July 20, 2023

New Framework for Transferring Personal Data from the EU to the United States

Client Updates

On July 10, 2023, the European Commission adopted an adequacy decision for the EU-U.S. Data Privacy Framework (the "DPF"). The adequacy decision concludes that the United States ensures an adequate level of protection – compared to that of the European Union – for personal data transferred from the EU to U.S.-based companies participating in the DPF.

What is the DPF?

The DPF provides EU individuals whose data would be transferred to participating companies in the United States with several new rights (e.g. to obtain access to their data, or obtain correction or deletion of incorrect or unlawfully handled data). In addition, it offers different redress avenues in case their data is wrongly handled.

The adoption of the DPF follows the invalidation of previous data transfer mechanisms from the EU to the U.S. ("Safe Harbor" and "Privacy Shield") by the Court of Justice of the European Union and is intended to allow data transfers from the EU to the U.S. in a manner that is compliant with the EU General Data Protection Regulation ("**GDPR**").

Essentially, companies can transfer personal data from the EU to U.S.-based companies that meet DPF requirements, without the need for additional transfer mechanisms, such as Standard Contractual Clauses ("**SCCs**").

The protection afforded under the DPF applies to any personal data transferred from the EU to organizations in the U.S. that have certified their adherence to certain principles detailed under the DPF with the Department of Commerce (the "**DoC**").

What should you do if you transfer personal data to the United States?

The DPF provides another legal alternative for transferring personal data from the EU to the United States. Accordingly, organizations should:

- review data processing agreements ("DPAs"), privacy policies and internal policies, and consider the need to update them in order to reflect the ability to rely on DPF for transfers of personal data

from the EU to the United States; and

- consider having a "Plan B" – an alternative data transfer mechanism to be used in case that DPF is invalidated by the EU courts (as was the case with the previous EU-U.S. transfer mechanisms).

We note that the DPF may also affect transfers of personal data from Israel to the United States under the Protection of Privacy Regulations (Transfer of Data to Databases Abroad), 5761-2001. However, the Israeli Privacy Protection Authority has yet to publish guidelines in that regard.

What should you do if you wish to receive personal data in the United States under the DPF?

Companies that wish to receive personal data in the United States based on DPF must meet the following (key) conditions:

- **GDPR Principles**. Adhere to data protection principles as required under the GDPR, such as purpose limitation, accuracy, lawfulness, data minimization and security.
- **Transparency.** Update the company's public privacy policy to reflect its adherence to the principles under the DPF; and provide links to (a) the DoC's website, (b) the DPF list of participating organizations ("**DPF List**"), and (c) the website of an appropriate alternative dispute settlement provider.
- **Individual rights.** Set up a mechanism to facilitate the rectification, amendment and deletion of personal data. If the data is used for direct marketing purposes – allow an opt-out right from the processing at any time.
- **Restrictions on onward transfers.** Prior to making an onward transfer of personal data, make sure that such transfer is made only for limited and specified purposes and based on an applicable contract with the third party that requires the third party to provide the same level of protection as guaranteed under the DPF principles.
- **Certification and Re-certification.** Companies that wish to rely on the DPF for EU-U.S. transfer of personal data are required to receive certification from the DoC and be added to the DPF List, re-certify on an annual basis, and make their privacy policy, which reflects their commitment to adhere to the principles of the DPF, publicly available.
- **Redress.** Provide effective and readily available independent recourse mechanisms by which complaints and disputes regarding data processing can be investigated and resolved.

The approval of the DPF by EU authorities will make it easier for companies to transfer personal data to, and store such data in, the United States. Whether you transfer personal data to the United States or receive personal data in the United States, you should take steps to prepare for using the DPF for such transfers.

Please feel free to contact us with any questions that you have on this matter.

This client update was prepared with the assistance of Melisa Poiron.

Assaf Harel, Partner Leads the Cyber & Privacy Practice and Rebecca Genis, Senior Associate.

* This update is intended to provide general and concise information only. It does not constitute a full or complete analysis of the issues discussed, and does not constitute a legal opinion or advice and therefore, should not be relied upon.

Key Contacts

Assaf Harel
Partner

Rebecca Genis Shepetovsky
Senior Associate