SHARDSECURE

White Paper

Microsharding for Cross-Border Data Protection

Cross-Border Data Protection: An Overview

In recent years, dozens of cross-border data protection laws have been passed to ensure the safe transfer and processing of personal data around the world. 71% of countries have adopted some form of data protection and privacy legislation, and another 9% have draft legislation on the books. Many international governmental organizations have also passed data privacy laws or released guidelines, including the European Union's General Data Protection Regulation (GDPR), the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, and the African Union Convention on Cyber Security and Personal Data Protection.

While these data privacy laws vary in their exact mechanisms and enforcement, most require companies to implement specific data retention policies, report data breaches to the relevant government agency, and receive the clear, informed consent of data subjects. Most also require specific security measures for cross-border data transfers and for processing personal data in the cloud. Ensuring compliance with each data privacy law can be a full-time job for an IT team.

Luckily, there are solutions to help organizations meet the security requirements of many cross-border data laws. In our white paper on GDPR/Schrems II compliance, we cover how ShardSecure's patented approach to data protection helps organizations satisfy specific requirements for GDPR-compliant processing of personal data in the cloud. Here, we'll discuss the benefits of microsharding for broader cross-border data protection.

The state of cross-border data protection

The importance of free data flows cannot be overstated. Cross-border data transfers are already estimated to contribute $2.8T to global GDP each year, with 2.5 quintillion bytes of data generated every day. The majority of this value comes from data transfers in traditional industries like agriculture, logistics, and manufacturing. Six billion consumers and 25 billion devices are expected to be digitally connected by 2025.

The G20 Ministerial Statement on Trade and Digital Economy makes it a point to state that the cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development. The nonpartisan Information Technology & Innovation Foundation think tank goes further, stating that a 1% increase in a nation's data restrictiveness cuts its gross trade output 7%, slows its productivity 2.9%, and hikes downstream prices 1.5% over five years.

"Restricting data flows has a statistically significant impact on a nation's economy — sharply reducing its total volume of trade, lowering its productivity, and increasing prices for downstream industries that increasingly rely on data," the think tank notes.

At the same time, personal data also needs to be protected from unlawful processing, poor security, and unauthorized access. Data leaks, loss, and theft must also be prevented so that highly sensitive information is not revealed. To provide this protection, a number of cross-border data privacy laws have sprung up, many of which frame digital privacy as a human right.

The most well known of these laws is the European Union's General Data Protection Regulation (GDPR). But many individual countries have also implemented their own standards and regulations, including:

- Australia's Privacy Act 1988
- Brazil's General Data Protection Law (LGPD)
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- Japan's Act on the Protection of Personal Information (APPI)
- South Korea's Personal Information Protection Act (PIPA)

Below, we'll cover specific data processing requirements under some of these key regulations.

Data protection under the GDPR

One of the strongest laws of its kind, the GDPR is designed to protect the privacy of personal data within the EU. It is extraterritorial in scope, imposing strict obligations on any organization, regardless of location, that processes EU personal data. This includes both American cloud service providers (CSPs) and any other third parties around the world that process, collect, store, and share personal data.

Enforceable since May 2018, the GDPR is intentionally broad to protect the privacy rights of all people in the EU, regardless of their citizenship or legal status. It carries fines of up to €20M, or up to 4% of the organization's annual global turnover from the preceding financial year, whichever is greater. In practice, this has resulted in recent penalties like Amazon's €746M fine (2021) and Instagram's €405M fine (2022).

To comply with the GDPR, organizations must:

- Clarify how people's personal data is collected, processed, used, and stored.
- Receive clear and informed consent from the data subject themselves before collecting, processing, or otherwise using that person's data.
- Allow people to control their own data, including moving, correcting, and deleting said data.
- Offer special protections for certain categories of sensitive data, including data about people's medical histories, race, religion, political opinions, and more.
- Incorporate adequate data security and privacy-by-design into their systems.
- Provide notifications when data breaches occur.
- And much more.

Schrems II and Use Case 5

Schrems II, the 2020 data privacy verdict issued by the European Union's Court of Justice, is a major facet of GDPR compliance. It invalidated the 2016 EU-US Privacy Shield data transfer mechanism, which provided a way for American companies to process data in compliance with the GDPR, on the grounds that it was insufficient to protect EU personal data. This decision in turn invalidated the entire legal basis for free data flows to the US.

The result of Schrems II is that organizations are now limited in terms of the data transfer tools they can use when handling EU personal data. Instead of relying on standard contractual clauses (SCCs), companies must make case-by-case assessments of recipient countries' data protection policies, and they must supplement their data transfer tools when needed.

In June 2021, the European Data Protection Board (EDPB) outlined how to make these assessments and clarified five key use cases comprising five acceptable types of supplementary measures to protect personal data. One of these, Use Case 5, focuses on split or multi-party processing.

