EU COURT BLOCKS TRANSFER OF PERSONAL DATA TO THE U.S. VIA ‘SAFE HARBOR’ ARRANGEMENT

James Castro-Edwards Wedlake Bell LLP
Jaap Kronenberg and Mark Jansen Dirkzwager advocaten & Notarissen

On October 6, 2015, the Court of Justice of the European Union (‘ECJ’) issued a ground breaking ruling, by blocking the transfer of personal data from Europe to U.S. undertakings relying on the U.S. Safe Harbor scheme. The ECJ judgement will not only affect U.S. businesses with affiliates in Europe, but IT-related service providers (particularly online services) with European customers. These businesses can no longer rely on the U.S. Safe Harbor to transfer personal information relating to their employees, customers and suppliers from Europe to the U.S.

The EU-US Privacy Shield agreement reached between the U.S. Government and the European Commission on February 2, 2016, was intended to fill the gap left by the ECJ decision. However, doubts have already been expressed as to the protection the Privacy Shield will afford EU citizens in practice, and at best it has some way to go before it can be used as a means of data transfer.

This article explains the key developments, considers the reaction in Europe (paying particular attention to the UK and the Netherlands) and suggests how U.S. businesses can address the change.

BACKGROUND: EUROPEAN DATA TRANSFERS, THE U.S. SAFE HARBOR DECISION, AND MAXIMILIAN SCHREMS

The European Data Protection Directive 95/46EC (‘Directive’) prohibits the transfer of EU citizens’ personal data to countries outside the European Economic Area, or EEA, that do not guarantee adequate protection. By way of Decision 2000/520, the EU Commission recognized the U.S. Safe Harbor as providing adequate protection. Since the decision, thousands of businesses have relied upon the U.S. Safe Harbor as a means of transferring their employees’, customers’ and suppliers’ personal data from Europe to the U.S. However, following the ECJ decision these businesses will need to consider alternative means of transfer or risk penalties.

The ECJ ruling follows Austrian law student Maximilian Schrems’ complaint to the Irish Data Protection Commissioner about the transfer of his personal information by Facebook Ireland to Facebook in the United States. Schrems’ complained after Edward Snowden publicly revealed the requisitioning from U.S. companies and the subsequent unbridled searching of personal information of EU citizens by the American National Security Agency. Schrems argued that such un fettered access to European citizens’ personal data demonstrated that the U.S. Safe Harbor did not adequately safeguard personal data to European standards. The Irish Data Protection Commissioner initially rejected the complaint, so Schrems appealed to the Irish High Court, which turned to the ECJ.

THE ECJ JUDGEMENT

The ECJ held that Decision 2000/520 ‘cannot eliminate or even reduce the powers available to the national supervisory authorities under the Charter of Fundamental Rights of the European Union and the Directive.’ In other words, even if the European Commission has adopted a decision, national supervisory authorities may, with complete independence, examine whether the transfer of personal data complies with the requirements of the Directive. Though only the ECJ may decide whether or not a commission decision is valid.

The ECJ found that U.S. authorities
were able to access European citizens’ personal data for purposes that were incompatible with the purposes for which it was transferred under the U.S. Safe Harbor scheme, and beyond what was strictly necessary and proportionate to the protection of U.S. national security. As such, European Citizens’ fundamental rights to respect for private life and for effective judicial protection were compromised. The ECJ found that the European Commission did not have competence to restrict national supervisory authorities’ powers and hence the Commission Decision was invalid.

The ECJ ruled that the Irish Data Protection Commissioner must examine Schrems’ complaint and decide whether the transfer of European Facebook users’ personal data should be suspended on the grounds that the U.S. does not ensure an adequate level of protection for personal data. If the Irish Commissioner concludes that personal data is not adequately protected, it must suspend the transfer.

