Building Bridges

The New Trans-Atlantic Data Privacy Framework

Introduction

The European Commission has recently issued an adequacy decision after carefully assessing the requirements of GDPR and provided a new mechanism of data transfer – EU-US Data Privacy Framework (DPF). This adequacy decision concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to companies participating in the EU-U.S. Data Privacy Framework. With the adoption of the adequacy decision, European entities can now transfer personal data to companies in the United States, without having to put in place additional data protection safeguards. This will be the third attempt to legitimise the Trans-Atlantic data transfer where the first 2, Safe Harbor and Privacy Shield, were invalidated by Court of Justice of the European union (CJEU).

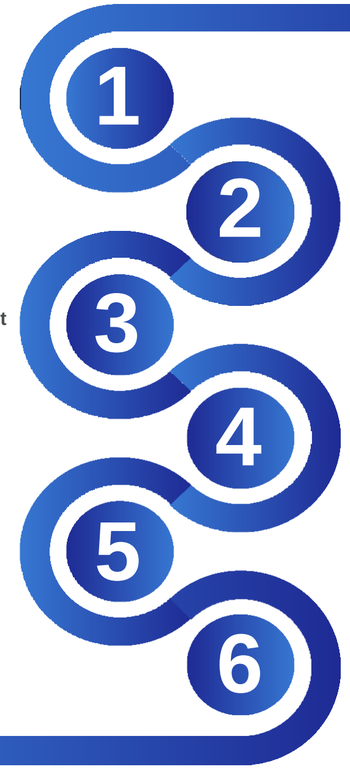
The U.S. Department of Commerce has issued the following advisory:

Privacy shield-certified organisations
Privacy Shield certifications must have their privacy policies updated to comply with the EU-U.S. Data Privacy Framework (DPF) Principles by October 10, 2023. They do not need to submit a new certification and can rely on the DPF adequacy decision.

UK extension to the DPF
Starting July 17, 2023, eligible organizations can certify under the UK Extension to the DPF, but cannot receive personal data transfers from the UK until the anticipated adequacy regulations come into force.

Swiss-US DPF
Starting July 17, 2023, the Swiss-U.S. DPF Principles will come into effect. Organisations previously certified under the Swiss-U.S. Privacy Shield must update their privacy policies but cannot rely on the Swiss-U.S. DPF until Switzerland recognizes its adequacy.

EU-US data privacy framework principles



Data accuracy, minimisation and security
Data should be accurate and up to date. Personal data must be limited to what is relevant for the purpose of the processing.

Purpose limitation and choice
Personal data should be processed lawfully and fairly. The data should be collected for a specific purpose and used for that purpose only.

Individual rights
Data subjects should have certain rights which can be enforced against the controller or processor.

Transparency
Data subjects should be informed of the main features of the processing for their personal data.

Accountability
Organisation must provide effective mechanisms to ensure compliance with the principles.

Restrictions on onward transfers
Transfers of personal data to a third-party controller or processor can only take place based on a contract between the organisation and the third party.

Timeline for data privacy framework

July 26 2000 — **Safe harbor**
The safe harbor adequacy decision is adopted by European Union.

October 6 2015
Safe Harbor declared invalid by Court of Justice of the European Union

July 12 2016 — **Privacy shield**
The EU-US privacy shield was formally adopted.

July 16 2020
CJEU declares EU-US privacy shield invalid.

March 25 2022
European Commission announces agreement in principle with US over new Trans-Atlantic data transfer framework.

October 3 2022
President Biden issues Executive Order on new framework.

July 10 2023 — **Data privacy framework**
European Commission adopted the EU-US Data Privacy Framework.

mazars

What is different this time?

A new set of rules and binding safeguards to limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security; US intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards.

A new two-tier redress system to investigate and resolve complaints of Europeans on access of data by US Intelligence authorities, which includes a Data Protection Review Court

The Commission will meet with the US Department of Commerce (DoC),the Federal Trade Commission (FTC) and the US Department of Transportation (DoT) for the monitoring and review of the decision.

Strong obligations for companies processing data transferred from the EU, which includes the requirement to self-certify that they adhere to the standards through the US Department of Commerce

Benefits of the framework

Adequate protection of European data transferred to the US, addressing the requirements of the CJEU

Competitive digital economy and economic cooperation

Continued data flows underpinning €900 billion in cross-border commerce every year

Durable and reliable legal basis

Safe and secure data flows

Conclusion

The European Commission believes that the United States provides a level of protection for personal data transferred from the EU to certified organisations in the US that is equivalent to the protections guaranteed by the General Data Protection Regulation (GDPR). This is ensured through transparency obligations and the administration of the EU-U.S. Data Privacy Framework by the Department of Commerce. The US has mechanisms in place to identify and punish infringements of data protection rules, and individuals have legal remedies to access, rectify, or erase their personal data. Any interference by US public authorities for law enforcement or national security purposes is limited to what is strictly necessary and is subject to effective legal protection.

How Mazars can help?

Mazars brings global knowledge on the evolving regulatory landscape and has developed its privacy framework to tailor solutions for your individual needs.

Our services –

Compliance reviews, maturity assessments and audits – for companies who want a check the status of their compliance against global legislation, standards, or frameworks. To identify gaps and develop a pragmatic approach to remediation.

Technical advisory and implementation services for those areas where you need expert support and an injection into your compliance programme.

DPO support services – to supplement your data protection officer or support with those mandatory tasks required for compliance

mazars

Contact us

Kartikeya Raman
Associate Partner, Consulting
Email: kartikeya.raman@mazars.co.in