EU Data Protection Solution

Ensuring Compliance with Global Privacy and Security Regulations

Facing unprecedented pressure from cyber threats and security regulators, global enterprises must ensure they implement appropriate data protection solutions to avoid potential breaches and fines of 20 million EUR, or 4 percent of annual revenue. Syncplicity helps companies modernize their IT infrastructure, enable the digital workplace, and reduce costs, while maintaining the highest level of data governance.

Syncplicity's hybrid-cloud architecture and data protection by design approach enable organizations to implement a transformational enterprise file sync and share (EFSS) solution that addresses global privacy laws and regional compliance challenges.

In this increasingly digital world, organizations must operate with a global mindset as well as an awareness of European data protection and sovereignty requirements. Whether your company is EU-based or does business across the EU region, it is critical to be aware of the state of your corporate data – where it's stored and transferred, who has access, and the geographical regulations it is governed by.

Syncplicity is designed to simplify data protection – providing our customers with a secure, comprehensive solution to meet European data protection and residency requirements –today and into the future. With monumental changes occurring in global privacy regulations, we do not believe that one simple architecture works for all users and content within enterprises. Syncplicity's 'data protection by default' strategy provides a flexible architecture with the necessary granular privacy, confidentially and data sovereignty controls built-in, giving our customers the right tools to adapt to evolving legislation and business requirements across the enterprise.

Syncplicity Hybrid Cloud Architecture

Our policy-driven hybrid cloud offers customers a choice of storage location. Enterprises, multi-nationals and state agencies need the flexibility to retain data in the region of their choice. Data can be stored in Syncplicity's EU Cloud Storage, on-premises, in a private cloud – or any combination – based on security and data protection requirements. By choosing the physical location of their Syncplicity StorageVaults, customers may avoid the legal challenges of data transfer across sovereign borders. The flexibility of our architecture provides organizations with options as regulations and business requirements evolve.

Syncplicity StorageVault Authentication (SVA)

Fear of government access and 'backdoors' to data have provoked scrutiny in the global privacy community, leading to drastic reforms in data regulations and enforcement. This unique feature – SVA – offers the highest level of security and control to assure compliance with the strictest data processing and confidentiality frameworks. Syncplicity SVA gives IT control over who has access to data and restricts government agencies, as well as insiders from unauthorized access.

Syncplicity EU PrivacyRegion

Customers choosing to locate their company account in the Syncplicity EU PrivacyRegion are assured that all of their data, including personal information (PII), metadata and file content, is kept within the EU borders. The architecture is a built on a distributed privacy model that allows users to work seamlessly from anywhere in the world, keeping their personal data stored and managed only in a specified region. Syncplicity's solution is unique in segregating all data to specific regions, while still providing users a 'single-pane-of-glass' experience and seamless collaboration across regions.

EU Cloud Storage

Enterprises can define multiple storage policies for their global deployments, leveraging on-premises storage, private cloud, and Syncplicity's EU cloud storage all within a single seamless user experience. Our EU Cloud Storage gives enterprises an additional choice and the ability to scale quickly to meet information governance requirements. Files can be securely shared globally, while maintaining control of where the data is stored and who manages the content.

EU Legal Frameworks

Model Clauses

Syncplicity's Data Protection Addendum incorporates the European Commissions' Model Contracts for the transfer of personal data to third countries. Model Clauses provide a legal framework to uphold the data protection requirements of the European Union. With the inclusion of Model Clauses, Syncplicity customers can continue to transfer personal data from the EU, when required.

TRUSTe Audit

Using industry recognised privacy solutions provider – TRUSTe – Syncplicity has gone through a third-party audit of its mobile, desktop and web applications. This included reviewing our policy and privacy practices to provide customers assurance of compliance with the latest EU data protection framework.

EU-US Privacy Shield Certification

Syncplicity participates in and has been certified as compliant with the EU-U.S. Privacy Shield Framework and Principles. Privacy Shield is a core part of today's data protection and legal framework, and certification demonstrates a commitment to addressing European data protection and residency concerns.

Any questions?
Please contact the Syncplicity Sales Team:
sales@syncplicity.com

www.syncplicity.com