SHARDSECURE

White Paper:

The EU-US Data Privacy Framework

Overview

In an increasingly globalized, cloud-based world, concerns about cross-border data processing and data transfers are growing. A significant number of countries have implemented data privacy and protection laws, and international regulations have sprung up to govern the flow of data among nations.

This white paper analyzes the new EU-US Data Privacy Framework, including how it addresses issues raised by the Schrems II data privacy case. It also identifies several concerns that experts have raised in response to the new framework, including the likelihood of a Schrems III challenge, and examines the EU's official July 2023 adoption of the adequacy decision. Finally, the white paper explores how ShardSecure's advanced data privacy solution keeps organizations in control of their data and mitigates cross-border data processing risks.

Data transfers and the EU-US Data Privacy Framework

The EU-US Data Privacy Framework is an agreement between the European Union and the United States to facilitate the free flow of data between countries. Brought about by an October 2022 executive order from US President Biden, the agreement seeks to protect data privacy and safeguard data transfers.

Data transfer is not defined precisely in the EU's General Data Protection Regulation (GDPR). However, most experts agree that data transfer can be interpreted as a type of data processing that involves transmission to and remote access from a non-EU/EEA (European Economic Area) country.

Because the right to privacy and data protection is enshrined in the European Union's constitution, data transfers are strictly governed by the EU Commission and are only permitted if:

- the country or organization of destination ensures an adequate level of protection for personal data
- an "essential equivalent" level of protection can be guaranteed by use of an approved transfer tool, or
- specific derogations are in use

Additionally, if any EU constitutional rights or freedoms are jeopardized by the laws or practices of foreign countries, then the data transfer to that destination must cease.

Because of the importance of data privacy to human rights and the importance of free data flows to commerce and communications, data transfers among different nations are increasingly regulated and complex.

Schrems II

Data transfers between the European Union and the United States underpin more than $1 trillion in annual trade. But they are complicated by the Schrems II ruling (c-311/18), a landmark data privacy case decided in 2020 by the Court of Justice of the European Union. The case invalidated the GDPR's 2016 EU-US Privacy Shield on the

grounds that it was insufficient to protect the privacy of personal data.

Schrems II was focused particularly on American national security laws that violate the GDPR, such as the US Foreign Intelligence Surveillance Act. According to the ruling, US surveillance laws do not limit access to data to what is "necessary and proportionate." As a result of Schrems II, data transfer from the EU to the US became virtually impossible under the GDPR without supplementary safeguard measures.

The October 2022 executive order

Signed on Oct. 7, 2022, the Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities is an agreement between the US and the EU that imposed additional safeguards on data access and collection by US intelligence agencies. The executive order (EO) was designed to address many of the concerns of Schrems II:

- It mandates safeguards and data handling requirements for "signals intelligence agencies."
- It defines a list of 12 legitimate objectives and 5 prohibited objectives to govern the collection.ollection of data by US intelligence agencies.
- It introduces data minimization and storage limitation principles.
- It allows the bulk collection of data only as a last resort, effectively limiting this form of data collection.
- It lays out a two-tier redress mechanism to improve independent oversight.

Concerns about the October 2022 EO

Despite the strengths of the EO, some experts believe it is insufficient to address the concerns raised in Schrems II about the collection of EU personal data by US intelligence agencies. Notably, the EO does not amend or replace existing US surveillance laws.

Chief among commentators' concerns:

- Data subjects are not notified when they are subjected to US intelligence activities — and therefore have little chance of exercising their rights.
- If data subjects lodge a complaint, they will only receive a blanket statement as to whether or not a data protection violation was identified. Subjects will not actually be given access to or information about any data collected on them.
- It is not a law passed by Congress, so it can be altered or withdrawn entirely by subsequent US presidents.
- The Data Protection Review Court operates under the US Attorney General's authority, casting doubts on its independence from the executive power.
- The US CLOUD Act — which allows federal law enforcement to compel US-based technology companies to provide requested data regardless of where that data is stored — is unaffected by the executive order.

