EU-U.S. Data Privacy Framework

On 10 July 2023, the European Commission adopted a new adequacy decision for EU-US data flows. This adequacy decision relates to the EU-US Data Privacy Framework (the "**Framework**") and concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to the US under the terms of this new framework as its protections are comparable to that of the EU.

Background

The General Data Protection Regulation ("**GDPR**") regulates data protection and privacy in the European Union. Article 45(3) of the GDPR grants the European Commission the power to decide that a non-EU country ensures an 'adequate level of protection' for personal data that is essentially equivalent to the level of protection granted within the EU. Following the invalidation of the previous adequacy decision on the EU-US Privacy Shield by the Court of Justice of the EU (CJEU) in the Schrems II decision, the European Commission and the US government entered into discussions on a new framework to address relevant issues. The Framework was the result of these discussions.

What is the effect of adequacy decisions?

An adequacy decision is a tool provided for under the GDPR to allow transfers of personal data from the EU to third countries. It is a finding by the European Commission that a third country offers a level of data protection that is essentially equivalent to that of the European Union. The effect is that entities are able to transfer personal data to participating companies without having to put in place additional safeguards. Personal data can flow freely and safely from the EU (including Norway, Liechtenstein and Iceland) to a third country without further obstacles and can be handled in the same way as transmission of data within the EU.

The Data Privacy Framework

In the adequacy decision, the Commission has carefully assessed the requirements that follow from the Framework as well as the safeguards and limitations that apply when personal data is transferred to the US that would be used for criminal law enforcement or national security by public authorities.

The Framework provides several new rights to EU individuals whose data would be transferred by participating EU companies to the US, for example the right to obtain access to their data or correction or deletion of incorrect or unlawfully handled data).

It also introduces new binding safeguards to address all of the concerns that were raised by the CJEU. This includes:

- limiting access to EU Data by US intelligence services to what is necessary and proportionate to protect national security;
- establishing a Data Protection Review Court (DPRC), to which EU individuals will have access to obtain redress regarding the collection and use of their data by US intelligence agencies before an independent and impartial redress mechanism;
- enhanced oversight of activities by US intelligence services to ensure compliance with limitations on surveillance activities.

US companies can certify their participation in the Framework by committing to comply with a detailed set of privacy obligations for example on the privacy principles of purpose limitation, data minimisation and data retention.

Next steps

The Framework entered into force on 10 July 2023 and will be subject to periodic reviews, the first being within one year of the adequacy decision. This is to be carried out by the European Commission together with representatives of European data protection authorities and competent US authorities in order to verify that all elements of the Framework have been fully implemented and function effectively in practice. Clerkin Lynch can assist with related compliance queries.

Mark Browne
Partner

Email:
markbrowne@clerkinlynch.com
Phone: 01 611 4400

Sara A. Hantash