What next for EU-US data transfers?

Pulina Whitaker, a partner in global law firm Morgan Lewis's London employment practice, examines the ECJ ruling on the **Safe Habor** agreement and its impact on EU and US data transfers

Data controllers and data processors

A "data controller" is an organisation that determines the purposes and means of processing the data. It has control over the data and any action which is taken with it. Data controllers have direct obligations under data protection laws, including the transfer of personal data outside the European Economic Area, which is broadly restricted without consent of the individual unless some permitted exemptions or derogations apply. Data controllers are, therefore, potentially liable for any breaches of data protection laws.

On the other hand, a "data processor" is an organisation that processes personal data on behalf of a data controller. They do not choose the purposes for which the data is processed, but take their instructions from the data controller. Under the current data protection regime, data processors have no direct obligations, but if a data controller wishes to engage a data processor, they must ensure that a written processing agreement is in place. This must include, for example, an obligation on the data processor to have appropriate technical and organisational measures in place to keep the personal data secure and a commitment that they will only act in accordance with the data controller's instructions. This position is likely to change under the new General Data Protection Regulation which is still being finalised. It is proposed that data processors will be directly liable for some data protection obligations.

EU-US Data Transfers

According to the European Commission, the United States is a country with "inadequate" data protection laws. In 2000, the European Commission and the US Department of Commerce, therefore, agreed to implement a self-certification programme for US organisations to receive personal data sent from Europe, provided the US organisations certified that they adhered to certain standards of data processing comparable with EU data protection laws so that EU citizens' personal data was treated as adequately as if their personal data had remained within Europe. This Safe Harbor programme is operated by the US Department of Commerce and enforced by the Federal Trade Commission. Over 4,000 organisations have current self-certifications of adherence to Safe Harbor principles (see **Safe Harbor List**).

Mr. Schrems complained in Irish legal proceedings that the Irish Data Protection Commissioner refused to investigate his complaint that the Safe Harbor programme failed to protect adequately personal data after its transfer to the US, in light of Edward Snowden's revelations about the NSA's PRISM programme. The question of whether EU data protection authorities have the power to investigate complaints about the Safe Harbor programme was referred to the European Court of Justice (ECJ).

Safe Harbor is invalid

The ECJ declared that the European Commission's decision to approve the Safe Harbor programme in 2000 is "invalid" on the basis that US laws fail to protect personal data transferred to US state authorities pursuant to derogations of "national security, public law or law enforcement requirements". Further, EU citizens do not have adequate rights of redress where their personal data protection rights are breached by US authorities.

The powers of national data protection authorities are significantly strengthened by this decision. They could suspend some or all personal data flows into the US in serious circumstances and where they have justifiable reasons for doing so. There is, however, a risk that one data protection authority could order that data transfers by an international organisation outside Europe be suspended from that jurisdiction whereas data transfers in other European jurisdictions are permitted. To mitigate this risk, the European Commission is entitled to issue EU-wide "adequacy decisions" for consistency purposes.

Other options to transfer personal data to the US

Safe Harbor-certified organisations should note there are other options to transfer personal data to the US, including express consent and the use of Binding Corporate Rules or EU-approved model clause agreements. Organisations with Safe Harbor certification or who use Safe Harbor-certified vendors should consider these options or discuss these other options with their vendors.

Model clauses are very commonly used. Other than in a few European countries such as Cyprus and Greece, there is no requirement to obtain a specific permit from the data protection authority to use model clause agreements. There are two forms:

• Controller – controller agreements; and
• Controller – processor agreements.

Currently, there are no approved processor-processor model clauses, but this is likely to change under the new General Data Protection Regulation.

There is, however, a risk that the Schrems decision could affect these other options of transferring personal data outside the European Economic Area. Other countries, as well as the US, have national security derogations which are likely to override the protection of personal data, however it is transferred, with the only exception of specific and informed consent from an individual to the transfer of his or her personal data to governmental authorities for national security purposes (which is unrealistic). We are awaiting guidance from the European Commission and a way forward on a possible Safe Harbor 2.0 by the end of January 2016.

The original article was published in **Payroll World**

The online version can be found here