

Unlocking secure data processing in the cloud

Whether it's sharing data for advanced analytics, collaborating with third parties internationally, or enabling faster speed to market, businesses are increasingly relying on the cloud. However, effective use of cloud technology is hindered by concerns around **data privacy and security, compliance with privacy regulations**, and the **inability to maintain data granularity**.

Enterprises that are unable to navigate these obstacles are often forced to forgo the cloud altogether, putting themselves at a **competitive disadvantage**.

“ If you are still contemplating the use of cloud technology, you are lagging behind 90% of major corporations that have already implemented a multi-cloud framework (451 Research). ”

Many companies that do use the cloud fail to implement adequate measures to safeguard their data. This results in **siloe data** confined to a specific cloud environment and increased **privacy vulnerability** once it leaves this environment.

“ CEOs see the twin challenges of cybersecurity and data sovereignty as the foremost risk factors impacting their businesses in 2023 and 2024 (IDC research). ”

Companies must develop a cloud security approach that:

- Allows data to maintain full utility and granularity in a cloud environment;
- Protects data in all its states - at rest, in transit, and in use - according to data regulations and internal policies;
- Unlocks all cloud data use cases;
- Enables faster speed to insight;

With Data Embassy, you can protect and use granular data in the cloud

The Anonos Data Embassy platform is the only technology that eliminates the tradeoff between data protection and data utility. The software combines privacy-enhancing technologies to control **what** identifying information is revealed, **to whom**, and for **what purpose**, allowing companies to protect and process data in the cloud without common restrictions.

How it works

First, protect; then store, share, and use highly granular data in the cloud

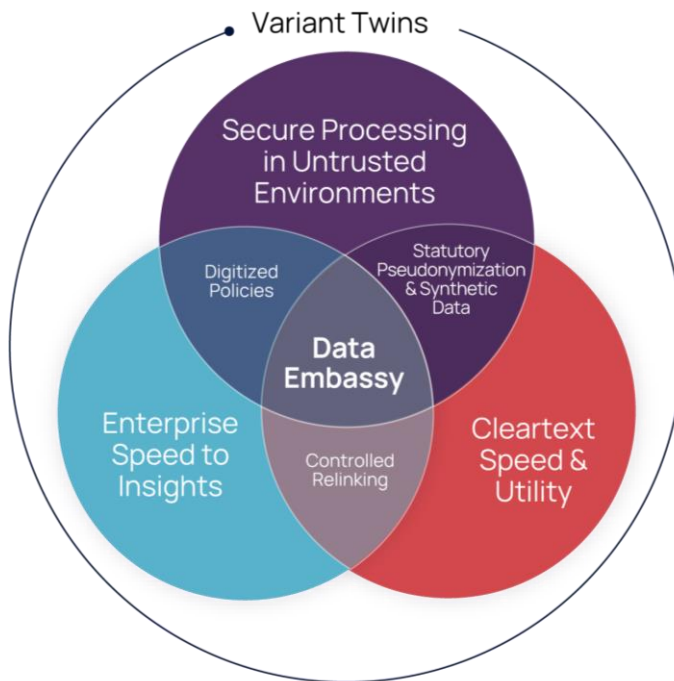
Data-at-rest encryption and access controls became the default modus operandi for securing sensitive data in the cloud. However, these methods can limit business insights and compromise data privacy because they:

- Only protect data within a trusted environment, leaving it vulnerable once it is moved;
- Isolate data, preventing it from being shared and combined for analytics, services, monetization, and enrichment.

Data Embassy works by creating non-identifiable yet 100% accurate variations of the source data, known as **Variant Twins**. Variant Twins are developed by applying a combination of techniques that **de-risk data without influencing its analytical value**. This data can be used beyond trusted environments, moved, and shared with third parties freely.

Data Embassy allows you to:

- **Anonymize your sensitive data before migrating to the cloud.** Synthesize sensitive data to create a new dataset that retains the statistical value of the original data while removing any personally identifiable information (PII). By irreversibly stripping away PII, synthetic data can be safely used in the cloud without compromising the privacy and security of the individuals.
- **Pseudonymize your sensitive data through Statutory Pseudonymization,** a combination of de-identification methods and dynamically changing codes to replace direct and indirect identifiers in the original data. Unlike data masking, which simply deletes sensitive information, Statutory Pseudonymization allows for authorized re-identification using the associated keys. This approach ensures that sensitive data remains protected in the cloud while still allowing for critical insights to be derived from the data.



