Overcome Data-Use Obstacles with Technical Controls

January 2023

ANONOS

ANONOS

Data without the drama™

Three Imperatives to Capturing Use-Case Value

1. Protect Data When in Use

A. Reduce Cost: Reduce the volume and availability of sensitive data vulnerable to internal and external data breaches/ ransomware attacks by processing either synthetic or transformed, non-identifying, protected versions of data whenever, wherever, and as often as possible; limit the relinking and access to identifying data i) only to use cases requiring it and then ii) only to a select group of people only for authorized purposes under segregated secure conditions.

1) Example: Millions of health records are concentrated in patient registries by pharma and medical device companies. Transforming sensitive fields into protected, non-identifying versions enables ongoing processing but avoids a reportable event under state laws, decreasing liability upon a breach from potentially billions of dollars to nothing.

   a) Enable InfoSec teams to demonstrate the existence of "protection in use" technologies (beyond encryption to protect data when at rest and in transit) to qualify for cyber insurance.

   b) Enable boards of directors and C-suites to satisfy financial reporting obligations to disclose to stockholders the efforts implemented to reduce cybersecurity risk.

B. Increase Efficiency

1) Remove bottlenecks and maximize the efficiency of scarce personnel resources and improve time to data insights by automating both data synthesis and the creation of transformed data sets that technically enforce data protection policies by embodying the subject-matter expertise of company resources to accelerate project approval.

   a) Example: An online retailer can automate digital enforcement of policies for handling different types of data in different situations to enable the unlimited processing of data volumes for use cases satisfying pre-established requirements. This enables more efficient use of scarce data science and privacy/legal resources and accelerates speed to insight by limiting the time necessary to review new use cases to include only the unique requirements of each new use case - on an exceptional basis only - since common requirements among different use cases have already been approved. Bespoke project reviews that previously took several months can be reduced to only a few days, a 16X+ increase in productivity because 4X as many projects can be approved, each in 25% or less of the time.

2) Improve the predictability of processing. The limitations of Consent and Contract in complex processing situations is one of the reasons that Legitimate Interests exists as an alternate legal basis under the GDPR. However, the Legitimate Interests legal basis requires satisfaction of three tests: (a) Legitimate Purpose, (b) Necessity, and (c) the Balancing of Interests test. The Balancing of Interests test requires that the legitimate interest of the controller must be balanced against the interests and rights of the data subject, including the use of appropriate technical controls to honor the data subject's rights to data protection and privacy. When satisfied, the Legitimate Interests legal basis provides greater predictability of operations.

   a) Example: While informed consent of clinical study participants is required under EU clinical study law, the implications of withdrawal of consent is very different for clinical trial legal purposes (where withdrawal of consent requires that no new processing of data occur but allows for retention of processing results to date) versus under the GDPR (where withdrawal of consent requires no further processing together with deletion of all processing to date). As a result, EU regulators recommend using a combination of informed consent for EU clinical trial purposes and compliant Legitimate Interests processing under the GDPR to avoid unnecessary disruption to clinical trials.

   b) Example: A financial services provider concerned about the limitations of Consent and Contract under the GDPR desiring to use data for machine learning to build predictive models, where subsequent relinking to identify is not required can use data synthesis to create compliantly anonymous data for that purpose.

C. **Increase ROI:** increase the availability of internal and external data sharing opportunities by enabling more predictable, scalable and audible compliant operations using technical controls to improve risk management.

1) Reduced risk and increased confidentiality of data sharing and combining using independent and unbiased auditable technical de-identification capabilities eliminates the risk of working with third-party de-identification/aggregation services having competitive commercial objectives.

   a) Example: A pharmaceutical company may be willing to increase internal and external data-sharing for innovation and discovery initiatives because of improved risk management capabilities that provide greater autonomy and control over data-sharing activities.

