MAPLES GROUP

UPDATE

Ireland Update: International Data Transfers

On 22 May 2023, the Irish Data Protection Commission ("DPC") published its long awaited decision on international data transfers by Meta Platforms Ireland Ltd ("Meta Ireland") to the US ("Decision")[1]. The DPC held that Meta Ireland had infringed Article 46 (1) of GDPR by transferring personal data in respect of its Facebook service to the US on the basis of standard contractual clauses ("SCCs") where such data was subject to indiscriminate surveillance by US intelligence services. The DPC imposed a fine of €1.2 billion on Meta Ireland, the largest GDPR fine imposed by any EU Member State data protection regulator to date. The Decision only binds Meta Ireland but impacts all organisations transferring personal data to US electronic communications service providers.

International Transfers

GDPR restricts the transfer of personal data outside of the European Economic Area ("EEA") unless one of a number of conditions are satisfied. These restrictions are aimed at ensuring personal data benefits from essentially equivalent protection when it leaves the EEA.

Chapter V of GDPR allows for personal data to be transferred outside of the EEA if:

(a) the European Commission ("Commission") has issued an adequacy decision in respect of the relevant country[2];

(b) one of a number of safeguards are put in place, such as SCCs or binding corporate rules; or

(c) one of a number of derogations apply, such as explicit consent or the transfer is necessary for public interest reasons.

EU-US Data Transfer Litigation

US authorities' intelligence activities concerning personal data transferred to the US from the EEA have been the subject of complaints for over a decade[3].

Schrems I

In 2000, the Commission adopted the 'Safe Harbour' decision which permitted EU-US personal data transfers provided that the US recipient voluntarily self-certified compliance with the Safe Harbour data protection principles.

In 2015, following a complaint by Max Schrems to the DPC and a preliminary reference ruling to the Court of Justice of the EU ("CJEU"), the

[1] https://edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/decision-data-protection-commission_en

[2] Adequacy decisions have issued for Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland and the UK.

[3] These activities are based on EO 12333 and Section 702 of the US Foreign Intelligence Surveillance Act ("FISA"). EO 12333 allows the NSA to access data 'in transit' to the US, by accessing underwater cables on the Atlantic floor. Section 702 of FISA surveillance programmes, such as PRISM and UPSTREAM, are authorised by the US Foreign Intelligence Surveillance Court on the basis of an annual certification by the US AG and Director of National Intelligence. They authorise large scale indiscriminate surveillance of personal data of non-US individuals transferred from the EEA for national security purposes. PRISM applies to internet service providers. UPSTREAM applies to telecommunications undertakings operating the 'backbone' of the Internet, i.e. the network of cables, switches and routers. Under both PRISM and UPSTREAM, the NSA can mandate the production of communications.

CJEU invalidated the Safe Harbour regime in its 'Schrems I' decision due to US intelligence authorities' rights of indiscriminate access to personal data transferred from the EEA and the absence of any enforceable rights for individuals impacted[4].

Schrems II

The Safe Harbour regime was replaced in 2016 by the Privacy Shield which sought to introduce rights for individuals via a Privacy Shield Ombudsman. Like the Safe Harbour regime, the Privacy Shield relied on voluntary self-certification with its data protection principles. It also allowed US organisations to derogate from the Privacy Shield principles to the extent necessary to meet US national security, public interest or law enforcement requirements. It was invalidated by the CJEU in its 2020 'Schrems II' decision as indiscriminate access to personal data transferred from the EEA by US public authorities for national security and law enforcement purposes remained problematic[5].

However, the CJEU upheld the validity of SCCs noting that organisations may need to adopt supplementary measures in order to ensure the law and practice of the relevant third country respects the essential equivalence of the EU data protection standards. Following this decision, the Commission issued updated SCCs in 2021 designed to address the CJEU's findings on SCCs[6].

Data Privacy Framework

Political negotiations for another adequacy decision for transfers to the US have been underway since 2020. In October 2022, the US President issued an Executive Order ("EO") announcing a new data privacy framework to address issues on lack of necessity and proportionality limits on US surveillance programmes and insufficient redress rights to challenge unlawful surveillance. The Commission is working on a new adequacy decision on the back of the data privacy framework.

The Decision

The DPC addressed three core questions in the Decision, namely whether: (i) US law provides an essentially equivalent level of protection; (ii) the SCCs can remedy the inadequate protection under US law; and (iii) there are supplemental measures that could address that inadequate protection.

Is US law essentially equivalent?

Relying heavily on the CJEU Schrems II decision, the DPC held that US law does not guarantee essential equivalence pointing to the unlimited access to personal data of non-US persons targeted via PRISM and the absence of enforceable rights in US courts against US authorities. The DPC reserved its position on surveillance carried out under EO 12333 and UPSTREAM but seemed to suggest that end-to-end encryption may be an effective safeguard for personal data subject to those programmes.

The Decision considered the impact of the data privacy framework but the DPC held that since it was not yet in place, it could not impact its analysis of US law equivalence.

Can SCCs remedy inadequate protection?

Meta Ireland transferred personal data to Meta US on the basis of 2010 and 2021 SCCs. The DPC held that the SCCs could not remedy the inadequate protection provided by US law as Meta Ireland cannot stop intelligence services access.

[4] Schrems I, Case C-362/14, 6 October 2015: https://curia.europa.eu/juris/liste.jsf?num=C-362/14
[5] Schrems II, C-311/18, 16 July 2020: http://curia.europa.eu/juris/documents.jsf?num=C-311/18
[6] Our 2021 SCCs update: https://maples.com/en/knowledge-centre/2021/6/international-data-transfers-new-transfer-sccs

Can the SCCs and supplemental measures remedy inadequate protection?

Meta adopted a number of organisational, legal and technical measures to protect personal data transferred to the US. These included: (a) policies addressing law enforcement requests and transparency reports; (b) employing industry standard encryption; and (c) implementing legal measures such as challenging unduly broad requests. The DPC was not satisfied that these supplemental measures would compensate for the inadequate protection provided by US law.

Article 49 Derogations

Meta Ireland sought to rely on certain Article 49 derogations but this was rejected by the DPC which held that the derogations could not be used for systematic, bulk, repetitive and ongoing transfers. The DPC did not rule out reliance on explicit consent but noted potential difficulties with consent given the requirement for transparency and practical difficulties with obtaining consent for all transfers.

The Fine

The Decision provides a stark example of the contrast between the DPC's approach to fines and that of other EU data protection authorities. The DPC questioned the effectiveness of a fine taking the view that suspension of transfers alone would *"right the particular wrongs identified"*. The €1.2 billion fine was only imposed following objections from other concerned data protection authorities and the binding decision of the European Data Protection Board.

Effect of the Decision

In addition to the fine, the DPC also ordered Meta Ireland to: (a) suspend data transfers to Meta US within five months; and (b) cease all unlawful processing within six months. Meta Ireland intends to appeal the Decision and seek a stay on the Decision. If the data privacy framework is not finalised by 12 October 2023 and Meta Ireland does not obtain a stay on the Decision as part of its appeal, it will be faced with withdrawing services from its EU users.

How the Maples Group Can Help

As noted earlier, the Decision only binds Meta Ireland but the analysis in the Decision impacts all organisations transferring personal data to US electronic communications service providers.

If you transfer personal data directly or indirectly to US electronic communications service providers (such as Microsoft, Yahoo, Google, AOL, Apple, Zoom, Skype and YouTube), please reach out to your usual Maples Group contact or the person listed below for further information.

Dublin

Claire Morrissey
+353 1 619 2113
claire.morrissey@maples.com

June 2023