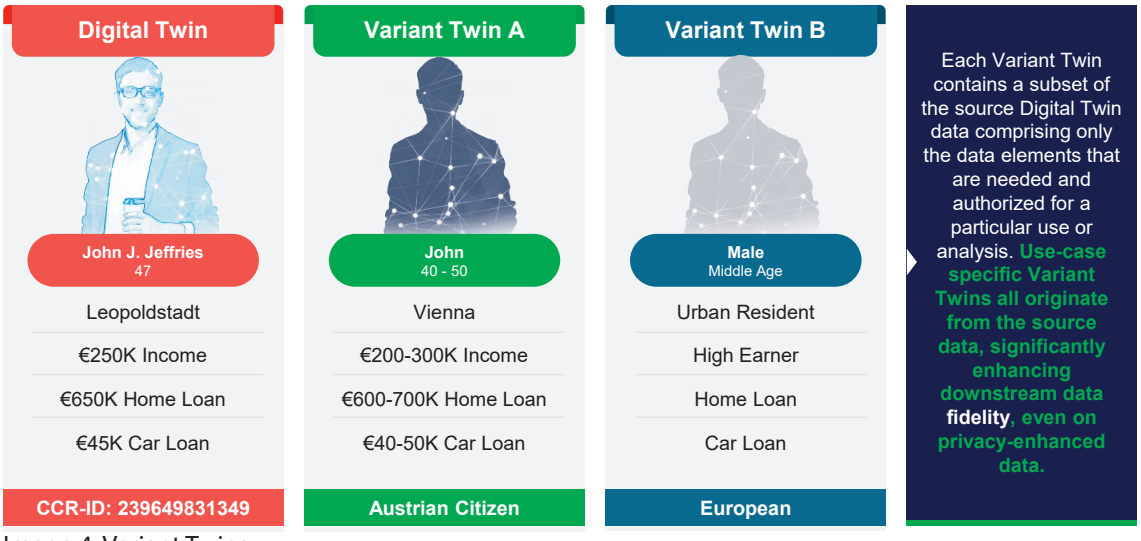


Image 4: Variant Twins

> Variant Twins are created to support different use cases and purposes

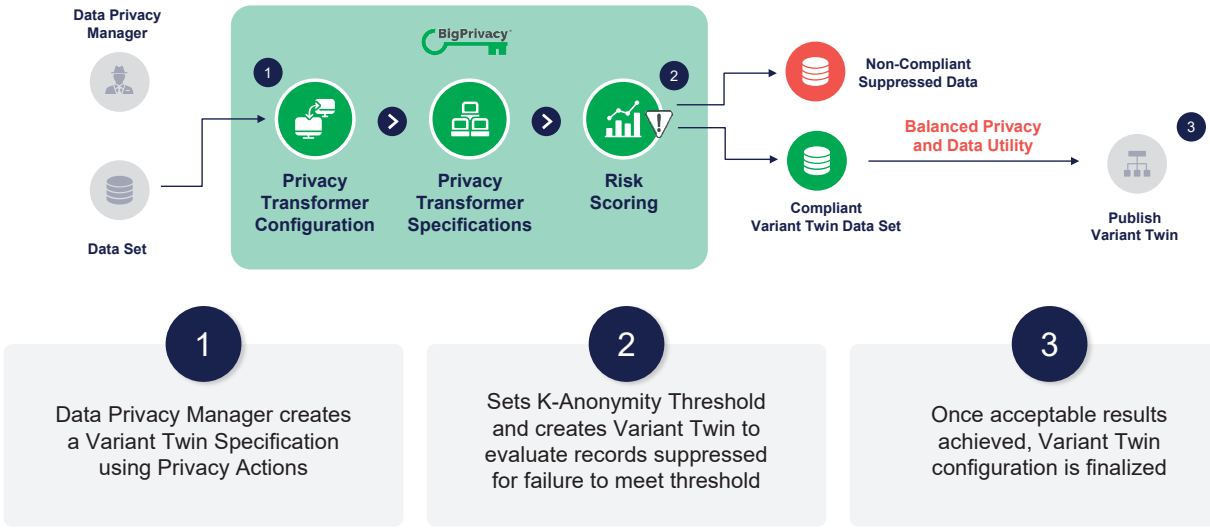


Image 5: Re-identification Risk Management

EXAMPLE

The following example illustrates how a Privacy Transformer creates a Variant Twin from an input dataset.

In the simple input dataset (see "A" in Image 6 below), there are four columns:

1. last name
2. bank balance
3. age
4. gender

CREATION OF A REPLACEMENT DYNAMIC DE-IDENTIFIER

The creation of a Replacement Dynamic De-Identifier (R-DDID) results in a fully randomised pseudonym uniquely generated for each row/record (see "B" in Image 6 below) using cryptographic pseudo-random number generation.

