October 2015. Newsletter No. 197188

EU Court of Justice declares Data Transfers to the U.S via Safe Harbor Invalid

On October 6, 2015, the Court of Justice of the European Union (**CJEU**) declared the Safe Harbor invalid. The Safe Harbor was a method to transfer Personally Identifiable Information (PII) of EU citizens to the United States. This has relevance to Israeli companies which collect PII from customers or employees who are EU citizens, and transfer it to the US, perhaps by storing the data in the cloud on servers located in the US. We will explain the background to the Safe Harbor, the CJEU decision, the impact for Israeli companies, and what alternatives they now have.

1. What is the Safe Harbor?

The EU Data Protection Directive (95/46/EC) requires companies which collect PII relating to EU citizens to retain such data within the European Economic Area (**EEA**) unless it is being transferred to a jurisdiction which ensures 'adequate' protection for such personal data. "Adequacy" can be established in a number of ways, one of which is a declaration of approval of a particular jurisdiction's regime for protecting personal data by the European Commission.

In 2011, Israel was determined by the EU to provide adequate protection for PII, and therefore PII may be freely transferred from the EU to Israel.

In contrast, the EU does not consider that United States overall law or practice provides adequate protection for PII. Because the US is such an important trading partner for the EU, however, the EU and US worked to craft a suitable arrangement. Therefore, in a decision from July 26, 2000, the European Commission declared that the Safe Harbor scheme negotiated with

the US provided adequate protection for personal data. Individual companies can self-certify their compliance with the Safe Harbor. Since that time, over 4,500 companies, including many Israeli-headquartered companies, have adopted the scheme to justify transfers of personal data to US affiliates.

2. Snowden revelations trigger discussion

In 2013, widely publicized revelations by Edward Snowden detailed the ability of US intelligence agencies, such as the NSA (National Security Agency), to undertake mass and indiscriminate surveillance without effective judicial oversight, including accessing personal data relating to EU citizens which had been transferred, to or stored in, the US.

In light of these revelations, Austrian law student Max Schrems brought a claim against Facebook in Ireland, stating that Facebook was not protecting his PII in transferring it to Facebook's US parent. The Irish Data Protection Authority (**DPA**) stated that it was bound by the Safe Harbor and would not look into the claims. Schrems sued. The Irish High Court referred the matter to the CJEU to determine whether an individual country's DPA had the right to review whether the Safe Harbor provided adequate protection or whether it was bound by the Commission decision from 2000.

In late September 2015, the EU Advocate General, Yves Bot, concluded in an influential advisory opinion that such collection of, and access to, personal data by US intelligence agencies is inconsistent with the fundamental rights for the respect for private life and the protection of personal data as set out within the European Charter. He further advised that the assessment of adequacy should be a matter for each national Data Protection Authority to determine. Accordingly, he believed the European Commission is not empowered to restrict the ability for national DPAs to suspend transfers of personal data where a national DPA does not believe that sufficient protections are in place in the recipient jurisdiction to protect such data.

3. Key findings

In light of that opinion, the CJEU issued its decision on October 6, leveling a number of criticisms at the EU Commission’s original decision in 2000 approving the Safe Harbor. The CJEU highlighted that:

- no consideration had been given to domestic US law as to whether it provided adequate protection for data;
- the carve-out for access to data for national security, crime prevention and other purposes was too broad; and
- there was no appropriate remedy for EU citizens.

In light of the above, it concluded that the EU Commission’s adequacy decision concerning the Safe Harbor is invalid.

For companies relying on the Safe Harbor as their only basis for legitimizing the transfer of personal data from the EEA to the US, this is no longer legal. They may very well be in violation of various contracts and, if a company is the data controller responsible for the transfer, it may

very likely be in violation of European data protection laws.

4. Impact on Israeli Companies

The Advocate General's opinion had raised the possibility that the Commission's adequacy determinations—for example, that PII could be transferred to Israel as if it were in the EU—could be re-opened by each national DPA. In the end, the CJEU did not adopt this position, and limited its opinion to the situation in the United States. Therefore, Israel's adequacy determination remains unaffected.

The Safe Harbor was, however, one permitted exemption for Israeli companies to transfer PII overseas from Israel under the Transfer Regulations, 2001. ILITA, the Israeli privacy regulator, has just issued an official statement that Israeli companies may no longer rely on this exemption.

For Israeli companies, the easiest way to comply with the Transfer Regulations will most likely continue to be through a written undertaking with an overseas company which receives the PII.

5. Alternative solutions

Companies relying exclusively on the Safe Harbor as the basis for its transfer of personal data from the EU to the US will need to find another basis for the transfer as soon as possible. This of course applies also to Israeli companies which are collecting data from EU residents. Unfortunately, none of the potential solutions are without its drawbacks. The primary options are:

(a) Consent of the data subject to the transfer. In most circumstances, the consent needs to be explicit, specific and fully informed to be valid. We advise clients to keep easily retrievable, written records of the consent in case there is a challenge. Consent is likely to be more possible for customers or website users, but less so for employees, as regulators tend to discount the ability of an employee to truly make an uncoerced decision about transferring PII if "requested" by their employer.

(b) Standard Contractual Clauses. The European Commission adopted several standard form agreements between transferors and transferees of data to ensure adequate protection of the transferred PII. While this simplifies the process, the parties need to agree on which form to use, including, for example, which party is the "controller" for EU data protection purposes. As this party is the one with primary liability for privacy breaches, parties often do not decide this issue up front. Furthermore, there are formalities which vary from country to country, such as whether the Model Contract needs to be filed with the DPA, or whether it needs DPA approval.

(c) Binding Corporate Rules. This permits transfers among affiliated companies. Each BCR need to be approved by one of the national DPAs. This is a lengthy process (potentially 18 months or more), and a very expensive one at that. So while this is a longer term option for some companies, it won’t be realistic for most.

6. What lies ahead?

As noted above, none of the potential solutions is perfect or applicable to every situation.

Consent is likely to be the best of the alternatives. Clients should review their privacy policies to make sure they are providing specific, detailed information of where the PII of EU citizens is being transferred, and should consider "check the box" approval for those transfers.

Consent is preferable because BCRs and Standard Clauses are subject to the same legal flaws that the CJEU noted apply to the Safe Harbor: a US recipient company could still receive a subpoena from the NSA or other US government agency to disclose the personal data of EU residents. Nevertheless, the EU's Data Privacy Working Group has just issued a statement that these methods will be acceptable for the time being.

The EU and US are already discussing a replacement for the Safe Harbor, with an informal deadline set by the EU's Working Group of January, 2016. In the meantime, rather than relying on a "one-size fits all" framework in the form of Safe Harbor, companies will need to review data flows in specific situations on a case-by-case basis.

This memorandum is provided solely for informational and educational purposes and should not be construed as a legal advice.
If you have any questions regarding the subject of this article, please contact the following attorneys or call your regular Meitar contact:
David Mirchin, Adv.; Tel. +972-3-6103199; Fax:+972-3-6103667; dmirchin@meitar.com