IDC

ANALYST CONNECTION

Sponsored by: Anonos

Statutory Pseudonymization is a key privacy-preserving strategy for navigating the complex business challenges of the cloud and multi-party data sharing.

Statutory Pseudonymization: A New Approach to Cloud Data Privacy and Security

January 2023

Questions posed by: Anonos

Answers by: Carla Arend, Associate Vice President, Cloud Research, and Ralf Helkenberg, Research Manager, European Privacy and Data Security

Q. Who is responsible for protecting data when it is in use — the cloud provider or the cloud user?

A. Many organizations underestimate the risks and responsibilities that they own or share with cloud service providers (SPs). All cloud SPs work under a shared responsibility model that defines the security framework in terms of which security measures a cloud SP will provide and which security measures the customer will implement.

While security responsibilities will differ based on the specific services a customer selects (e.g., infrastructure as a service [IaaS], platform as a service [PaaS], or software as a service [SaaS]), cloud SP customers are ultimately responsible for protecting their data when it is in use to ensure compliance with regulatory, contractual, and other legal obligations. It is important for cloud customers to fully understand the sliding scale of cloud data security responsibilities that cannot be outsourced to the cloud SP. In broad terms, the cloud SP is responsible for the security of the cloud platform, and the customer is responsible for the security and compliance of its data, applications, and users on the cloud platform.

Q. Do perimeter and access controls offer adequate data protection?

A. The attack surface that organizations need to protect has expanded as a result of the shift to hybrid work, greater reliance on cloud services, accelerated digitalization, and sprawling data infrastructures across a multitude of locations. This great reshuffle requires organizations to rethink their data governance strategy and upgrade their privacy and security infrastructure to cater to these new and diverse IT environments.

Traditional perimeter-based security measures, such as access management, firewalls, and intrusion detection and prevention systems, no longer provide sufficient protection of corporate data when it is shared between multiple parties or processed in the cloud. Similarly, traditional end-to-end encryption offered by cloud SPs typically protects only data at rest and in transit. Sensitive data when processed in the open is unprotected and at risk of exfiltration.

If a data breach occurs, a cloud SP may offer to reimburse customers for fines, notify customers of government data production requests to the extent permitted, and pledge support for customers' standard contractual clauses (SCCs) and binding corporate rules (BCRs). However, these actions don't insulate customers from legal exposure for failing to protect the data while it was in use. They may provide some relief after the breach has occurred, but reimbursement for fines does not compensate for business disruptions caused by injunctions that prevent data access or negative publicity. Notifying customers about government data production requests is not always possible and is sometimes prohibited under applicable laws. And hosting data on EU-based servers does not prevent all disclosure risks from foreign governments.

Data de-identification through Statutory Pseudonymization closes the security gap by protecting data in use, thereby enabling organizations to collaborate as well as analyze and share data across borders and platforms in a privacy-compliant and secure manner.

Q. What is Statutory Pseudonymization?

A. Established under the General Data Protection Regulation (GDPR), Statutory Pseudonymization is a new legal and technical standard for mitigating data protection risks, and it has been identified by the European Data Protection Board (EDPB) as one way to lawfully process EU personal data in the U.S. cloud.

While traditional pseudonymization involves simple tokenization or masking, Statutory Pseudonymization is very different. In its final recommendations for Schrems II compliance, the EDPB set out the following five requirements for using Statutory Pseudonymization to lawfully process EU personal data in the cloud:

- » **Protect *all* data elements,** including both direct and indirect identifiers.
- » **Protect against singling out attacks** with either k-anonymity or aggregation.
- » **Use dynamism** to ensure the use of different tokens at different times for different purposes and at different locations so that re-linking is technologically prevented.
- » **Include non-algorithmic lookup tables** to account for the vulnerability of cryptographic techniques.
- » **Control re-linkability** to ensure source data is held separately by the data controller and available for re-linking only for authorized purposes.

Statutory Pseudonymization provides data protection by design and default to ensure appropriate security against internal and external threats, thus enabling sensitive data to be used for cloud computing and across data-sharing ecosystems.

Q. If Statutory Pseudonymization solves the problem of thoroughly protecting data, why isn't everyone using it?

A. While Statutory Pseudonymization is not a "silver bullet" or "golden shield" that solves all data security problems, it provides significant benefits. First, it does not require additional processing speed, and it produces the same accuracy of results as processing equivalent unprotected cleartext. Second, when implemented correctly, Statutory Pseudonymization reduces complexity by enabling scalable and predictable enforcement of pre-approved controls so that multi-party data-sharing and analytics projects move faster to deliver business outcomes.

Organizations that continue to rely exclusively on perimeter and access controls, together with encryption when data is at rest and in transit, are processing unprotected cleartext and therefore face potential exposure for failing to protect data when in use. But government and industry are often slow to change due to the up-front adjustments to existing operations and associated processes. However, consumers and regulators are requiring more data privacy, security, and governance, and data-driven enterprises are realizing the ROI in shifting from reactive to proactive data protection postures. With Statutory Pseudonymization, data privacy and accuracy are preserved, so organizations and their stakeholders benefit.

Q. Is it easy to transform data into a format that meets Statutory Pseudonymization requirements?

A. Yes, cleartext data can be transformed into a Statutorily Pseudonymized format behind a firewall before an organization submits it to the cloud. Alternatively, after an organization sends encrypted data to the cloud, cleartext can be decrypted and transformed into a Statutorily Pseudonymized format by leveraging confidential computing capabilities from a cloud SP. After data is transformed into a Statutorily Pseudonymized format, it can be processed anywhere for analytics, machine learning, artificial intelligence, and other uses.

By securely processing data in use as often as possible, organizations have a more defensible position when they need to re-link to identifying data — on an exception basis — to support use cases that require identity.

About the Analysts

	Carla Arend, *Associate Vice President, Cloud Research* Carla Arend is an Associate Vice President with the European research team and heads up IDC's European cloud research. Arend provides industry clients with key insight into market dynamics, vendor activities, and end-user adoption trends in the European cloud market. As part of her research, she covers topics such as how European organizations are adopting cloud, how cloud drivers and inhibitors are evolving, cloud management, cloud security, data management in the cloud, IoT and cloud, AI and cloud, DevOps and cloud, as well as GDPR impact on cloud and cloud code of conduct.
	Ralf Helkenberg, *Research Manager, European Privacy and Data Security* As research manager for the European Security group, Ralf Helkenberg provides insight and analysis on the European privacy and data security markets. His research covers the evolving regulatory landscape and the market dynamics and technology trends within privacy management, de-identification, data discovery, encryption, key management, and data loss prevention.

MESSAGE FROM THE SPONSOR

About Anonos

Anonos is a global innovator in data privacy and security, providing the only software platform that protects data in use with total accuracy. Its patented Data Embassy software transforms source data into Variant Twins: non-identifiable yet 100% accurate variations of source data required for specific use cases to achieve desired business outcomes. Because multilevel data privacy and security controls are embedded into the data and technologically enforced, Variant Twins can travel anywhere – across departments, outside the enterprise, or around the globe. Therefore, projects for capturing valuable insights can advance without compromising privacy, security, accuracy or speed.

To learn more, schedule a briefing at anonos.com.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.