SHARDSECURE

White Paper:

Strengthening 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 bodies 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 transferring data across borders, securing data at rest, and processing personal data in the cloud.

Ensuring compliance with each data privacy law can be a full-time job for IT and security teams. Fortunately, there are solutions focused on helping organizations meet the security and privacy requirements of many cross-border data laws.

The state of cross-border data protection

The importance of free data flows to commerce cannot be overstated. Cross-border data transfers are already estimated to contribute $2.8 trillion to global GDP each year, with 2.5 quintillion bytes of data generated every day. The volume of data will likely continue to grow, as an estimated six billion consumers and 25 billion devices are expected to be digitally connected by 2025.

In general, 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 states that a 1% increase in a nation's data restrictiveness cuts its gross trade output by 7% and slows its productivity by 2.9%: "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."

At the same time, personal data also needs to be protected from unlawful processing, internal/external threats, and unauthorized access. Data leaks, loss, and theft must be prevented so that highly sensitive information is not disclosed publicly, and digital privacy must be recognized as a human right.

Below, we'll cover specific data processing requirements under some key cross-border data protection laws. The most familiar is the EU's General Data Protection Regulation (GDPR), but many 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)

Data protection under the GDPR

One of the best known data protection laws, the GDPR is designed to protect the privacy of personal data within the EU. It imposes strict obligations on any organization that processes, collects, stores, or shares EU personal data, including American cloud providers.

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 company's annual global turnover from the preceding year. In practice, this has resulted in recent penalties as large as €746M (Amazon, 2021) and €1.2 billion (Meta, 2023).

Compliance with the GDPR is complicated by Schrems II, the 2020 data privacy case that invalidated the legal basis for free data flows from the EU to the US. In response to the ruling, the European Data Protection Board (EDPB) outlined five acceptable types of supplementary measures to protect personal data. In our white paper on GDPR/Schrems II compliance, we explain how ShardSecure's technology has been validated by independent privacy attorneys to meet the requirements of Use Case 5 of the EDPB's recommendations.

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. Depending on the law, the penalties for noncompliance can range from hundreds of thousands of dollars to multi-million dollar fines.

There are strong overall similarities among many cross-border data frameworks. For instance, most organizations must:

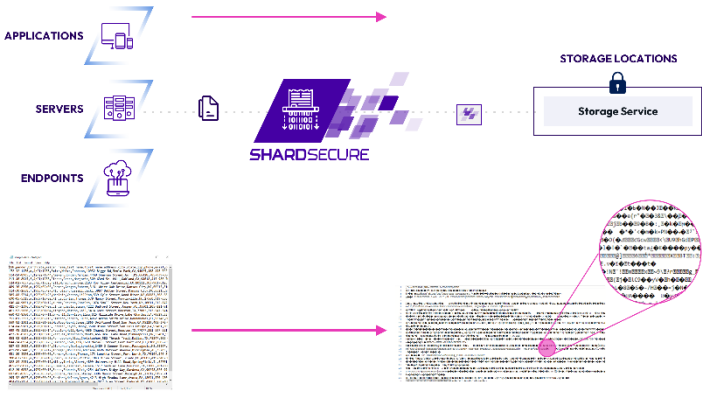
- Receive the clear, informed consent of data subjects before collecting, processing, storing, or otherwise using their data.
- Implement strong data security safeguards, including privacy-by-design.
- Create data retention policies, binding corporate rules, and data processing agreements.
- Allow data 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.

ShardSecure for cross-border data protection

The ShardSecure platform offers several benefits for compliance with cross-border data protection. By providing advanced data privacy, separating data access from infrastructure access, and addressing data residency and sovereignty concerns, ShardSecure helps organizations secure data wherever it is stored.

Data privacy and separation of duties

The ShardSecure platform offers an innovative approach to file-level encryption. Our platform separates data access from infrastructure owners and cloud providers by encrypting data before it is stored within the final storage service or location. Since the data within the storage service or location is already encrypted, storage admins, cloud admins, and cloud providers alike are rendered unable to read or access the data.