This row-unique R-DDID is a pseudonym for the entire record and enables controlled relinking to all elements for that record in the original source data record when authorised as described earlier. Thus, while the field "last name" is suppressed and not included in the example Variant Twin, it remains available for use in subsequent authorised processing.

Maximising data protection and maximising data utility have previously been approached as irreconcilable objectives. Variant Twins simultaneously achieve both objectives.

Variant Twins enable privacy engineers to achieve the benefits of the first goal of data protection while also achieving the second goal of maximising data utility. **This allows organisations to have it both ways - i.e., enabling them to "Have Their Cake and Eat it Too".**

PRIVACY TRANSFORMER CONFIGURATION

The Privacy Transformer is configured with a number of Privacy Actions. For example, the "balance" field is transformed into a new "balance_bin" field by rounding to the nearest thousand (see "C" in Image 6 below).

We create two different output fields pertaining to age, "age_bin1" and "age_bin2." The first, group values into bins, defined by 10-year ranges. Each occurrence of a specific age_bin1 value is then assigned a deterministic pseudonym called an Association De-Identifier (A-DDID).

By default, A-DDIDs are unique between tables and fields and consistent within fields, to reduce the risk of unauthorized re-identification. However, these can be configured to be consistent across fields or tables when required. The result of binning in the output dataset is four different pseudonymised bins, with two records belonging to the same bin "Age_KXYC" (see "D" in Image 6 below).

The second output field created pertaining to age is called "age_bin2" which creates bins of custom step size, included as cleartext. In this example, ages are binned between 18 and 25 and between 25 and 60 (see "E" in Image 6 below).

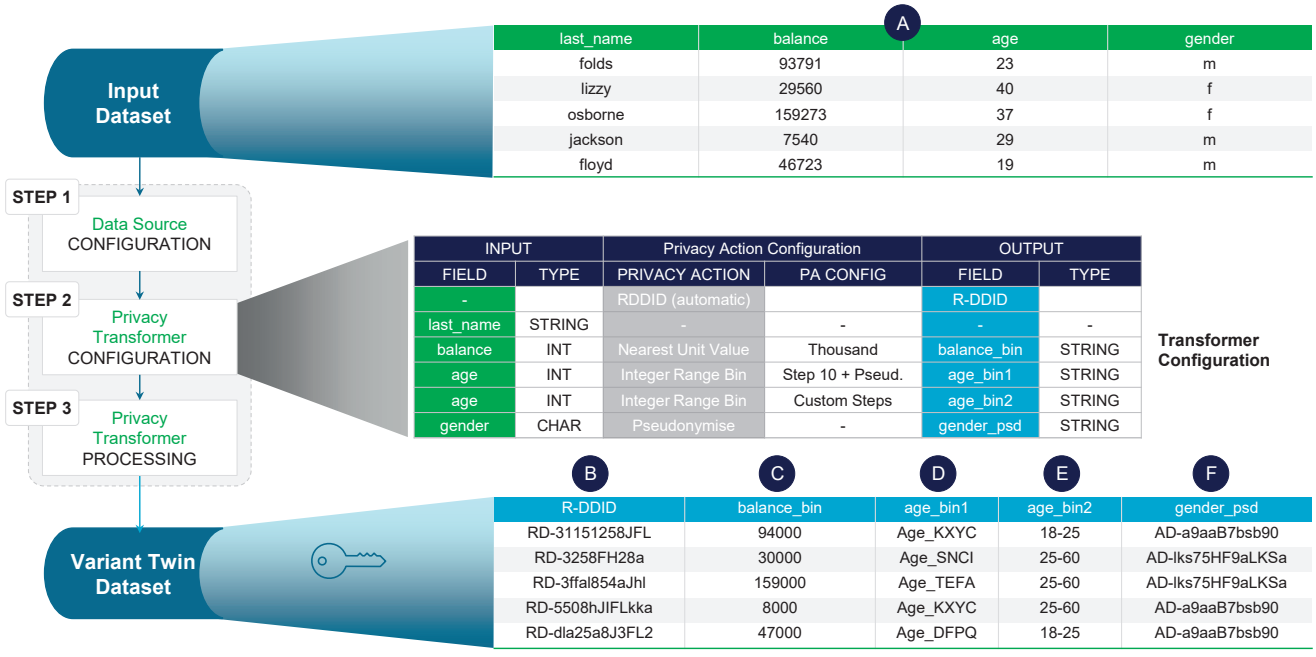


Image 6: BigPrivacy Internal Processes

The final step is the creation of two deterministic pseudonyms representing gender for male and female: AD-a9aaB7bsb90 and AD-lks75HF9aLKSa (see "F" in Image 6 above).