The Austrian activist and lawyer Maximilian Schrems and his nonprofit organization NOYB noted in a preliminary response that the EO seems to fail in meeting the requirements of Schrems II. Their response pointed out, among other shortcomings, the continuance of "bulk surveillance" and a "court that is not an actual court." They also suggested that, although the EO uses words like "necessary" and "proportionate" that suggest compliance with Schrems II, those words do not actually carry the same legal meaning in the US as they do in the EU.

Similarly, the American Civil Liberties Union (ACLU) released a statement that "Although the executive order is a step in the right direction, it does not meet basic legal requirements in the EU, leaving EU-US data transfers in jeopardy going forward."

The July 2023 approval of the EU-US framework

After an eight-month adoption process, the EU officially adopted an adequacy decision for the EU-US Data Privacy Framework in July 2023. This adequacy decision means that the additional safeguards included in the October EO and the Data Privacy Framework have been determined to provide an adequate level of protection for personal data transferred from the European Union to the United States.

Upcoming changes for organizations

Eligible US companies can self-certify their compliance with the new Data Privacy Framework website through the US Department of Commerce.

Organizations should also watch the courts, as experts expect that the framework's validity will be challenged by privacy activists. Max Schrems, the Austrian privacy activist responsible for the Schrems II case, has already announced his intention to file a new suit about the Data Privacy Framework, and it seems likely that there will be

a Schrems III. As such, businesses should prepare for the adequacy decision to be repealed in anywhere from 2 to 4 years.

Finally, organizations should look to improve their data privacy solutions. By protecting their data as comprehensively as possible now, businesses will find themselves better prepared for future regulatory changes as the EU-US Data Privacy Framework continues to evolve.

Using the ShardSecure platform to mitigate data privacy risks

The ShardSecure platform provides agentless file-level protection to mitigate data privacy risks, wherever data is stored. The platform protects unstructured data in files, folders, and storage locations, separating data access from infrastructure owners like cloud admins to ensure strong confidentiality.

The ShardSecure platform is deployed as an abstraction layer between existing application and storage infrastructure, where it performs advanced file protection without the need for agents. This approach reduces complexity and makes sensitive data unintelligible to unauthorized users, ensuring data privacy for cross-border data transfers.

Support for data privacy and compliance

ShardSecure meets the European Data Protection Board's requirements as a supplemental technology to enable cross-border data transfers under the GDPR. The ShardSecure platform is a split processing technology that can be easily deployed in a multi-party processing environment, meaning that it allows organizations to store and process data safely under the EDPB's Use Case 5.

As cyber audit and assurance firm UHY Advisors states: "ShardSecure has the potential to lower cyber risks and compliance costs while maintaining compliance with the spirit of European and US data protection regulations."

For a more detailed explanation on how the ShardSecure platform mitigates data transfer risks, see our white paper on GDPR compliance.

Embedded data control

The ShardSecure platform keeps organizations in control of their data, addressing data sovereignty and residency concerns. Companies can utilize the cloud and on-premises storage providers of their choice, in the geographic locations and jurisdictions of their choice. This gives organizations the control they need to mitigate data transfer risks and stay compliant with rapidly changing cross-border data regulations.

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 to a multi-cloud architecture. Data access also functions consistently across all clouds without the need to implement specific APIs or connectors.

Conclusion

The digital world is changing fast, and even major agreements like the EU-US Data Privacy Framework may be valid one day and struck down the next. What is deemed sufficient for securing cross-border data transfers today may become insufficient in the near future.

The ShardSecure platform helps organizations stop chasing regulations and meet stringent EDPB data protection requirements. With strong data security, privacy, and resilience, ShardSecure allows companies to regain control of their data, wherever it may reside.

For our BrightTALK webinar on the EU-US Data Privacy Framework, click here. To learn more about how ShardSecure maintains data privacy and meets Use Case 5 of Schrems II, contact us today.

@ShardSecure
@ShardSecure
@ShardSecure

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

info@shardsecure.com