**REACTIONS TO THE ECJ DECISION**

In the UK, the Directive is implemented into national law by the Data Protection Act 1998, enforced by the Information Commissioner’s Office (‘ICO’). Following the ECJ decision, the ICO observed the Safe Harbor was only one of a number of potential data transfer solutions, cautioned that companies should not rush to alternative measures until the implications of the ECJ decision have been fully ascertained, and confirmed that it would be issuing guidance in due course. The ICO also reiterated that as well as Model Clauses and Binding Corporate Rules, data controllers established in the UK can rely on their own adequacy assessment of data recipients, leaving businesses with a range of alternatives to the Safe Harbor.

In the Netherlands, the Directive takes effect by way of the Dutch Privacy Act, the Wet Bescherming Persoonsgegevens, 2000 (‘WBP’), enforced by the Dutch data protection authority the Autoriteit Persoonsgegevens. The Dutch Minister of Justice has taken the view that not only is the transfer of personal data unlawful from the date of the ECJ decision, but also any transfers made prior to the decision (though this point seems to be inconsistent with the ECJ ruling). The Minister further advised that as long as no EU solution is found, companies should consider alternative solutions for transferring data to the U.S. With this in mind, U.S. companies with a presence in the Netherlands should be aware that as of January 1, 2016, the Dutch DPA has been able to issue penalties up to €820,000 (US$920,000) for breaches of the WBP.

Both the UK and Dutch authorities will look to the Article 29 Working Party for guidance. The Article 29 Working Party is an independent body appointed under the Directive, to advise European data protection authorities. Its view is that massive and indiscriminate surveillance is incompatible with the EU legal framework, and that data transfer tools are not the solution to the issue; countries where state authorities can access information beyond what is necessary in a democratic society cannot be considered safe destinations for data transfers. However, the Working Party has stated that while it considers the impact of the ECJ judgement, Binding Corporate Rules and Standard Contractual Clauses remain valid transfer solutions.

In the U.S., industry groups and trade associations have expressed concerns that the decision will lead to uncertainty for businesses. Observers both in Europe and the U.S. note that the judgement could potentially call into doubt other data transfer solutions such as Binding Corporate Rules and Model Clauses. U.S. tech companies in particular, many of whom derive significant revenue streams from Internet advertising, have called for the swift conclusion of a Safe Harbor version 2.0.

**THE EU-US PRIVACY SHIELD**

Following widespread calls from Europe and the U.S. for a replacement for the Safe Harbor, the European Commission and the U.S. Government agreed on February 2, 2016, the EU-US Privacy Shield. The EU-US Privacy Shield includes a number of measures to protect European citizens’ personal data, including: requiring U.S. companies to commit to processing EU personal data in accordance with a number of standards; imposing access restrictions upon U.S. government agencies when they access EU citizens’ personal data (subject to an annual EU / U.S. joint review); and introducing a number of means of redress for European citizens including recourse to a U.S. ombudsman.

However, the EU-US Privacy Shield is not home and dry yet: the European Commission still has to publish an adequacy decision, obtain advice from the Article 29 Working Party and consult with a committee composed of representatives from the Member States. The outcome is not a foregone conclusion; many European privacy advocates have dismissed the Privacy Shield as no more than a re-heated Safe Harbor. Further, the lasting effect of the ECJ Decision is that national data protection authorities may call the Privacy Shield into question if it does not appear to adequately protect EU citizens’ personal data.

**COMMENT**

Many U.S. businesses with offices or clients in Europe will be wondering how to address the change. A crucial starting point is to assess the personal information they hold, where it is transferred internationally, and how it is protected. The appropriate data transfer solution for a particular enterprise will then depend on the specific circumstances. U.S. businesses should be aware that the EU-US Privacy Shield is not necessarily the ‘cure all’ solution; it has some way to go before being recognized as providing adequate protection, and even if it is accepted, it may still be challenged at any point by European data protection authorities or privacy activists such as Max Schrems.

For U.S. businesses, this may seem a daunting challenge. While conducting a data transfer review may not be a small undertaking, nor is it an insurmountable one. However, with European data protection authorities likely to take enforcement action against unlawful transfers, and looming agreement of the EU General Data Protection Regulation (which could introduce fines of up to 4% worldwide annual turnover or €20,000,000), U.S. businesses must act now to address the risk.