July 14, 2016

Data Protected? Europe Adopts the EU-US Privacy Shield

Following the recent approval by the Article 31 Committee (which includes representatives of the European Union ("**EU**") Member States) of the final version of the EU-U.S. Privacy Shield ("**Privacy Shield**"), the European Commission ("**Commission**") adopted the Privacy Shield on 12 July 2016.

Following the launch of the Privacy Shield, Commissioner Věra Jourová commented: "The EU-U.S. Privacy Shield is a robust new system to protect the personal data of Europeans and ensure legal certainty for businesses. It brings strong data protection standards that are better enforced, safeguards on government access, and easier redress for individuals in case of complaints. The new framework will restore the trust of consumers when their data is transferred across the Atlantic. We have worked together with the European data protection authorities, the European Parliament, the Member States and our U.S. counterparts to put in place an arrangement with the highest standards to protect Europeans' personal data."

The Former Safe Harbor Framework

The forerunner to the Privacy Shield – the Safe Harbor framework – allowed EU-based data controllers to transfer personal data to Safe Harbor members in the USA while ensuring an adequate level of protection for such personal data.

Safe Harbor was invalidated in October 2015 by a European Court of Justice decision for two main reasons. First, U.S. intelligence services were able to gain access to personal data transferred to a greater extent than strictly necessary or appropriate for the protection of national security, and second, non-U.S. citizens were unable to obtain legal remedies in the USA for misuse of their data.

The Privacy Shield

The Privacy Shield, which is intended to replace Safe Harbor, comprises a data protection self-certification framework for companies transferring personal data of EU citizens to the USA. The Privacy Shield will ensure stronger protection for TransAtlantic data flows and will protect the fundamental rights of individuals whose personal data is transferred to the USA by data controllers to whom EU data protection legislation applies. It will also provide legal certainty for businesses involved in TransAtlantic data transfers.

The Privacy Shield will apply to both data controllers and data processors and is based on seven core privacy principles, including notice; choice; security; data integrity and purpose limitation; access; accountability for onward transfer; and recourse, enforcement and liability (the "Principles"). It is regarded as being fundamentally different from Safe Harbor, imposing clear and strong obligations on companies handling personal data and ensuring that the rules are adhered to and enforced in practice.

Following the political agreement of 2 February 2016 between the Commission and the U.S. Government on a new framework for TransAtlantic exchanges of personal data for commercial purposes, the Commission originally presented a draft decision on the Privacy Shield on 29 February 2016. The Article 29 Working Party, the European Parliament and the European Data Protection Supervisor all criticized the original draft and requested amendments.

The final version of the Privacy shield addresses the following matters:

- ***Annual Joint Review Mechanism:***
  - An annual joint review mechanism conducted by the Commission and the U.S. Department of Commerce, together with associate national intelligence experts from the U.S. and European Data Protection Authorities will oversee the functioning of the Privacy Shield. A public report will be issued by the Commission to the European Parliament and the Council.
- ***U.S. Government Access:***
  - U.S. government access will be subject to clear safeguards and transparency requirements. The U.S. has assured the EU that public authorities' access for national security and law enforcement purposes will be subject to clear limitations, safeguards and oversight mechanisms, preventing generalized access. There will also be redress mechanisms in this regard for the first time.
  - Indiscriminate mass surveillance of European citizens personal data transferred to the U.S. under the Privacy Shield will not be permitted.
  - Bulk data collection may only take place in accordance with specific pre-conditions and should be as focused as possible. The Privacy Shield includes safeguards for using data in these special circumstances.
  - The U.S. Secretary of State has implemented a redress process for individuals in respect of complaints or enquiries individuals may raise in a national intelligence context through an Ombudsperson mechanism that will be independent of the U.S. intelligence services.
- ***Data Handling Obligations:***
  - There are stringent requirements on companies handling data.
  - The U.S. Department of Commerce will carry out regular reviews of participating companies to make sure that they are complying with the rules (if not, sanctions will be applied and companies could be removed from the Privacy Shield list). There will be effective supervision mechanisms.
  - The rules on onward transfers of personal data to third parties should ensure the same level of protection for personal data that is transferred by companies participating in the Privacy Shield.
- ***Protection of Individual Rights:***
  - Individuals who believe that their data has been misused under the Privacy Shield framework will have access to a number of affordable and accessible dispute resolution mechanisms.
  - If complaints cannot be resolved by participating companies themselves, free alternative dispute resolution mechanisms will be available.Individuals can also approach their national data protection authorities, who will work with the Federal Trade Commission to ensure that EU citizens' complaints are reviewed and resolved.
  - An arbitration mechanism will be available as a final means of resolution if cases are not resolved through other methods.
  - As noted above, national intelligence-related issues will be resolved through the Ombudsperson mechanism.

