ANONOS

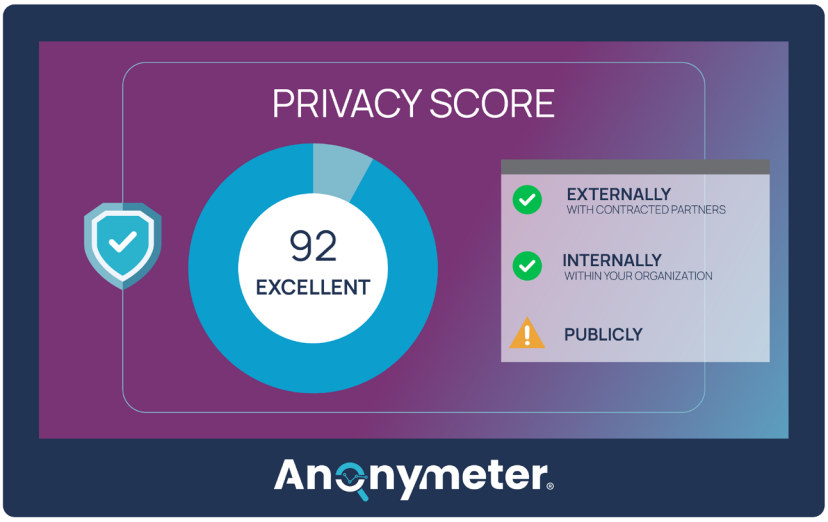
Data without the drama ™

Anonymeter®

The Tool for Evaluating Privacy Risks in Your Synthetic Data

Enterprises increasingly use synthetic data for privacy-preserving sharing of sensitive information. However, privacy risks cannot be fully eliminated. To comply with regulations, it is crucial to assess and document residual privacy risks.

Anonymeter is a software tool that measures the three main re-identification risks in synthetic tabular datasets, giving a comprehensive view of privacy vulnerabilities. Anonymeter is relevant for organizations using synthetic data due to its comprehensive, scalable framework for assessing and mitigating privacy risks. It helps organizations demonstrate the lawful anonymity of synthetic datasets in the sense of the General Data Protection Regulation (GDPR).



96%	92%	92%
INFERENCE SCORE	LINKABILITY SCORE	SINGLING OUT SCORE

> "The results produced by the tool Anonymeter should be used by the data controller to decide whether the residual risks of re-identification are acceptable or not, and whether the dataset could be considered anonymous. Anonymeter is a valuable tool, relevant in the context of personal data protection."

CNIL.

CNIL Technology Experts Department

1 Learn more at www.anonos.com/products/anonymeter

> Anonymeter has been presented in a peer-reviewed scientific paper and accepted at the 23rd Privacy Enhancing Technologies Symposium, which demonstrates its relevance and impact in the field of PETs."

Use Synthetic Data with Confidence

Evaluated by the French Data Protection Authority, CNIL, Anonymeter is easy to use, scalable, and robust, making it the perfect add-on for any organization that needs to protect sensitive data.

Comprehensive and Versatile Privacy Evaluations

Anonymeter is the only framework that measures the Singling-Out, Linkability, and Inference risks, the three criteria legally associated with re-identification risks. It is sensitive enough to detect even small amounts of privacy leaks, making it a useful tool for evaluating privacy risks in synthetic data or other data protection techniques. Anonymeter can be applied to a variety of datasets regardless of their data type.

Meets Regulatory Requirements

CNIL recognizes that Anonymeter is aligned with the European General Data Protection Regulation (GDPR) and is the first tool to introduce a coherent and legally aligned evaluation of the three key indicators of factual anonymization for each use case with synthetic data.

Interpretable and Easy-to-Use

Anonymeter is easy-to-use and interpretable by privacy engineers and compliance teams. It requires only basic data analysis skills to interpret its results and is easily incorporated into synthetic data generation and data governance pipelines.

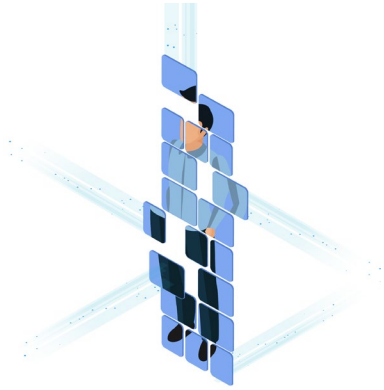
Fast and Efficient

Anonymeter simplifies synthetic data privacy evaluation, allowing organizations to reduce the time spent on developing compliant and robust privacy assessments. With Anonymeter, organizations can quickly identify and thus mitigate privacy risks, saving time and money.

Open Source and Modular

Anonymeter is open source, enabling transparency and community contributions. The tool allows for the integration of additional attack-based privacy metrics, making it an evolutive tool.

Linkability evaluator



Inference evaluator

Singling Out evaluator

Assess the Privacy Risks Associated with Synthetic Datasets

Anonymeter evaluates how an attacker can re-identify individuals in the dataset or infer sensitive information about them. It uses a range of metrics that specifically capture the de-anonymization attacks recommended by EU advisory body WP29, addressing various aspects of privacy risks:

- **Singling-out risk:** This metric measures the likelihood that an attacker can isolate a specific individual in the dataset. Anonymeter evaluates this risk by searching for unique combinations of attributes occurring for an individual in the dataset.
- **Linkability risk:** This metric measures the likelihood that an attacker can link two or more records in the dataset that correspond to the same individual, even if the individual's identity is unknown. Anonymeter evaluates this risk by analyzing the overlap of attribute values between different records in the dataset.
- **Inference risk:** This metric measures the likelihood that an attacker can infer sensitive information about an individual in the dataset based on their non-sensitive attributes. Anonymeter evaluates this risk by analyzing the correlations between different attributes in the dataset.

Anonymeter produces reports that summarize the privacy risks associated with the dataset and provides recommendations for mitigating those risks. Anonymeter also differentiates between privacy risks and useful information in synthetic data, ensuring that only privacy leaks are identified while preserving the utility of the data.

Share Compliant Synthetic Datasets

Anonymeter is useful for enterprises and data users concerned with the security and legal compliance of their synthetic data:

- **Synthetic data publishing:** Anonymeter can assess privacy risks in synthetic datasets used for research or publication, ensuring sufficient anonymization to protect individuals' privacy.
- **Synthetic data sharing:** Anonymeter can evaluate privacy risks in synthetic datasets shared with third parties, ensuring sufficient anonymization to prevent re-identification or sensitive information inference.
- **Compliance with privacy regulations:** Anonymeter can assess privacy risks in datasets to ensure compliance with privacy regulations like GDPR, HIPAA, or CCPA. It helps organizations meet the privacy standards required by these regulations for data anonymization.

Protect your data and comply with privacy regulations using Anonymeter. Try the open-source version today and see how easy it is to assess and mitigate privacy risks in your datasets.

Visit our website to get started.

Anonymeter version 1.0 measures re-identification risks in synthetic tabular datasets. Anonymeter version 2.0, which is currently under development, also measures re-identification risks in Statutorily Pseudonymized data.