2) Multi-use controls can reduce the risk of data misuse and unauthorized re-identification while preserving 100% accuracy compared to processing equivalent cleartext by leveraging a "privacy toolbox" approach that makes the best available techniques, alone or in combination, available to achieve desired business outcomes. By not relying on the capability of any one technique, users can avoid results that fail to reconcile data protection and utility goals.

   a) Example: During the last 2-3 years, severe limitations of single-use anonymization/de-identification techniques that were the standard for years have been highlighted due to the risk of revealing identity in subsequent processing. For example, the ability to re-identify data subjects from purportedly "anonymized data" - and keeping a copy of the source data - exposes the data controller to the full jurisdiction and liability under the GDPR. Similarly, numerous U.S. state laws now require additional limitations on the processing of data de-identified in accordance with HIPAA requirements, which do not adequately protect data from subsequent relinking to identity. In contrast, new advanced multi-use controls (like Anonos' Variant Twins) reduce the risk of data misuse and unauthorized re-identification while preserving 100% accuracy compared to processing equivalent cleartext by leveraging a "privacy toolbox" approach that makes use of the best available techniques to achieve desired business outcomes while reconciling conflicts between data protection and utility.

2. Remediating Data That Is Too Sparse/Biased/Withdrawn/ Withheld

A. **Limited datasets** - Synthetic data generation can help create additional data when available real-world data is too sparse or biased to enable robust AI/ML model development.

   1) Example: A medical device manufacturer that has completed a clinical trial for one bedside monitoring device could use synthetic data to refine applications for other bedside monitoring devices to better predict alarms and categorize them for improved caregiver response.

B. **Retention of information value** to enable desired business outcomes following the exercise of delete my data/right to be forgotten rights.

   1) Example: Transforming identifying customer data into a non-identifying version following a delete my data request enables non-identifying information value to be retained to avoid prior customers from trying to claim first-time customer discounts.

3. Satisfying Requirements for Surveillance-Proof Processing

A. **Schrems II**

   1) Example: Lawful processing of EU personal data in U.S.-operated clouds by using technical supplemental measures that prevent surveillance of data at an identifying level without the use of "additional information held separately and securely by the data controller in the EU.

B. **CLOUD Act**

   1) Example: Lawful processing of anonymized EU personal data on EU servers operated by U.S. firms by using synthetic data, preventing surveillance of data at an identifying level.

ANONOS

Data without the drama™

These summaries of Anonos-sponsored IAPP webinars feature the perspective of global experts on the requirements and benefits of technical controls to overcome obstacles for maximizing data utility and protection.

Data Without the Drama Webinar Series

Sponsored by Anonos with IAPP

Government and industry want to take advantage of:

- Economies of scale provided by cloud-based infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) delivered via networks of global sub-contractors and cloud processors; and
- AI, ML, advanced analytics, and other capabilities outside the scope of their internal capabilities offered by third parties, often as cloud-based software-as-a-service (SaaS) offerings.

This webinar series highlighted how the following can be achieved, enabling secure use of IaaS, PaaS and SaaS cloud-based offerings:

- **Breach-Resistant Processing**
- **Lawful Basis for Secondary Processing and International Data Transfers**
- **Defensible Data Supply Chain Sharing and Processing**

Webinar #1

Managing Data Breach Liability & Exposure

(26 October 2022)

anonos.com/webinars/managing-data-breach-liability-exposure

Data breaches are becoming increasingly common, and in some cases have resulted in criminal liability for the individuals who mishandled the response. The webinar examined how Statutory Pseudonymization helps to increase companies' cyber resiliency.

43% of webinar attendees answered **"yes"** when asked if they had suffered an external data breach.

62% answered **"yes"** when asked if they had experienced an internal data breach.

Key Highlights:

Statutory Pseudonymization:

- Reduces organizations' obligations under the GDPR, as far as notification to data subjects and regulators.
- Protects data, rendering it useless to any attacker in the event that a breach occurs.
- Allows organizations to obtain more comprehensive cybersecurity insurance.
- Enables compliance with minimization and purpose limitation.
- Facilitates secondary uses of data.
- Protects data both internally and externally.

All organizations have statutory obligations to notify individuals and regulators, when a breach occurs. However, these obligations are reduced if Statutory Pseudonymization has been applied. Odia Kagan (Fox Rothschild) noted that if organizations had "used pseudonymization [to protect data that had been subject to a breach] then that may have resulted in [it] not being a reportable breach." By protecting data in line with GDPR recommendations, organizations reduce their breach exposure in the first instance, as well as compliance obligations.

