

# Solution Brief

## Balancing Cost Savings with Cross-Border Data Protection Laws

Learn how organizations can gain the freedom to store their data with the cloud providers of their choice, in the geographic locations of their choice, and still maintain compliance with strict data regulations like the GDPR.

Cross-border data regulations can have serious consequences for companies. Failure to comply can bring major financial penalties.

Regulation	Penalty for noncompliance	Penalty in USD
Brazil's General Data Protection Law (LGPD)	Up to 2% of the organization's annual revenue in Brazil	Over \$9 million
Canada's Consumer Privacy Protection Act (CPPA)	Up to 5% of the organization's gross global revenue from the previous financial year	Over \$25 million
China's Personal Information Protection Law (PIPL)	Up to 5% of the organization's global revenue from the previous year	Over \$1.2 billion
The European Union's General Data Protection Regulation (GDPR)	Up to 2% of the organization's annual global revenue	Over \$21 million
India's Digital Personal Data Protection Act	Up to 5 billion rupees	Over \$61 million
South Korea's Personal Information Protection Act (PIPA)	Up to KRW 50 million	Over \$50 million



### Cost savings and compliance — can they coexist?

Like most organizations around the world, European businesses want to find the most cost-effective storage options for their data. In many cases, this means using major US cloud providers like AWS, Azure, and GCP.

However, strict cross-border data privacy laws like the EU's General Data Protection Regulation (GDPR) make it difficult to realize these cost savings. To maintain compliance with the GDPR and similar cross-border data regulations, organizations must generally provide sufficient protection against regulatory inspection by other countries and avoid infringing on the Charter of Fundamental Rights of the European Union for European data subjects.

Because European data owners generally cannot be assured that American cloud storage providers are handling personal data with sufficient protection, they can't ensure compliance with the GDPR. The same goes for other strict cross-border data regulation laws, like

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and Japan's Act on the Protection of Personal Information (APPI), which similarly require organizations to protect personal data at all times.

This leaves organizations without a good option for migrating to the cloud. Luckily, though, many cross-border data regulations allow for organizations to supplement their data protection with certain technical safeguards. Enter microsharding.



### The freedom and flexibility to store data anywhere

ShardSecure facilitates cost savings by allowing you to store your data wherever you want. Prefer to keep some data on-premises? No problem. Want to use several different cloud providers in different parts of the world? Not an issue — none of them will be able to read your data.

Even if microsharded data is subpoenaed or exposed in a breach, you remain in full control. Unauthorized users — including attackers and third-party cloud providers — cannot read your data even if they gain access to it.



### How we prevent unauthorized access

Our patented Microshard™ technology desensitizes data by shredding it into tiny microshards and distributing those microshards across multiple customer-owned storage locations. The result is that each location only contains an unintelligible fraction of a whole dataset. Unlike encryption, which can be broken, this microsharding process renders data completely useless to outside users.

In the unlikely scenario that someone is able to gain access to all the microshards from every storage location for a given data set, that collection of microshards still can't be reconstructed. Here's why:

- The microsharding process strips filenames, file extensions, and all other identifying metadata.
- The microshard size is user-configurable.
- Organizations can choose to add a configurable amount of poison data in the microsharding process.



### Maintaining control of your data, wherever it is

Microsharding helps satisfy cross-border data protection requirements by allowing companies to retain control of their own data. But it also offers a great deal of flexibility. Organizations can 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.

We make the number and location of your storage locations user-configurable, so microsharded data can be stored in different jurisdictions. Data can be distributed 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.

Microsharding also does not rely on keys, so the issues of third-party key ownership and key management that can arise in cross-border data protection policies are nonexistent. It's not possible for a third party to deploy their own instance of ShardSecure to reassemble microsharded data.

## Learn more


ShardSecure integrates seamlessly with your existing security controls and cloud storage providers for ease of deployment. Data migration and microsharding happen in the background with just a few clicks and do not introduce any significant performance lag or changes for users.

If you're interested in how ShardSecure meets the requirements of the GDPR specifically, check out our [GDPR white paper](#) for an in-depth analysis of microsharding and Use Case 5 of Schrems II. Or, to learn more about microsharding and cross-border data protection in general, follow us on [social media](#) or visit us [online](#).

 @ShardSecure

 @ShardSecure

 @ShardSecure

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

 [info@shardsecure.com](mailto:info@shardsecure.com)

**SHARD  
SECURE**