Briefing

BURGES SALMON

Data protection update

CJEU rules US Safe Harbour Agreement no longer valid

Summary

This week the Court of Justice for the European Union (CJEU) passed **judgment** on a case concerning the transfer of personal data from Europe to the USA. The outcome of this case is that organisations can no longer rely solely on the terms of the EU/US Safe Harbour Agreement to ensure that they are compliant with data protection laws in respect of the transfer of personal data to the USA. Organisations should review any new or ongoing transfers of data to the USA and ensure that adequate contractual safeguards or corporate rules are put in place.

International transfers of personal data

Whenever an organisation in the EEA (the EU member states plus Norway, Iceland and Liechtenstein) collects, controls or processes data about European individuals, that organisation is subject to the provisions of EU data protection law. These laws seek to safeguard the fundamental rights and freedoms of European citizens and impose restrictions on how personal data can be stored and used.

Where organisations seek to transfer data out of the EEA, the EU imposes further restrictions and places an absolute prohibition on transferring European data out of the EEA unless certain criteria are met. Only those countries and organisations that are able to provide an 'adequate' level of data protection (that is, comparable to European standards) are exempt from this rule. Since 2000, the USA has been considered as having 'adequate' data security standards as a result of the EU/US Safe Harbour Agreement.

However, since the revelations by Edward Snowden in 2013 regarding the direct access capabilities of American security agencies, the credibility of the USA as an 'adequate' jurisdiction has been doubted, leading to legal challenges of the Safe Harbour regime.

Schrems v Data Protection Commissioner

Any shortcomings of the Safe Harbour Agreement have the potential to affect vast numbers of European citizens who have their personal information stored on servers in the USA.

In particular, Facebook's data transfer activities were the target of a complaint by Austrian privacy campaigner (and Facebook user), Mr Max Schrems. In light of the Snowden disclosures, Schrems asked the Irish Data Protection Commissioner (DPC) to investigate the lawfulness of data transfers by Facebook Ireland Limited (Facebook's European arm) of Schrems' personal data to Facebook servers located in the USA. This complaint was rejected by the Irish DPC on the basis that the USA had been officially and conclusively declared 'adequate' to receive European data by the European Commission.

What is the Safe Harbour Agreement?

The EU/US Safe Harbour Agreement was drawn up in 2000 as a means of wholesale approval of data transfers from Europe to the USA. This is due to a European Commission decision that the Safe Harbour Agreement is sufficient to ensure that the fundamental rights of European citizens will be upheld whenever their data is transferred to the USA.

American organisations seeking to receive European data sign up to the agreement voluntarily, which is self-certification that they will comply with European data protection standards.

Over 4,000 American entities have signed up to the terms of the Safe Harbour Agreement, which has allowed them to receive unscrutinised transfers of personal data from across the Atlantic, on the assumption that adequate protection will be given to that data.

The CJEU ruling

On appeal and referral to the CJEU, it was found that Mr Schrems' complaint should, in fact, have been investigated by the Irish DPC in light of the Snowden disclosures, which revealed a level of interference with European personal data by American security agencies that is incompatible with EU data protection laws. Subsequently, the CJEU also declared the Safe Harbour Agreement itself to be invalid, as it no longer provides sufficient protection to European citizens when their personal data is transferred to the USA. As a result, the CJEU has declared the European Commission adequacy finding in respect of the USA to be invalid for failure to comply with Article 25(6) of the Data Protection Directive.

continued over

Invalidity of the Safe Harbour Agreement

The CJEU emphasised that the Safe Harbour regime has a number of specific shortcomings that render it an ineffective safeguard for European data protection standards. Importantly, although the Agreement imposes obligations on the organisations that sign up to it, the American public authorities are not themselves required to comply with its principles, nor do they maintain separate domestic laws or international commitments that achieve the same result. When combined with the lack of an independent mechanism to supervise and detect infringement of Safe Harbour in the USA, in the eyes of the CJEU, the Agreement does little more than establish an unregulated self-certification scheme for American organisations.

Further, the CJEU observed that the Safe Harbour principles are circumvented through the inclusion of wide loopholes in the Agreement that aim to protect American 'legitimate interests'. Snowden's disclosures revealed that these carve-outs are invoked without limitation by American government agencies and that Safe Harbour signatories are compelled to comply with requests from those agencies.

Who is responsible for making and enforcing data protection law in Europe?

The European Commission

Under Article 25(6) of the Data Protection Directive, the European Commission has the ability to make 'adequacy findings'. This is a binding decision that a particular non-EEA country maintains data protection standards comparable to those afforded in Europe.

The Commission made an adequacy finding in respect of the USA on the basis of the Safe Harbour Agreement in 2000.

Data Protection Commissioners

The EU requires that each Member State must have a Data Protection Commissioner to act as a watchdog for data protection law. It must be an independent body and, under Article 28 of the Data Protection Directive, it has powers to investigate and suspend data processing or transfer where these activities do not comply with EU standards.

In the UK, this role is undertaken by the Information Commissioner's Office (the ICO).

What next?

For businesses operating in Europe and the USA, the significance of this decision should not be under-estimated.

The immediate repercussion of this judgment is that transfers of personal data from Europe to the USA made solely on the basis of the protection afforded by the Safe Harbour Agreement are no longer compliant with data protection law, and organisations that carry out such transfers should reconsider how they will comply with their data protection obligations.

Where transfers of data to the USA are still necessary, organisations should consider putting in place model data protection contractual clauses in respect of those transfers, or setting up corporate rules in respect of intra-group transfers of data.

It is also worth noting that, in the absence of an EU-wide blanket authorisation for transfers of personal data to the USA, each Member State may need to create their own regulatory mechanism to plug the gap left by the CJEU's declaration of invalidity of the Safe Harbour Agreement. The UK Information Commissioner has issued a **response** to the CJEU ruling and recognises that it will take organisations some time to ensure that their transfers of data to the USA comply with data protection law.

In the test case itself, Mr Schrems' complaint will return to the Irish DPC, who must undertake a proper investigation of Facebook's data transfer practices. If the Irish DPC decides that Facebook's activities have not provided adequate protection for European Facebook users then it may suspend transfers of personal data to American servers with immediate effect.

Contact

For further information, please contact:

Andrew Dunlop
Partner

+44 (0) 117 902 2786
andrew.dunlop@burges-salmon.com

David Varney
Associate

+44 (0) 117 902 7261
david.varney@burges-salmon.com