Recent Updates

The final version of the Privacy Shield takes into account the views of the Article 29 Working Party, the European Parliament and the European Data Protection Supervisor in a number of areas. For example:

- Regarding onward transfers of personal data to third parties by Privacy Shield companies, the requirement to provide the same level of protection has been clarified further and now obliges third parties to inform the Privacy Shield company if it is no longer able to ensure the appropriate level of data protection, following which the Privacy Shield company will have to take appropriate measures.
- Existing limitations on data retention have been clarified. Privacy Shield companies may only keep personal data for as long as this serves the purpose that such data were collected for.
- Regarding the bulk collection of data, the Office of the Director of National Intelligence in the USA clarified through a further document how bulk collection of personal data could only be used under specific pre-conditions and should be as targeted as possible (as noted above), especially through the use of filters and the requirement to minimize collection of non-pertinent information.
- The functioning and independence of the Ombudsperson mechanism was clarified, especially regarding its independence and cooperation with other independent oversight bodies with investigatory powers.

What Next?

The adequacy decision entered into force on 12 July 2016 following notification of the EU Member States. In the USA, the Privacy Shield will be published in the Federal Register and the U.S. Department of Commerce will begin operating the Privacy Shield and will monitor the compliance of Privacy Shield companies' privacy policies. U.S. companies will be able to certify with the Commerce Department from 1 August 2016. Companies can apply to register on the Privacy Shield list maintained by the U.S. Department of Commerce and must self certify annually that they meet the data protection requirements of the Privacy Shield.

The Principles apply to Privacy Shield companies immediately on certification; however, acknowledging the fact that the Principles will impact third-party commercial relationships, organisations that certify to the Privacy Shield in the first two months following its effective date must ensure that existing third-party commercial relationships conform with the Accountability for Onward Transfer Principle within nine months from the date that they certify to the Privacy Shield at the latest. During the interim period, where organisations transfer personal data to third parties, they shall apply the Notice and Choice Principles, and, where personal data are transferred to third parties acting as agents, ascertain that the agent is obliged to provide at least the same level of protection as is required by the Principles.

The Commission will also publish guidance for citizens explaining the remedies available to individuals who feel that their personal data have been used in breach of the relevant data protection rules.

Comment

It is hoped that adoption of the Privacy Shield will resolve some of the recent uncertainty regarding TransAtlantic personal data flows, which would be a welcome development for many EU- and U.S.-based companies. Now that it is in force the issue for many companies will be whether or not to elect to self-certify. The most likely candidates to sign up over the coming weeks are large technology companies and other data controllers for whom alternative mechanisms are administratively, politically or technologically too challenging to implement. For others, especially smaller sized organizations with lower volumes of international data transfers, there will need to be serious consideration of the cost versus benefit of modifying working practices, policies and procedures, and having to renegotiate third party contracts, to ensure compliance with the enhanced Principles. These steps may require certifying U.S. companies to go well beyond what a typical EU company has to do or that it already has in place.

Organizations should now consider and determine if the benefits of the Privacy Shield for their business outweigh its burdens when compared to other options for legitimization. In addition to this, and to ensure that this topic remains open for debate and discussion, the constant threat of a legal challenge as to whether the Privacy Shield goes actually far enough to protect the personal data of European citizens, remains.