Pseudonymization to support data privacy and maximize data utility

Building a better working world

What is pseudonymization and how does it support data privacy?

This whitepaper explores the challenges associated with data privacy and how organizations can use pseudonymization to protect data while achieving their business objectives. It is coauthored by Anonos, a provider of scalable, global pseudonymization and data protection software.

ANONOS

Anonos offers a single solution that minimizes risk and maximizes the utility of data globally.

What is pseudonymization and how is it different than anonymization?

Data privacy laws and regulations generally apply to “personal information” or information that identifies or is associated with identified individuals. Anonymization and de-identification techniques, therefore, reduce or eliminate data privacy compliance requirements. However, these techniques can greatly diminish the utility of the underlying personal information for business processes.

Pseudonymization provides high data utility and reduces data privacy risk, as summarized in the table below. It protects data throughout the data lifecycle (e.g., in transit, at rest, in use) while preserving the utility of the personal information for business processes.

Data format	Anonymized	Pseudonymized	Plain text
Relative data privacy risk	Low	Medium – low	High
Data utility	Low	High	High

The benefits of implementing pseudonymization from Anonos include improved data utility, accuracy in data analytics, and data minimization while reducing re-identification risk.[1]

Organizations are leveraging pseudonymization for many reasons, including:

1. Protecting data during analysis in cloud environments.
2. Privacy compliance with sector-specific laws and regulations (e.g., Health Insurance Portability and Accountability Act (HIPAA)).
3. Minimization of harm to data subjects in the context of data breaches.
4. As a supplementary measure for cross-border data transfers subject to the General Data Protection Regulation (GDPR).

Although this whitepaper focuses on the GDPR supplementary measure use case, organizations can apply pseudonymization to use cases that demand data protection with high data utility for business processes.

[1] “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data,” *European Data Protection Board,* www.anonos.com/?hsLang=en&__hstc=119096022.5e4638bb48a2e9f01ad915612534b67e.1647817303464.1647817303464.1647817303464.1&__hssc=119096022.2.1647817303464&__hsfp=351942391, June 18, 2021.

Pseudonymization can help protect data throughout the data lifecycle

Using pseudonymization to support compliance with Schrems II (GDPR)

The Schrems II decision in July 2020 and the subsequent guidance from the European Data Protection Board (EDPB) effectively require the use of data protection techniques (e.g., pseudonymization, anonymization, encryption) referred to as "supplementary measures" for transfers of personal data from GDPR jurisdictions to the United States and most other countries.[2]

The EDPB's guidance includes a use case, labeled here as the "cloud provider use case" involving transfers of personal data from data controllers in GDPR jurisdictions (e.g., European Union countries and countries with a GDPR adequacy decision such as South Korea and Japan) to cloud service providers in non-GDPR jurisdictions.

The cloud provider use case assumes that a transfer requires supplemental data protection measures.[3] The table below breaks the cloud provider use case included in the EDPB's guidance into three steps to illustrate the data protection challenge most organizations with transcontinental data flows will encounter.

Step	1	2	3
Actor	Data controller in a GDPR jurisdiction	Cloud service provider, non-GDPR jurisdiction	Cloud service provider, non-GDPR jurisdiction
Action	Encrypts cleartext data, sends data and key through an encrypted channel to a cloud service provider	Receives encrypted cleartext data, stores data in the cloud and places key in a vault	Uses the key to decrypt the data and process it in cleartext according to the controller's instructions
The data is protected:	✓ At rest ✓ In transit	✓ At rest	X Not protected in use

- The EDPB stated that the level of data protection highlighted in step 3 was insufficient to "prevent that access from infringing on the data subject's fundamental rights."
- **Encryption typically** protects data in transit and at rest but not data in use, with narrow exceptions such as homomorphic encryption. This makes it difficult to control data after it is received (e.g., in a shared cloud environment), increasing privacy compliance risk.

Benefits of pseudonymization over encryption in the use case above:

