Client Update – Transferring EU Personal Data to the US under the New EU-US Privacy Shield Agreement

Dear clients and friends,

The European Commission ("**EC**") and the US Department of Commerce have finalized the anticipated agreement for **the new framework allowing the transfer of personal data outside the European Union to US-based companies**.

After its formal approval in the near future, this new framework, named the EU-US Privacy Shield ("**the Privacy Shield**"), will replace the previous Safe Harbor framework which was invalidated last year by the European Court of Justice.

Following such approval, the transfer of personal data to US-based companies certified under the new Privacy Shield scheme will be allowed under EU law without the need to implement other special contractual and administrative mechanisms.

In parallel, the level of **enforcement of privacy protection compliance** by US regulators is expected to increase as a consequence of the US obligations under the agreement with the EU.

In this update, we are setting out the background regarding this development and elaborate on the **practical implications of the Privacy Shield framework**.

We will be glad to further assist in advising on the steps to be taken for the Privacy Shield implementation.

Best regards,

Ariel Yosefi, Partner
Head of AdTech and Technology Compliance
Herzog Fox & Neeman

Background

Under the EU legal regime, the transfer of personal data from the EU to another country is restricted and subject to various conditions. The EC is authorized to afford recognition to certain countries which offer an **adequate level of privacy protection**, in order to allow the transfer of personal data from the EU to these countries without the need to comply with the other restrictions and conditions.

The United States has never afforded this level of recognition by the EC. However, the EC recognized a similar level of adequacy in the case of transferring personal data to US-based companies which have participated in the self-certification scheme - "the Safe Harbor".

As we previously reported, in October 2015, the European Court of Justice found that **the EC's previous decision to afford recognition to the Safe Harbor framework is invalid** given that the Safe Harbor framework enables interference by US public authorities with an individual's privacy rights.

On 29 February 2016, after two years of negotiations which began before the ECJ ruling, the EC has now announced the finalization of an agreement between the EU and the US which will shortly allow the formal issuance of a Decision on the Adequacy of the Protection ("**the Adequacy Decision**"). The effect of the Adequacy Decision, which is subject to a formal adoption by the College of Commissioners, is that **personal data may be transferred from the EU to self-certified US-based companies, without any further restrictions**.

The objective of the Privacy Shield is to enhance and strengthen the **obligations on US-based companies to protect the personal data of EU citizens** as well the **monitoring and enforcement** mainly by the Department of Commerce and the Federal Trade Commission ("**FTC**"), including through increased cooperation with the relevant European Data Protection Authorities.

What is the Privacy Shield?

The Privacy Shield includes a **self-certified program** under which US-based companies could voluntarily agree to abide by **several data protection principles** in order to allow the transfer of personal data from the EU to US-based companies.

In practice, US-based companies which seek to enjoy the level of free personal data transfer from the EU, will need to **register annually on the Privacy Shield List** and **certify their compliance with the detailed privacy principles and practices** ("**Privacy Principles**"). The Privacy Principles include the following main requirements:

- **Notice**
  Companies will need to **provide information to data subjects** with regard to the processing of their personal data (including the type of personal data collected, the purpose of processing, a right of access and choice).

- **Choice**
  - Companies will need to grant data subjects the **option to "opt out" from the processing** of their personal data, if such data shall be disclosed to a third party or used for a different purpose than originally agreed.
  - With regard to the use of personal data for **direct marketing purposes**, the companies are required to grant the data subjects the option to "opt out" at any time.
  - In case the companies process **sensitive categories of data**, such as political opinions, sex preferences, health data, they must obtain the data subject's **affirmative express consent**.

- **Security**
  - Companies must also provide **reasonable and appropriate security measures** to safeguard the personal data of data subjects.
  - In the case of **sub-processing**, companies are required to sign an agreement with the sub-processor guaranteeing the **same level of protection** as provided by the Privacy Principles.

- **Data integrity and purpose limitation**
  Companies must ensure that personal data will be limited to what is **relevant for the purpose of the processing**, **accurate**, **complete** and **current**.

- **Access**
  - Companies are required to provide data subjects with the right to obtain from them a **confirmation of whether they process personal data** related to them.
  - Data subjects must be given the **opportunity to correct**, **amend** or **delete** personal data where it is inaccurate or has been processed in violation of the Privacy Principles.

- **Accountability for onward transfer**
  In case the companies wish to transfer personal data to other data processors, they must ensure that this **transfer is made on the basis of a contract which provides the same level of protection as** the one guaranteed by the Privacy Principles.

- **Enforcement and Liability**
  - Companies must provide **mechanisms in order to ensure compliance** with the Privacy Principles and to put in place an **effective redress mechanism** to deal with the complaints of EU data subjects with regard to their personal data processing. Companies are required to resolve complaints within 45 days. Alternatively, EU citizens can refer their complaints to their national Data Protection Authorities, which will work with the FTC to ensure that complaints are investigated and resolved.

- Companies must designate an **independent dispute resolution body** to investigate and resolve data subjects' complaints and to provide an appropriate recourse free of charge to the data subject.
- Companies must take measures to verify that their **published privacy policies** conform to the Privacy Principles.

Compliance with the Privacy Shield

US-based companies which will rely upon the Privacy Shield in order to transfer personal data of EU citizens from the EU to the US, but fail to comply with the Privacy Principles, will be removed from the Privacy Shield List and will be required to delete the personal data received under the EU-U.S. Privacy Shield.

In addition, **the FTC is set to give priority to referrals regarding non-compliance with the Privacy Principles in order to determine whether "unfair or deceptive" practices have been performed by the companies**.

It should be noted that under EU law regime, the transfer of personal data from the EU to US may **still also rely upon the existing alternative methods**. For example, by putting into place contractual means governing the transfer of data containing the **appropriate clauses**, which have been approved by the EC as providing adequate contractual protection or if other **certain conditions** are met (for example: if the unambiguous consent of the data subject was obtained for the cross-border transfer or if the transfer is otherwise required by law).

Next Steps

In order for the Privacy Shield to be officially accepted by the EU, an opinion by the Member States' data protection authorities (the "Article 29 Working Party") and the European Data Protection Supervisor must first be provided with regard to the Adequacy Decision's draft. This stage may give rise to difficulties and criticism raised by various European data protection authorities. In addition, an approval from a special committee, composed of representatives of Member States, must be obtained before the **final adoption of the decision by the College of Commissioners**.

In the meanwhile, we encourage all of our US-based clients who transfer personal data of European citizens to the US and wish to be certified pursuant to the new framework to take **the appropriate steps to comply with the Privacy Shield's privacy principles and practices.**

We will of course be glad to assist with any questions concerning the Privacy Shield framework and its ramifications.