CYBER RISKS

EU-US PRIVACY SHIELD

Last month the European Commission and the U.S Department of Commerce reached a political agreement on a framework for the transatlantic exchanges of personal data, referred to as the EU-US Privacy Shield.

The Privacy Shield was required following the ECJ Ruling in October 2015 that Safe Harbor - the framework which certified American companies as providing adequate protection for personal data from the EU, as required by the EU Data Protection directive – was declared invalid. For more information on this decision see our previous bulletin.

The Privacy Shield, which is the product of months of intense negotiations, aims to protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses transferring the data.

The deal is extremely important for both sides, as nearly all data that is exchanged between the two regions will depend on the efficacy of this agreement. U.S. Secretary of Commerce Penny Pritzker said the new framework "underpins $260 billion in digital services trade across the Atlantic," and provides "a modernized and comprehensive framework that addresses the concerns of the European Court of Justice and protects privacy."

What does the Privacy Shield contain?

- **Stronger obligations on companies and robust enforcement:** the new arrangement aims to be more transparent and contain more effective supervision mechanisms to ensure companies respect their obligations. There are also tightened restrictions on forwarding data to third parties.
- **Safeguards and transparency obligations on US government access:** for the first time, the U.S. government has provided written assurances that any access of public authorities for national security purposes will be subject to clear limitations and safeguards. The U.S. will provide an annual written commitment that it does not conduct mass or indiscriminate surveillance of EU citizens.
- **Protection of European citizens through redress option.** Europeans will have the possibility of redress through an Ombudsman mechanism that will be independent from national security.

Complaints will be resolved within 45 days. There will be a free ADR solution and Europeans can approach their national Data Protection Authorities who will work with the U.S. to ensure complaints are investigated and resolved.

- **Annual joint review:** the functioning of the Privacy Shield will be monitored regularly by the European Commission and the U.S. Department of Commerce. The Commission will also hold an annual privacy summit to discuss developments in U.S. privacy law and their impact on EU citizens.

Does the Privacy Shield solve the problems of Safe Harbor?

It was hoped that the court decision and subsequent negotiation would prompt the U.S. to seriously review its surveillance policies. The Safe Harbor program was deemed inadequate by the EU primarily because it was considered that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life." The Court considered that the U.S. government being able to indiscriminately spy on non - U.S. citizens undermined any assurance provided by an American company that it was compliant with the EU's data protection standards.

The proposed reform purports to overcome that issue, however, the agreement includes six exceptions when data can be collected in bulk. These include detecting and countering certain activities of foreign powers; counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to U.S. or allied armed forces; and combating transnational criminal threats, including sanctions evasion. These exceptions are broad, undefined and are difficult to reconcile with the assurances provided in relation to bulk collection of personal data.

If EU citizens are unhappy with the way their data is collected, there are supposed to be adequate methods of redress available. Following the announcement of the Privacy Shield, the Judicial Redress Act was signed into law by President Obama. This law was designed to give EU citizens the same protections under the Privacy Act as offered to U.S. citizens, however, the Act has been criticised due to its large number of limitations, including that federal agencies can exempt themselves if they declare that the investigatory material has been "compiled for law enforcement purposes". Further, the independence of the proposed Privacy Shield Ombudsman has also been questioned due to its position within a U.S state government department that supervises and directly benefits from the advice of the intelligence agencies.

The European Commission and EU officials have attempted to address concerns regarding the 'written assurances' from the U.S. and vowed that privacy complaints would be addressed without interference from the U.S. government. However, until a blanket assurance on this point can be provided, the Commission has not established that the U.S. system of privacy laws are essentially equivalent to the EU;

that data subjects have real rights against disproportionate processing in the U.S. and that if there is disproportionate or illegal processing then citizens can have their personal data deleted and will be appropriately redressed.

As said by Max Schrems, the Austrian privacy activist who originally brought down the Safe Harbor agreement, "With all due respect…a couple of letters by the outgoing Obama administration is by no means a legal basis to guarantee the fundamental rights of 500 million European users in the long run, when there is explicit U.S. law allowing mass surveillance."

Conclusion

It is not clear that the Privacy Shield adequately deals with any of the requirements of the original ECJ decision. There is still a program of mass surveillance against non-U.S. persons, EU citizens do not have an effective remedy against the surveillance programs, and the proposed redress options are not sufficiently independent.

The Privacy Shield proposal has not yet been signed. The next step is for a committee composed of representatives of the Member States and the EU Data Protection Authorities (Article 29 Working Party) to review the agreement. They will give their opinion, expected in April or May, on whether the proposed framework provides sufficient privacy protection.

Although this opinion isn't binding, EU Data Protection Authorities investigate privacy complaints and can potentially stop data transfers to the U.S. so it will be interesting to see how far the Member States are willing to push back on the agreement. While we can expect them to raise a series of challenges to this compromise, there is also industry pressure to get the agreement implemented as quickly as possible due to the countless technology companies who are currently uncertain about how to handle their data.

Samantha Wilson
Associate
T: 0203 697 1906
M: 07780 221676
E: samantha.wilson@cpblaw.com