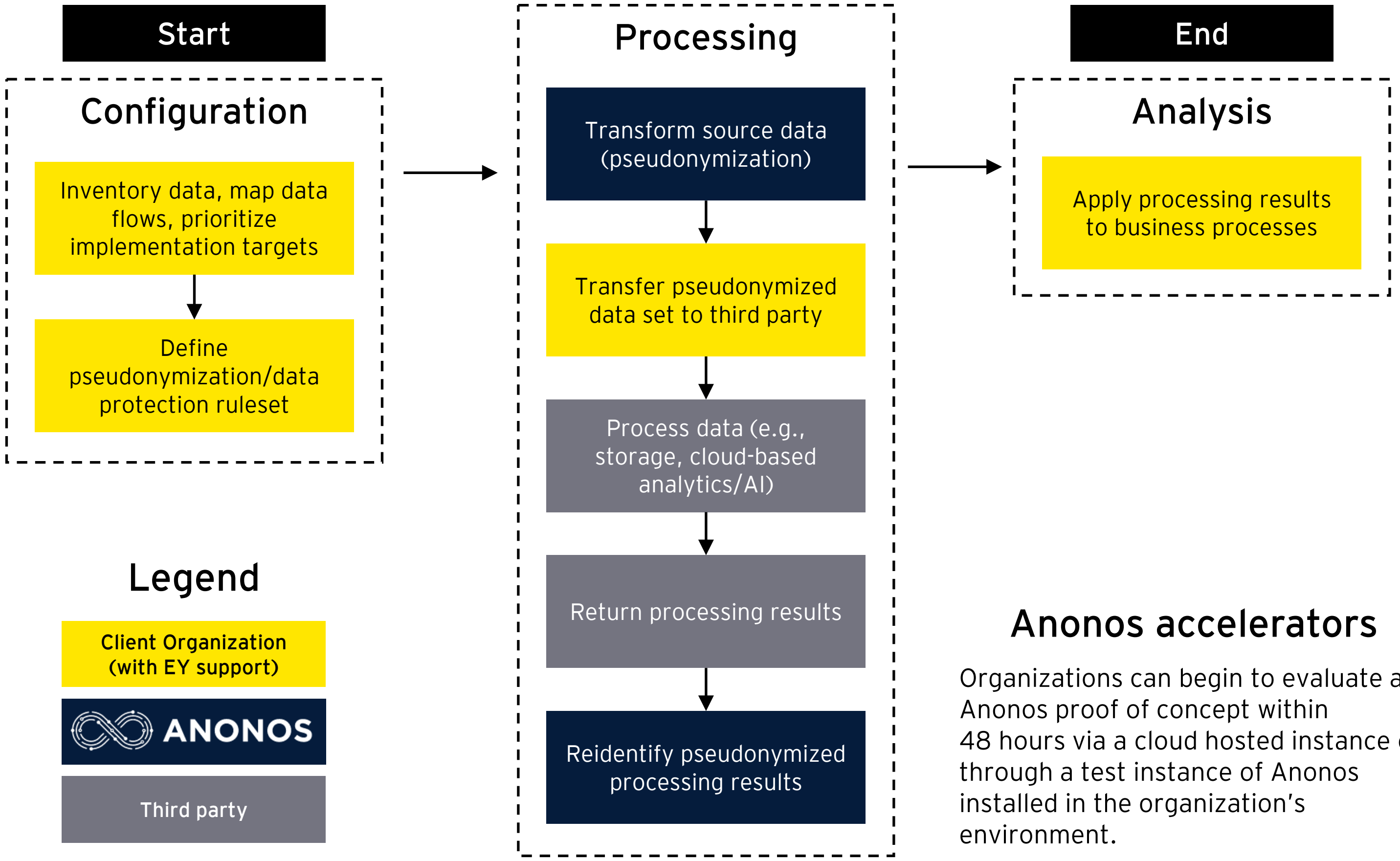
- The data sent by the controller is not "cleartext" data
- The controller is the only party that can reassociate the personal data with a data subject
- The controller can disassociate a data subject's identity while providing the cloud service provider with only the information needed to execute the processing
- The controller can apply the processing results to its data by reassociating the data subject identity later within a GDPR jurisdiction

[2] Ibid.

[3] Note that the EDPB's guidance includes additional steps transferring organizations must take before transferring personal data, including conducting a transfer impact assessment and assessing the legal protections in the destination country.

Representative pseudonymization implementation

Diagram of Anonos pseudonymization deployed in an organizational environment



Start

Configuration

Inventory data, map data flows, prioritize implementation targets

Define pseudonymization/data protection ruleset

Processing

Transform source data (pseudonymization)

Transfer pseudonymized data set to third party

Process data (e.g., storage, cloud-based analytics/AI)

Return processing results

Reidentify pseudonymized processing results

End

Analysis

Apply processing results to business processes

Legend

Client Organization (with EY support)

ANONOS

Third party

Anonos accelerators

Organizations can begin to evaluate an Anonos proof of concept within 48 hours via a cloud hosted instance or through a test instance of Anonos installed in the organization's environment.

Highlights of Anonos pseudonymization:

Once data has been pseudonymized with Anonos, only the data controller can re-identify the data.	Pseudonymized data can be relinked accurately and on demand.	Anonos supports real-time pseudonymization for streaming data transfer use cases.

