SHARDSECURE

Solution Brief

GDPR Compliance

Learn how ShardSecure's platform helps companies address their GDPR obligations and security risk in the storage locations of their choice.

The European Union's General Data Protection Regulation (GDPR) is designed to protect the privacy of personal data within EU member countries. It imposes strict obligations on any organization, regardless of location, that processes EU personal data.

GDPR compliance has been complicated by legal challenges to certain privacy practices. In its 2020 Schrems II ruling, the Court of Justice of the European Union invalidated the basis for free data flows to the US and cast doubt over the European Commission's Standard Contractual Clauses (SCC). As a result of this court case, the European Data Protection Board released a list of supplementary measures and use cases, including both technical and organization safeguards, to help organizations comply with the GDPR.

Below, we'll explain how ShardSecure meets Use Case 5 of Schrems II for GDPR compliance. We'll also explain our platform's other benefits for data privacy, sovereignty, and regulatory compliance.

How ShardSecure Supports GDPR Compliance

ShardSecure's platform offers a split processing technology that easily can be deployed in a multi-party processing environment. By using ShardSecure, companies can process and store their data wherever they like while staying compliant with the GDPR and the Schrems II ruling.

Use Case 5: Split- or Multi-Party Processing

Use Case 5 of Schrems II explicitly refers to "split or multi-party processing" as a generally acceptable supplementary measure. Splitting information into smaller pieces prior to transmission and distributing those pieces across multiple processors, locations, and jurisdictions in such a way that no piece can be reconstructed by a single processor will effectively eliminate the privacy risks at the center of the Schrems II case.

ShardSecure's technology fits the definition of split or multi-party processing in Use Case 5. Our platform shreds data into tiny pieces and distributes those pieces across multiple customer-owned storage locations, eliminating the impact of unauthorized access.

Separating Data Access from Infrastructure Providers

Strong data privacy is an important aspect of GDPR compliance. In order for companies to leverage the data storage services they want — particularly storage with US public cloud providers — they must implement privacy safeguards to protect personal data. This includes protection from cloud admins, local storage admins, and other third-party infrastructure providers who typically have access to stored data.

ShardSecure provides advanced data privacy by separating data access from these infrastructure providers. Our technology maintains the confidentiality of unstructured data and metadata regardless of where it's stored, rendering EU personal data unintelligible to all unauthorized users.

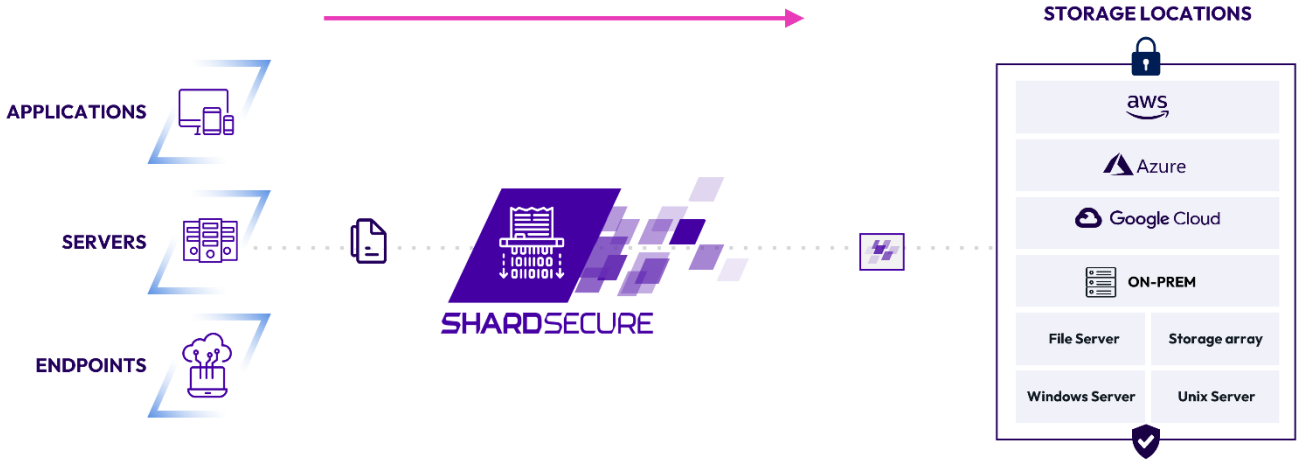
Supporting Data Sovereignty

Our technology allows organizations to store their data in the locations of their choice, including on-prem, cloud, and multi- or hybrid-cloud configurations. Specifically, ShardSecure functions as an abstraction layer between a customer's application servers and a customer's hybrid-cloud or multi-cloud storage. At no time is customer data stored in or accessed ("read") by the ShardSecure platform, allowing companies to remain in total control of who has access to their data.

Simple Integration, Powerful Privacy

ShardSecure does not require the use of agents, providing advanced file-level protection without complicated integration or management. It also allows for instant data access and fast data migration with just a few clicks.

ShardSecure is easy to manage and has a minimal impact on operations teams. It offers transparent implementation with no need to change user behaviors or data flows. It is quick and seamless to integrate, with minimal code changes needed for integration.



Organizations in breach of the GDPR can be fined up to 4% of their annual turnover or up to €20M, whichever is largest.

As of September 2021, more than 800 GDPR fines have been issued, including a €50M fine for Google, an €18.4M fine for Marriott International Hotels, and a €746M fine for Amazon.

Learn more...

ShardSecure integrates seamlessly with your existing security controls and cloud storage providers for ease of deployment. In addition to GDPR compliance, we provide agentless file-level protection, cloud resource optimization, strong data resilience, and native cloud-based ransomware protection. To learn more about our technology, 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