Joe Swanson (Carlton Fields) noted the crucial role that measures such as Statutory Pseudonymization can play in protecting organizations from the consequences of a breach once one has occurred, explaining that plaintiffs must always show that the breach caused harm. He noted that they would be "hard pressed to show that there was an injury when the data was otherwise unusable," such as when it has been pseudonymized in compliance with the GDPR. Gary LaFever (Anonos) agreed, explaining that "if you've in fact protected the data, so it's not revealing identity, then it's unlikely to result in harm."

Magali Feys (AContrario Law) also raised a key point, that from an insurance standpoint, organizations will also be more able to obtain cybersecurity insurance if they can show that they are using approaches such as pseudonymization to protect the data and protect the privacy of data subjects. Joe Swanson described it as a "game changer from a third party liability standpoint," with Magali Feys further explaining that "in contractual negotiations with regard to your limitation of liability cap … being able to refer to a good insurance policy is fundamental."

Odia Kagan noted that when it comes to data collection, "don't keep more than you need," explaining that "if it's not there, a hacker can't get to it." She went on to explain that "pseudonymization … both allows you to comply with your data minimisation, it is more likely to allow more secondary uses to fall in the umbrella of compatibility, and then also you know that at the "deep end" it minimizes the consequences of breach." This highlighted the multi-purpose benefits of Statutory Pseudonymization. Odia Kagan also explained that "Colorado actually lays out what you need in order to satisfy the components for compatibility and one of them they're saying is the existence of additional safeguards, such as encryption or pseudonymization … Pseudonymization is one way to enable compatible secondary uses of the data."

Importantly, Joe Swanson noted that a data breach can also be "malicious acts by an insider … an employee leaving and looking to start a business and taking with him or her a bunch of personal information … And then there's also just human error [such as] leaving a laptop in a taxi cab or losing a thumb drive somewhere." Statutory pseudonymization protects against data breach in both of these cases, by protecting data for both authorized persons and authorized uses, no matter where the data is.

Webinar #2

Operating the U.S. Cloud Under Schrems II

(3 November 2022)

anonos.com/webinars/operating-the-us-cloud-under-schrems-ii

80% of webinar attendees rated software-as-a-service as the most important cloud-enabled capability that their organizations need to use.

86% of webinar attendees believe the new proposed EU-US Data Privacy Framework will fail to withstand judicial scrutiny and not be sustainable because it fails to address Schrems II requirements for supplementary technical measures.

Organizations are evaluating the use of technical measures to protect data when processed in the cloud given the critical importance to their commercial operations, particularly after the Schrems II ruling that struck down the EU-US Privacy Shield. This webinar explored how Statutory Pseudonymization addresses the legal issues surrounding the use of U.S.-operated clouds to enable lawful data transfers.

Key Highlights:

- Organizations are protecting data at rest and in transit with encryption and access controls, but often no controls are used to protect the data when it is being processed in cleartext. Numerous data breaches and enforcement actions highlight this issue.
- Technical controls that protect data in use are important for protecting against breach and making desired processing in U.S. operated clouds lawful.
- EU and US laws are often in conflict. Technical controls can help to bridge conflict-of-laws issues.
- The Schrems II ruling has sparked new interest in the CLOUD Act, and the interplay between US cloud companies, other US companies, and EU data subject rights.
- Technical measures can protect against CLOUD Act requests and help reconcile Schrems II issues with EU data subject data.
- Statutory Pseudonymization is one way for organizations, governments, and companies to process data in a way that is predictable and lawful to enable data-driven insights.

Magali Feys (AContrario Law) noted some of the key political issues, particularly that the EU and US are coming from different political and historical settings, explaining that we "cannot really expect that the US is going to turn 180 degrees to adopt European philosophy." Cynthia O'Donoghue (Reed Smith) continued, explaining that there is always a "tension between interpretation of enforcement, what the law says, and what treaties or other mechanisms might be in place … technical controls help to bridge the differences between laws."

