The European Commission launches the EU-US Privacy Shield: stronger protection for transatlantic data flows

Isabela Crespo Vitorique and Iban Díez López
Senior Associates of the IP-IT Practice Area, Gómez-Acebo & Pombo

On 12 July 2016, the European Commission approved the arrangement known as the EU-US Privacy Shield, which provides a legal framework for data flows between the two continents that protects more effectively individuals' fundamental rights and personal data. This agreement lays down the conditions for transatlantic data flows between companies in the European Union and the United States, delivering the same guarantees as those offered by European legislation and satisfying the requirements identified by the Court of Justice of the European Union in its judgment of 6 October 2015, which quashed the previous Safe Harbour scheme. This agreement also includes certain assurances and safeguards to avoid massive surveillance of European citizens' data by US intelligence services.

1. The Privacy Shield as a framework for the safe flow of data between US and EU companies. Replacement of the Safe Harbour scheme

As occurred with the previous Safe Harbour scheme, the Privacy Shield is based on a system of self-certification by which US companies commit to a set of *privacy principles* in respect of the processing of personal data from the European Union:

- *Notice Principle:*

  US companies are obliged to provide information to data subjects on a number of key elements relating to the processing of their personal data (e.g. type of data collected, purpose of processing, right of access and choice, conditions for onward transfers and liability).

- *Choice Principle:*

  US companies must obtain individuals' formal consent before disclosing sensitive personal data thereof to third parties.

- *Security Principle:*

  US companies must evaluate security risks in the processing of personal data and must take steps to mitigate such risks to the maximum extent possible. In the case of sub-processing, organisations must conclude a contract with the sub-processor guaranteeing the same level of protection as provided by the Principles.

- *Data Integrity and Purpose Limitation Principle:*

  US companies must ensure integrity of the personal data obtained and may not process it in a way that is incompatible with the purpose for which it was originally collected or subsequently authorised by the data subject.

- *Access Principle:*

  US companies must provide confirmation of whether it is processing personal data related to individuals and, if so, have such data communicated within reasonable time.

Individuals may request access to their personal information at any time and with no prior justification.

- *Accountability for Onward Transfer Principle:*

  Personal data transfers to third-party controllers or processors may only be carried out for limited and specified purposes. Furthermore, data subjects must be informed as to such onward transfers under the Notice Principle outlined above.

- *Recourse, Enforcement and Liability Principle:*

  US companies must provide robust mechanisms to ensure compliance with the other Principles and must annually report on such compliance through the renewal of their self-certification, providing evidence of the measures taken to effectively comply with the Privacy Shield principles. Any company that fails to demonstrate compliance with such requirements will be removed from the list of companies that have self-certified their adherence to the Principles (Privacy Shield List) and will be subject to economic sanctions.

US companies that voluntarily decide to be included in the Privacy Shield List must first take the necessary measures to ensure compliance with all these Principles, after which they may apply for a Privacy Shield certification from the Department of Commerce, which will keep an *updated list of the companies that have self-certified their adherence to the Principles*. As explained above, companies must annually re-certify their participation in the framework.

The US Department of Commerce must ensure that companies that have failed to renew continue complying with Privacy Shield-related requirements with respect to the data they collected when they were still certified. The companies must continue to apply the Principles for as long as it processes such information;

This framework provides *mechanisms to ensure effective application of and compliance with* the Privacy Shield Principles by the self-certified companies. Ideally, complaints by individuals affected by non-compliance will be resolved by the company in question or, as the case may be, such company will offer alternative dispute resolution mechanisms at no cost. Individuals may also refer their complaints to their national data protection authorities, which will cooperate with the US Department of Commerce to ensure that EU citizens' complaints are investigated and resolved. An arbitration option is available as a last resort for complaints that have not been resolved by either of the above mechanisms.

In addition, it is worth noting that, to date, Spanish companies related to participating US organisations are not subject to any requirements.

2. Assurances to avoid abusive massive surveillance of European citizens' data for national security purposes

This framework provides clear safeguard and transparency obligations on US government access to EU citizens' data. The United States has given the European Union assurances that access by public authorities to EU citizens' data for security purposes is subject to limitations, safeguards and oversight mechanisms. Also for the first time, everyone in the EU will benefit from redress mechanisms in this area. The US has ruled out indiscriminate mass surveillance on personal data transferred to the US under the EU-US Privacy Shield arrangement. The Office of the Director of National Intelligence further clarified that bulk collection of data could only be used under specific preconditions and needs to be as targeted and focused as possible. The US Secretary of State has established a redress possibility in the area of national intelligence for Europeans through an Ombudsperson mechanism within the Department of State.

3. Next steps

This framework will be notified to the Member States and will thereby come into force immediately. On the US side, the Privacy Shield framework will be published in the Federal Register. Once US companies have had an opportunity to study the framework and update their compliance, companies will be able to certify with the Department of Commerce as from 1 August.

In parallel, the Commission will publish a short guide for citizens explaining the available remedies in case an individual considers that his personal data has been used without taking into account the data protection rules.

Domestically, it is worth noting that as of yet no statement has been issued by the Spanish Data Protection Authority (*Agencia Española de Protección de Datos*) concerning the final approval of the Privacy Shield framework. We await their opinion and view on the subject.