For illustrative convenience, the pseudonyms for "age_bin1" and "gender_psd" have been formatted to be much shorter in length.

BigPrivacy enables format preserving pseudonyms to allow for the utility they provide to be accessed in compliance with predetermined format requirements when necessary. When using format preserving pseudonyms, privacy engineers need to recognize the reduced size of the domain space for potential pseudonyms, and ensure the result still provides adequate privacy protection for the context of the intended processing.

The default format for pseudonyms is 32 characters (256 bits) for R-DDIDs and A-DDIDs, which is noted by ENISA[3] as **being considered secure even for post-quantum computing.[7]**

REDUCING THE RISK OF BIAS

By using pseudonyms to represent sensitive fields such as age ranges and gender, data analysts can process data without knowledge of the actual values, thus making the results of analysis more privacy-respectful and less identifying. This also reduces the risk of conscious or subconscious bias since data analysts cannot see the values underlying the pseudonyms and thus cannot make assumptions about the data subjects.

It is worth mentioning again, when referential integrity between fields/data sets is not required, by default different A-DDID pseudonyms are created for each field/data set for the same underlying value. Alternatively, the system default of creating different A-DDID pseudonyms can be overridden. This creates a consistent value between designated fields/datasets by using the same key with HMAC to create the relevant A-DDID pseudonyms.

Section 5

CONCLUSION

Variant Twins enforce statutory requirements (e.g., GDPR) and contractual requirements by digitising them. That is, Virtual Twins enable transformation of analogue (policy or contract-based) controls into digital (technically enforced) controls, which are then embedded into and flow with the data as Variant Twins to support "demonstrable accountability."

Variant Twins support GDPR compliant Pseudonymisation and Data Protection by Design and by Default to satisfy the balancing of interest test requirements for Legitimate Interest processing

enabling ethical and lawful data analytics, machine learning, AI, sharing and combining.

Anonos Variant Twin technology creates privacy-respectful ethical and sustainable data assets that:

1. **Deliver the Resistance to Re-Identification** of "Anonymised" Data
   a) For "locally protected" internal use
   b) For "globally protected" data sharing and combining
2. **Retain the Lawful Controlled Re-linkability** of Pseudonymised Data
3. **Preserve 100% of the Accuracy and the Full Utility** of Source Data
4. **Activate Express Statutory Benefits** of GDPR Pseudonymisation
5. **Enable Lawful Secondary Processing**

> Variant Twins enable digital controls to support GDPR compliant Pseudonymisation and Data Protection by Design and Default

ABOUT ANONOS

When you cannot rely on consent for data...Anonos® state-of-the-art pseudonymisation technology enables lawful repurposing of data while preserving 100% accuracy to maximise data utility. Anonos expands opportunities to ethically process, share and combine data in compliance with evolving data privacy regulations.

Anonos is the first and only company that resolves the conflicts between protecting the rights of individuals and achieving business and societal objectives necessary for lawful and ethical global repurposing of data for analytics, AI, ML, sharing, combining, and secure Multi-Party Computing (MPC). Gartner awarded Anonos "Cool Vendor" status for its innovative BigPrivacy® technology that creates non-identifying Variant Twins® that transform data into privacy-respectful data assets that embed privacy policies, via digital controls, at the data element level to satisfy statutory and contractual requirements for lawful data use. Learn more at www.pseudonymisation.com

SOURCES

[1] https://www.washingtonpost.com/opinions/our-privacy-regime-is-broken-congress-needs-to-create-new-norms-for-a-digital-age/2019/01/04/c70b228c-0f9d-11e9-8938-5898adc28fa2_story.html

[2] 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.

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

[4] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

[5] https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

[6] Controlled Relinkable Dynamic De-Identifiers consist of Replacement De-Identifiers (R-DDIDs) and Association De-Identifiers (A-DDIDs), as more fully described above.

[7] The term "post-quantum computing" (also referred to as quantum-proof, quantum-safe or quantum-resistant computing) refers to the ability to overcome the increasing vulnerability of cryptographic algorithms, otherwise thought to be secure, that can be efficiently broken by a sufficiently strong quantum computer.