Guaranteed privacy in accordance with data privacy regulations and internal policies

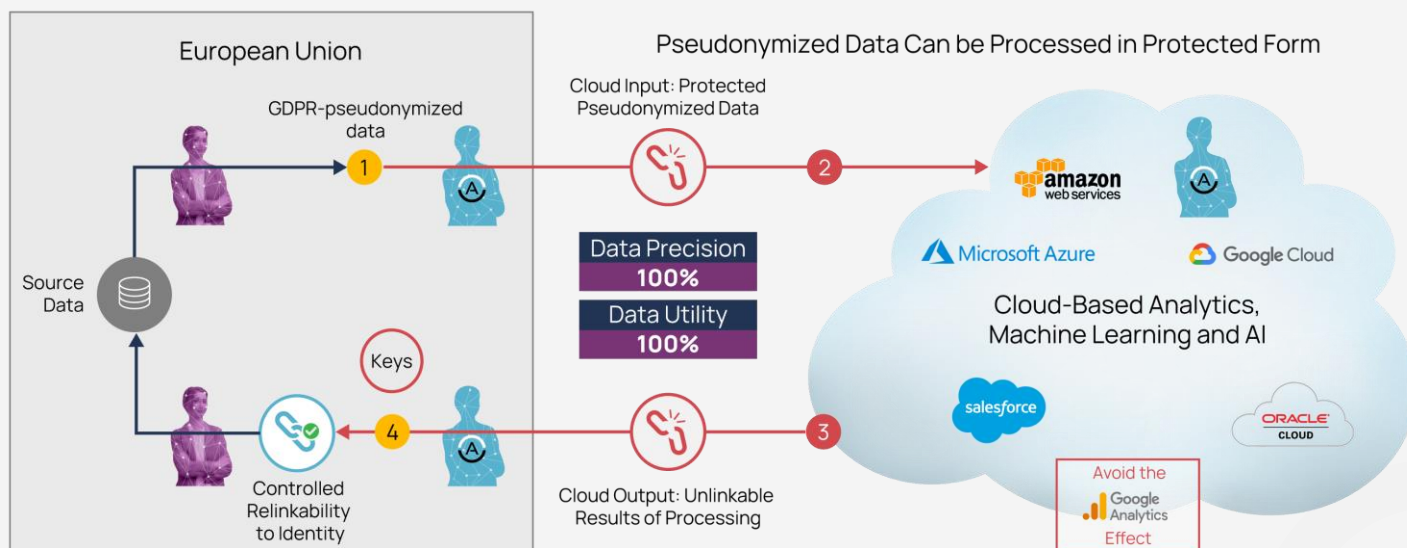
As a result of the Schrems II decision, the European Data Protection Board (EDPB) has issued [recommendations](#) that call for technical supplementary measures to prevent third-country surveillance. These obligations are especially relevant to cloud use cases, which frequently involve transferring data to third countries for storage or maintenance. Cloud tools and vendors like Amazon Redshift are often utilized in these instances.

A secure cloud infrastructure alone is insufficient for ensuring proper data protection in the cloud. It necessitates a comprehensive approach to maintain data privacy and security at all stages within the cloud

ecosystem: **at rest** (stored in the cloud), **in transit** (moving between cloud locations or applications, shared), and **in use** (processed).

- Data Embassy allows you to **protect it before it even reaches the cloud**, ensuring privacy, granularity and utilization for any use case.
- To guarantee and demonstrate the protection of sensitive data in the cloud, Data Embassy offers a set of **privacy evaluations that measure the level of privacy**. This is achieved through testing Variant Twins data against known re-identification attacks.

Migrating pseudonymized data to the cloud with Data Embassy



All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

“

Thanks to the Anonos solution, we were able to facilitate our data analytics project. With the help of Data Embassy, our team could securely share data with a partner in the cloud, all while maintaining the privacy and utility of our data.”

CTO at an international
IT management company






“

Data Embassy was a critical asset in enabling us to undertake a large cloud migration project while adhering to data regulations. Using Variant Twins, we were able to migrate our data to a cloud warehouse and demonstrate mathematically that our data protection is robust against re-identification attacks.”

DPO at a European bank

Through securing **data at rest, in transit, and in use**, Data Embassy powers more cloud use cases, lowering the risk of breaches and reducing cyber insurance expenses.

The benefits of using Data Embassy:

-  Data protection by design & by default
-  Faster time to access and insights for your team and authorized parties
-  Compliant customer and enterprise data migration, processing, and sharing in line with the GDPR & Schrems II
-  Maintaining the full granularity and utility of protected data
-  Maximized value through utilization with your current tech stack and cloud providers



Resolve the data protection
in the cloud dilemma

Contact us

Anonos is a global software company that provides the only technology capable of protecting data in use with 100% accuracy, even in untrusted environments, making otherwise restricted assets accessible to expand and expedite data-driven initiatives.

Anonos Data Embassy dynamic de-identification, pseudonymization and anonymization systems, methods and devices are protected by an intellectual property portfolio that includes but is not limited to: Patent Nos. CN ZL201880044101.5 (2022); JP 7,064,576 (2022); CA 3,061,638 (2022); AU 2018258656 (2021); US 11,030,341 (2021); EU 3,063,691 – Austria, Belgium, Croatia, France, Germany, Ireland, Italy, Luxembourg, Netherlands, Switzerland and United Kingdom (2020); CA 2,975,441 (2020); US 10,572,684 (2020); CA 2,929,269 (2019); US 10,043,035 (2018); US 9,619,669 (2017); US 9,361,481 (2016); US 9,129,133 (2015); US 9,087,216 (2015); and US 9,087,215 (2015); plus 70+ additional domestic and international patent assets. Anonos, Data Embassy, Variant Twin and Data Without the Drama are trademarks of Anonos Inc., protected by federal and international statutes and treaties.