MAYER·BROWN

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Managing International Data Transfers After EU-US Safe Harbor Framework Invalidated

Scenario

A large international corporation is involved in litigation in the United States. It has received discovery requests that necessitate the review and potential disclosure of extensive records located within the European Union (EU). The company has learned that the European Court of Justice (ECJ) has recently declared the EU-US Safe Harbor framework invalid. It wishes to understand whether this ruling has any implications for its proposed approach to review and disclosure.

Background and Decision

Under the EU Data Protection Directive (the Directive), transfers of personal data from the European Union to territories outside the European Union are only permitted if adequate protection is ensured for that data in the territory to which it is transferred. The Directive provides that the European Commission (EC) may find that a third country ensures an adequate level of data protection through its domestic law or international agreement. EC Decision 2000/520 stated that adequate protection is provided by US businesses that sign up to the Safe Harbor principles.

In 2013, Max Schrems, a Facebook subscriber from Austria, filed a complaint with the Data Protection Commissioner (DPC) of Ireland requesting that the DPC prevent Facebook in Ireland from transferring his personal data to the United States under the Safe Harbor framework on the basis that US law and practice did not ensure adequate protection of that data. Schrems challenged the Irish DPC's conclusion that it was bound to permit the transfer of the data by EC Decision 2000/520. In support of his complaint, Schrems cited the revelations published by Edward Snowden concerning the US National Security Agency's surveillance of data held by Safe Harbor participants.

The case was referred to the ECJ, which determined that the current Safe Harbor framework did not ensure an adequate level of protection under the Directive and that Decision 2000/520 was invalid. In particular, the ECJ found that because US national security, public interest and law enforcement requirements overrode Safe Harbor principles, this gave rise to potential interference by US public authorities with the fundamental rights of the data subjects. Notably, the ECJ found that EU data subjects had no administrative or judicial means of redress in relation to such interference.

Consequences of the *Schrems* Decision

The ECJ decision affects companies that rely solely upon the Safe Harbor framework to transfer personal data from the European Union into the United States.

Recognizing the potential for panic created by this decision, various EU-national DPCs have announced that they will work on guidance for those affected by the decision, rather than rushing to enforce its effect. While this should give organizations some breathing space in which to consider whether practical alternatives are available, any potentially affected organization should commence an urgent review of its position.

Next Steps

In the scenario above, it will be important for the company to identify the data that might be transferred, ascertain whether it includes personal data and identify the basis upon which it will be transferred.

If, for instance, the collection and review will be conducted or supported by a third-party Legal Process Outsourcing (LPO) provider and involve the transfer of data into the United States, then confirmation should be sought on the specific regime under which this will take place. If the LPO provider is relying solely on having signed up to the Safe Harbor framework, then alternative avenues should be explored.

Transfers Under Article 26(1)(d)

Article 26(1)(d) of the Directive provides that transfers of personal data may take place where they are necessary for (among other matters) the purposes of establishing, exercising or defending legal rights. The Article 29 Working Party, an independent European advisory body on data protection established under the Directive, acknowledged in its Working Paper 114 that transfers of data for pre-trial discovery or disclosure in US proceedings may fall within this provision. However, they emphasize that, because it is a derogation from the Directive's prohibition against transfers to territories that do not provide adequate protection for personal data, the provision must be construed strictly. So, for instance, the bulk transfer of broad categories of data not yet reviewed for potential relevance would not be protected.

It is also important to note that the collation and review of data for potential disclosure constitutes "processing" of data under the Directive. Article 7 of the Directive, which permits processing of data for the purposes of the legitimate interests of the data controller, can potentially apply to such collation and review. However, the Article 29 Working Party noted (in the same working paper) that:

- A strict interpretation must be applied to the derogation;
- The interests of the data subject must be balanced against the legitimate interests of the controller; and
- That will involve considering such procedures as anonymizing or pseudonymizing data and pre-filtering irrelevant data.

Consent

Processing and transfer of personal data may be done with the data subject's consent. However, any such consent must be clear and unambiguous, freely given, specific and informed. Further, national DPCs have regularly expressed caution regarding exclusive reliance upon consent (which can be withdrawn). Further, as a matter of practicality, there may be several data subjects in relation to a single record.

Alternative Regimes Under Which Data Is Transferred

Alternative arrangements exist under which data is transferred internationally by organizations, although the establishment of such arrangements is typically time consuming and costly. These arrangements include:

- Binding Corporate Rules: this option is available (only) to multinational organizations regarding transfers within their group. These rules create rights for individual data subjects and obligations for the group companies. However, implementation is potentially complex and expensive (requiring the approval of each affected national DPC).
- EC model clauses: the EC has approved certain sets of standard contractual clauses as providing adequate levels of protection. The clauses cannot be altered in any way or they will be ineffective. Some EU member states require notification to, or approval by, the relevant national DPC.

An anticipated consequence of the reasoning behind the *Schrems* decision (that is, the inadequacy of the framework to protect personal data from unrestricted access by US authorities) is the further scrutiny of the adequacy of the protection provided under these other methods of data transfer.

Conclusion

Negotiations regarding the Safe Harbor regime have been proceeding between the EC and the US Department of Commerce since 2013. These discussions have not yet resulted in a concluded agreement and *Schrems* will increase the pressure to reach a mutually satisfactory position. Whatever the outcome, in the meantime, organizations affected by *Schrems* need to act promptly.

For inquiries related to this Tip of the Month, please contact Edmund Sautter at esautter@mayerbrown.com or Kim Leffert at kleffert@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com, Ethan Hastert at ehastert@mayerbrown.com, or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.