Statice

Privacy and data protection with Statice

At Statice, we give your enterprise the tools to generate demonstrably anonymized data. Our risk-informed approach addresses the shortcomings of current data protection methods and fills the legal requirements for anonymization. We guarantee you maximum privacy and a compliant data protection mechanism so you can focus on making the most of your data.

Data protection beyond pseudonymization

Using **anonymized data** is ideal for many companies seeking to generate insights without the constraints imposed by personal data regulations.

When customers or patients are no longer re-identifiable, datasets are safer to use and processable outside the GDPR scope.

However, the **traditional techniques** that alter sensitive information, such as pseudonymization, data masking, or aggregation, **present a high privacy risk**.

Removing personal information, such as names or addresses, is not legally enough to anonymize data.

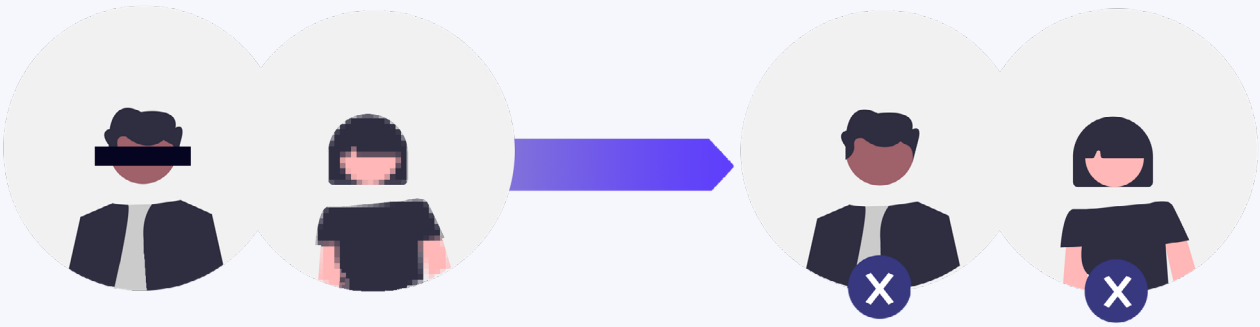
Given enough information, it's almost always possible to re-identify individuals from non-personal data. This risk constantly increases as the amount of publicly available information rises, multiplying the possibility of combining datasets to re-identify people.

Privacy-preserving synthetic data for anonymization

To ensure privacy, enterprises should **treat any customer or patient data as personal information** or expose themself to privacy disclosures and compliance fines.

However, this raises a challenge regarding data access enablement or maintaining data integrity for analysis. We designed our technology to address traditional data protection methods' pitfalls and anticipate technology or regulatory changes.

To do that, we approached **privacy risks both proactively and defensively.**



Pseudonymized or masked data can lead to individuals' re-identification.

Our comprehensive approach to privacy protection

Privacy-by-design

Our anonymization method treats all original data records as personal data. It **anonymizes your entire dataset**.

The software doesn't learn the specificity of individuals in the data. Instead, it focuses on the statistical properties of the datasets. There is **no one-to-one relationship with the original data** in the final synthetic data, which makes this approach, contrary to other anonymization methods, irreversible. There is no key to returning from the synthetic records to the original ones.

Additionally, you can **use Differential Privacy**, a robust privacy protection technique, in the synthesization process. This method uses noise to mask the presence of any particular individual in the input data.

Risk-based approach

We provide privacy evaluators that let you **run known privacy attacks on your synthetic data**. These evaluations are autonomous and let you measure the re-identification risks.

You can verify that **no attackers could link your** synthetic data to customer data records.

You can also ensure that the synthetic data doesn't leak any specific sensitive information from the original data.

Finally, you can confirm that no attackers could determine the presence of an individual in the synthetic dataset.

For which results?

Our protection mechanisms guarantee you **a safe synthetic data asset** that can not lead back to your customers' or patients' information.

In addition, with our **privacy metrics and evaluators,** you can assess and demonstrate that re-identification is sufficiently impossible.

Our approach and features ensure that your synthetic data is **private and safe**. Secondly, they make the generated synthetic data **legally compliant with the GDPR requirements** for data anonymization.

You and your team can use the data safely without the precautions imposed on personal data.

Get in touch to discover more about our solution

www.statice.ai/contact