SHARDSECURE

White Paper

Microsharding and the New 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 like the GDPR and the APEC Privacy Framework have sprung up to govern the flow of data among nations.

This white paper breaks down one such regulation: the new EU-US Data Privacy Framework. In it, we examine the October 2022 executive order that established the EU-US Data Privacy Framework, plus how this framework responds to concerns raised by the landmark Schrems II data privacy case. We also identify several concerns that experts have raised in response to the October EO.

The white paper goes on to discuss the six-month adequacy decision process by which this framework will be either adopted or rejected by the European Commission, as well as potential next steps for organizations and the likelihood of a Schrems III challenge. Lastly, it explains how microsharding offers an advanced data privacy solution that keeps organizations in control of their data and helps mitigate cross-border data processing risks.

Data transfers and the EU-US Data Privacy Framework

The new EU-US Data Privacy Framework is an agreement between the European Union and the United States designed to facilitate the free flow of data between countries. Brought about by an October 2022 executive order from the President of the United States, 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 countries are increasingly regulated and complex. Although the new EU-US Data Privacy Framework has not been adopted by the European Union yet, it does raise important questions about the future of data transfers among countries.

Schrems II

Data transfers between the European Union and the United States are further 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 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 of data by US intelligence agencies.
- It introduces a "necessity and proportionality" test.
- 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 be implemented by the Civil Liberties Protection Officer of the Office of the Director of National Intelligence and by a newly established Data Protection Review Court to ensure 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.
- Finally, 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."

Next steps for EU-US data transfers

Although it is a concerted attempt to address the concerns raised in Schrems II, the EO does not replace the invalidated 2016 EU-US Privacy Shield. It also does not act as an adequacy finding — but it does pave the way for the adoption process. This adoption process is expected to take around six months and will require the European Commission to release a new draft adequacy decision, obtain the approval of the European Data Protection Board (EDPB) and EU member states, and withstand scrutiny from the European Parliament.

The ultimate goal in the adoption process is for the European Commission to recognize the EO's framework as "essentially equivalent" to the protections provided under the GDPR and to facilitate the flow of EU-US data transfers.

What steps should organizations take?

In light of the pending decision, businesses should continue to carry out their Transfer Impact Assessments (TIA) following the usual EDPB recommendations until the new transfer mechanism is in place. They should also continue to employ their Standard Contractual Clauses or alternative mechanisms.

Organizations should also keep an eye on the courts. As soon as the adequacy decision is implemented, experts expect that its validity will be challenged by privacy activists, and it is not unlikely 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.

Closer to home, organizations should revisit their cloud strategy and their data protection solutions. There are many factors to consider, from shifting security regulations to technical safeguard measures and beyond. By protecting their data as carefully as possible now, companies will find themselves better prepared for future regulatory changes, whatever they may be.

Using microsharding to mitigate data transfer risks

Microsharding works by splitting data into very small pieces (microshards) and distributing those pieces across multiple storage locations. It essentially desensitizes data for the cloud, preventing any unauthorized user or entity from reconstructing the microshards. This approach, coupled with self-healing data, provides strong data confidentiality, integrity, and availability.

Our patented Microshard™ technology can ease the burden of compliance with the GDPR and Schrems II through Use Case 5, which defines "split or multi-party processing" as a generally acceptable supplementary measure for data transfers. Microsharding effectively eliminates the risk of the laws and practices of foreign countries impinging on the safeguards of the SCCs and other approved transfer tools.

For a more detailed explanation on how microsharding meets the requirements of Use Case 5 and neutralizes data transfer risks, please see our white paper on GDPR compliance.

Ease of access and integration

Microsharding allows instant access to data when it's needed, with no lag time introduced by ShardSecure. It also allows for fast, seamless migration of data between different storage locations. Microsharding happens in the background as a zero-downtime event, with no impact to applications and no visible changes to employee interfaces.

A transparent, vendor-agnostic solution, ShardSecure looks like a storage location to other applications. With an S3-compatible API and iSCSI module, microsharding is extremely easy to integrate into existing workflows.