Panelists particularly noted the revival in interest in relation to the U.S. Clarifying Lawful Overseas Use of Data (or CLOUD) Act after the Schrems II ruling. Despite the fact that the CJEU didn't mention the CLOUD Act in their ruling, Alex van der Wolk (Morrison & Foerster) highlighted that "the DPAs, the authorities in Europe have started to cite … the Schrems II decision on the CLOUD Act because they say even though there may not be an actual transfer upfront, that potential [for a transfer] is what is making it problematic." This indicated the far-reaching nature of the Schrems II case, and the need for measures such as Statutory Pseudonymization that can help organizations to comply with Schrems II and resist CLOUD Act requests, reconciling US and EU law in the absence of a reliable cross-border treaty. Gary LaFever (Anonos) explained that "a lot of people would like to take advantage of what the cloud has to offer … [so] how do we enable all organizations, governments, and companies to do so in a way that actually is predictable and lawful? … it is possible to protect data in untrusted environments like the U.S. cloud using Statutory Pseudonymization."

Webinar #3

Preventing Data Supply Chain Issues Under the U.S. CLOUD Act and EU Law

(9 November 2022)

anonos.com/webinars/preventing-data-supply-chain-issues-us-cloud-act-eu-law

100% of the audience said the sharing and processing of data with other legal entities and third parties is necessary for their organizations.

97% of the audience also indicated that the potential liability from data supply chain partners failing to protect data when in use is an issue for them.

91% At the close of the webinar, 91% of the audience said they either (i) realize their organization should be using Statutory Pseudonymization because of the benefits it provides or (ii) they would like to learn more about Statutory Pseudonymization.

As evidenced by our in-webinar polling, data sharing and processing with other legal entities and third parties is necessary for organizations to operate. However, significant liability issues can arise when data supply chains flow outside the organization's control; if data is processed as unprotected cleartext, cloud providers and users are subject to joint and several liability for data breaches. This webinar discussed how Statutory Pseudonymization improves compliance and mitigates risk when processing European Union and other foreign data using the U.S. cloud and related technology.

Key Highlights:

- The use of the U.S. cloud as part of organizational data supply chains is critical and needs to continue for both operational and business reasons.
- Joint and several liability and the shared responsibility model apply to the use of the cloud, for cloud providers and cloud users. Increasing technical protections such as through the use of Statutory Pseudonymization can reduce the risk of breach and help organizations more easily obtain cybersecurity insurance.
- Schrems II and other guidance does not intend to prohibit the use of the U.S. cloud: instead, compliant use is the intention by leveraging technical controls.
- Access controls and encryption only protect data in transit and in storage, but most data is still processed in cleartext, leaving it vulnerable to breach.
- The U.S. cloud can be used in a compliant manner with appropriate technical and organizational controls.
- Statutory Pseudonymization allows EU-US transfers and compliant processing, including compliant further processing in the cloud for AI, ML and analytics.

When it comes to the CLOUD Act and Schrems II, Herald Jongen (Greenberg Traurig LLP) explained that there has been a "debate in Europe about whether we should use EU companies only or EU-based clouds only or EU only clouds," but that this is a false solution that is not necessary. Importantly, by avoiding the cloud Magali Feys (AContrario) raised the issue that customers may end up keeping their data somewhere "less secure than in a trusted cloud environment … it's not about avoiding EU-US data transfers. I don't think that was ever what the Schrems II decision was about. Rather, when you do it, you must implement technical safeguards and organizational safeguards in addition to addressing legal and ethical requirements." Mark Webber (Fieldfisher) continued, noting that "The ability to control [the protection of data] is what we're talking about. As a controller, you must pay attention to the details of end-to-end processing and understand where the data comes from and where it goes, and maintain control throughout the entire data supply chain. You must be able to protect data as it cascades and moves around … You've got to be in control over data no matter where it is used."

In the context of ESG and other broader corporate issues, he also noted that the question of data protection and the ethical use and processing of data is now a "Board level issue" from a risk perspective. But this does not mean that the US cloud should be avoided completely. Herald Jongen reassured webinar attendees that "compliant use of the cloud with US cloud providers is absolutely possible." In particular, Gary La Fever (Anonos) noted that by "implementing technical controls with the right legal analysis and the right context, you can dramatically reduce the processes that require unprotected cleartext." Specifically, the use of Statutorily Pseudonymized data helps you to continue EU-US data transfers, the use of the US cloud, and it "limits your exposure for data breach," while being able to maintain "100% accuracy without requiring additional processing time or expense than used when processing unprotected cleartext."