REFERENCES TO ENISA DO NOT INDICATE ANY RELATIONSHIP, SPONSORSHIP, OR ENDORSEMENT BY ENISA. ALL REFERENCES TO ENISA ARE INTENDED TO CONSTITUTE NOMINATIVE FAIR USE UNDER APPLICABLE TRADEMARK LAWS

APPENDIX

Cross Reference of Anonos BigPrivacy Pseudonymisation Capabilities to Guidance by ENISA

Advances in pseudonymisation state of the art in beyond ENISA recommendations January 2020	Anonos BigPrivacy
Deterministic Pseudonymisation Applied to Indirect Identifiers	✓
Granular Controlled Relinking to Source Data	✓
Field Deterministic Pseudonymisation	✓
Table Deterministic Pseudonymisation	✓
Document Deterministic Pseudonymisation	✓

ENISA recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation November 2018 **https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions**	Section	Anonos BigPrivacy
Personal identifiers replaced with pseudonyms	2.1.1	✓
Pseudonyms do not allow the direct derivation of personal identifiers	2.1.1	✓
Personal data can no longer be attributed to a specific data subject without the use of additional information	2.1.2	✓
Pseudonyms applied to direct and indirect identifiers	2.1.2, 2.1.3	✓
Reversal of pseudonymisation is non-trivial in absence of additional information	2.1.2	✓
Additional information kept separately using technical and organizational controls to limit access	2.1.2	✓
Anonymisation techniques used to further reduce the possibility of third parties inferring identity	2.2	✓
Single input results in a decoupled pair of outputs: pseudonymous data and additional information necessary to reidentify	2.3	✓
Identify of data subjects hidden in the context of a specific data processing operation	2.3	✓
Any recipient or third-party having access to pseudonymised data cannot trivially derive the original data set and identity of data subjects	2.3	✓
Support for unlinkability across different data processing domains	2.3	✓
Support for accuracy by retaining access to both pseudonymised output and additional information necessary to reidentify	2.3	✓
Does not use Hashing without key or salt to generate pseudonyms	3.2	✓
Offers keyed hash function (HMAC, SHA2/3, 256+ bit keys) to generate pseudonyms	3.3	✓
Offers AES Symmetric Encryption with 256+ bit key as an alternative to generate pseudonyms	3.4	Evaluating Potential
Offers tokens (randomly generated values) as pseudonyms	3.4	✓

ENISA recommendations on shaping technology according to data protection and privacy provisions - Pseudonymisation techniques and best practices November 2019 **https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices**	Section	Anonos BigPrivacy
Enables a Risk-Based Approach accounting for required protection and utility/ scalability	Exec Summary	✓
Advances the State of the Art	Exec Summary	✓
Complies with GDPR Definition of Pseudonymisation	2	✓
Utilizes one or more Pseudonymisation Functions	2	✓
Utilizes a Pseudonymisation Secret	2	✓
Has a Recovery Function for Pseudonymisation Functions	2	✓
Uses a Pseudonymisation Mapping Table	2	✓
Attack Resistance	4.3	✓
Pseudonymisation Secret Discovery Attack Resistant	4.3.1	✓
Re-Identification (Linkage) Attack Resistant	4.3.2	✓
Discrimination (Inference) Attack Resistant	4.3.3	✓
Brute Force Attack Resistant	4.4.1	✓
Dictionary Search Resistant	4.4.2	✓
Utility and Data Protection Maximization	4.5	✓
Pseudonymisation Techniques	5.1	✓
Does not make use of Counters	5.1.1	✓
Uses Cryptographic Random Number Generator	5.1.2	✓
Does not use Cryptographic Hash Function with or without salts, peppers	5.1.3	✓
Uses MAC - keyed hash (HMAC)	5.1.4	✓
Uses Symmetric (deterministic) Encryption	5.1.5	Evaluating Potential
Uses Asymmetric (public/private) encryption	5.1.5	Evaluating Potential
Pseudonymisation Policies	5.2	✓
Supports Deterministic Pseudonymisation	5.2.1	✓
Supports Document Randomized Pseudonymisation	5.2.2	Evaluating Potential
Supports Fully Randomized - RDDIDs - both row and field level	5.2.3	✓
Offers Recovery Function (Reversal of Pseudonymisation)	5.4	✓
Protects Pseudonymisation Secret	5.5	✓
Advanced Pseudonymisation Techniques	5.6	✓
Supports Merkle Trees - hashes of sets of hashes	5.6	Evaluating Potential
Supports Hash Chains	5.6	Evaluating Potential
Bloom Filters	5.6	Evaluating Potential
Controlled Pseudonym Linkability	5.6	✓
K-Anonymity	5.6	✓
Aggregation/Generalization/Binning	5.6	✓
Rounding	5.6	✓
Masking	5.6	✓
Differential Privacy	5.6	Evaluating Potential
Prefix/Suffix-Preserving Pseudonymisation	6.2.1	✓
Format Preserving Pseudonymisation	7.4	✓

Anonos®

BigPrivacy® Unlocks Data

A Comparison to ENISA Guidance on Pseudonymisation

WWW.PSEUDONYMISATION.COM

CONTACT US AT
LearnMore@anonos.com