

Overview of the newly adopted EU-U.S. Privacy Shield

Posted on Tuesday 18th of October 2016 in Employment, Pensions & ImmigrationIP, IT & Media

After two and a half years of negotiations with the U.S. authorities and the invalidation of the Safe Harbour decision by the European Union Court of Justice, the European Commission adopted, on 12 July 2016, the new legal framework for the transatlantic transfers of personal data, called the “EU-U.S. Privacy Shield”. Here is an overview of this new legal framework.

Background to the Privacy Shield

As a rule, the transfer of personal data outside the EU is only possible to third countries that ensure an **“adequate level of data protection”** in terms of protecting the private life and basic freedoms and rights of individuals. It is up to the European Commission (**“EC”**) to decide whether a third country ensures such protection.

Transfers of personal data to a country which does not offer an adequate level of data protection are not impossible but in most cases require the prior authorisation of the competent national data protection authority (**“DPA”**) and that authorisation is only granted – among other requirements and basically – if there is an agreement between the sender and the recipient of the data containing the conditions of the personal data transfer and in line with the European data protection requirements.

The EC has recognised very few countries offering an “adequate level of data protection”. The U.S., as such, is not part of this very close circle. However, on 26 July 2000, the EC adopted a decision recognising the “Safe Harbour Privacy Principles” and “Frequently Asked Questions”, issued by the U.S. Department of Commerce, as providing adequate protection for the purposes of personal data transfers from the EU to the U.S. (**the “Safe Harbour Decision”**).

The Safe Harbour Decision therefore allowed the free transfer of personal data, for commercial purposes, from companies located in the EU to companies located in the U.S. that have adhered to the Safe Harbour principles.

Since 2013, the EC has expressed concerns about the adequacy of the Safe Harbour Decision, especially because of the significant increase in data flows between the EU and the U.S. and reports about alleged mass surveillance by U.S. National Security Agency. Consequently, in 2014 the EC initiated talks with the U.S. authorities in order to reform the Safe Harbour framework.

In addition, on 6 October 2015, the European Union Court of Justice (“ECJ”) invalidated the Safe Harbour Decision. Data controllers were therefore no longer allowed to rely on the Safe Harbour mechanism in order to transfer personal data to the U.S. Following the ECJ decision, the EC intensified the negotiations with the U.S. Department of Commerce on a new data transfer agreement, which was adopted at the beginning of this year, the “Privacy Shield”.

After amendments (deemed necessary by the Article 29 Working Party, composed of representatives of the EU DPAs, the European Data Protection Supervisor and the EC), the EC confirmed, on 12 July 2016, that the

Privacy Shield Framework was adequate to enable data transfers from the EU to the U.S.

This new framework came into operation on **1 August 2016**.

How does it work?

As with the former system, the Privacy Shield is based on **self-certification** of the companies located in the U.S. These companies have to register on a list managed by the U.S. Department of Commerce, and self-certify that they meet the Privacy Shield high data protection standards. The registration has to be renewed every year.

The U.S. Department of Commerce will ensure, through **active verifications**, that self-certified companies comply with the Privacy Shield's requirements, and those which are in repeated breach will be removed from the list.

The new legal framework **enhances the obligations of self-certified companies** handling personal data of EU data subjects and **strengthens the rights of individuals** in particular regarding the risk of mass surveillance by U.S. intelligence services.

Key changes

■ Strengthened privacy principles:

- **Enhanced responsibility for onward transfers**, which are possible only on the basis of a contract, for limited and specified purposes and solely if the contract provides at least the same level of protection as the Privacy Shield;
- **Greater transparency** of the self-certified companies, particularly regarding their privacy policies.

■ Better supervision, monitoring and enforcement by the U.S. authorities of compliance with the Privacy Shield principles.

■ Clear safeguards against mass surveillance: as a rule, U.S. intelligence services undertake **targeted collection** of personal data through the use of filters. **Bulk collection** could exceptionally be used to counter specific threats such as espionage, terrorism, weapons of mass destruction, or threats to cybersecurity. Besides, EU data subjects who believe that their personal data were unlawfully collected or used by U.S. authorities for national security purposes can address complaints to a new independent body - **the Ombudsperson**.

■ Effective and affordable dispute resolution remedies for EU data subjects: Data subjects who consider that the processing of their personal data infringes the Privacy Shield's principles can use several remedies: i) lodge a complaint directly with the **self-certified organisation**, ii) use **Alternative Dispute Resolution**, iii) address the complaint to an EU **national DPA**, which will forward the complaint, or iv) use the Privacy Shield **arbitration** mechanism as a last resort. Individuals can also use judicial remedies available under U.S. law (e.g. invoke breach of contract).

More to follow?

After a blocking period of several months for automatic transfers of data from the EU to the U.S., these transfers

can be re-launched thanks to the Privacy Shield, provided that the U.S. companies adhere to the Privacy Shield.

The Privacy Shield may, however, not impede EU companies from relying on other legal instruments to transfer personal data to the U.S., such as the **Binding Corporate Rules** or a data transfer agreement based on **Standard Contractual Clauses** approved by the EC.

The Commission and the U.S authorities will monitor the functioning of the Privacy Shield annually. Where the framework fails to ensure an equivalent level of protection to that provided by the EU laws, the adequacy decision can be suspended or even repealed.

The Privacy Shield will also need to pass the test of the new EU regulation[1], which take effect on 25 May 2018, as well as a new potential claim before the ECJ.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which repeals the Directive 95/46/EC and lays down rules on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Your contact(s)



Virginie LIEBERMANN

Counsel

Avocat à la Cour, Member of Luxembourg Bar, 2008

virginie.liebermann@molitorlegal.lu