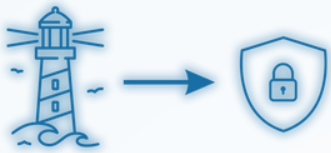
The New EU-US Data Privacy Framework

Balancing Free Data Flows, National Security and Privacy

Background

The International Safe Harbor Privacy Principles were taken down in the Schrems I case in light of the Snowden revelations and were substituted by the Privacy Shield Framework.



The issue

The Privacy Shield Framework, relied upon by 5,300+ businesses, was again invalidated by the European Court of Justice (ECJ) in the Schrems II case.

The reason

US law failed to offer the same level of data protection as the GDPR by allowing intelligence agencies to conduct surveillance activities that compromised EU fundamental privacy rights.

The new goal

To address the EU's privacy concerns and establish a new agreement for secure and lawful data transfers from the EU to the US.

What has changed?

Necessity and proportionality

The Data Privacy Framework (DPF) offers a more balanced approach between the pursuit of intelligence goals and the impact on the privacy of individuals, one defined by legitimate purposes that limit bulk surveillance activities.

Data Protection Review Court

An independent and impartial redress mechanism for EU individuals to lodge complaints regarding the collection and use of their data by US intelligence agencies is established.

How will it benefit startups?

Legal certainty

Startups are assured that they are transferring data to US-based companies relying on the DPF in a lawful manner.

Less time and resource-constraint

Less time and resource constraints: startups do not need to rely on other, more burdensome mechanisms like SCCs and BCRs to transfer data.

How to participate?

US-based organisations previously relying on the Privacy Shield must update their privacy policies to reference the EU-US DPF within three months.

Organisations that want to participate in the DPF can voluntarily do so by self-certifying to the US Department of Commerce and adhering to the Principles set by the agreement.

Organisations that transfer data from the US to the EU that do not join the DPF will have to rely on other mechanisms, like Standard Contractual Clauses or Binding Corporate Rules.

What's next?

1. To participate in the DPF, businesses have to self-certify and comply with its principles and other requirements within three months.
2. Privacy activist Schrems as well as others have voiced their concerns about the legality of the agreement, announcing their intentions to challenge it before the ECJ.
3. The ECJ, which invalidated the two previous agreements, the Privacy Shield and the Safe Harbour, will assess the legality of the new DPF.

Will startups step again into an uncertain legal limbo? If so, a future-proof agreement is necessary!