As will be discussed below, ShardSecure fits the criteria for Use Case 5. Our Microshard technology splits personal data in a way that makes it uninterpretable and unintelligible to unauthorized parties.

Data protection under other cross-border data regulations

While the GDPR is the best-known data protection law, 137 out of 194 countries have passed their own legislation to ensure the security of personal data. The severity of cross-border data laws can vary, with countries like China, South Africa, Canada, and Singapore instituting some of the strictest legislation.

The exact means of complying with these laws varies, but there are strong overall similarities among many cross-border data frameworks. For instance, most organizations must:

- Receive the clear, informed consent of data subjects before collecting, processing, storing, or otherwise using their data.
- Implement strong data security safeguards, including privacy-by-design.
- Create data retention policies, binding corporate rules, and/or data processing agreements.
- Allow data subjects to transfer, correct, delete, and/or control the use of their own data.
- Report data breaches to the relevant government agencies and to data subjects.

The penalties for noncompliance with cross-border data protection laws can range from six figures to multi-million dollar fines. For a more detailed breakdown of common cross-border data protection fines, visit our cross-border data protection solution brief.

Microsharding for cross-border data protection

Microshard technology works by splitting data into very small pieces (microshards) and then distributing those containers to multiple customer-owned storage locations. The microsharding process ensures that data is unintelligible to unauthorized users, including cloud providers and global organizations. It was created for the express purpose of preventing third-party entities from reassembling data. Unlike encryption, it cannot be broken.

Maintain compliance by maintaining control

Ultimately, Microshard technology helps with cross-border regulatory compliance by keeping control of data in the hands of the data owner.

With ShardSecure, organizations can configure the number and geographic location of their storage containers, meaning that they can use a mix of on-premises and cloud storage providers. They can also store data in the jurisdictions of their choice, and they can employ multi- or hybrid-cloud architectures if they choose. This flexibility allows companies to mitigate data transfer risks and data sovereignty concerns.

No storage provider will be able to read an organization's information; not even ShardSecure can store or read customer data. Even if microsharded data is subpoenaed or exposed in a breach, the organization remains in full control.

Preventing unauthorized access

There are a number of measures in place to prevent microshards from being reconstructed. Even in the highly unlikely scenario that someone is able to gain access to all the microshards from every storage location for a given data set, those microshards still cannot be reassembled.

First, the microsharding process strips filenames, file extensions, and all other metadata. That means that no set of microshards contains enough identifying information for attackers to figure out how to reassemble them.

Second, organizations can choose to add a configurable amount of poison data to their real data. Unauthorized users have no way of knowing which data, or how much of it, is real and which is a decoy.

Third, microsharding does not rely on keys, so the issues of third-party key ownership and key management are nonexistent. This also means that, unlike encryption, microsharding cannot be "cracked" by well-resourced attackers, and it does not face imminent risks from quantum computing.

Finally, it's not possible for a third party to deploy their own instance of ShardSecure to reassemble data, as there are multiple components within the ShardSecure solution that must be used in concert with both each other and the complete data set. Once it has been microsharded, data can only be reconstructed by the original owner.

Microsharding for Schrems II and the GDPR

Microsharding allows organizations to meet compliance with the GDPR and the Schrems II ruling. Microshard technology is a split processing technology that can be easily deployed in a multi-party processing environment. As such, it allows organizations to process and store data safely under Use Case 5 of Schrems II.

Organizations should always consult a lawyer before making changes to GDPR or other regulatory compliance processes. See our GDPR/Schrems II white paper to learn more about how microsharding meets the requirements of Use Case 5.

Ensuring data resilience, availability, and integrity

In addition to protecting data from being read by unauthorized users, Microshard technology also prevents it from being lost, deleted, tampered with, or otherwise compromised in outages and attacks.

Our self-healing data uses multiple data integrity checks to detect any form of tampering with microsharded material. If any problems are detected, automatic controls begin to reconstruct the affected data immediately and transparently, returning it to its original state. Security teams are alerted, and data is reassembled in real-time to avoid costly downtime and disruption to users.

This feature keeps data available and accurate — even in the face of ransomware attacks, cloud provider outages, and more. As a result, organizations maintain their critical operations, uphold their business continuity, and avoid a reportable security breach.

Ease of access and integration

Despite its powerful data security and resilience features, Microshard technology has no significant impact on applications and no visible changes to employee interfaces. Microsharding happens in the background as a zero-downtime event, and it allows instant access to data when it's needed. It also allows for fast, seamless migration of data among different storage locations with just a few clicks.

