View this email in your browser

Invalidation of Privacy Shield – What does this mean for Israeli companies?

July 19, 2020

You should read this if:

♦ You have a Privacy Shield certification;

♦ You have committed vis-à-vis your customers to have and maintain a Privacy Shield certification;

♦ Your service providers (including, hosting companies, CRM tools, SAAS services that you use, etc.) have stored or transferred your personal data outside of the EU relying on a Privacy Shield registration; or

♦ Like us, you simply love privacy and technology.

1. In a nutshell: What happened? Why was the Privacy Shield invalidated?

♦ Despite the efforts of the European Commission in establishing the Privacy Shield framework, on July 16, 2020, the Court of Justice of the European Union issued a judgment declaring the EU-U.S. Privacy Shield as "invalid".

♦ In the CJEU's view, the domestic law of the United States on the access and use by U.S. public authorities in surveillance contexts are not equivalent to those required under EU law. In plain English, the domestic law of the United States, which provides certain surveillance rights to the US government, in not compatible with the natural rights granted to EU citizens under the European Charter of Fundamental Rights.

♦ As a result of the CJEU decision, the EU-U.S. Privacy Shield Framework is no longer a

valid mechanism to comply with EU data protection requirements (e.g. GDPR).

♦ In practical terms, this decision and its consequences are relevant when companies/businesses:

- transfer personal data from the European Union to the United States,
- store in the US personal data originating from the EU, or
- access from the US personal data originating from the EU.

It is going to take some time for businesses, privacy professionals and regulators to fully "process" the implications of the CJEU decision. In the meanwhile, we have put together some preliminary answers to various questions that have arisen so far.

2. Does this decision relieve companies with a privacy shield registration of their obligations?

♦ No. The U.S. Department of Commerce has clarified that it "will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List. Today's decision does not relieve participating organizations of their Privacy Shield obligations."

♦ Therefore, if you have a Privacy Shield registration, you should continue to comply with the Privacy Shield principles in order to decrease the risk of enforcement actions in the US. If you have not yet paid the Privacy Shield fees, you may wish to consult with us prior to doing so. In this context, you should not publish or publicly state that your company is Privacy Shield compliant, if it actually is not or the application has not been fully completed, since this can trigger enforcement actions by the FTC.

3. Will it be better to store personal data in the EU and avoid transfers of GDPR personal data from the EU to the US?

♦ While storing or keeping data in the EU is not required by EU law, being pragmatic, it will probably be safer and simpler to store personal data subject to the GDPR ("GDPR Personal Data") in the European Union (which no longer includes the UK). To the extent possible and commercially reasonable, we would also recommend companies to consider whether access from the US to GDPR Personal Data or transfers of GDPR Personal Data to the US are absolutely necessary. Note that access from the US would also be considered a "transfer" for the purposes of the GDPR.

♦ Keeping/storing GDPR personal data in the EU, avoiding access to it from the US and avoiding transfers to the US will likely result in less regulatory obligations and simpler negotiations with EU-based customers. For these reasons, we would not be surprised if some Israeli businesses decided to restructure their architecture to store GDPR personal data in the EU and access it from the EU or Israel only.

♦ Alternatively, if not in the EU, it should also be safer to store, access or transfer GDPR Personal Data to countries which have been declared as "Adequate" by the European Union. See a list of these countries here.

♦ Finally, in some cases, some businesses may want to explore the possibility of storing GDPR Personal Data fully on customers' premises or on private clouds.

4. Does this decision affect the Adequacy Decision granted by the EU Commission with respect to Israel?

♦ No. It does not. If you are storing GDPR Personal Data in Israel, or accessing it from Israel or transferring it from the EU to Israel, you can continue to do so. The CJEU decision does not change this.

5. What if I still want to transfer to the US?

♦ Generally speaking, you can. Nothing in EU law prevents you from storing or accessing personal data in the US or transferring it from the EU to the US.

♦ However, given this judgment, you will need to consider another transfer mechanism (not the Privacy Shield). Of course, this will require in many cases agreeing with your customers on the fact that their GDPR personal data will be stored in the US, accessed from the US or transferred to the US and may require you to enter into additional agreements or amendments to your current agreement with customers / service providers.

♦ In this context, we expect lengthier and more complex negotiations with EU customers when discussing these topics.

6. Does this decision affect the Standard Contractual Clauses mechanism that allows for transfers of personal data outside the EU?

♦ Partially. The CJEU held that Standard Contractual Clauses remain valid, but businesses must verify the overall context of the transfer, including whether the country of destination, access or storage offers sufficient safeguards for protecting individuals' personal data. In short, the option to rely on Standard Contractual Clauses for data transfers is possible but needs to be assessed on a case by case basis. Businesses will have to assess the level of appropriate safeguards provided by the country of destination, storage or access to determine whether SCCs are an available mechanism for them (or not).

♦ In our view, this requirement poses a HUGE challenge to many Israeli companies, since it requires them to determine whether the country of destination (the US, for example) protects personal data in the same way the EU does. In other words, they need to analyze the US privacy system as a whole and determine whether it is equivalent to the EU one. As one can imagine, this analysis will likely be very complex for small or medium sized businesses and startups, so we anticipate that more and more Israeli companies will prefer to store in, access from, and transfer GDPR Personal Data to the EU or to countries declared Adequate.

♦ One option is to continue relying on the Standard Contractual Clauses for now and to migrate to future enhanced Standard Contractual Clauses if/when as they become available. Whilst this may reduce the immediate action items, the potential consequences of this approach would remain to be seen.

7. What about the Swiss-US privacy shield?

♦ It is not affected by the CJEU decision and, therefore, continues to be valid.

8. What other immediate steps do I need to take?

At a minimum, we recommend the following actions:

⇒ To the extent you do not know or do not remember, reach out to your service providers (including, hosting companies, CRM tools, SAAS services that you use, etc.) to ask whether they rely on the privacy-shield mechanism and ask whether they have (or expect to have) another transfer mechanism in place. Larger providers will likely

have another transfer mechanism in place (such as the Standard Contractual Clauses or Binding Corporate Rules).
⇒ To the extent your customers requested and/or you committed to maintain a privacy shield certification, you may want to revisit your customer agreements and, in some cases, you may need to amend them.
⇒ To the extent that your customer agreements include specific provisions regulating the invalidation or modification of transfer mechanisms (including the Privacy Shield), you should follow and honor them.
⇒ Update your template data processing agreements and policies, including those which mentioned the privacy shield certification or regime.
⇒ Discuss with us whether you need to update your internal (intercompany) data processing agreement.

If you have questions or would like to discuss, reach out to your regular privacy contact or attorney.

Contact Information

Ignacio Gonzalez, Partner
+972-3-6103970
ignaciog@meitar.com

For additional information about our firm's Technology and Intellectual Property group, click here.

To join our newsletter click here

/