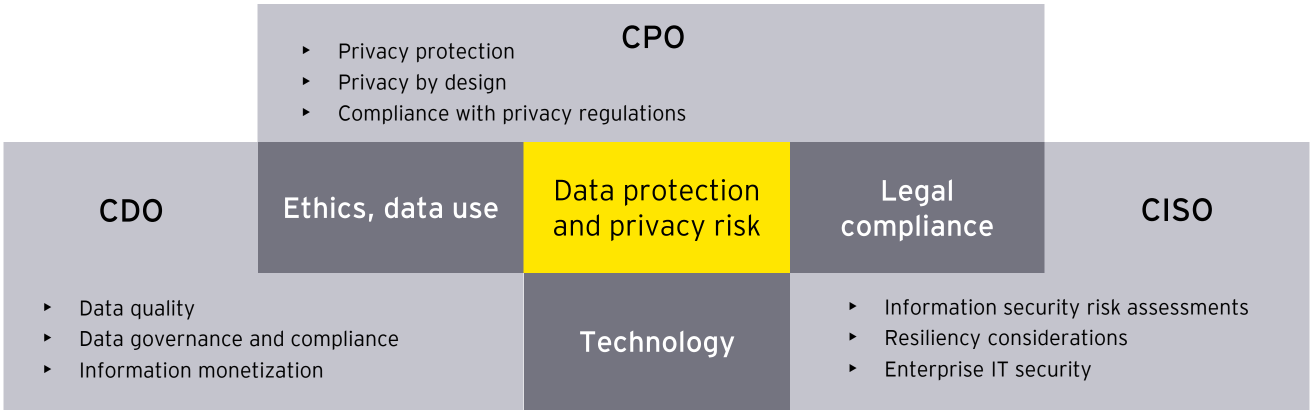
Key components of EY services that support Anonos implementations:

- **Operating Model:** Determine the scope of deployment, define roles and responsibilities, and develop detailed implementation project plans to meet key organizational objectives.
- **Change management:** Develop and document Anonos user stories, personas and use case profiles to support program objectives.
- **Data privacy:** Assess current privacy risk management processes, review data inventories, IT architecture, and data flow maps, identify existing privacy controls, capabilities and in-scope legislative and regulatory requirements, and identify in-scope systems and processes to prioritize targets for Anonos deployment.

Regulatory developments and market trends

Data protection and privacy risks are on leadership's agenda.
Pseudonymization can help mitigate data protection risks and contribute to other data-driven objectives.

Data protection and privacy risks are priorities officers share



CPO

- Privacy protection
- Privacy by design
- Compliance with privacy regulations

CDO

- Data quality
- Data governance and compliance
- Information monetization

Ethics, data use

Data protection and privacy risk

Legal compliance

Technology

CISO

- Information security risk assessments
- Resiliency considerations
- Enterprise IT security

Global regulatory developments

Regulators continue to reference and recommend pseudonymization as an effective data protection measure.

For example, the data privacy authority in France – Commission nationale de l'informatique et des libertés (CNIL) – published a white paper on digital payments and data privacy in November 2021 that stated:

"Due to the inherent difficulty in anonymizing payment data as well as the data's potentially sensitive nature, the **CNIL also recommends focusing on data pseudonymization**, data minimization, the determination of appropriate retention periods, and the careful selection of third-party recipients in order to comply with the principles of the GDPR, including obligations to ensure privacy by design and by default."[4]

Global market trends

Large technology providers are beginning to implement pseudonymization as a data protection method.

For example, Microsoft announced in September 2021 that:

Microsoft 365 Usage Analytics is changing how usage analytics data is collected in Microsoft 365 to help organizations comply with local privacy laws. In an effort to better protect the privacy of its customers, **Microsoft will change how usage analytics data is collected in Microsoft 365 to "pseudonymize user-level information" by default.**[5]

[4] "Quand la confiance paie: Les moyens de paiement d'aujourd'hui et de demain au défi de la protection des données," , www.cnil.fr/sites/default/files/atoms/files/cnil_livre_blanc_2-paiement.pdf, September 2021. *Commission nationale de l'informatique et des libertés*

[5] "Privacy changes to Microsoft 365 Usage Analytic," James Bell, *Microsoft 365 Blog,* techcommunity.microsoft.com/t5/microsoft-365-blog/privacy-changes-to-microsoft-365-usage-analytics/ba-p/2694137, August 30, 2021.

Contacts and contributing authors

Contacts

Reese E Solberg
Ernst & Young LLP
+1 206 262 7156
reese.solberg@ey.com

Angela Saverice-Rohan
Ernst & Young LLP
+1 213 379 4031
angela.savericerohan@ey.com

Scott Margolis
Ernst & Young LLP
+1 303 885 7728
scott.margolis@ey.com

Gary LaFever
Anonos inc
+1 303 747 3610
gary@anonos.com

Joseph Sommer
Ernst & Young LLP
+1 201 551 5231
joseph.sommer@ey.com

Adam S. Wright
Ernst & Young LLP
+1 602 322 3041
adam.wright@ey.com

Annabel Dalby
Ernst & Young LLP
+1 212 773 4218
annabel.dalby2@ey.com

Contributing authors

Sebastiano Rupp
Ernst & Young LLP

Lillyana Daza Jaller
Ernst & Young LLP

US SCORE no. ___________
2204-4023068
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com