By protecting the data itself, ShardSecure's approach can mitigate common vulnerabilities created when data owners rely solely on the security controls of their infrastructure provider. The approach also avoids the shortcomings of common encryption technologies by helping organizations:

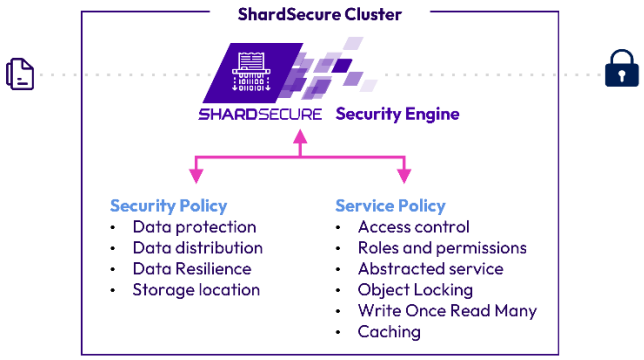
- Adopt a least-privilege access model (ensuring that storage admins, cloud admins, and cloud providers cannot read sensitive data)
- Fully realize the benefits of a Zero Trust architecture (removing access for even the storage service provider)
- Prevent unauthorized third-party access (ensuring that data residing within another service is not sensitive)
- Protect cross-border data transfers (ensuring that data does not violate jurisdictional regulations)
- Achieve data privacy (ensuring that data cannot be read by organizations from other jurisdictions, as with EU personal data stored within American cloud provider services)

Addressing data residency and sovereignty concerns

ShardSecure helps organizations maintain control of their data, regardless of where it's stored. The platform gives organizations the freedom to use the cloud storage providers of their choice, in the geographic locations and jurisdictions of their choice, to mitigate data transfer risk and address data sovereignty concerns. Specifically, the ShardSecure platform can distribute data across different regions of a single cloud provider, across multiple cloud providers, or across a hybrid mix of on-premises storage and one or more cloud providers.

ShardSecure also supports dynamic data routing for data that needs to be stored within a certain jurisdiction (e.g., European data that must reside within the EU, Chinese data that must reside within Chinese services). This dynamic routing can be based on tagging or metadata and makes it simple for global organizations to comply with data residency requirements within a single interface.

Additionally, ShardSecure supports a policy-driven approach to protecting critical data. Different jurisdictions and regulatory bodies may require different approaches — for example, encrypting data versus storing data in certain locations versus distributing data across different jurisdictions. ShardSecure can apply dynamic policies based on the data itself and therefore automatically protect that data in accordance with the relevant jurisdictional requirements. This approach enables global organizations to adopt a flexible data protection strategy without requiring a one-size-fits-all approach to data sovereignty and residency.



Supporting GDPR compliance

ShardSecure's platform offers a split processing technology that can be easily deployed in a multi-party processing environment, allowing organizations to process and store data securely for compliance with the GDPR and Schrems II.

ShardSecure is validated by independent privacy attorneys to meet the requirements of Use Case 5 of the EDPB's recommendations for cross-border data transfers, allowing organizations to store EU personal data within a US cloud provider without violating the GDPR. (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.

Unified, multi-protocol platform across multiple clouds

ShardSecure supports interfaces like S3 for object storage, iSCSI for block storage, and SMB/NFS for file storage to integrate with any application, server, or other service leveraging cloud storage.

Since the ShardSecure platform acts as an abstraction layer, it can consolidate all storage interfaces into one, even though each cloud provider may support a different data storage interface. This approach reduces the complexity associated with migrating data to a multi-cloud architecture. With ShardSecure, data access works the same across all clouds without the need to implement specific APIs or connectors.

Conclusion

In a world of global commerce and global cyberthreats, cross-border data regulations are only becoming more numerous and complex. Meeting the burden of compliance can be a challenge for organizations of all sizes.

ShardSecure platform offers advanced data privacy and security for cross-border data protection. By allowing organizations to control where their data is stored, ShardSecure simplifies cross-border compliance efforts and strengthens data confidentiality. For more information, visit us online or schedule a demo.

@ShardSecure
@ShardSecure
@ShardSecure

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

info@shardsecure.com