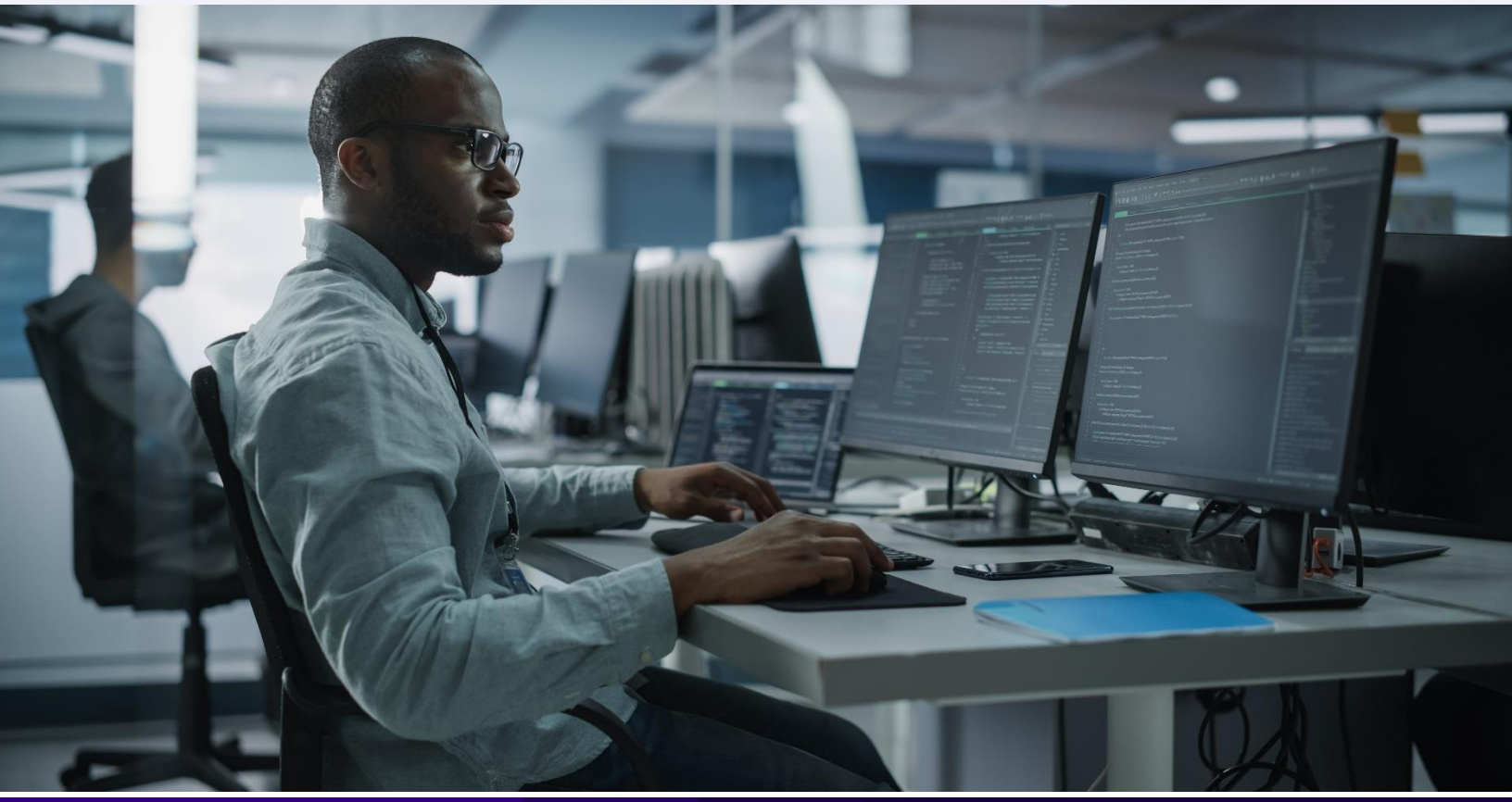
A transparent, vendor-agnostic solution, ShardSecure appears to other applications as a storage location. Its S3-compatible API and iSCSI module mean that microsharding is extremely easy to manage and quick to integrate; only one line of code change is required. Companies can use ShardSecure to maintain control of their data and meet cross-border data protection requirements without making changes to existing workflows, retraining employees, or redeveloping applications.

Conclusion

In the world of global commerce and global cyberthreats, cross-border data regulations are only becoming more numerous and more onerous. Meeting the burden of compliance while maximizing cost savings can be a challenge for many organizations.

ShardSecure offers an innovative approach to cross-border data protection. With its split processing technology, self-healing data, ease of integration, and ability for organizations to control where their data is stored, Microshard technology makes compliance achievable and cost-effective for organizations around the world.

For more information on microsharding and cross-border data protection, visit us online or schedule a demo today.



@ShardSecure
@ShardSecure
@ShardSecure

101 Avenue of the Americas
9th Floor, New York, NY 10013
United States of America

info@shardsecure.com