Embedded data control

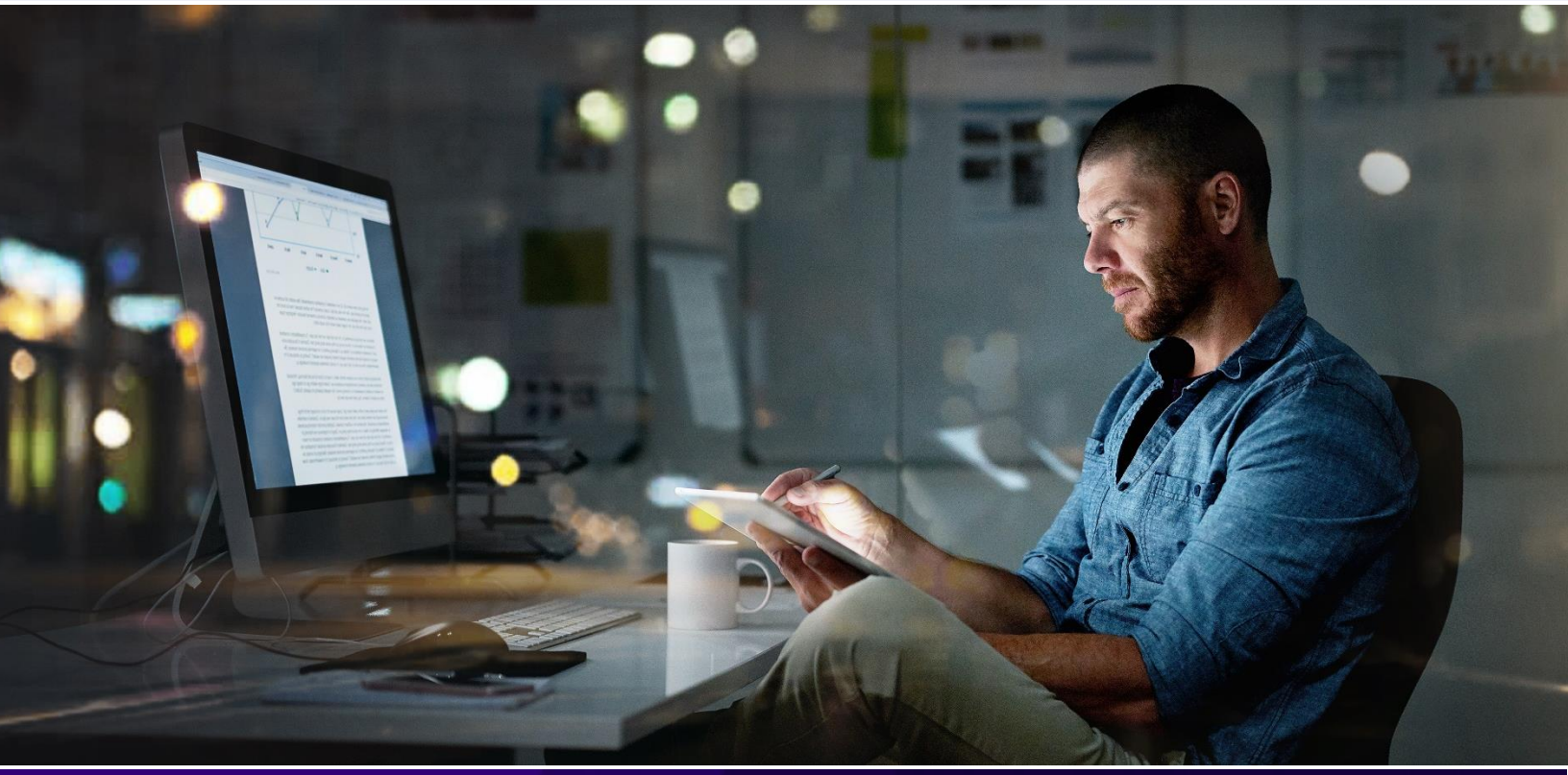
Microsharding keeps organizations in control of their own data — a crucial aspect of EU-US data transfers. With ShardSecure, organizations can use the cloud and on-premises storage providers of their choice, in the geographic locations and jurisdictions of their choice. The number and type of storage locations is also user-configurable. This gives companies the control they need to mitigate data transfer risks and stay compliant with rapidly changing cross-border data regulations.

Conclusion

The digital world is changing fast. Even major data agreements like the EU-US Data Privacy Framework may be valid one day and struck down the next. What works for EU-US data transfers today may well be insufficient in the near future.

Microsharding helps organizations adapt to the changing digital landscape and stop chasing regulatory compliance. With strong data privacy, security, and resilience, it helps companies meet EDPB requirements and protect their data, wherever it may reside.

For our BrightTALK webinar on microsharding and 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