

אפריל 26, 2026

## **Cross-Border Data Transfer Agreements – the Position of the Israeli Privacy Protection Authority**

### **Client Updates**

On April 13th, 2026, the Israeli Privacy Protection Authority (the "**Authority**") published a [Position Paper](#) (link in Hebrew) on the interpretation of Section 2(4) of the Protection of Privacy Regulations (Transfer of Data to Databases Abroad), 5761-2001 (the "**Position Paper**" and the "**Regulations**", respectively). In the Position Paper, the Authority expressed an expansive view on both the extraterritorial application of Israeli privacy protection legislation and the content of data transfer agreements.

### **Background**

The Regulations prohibit the transfer of personal data from an Israeli database outside of Israel's borders, except when one or more of the (alternative) conditions outlined under Section 2 of the Regulations are met. One such condition, specified under Section 2(4), permits the transfer if "the data is transferred to a person bound by an agreement with the owner of the database from which the data is transferred, to comply with the conditions for the ownership and use of the data applying to a database in Israel, with necessary modifications". The Position Paper focuses on this condition, particularly on the phrase "with necessary modifications".

### **Extraterritorial Application of the Privacy Protection Law**

The Position Paper contains an expression of the Authority's view on the extraterritorial application of the Privacy Protection Law, 5741-1981 and the regulations enacted thereunder (collectively, the "**Privacy Protection Law**"). In the Position Paper, the Authority notes that there may be databases abroad that will be subject to all the provisions of the Privacy Protection Law, even if their owners are not registered in Israel.

Furthermore, the Authority clarifies that in cases involving the transfer of data between a database owner in Israel and a holder of a database (the equivalent of a 'data processor') located outside Israel, the holder is required to comply with the material obligations of the Privacy Protection Law. The Authority's position implies, for instance, that an American company offering cloud storage services to Israeli companies is directly subject to the Privacy Protection Law, even if it has no physical presence in Israel.

### **Content of the Data Transfer Agreement**

In the Position Paper, the Authority clarifies that "the conditions for the ownership and use of the data applying to a database in Israel" are not limited to the Privacy Protection Law but include all legislation in

the areas of privacy and data protection. The Authority also clarifies its position that personal or organizational circumstances of the data recipient that do not allow compliance with these laws do not constitute a “necessary modification.” Rather, this standard should be examined objectively. For example, non-compliance with the database registration requirement or the obligation to notify the Authority of a database under the Privacy Protection Law will be considered a necessary modification if such obligations do not exist in the country to which the data is transferred.

Regarding the components of the data transfer agreement, the Authority clarifies that the agreement must include the data recipient’s commitment to fulfill obligations towards the data subject that are identical to, or at least materially similar in substance to, those set out in the Privacy Protection Law. This includes, for example, the prohibition of using the data for purposes other than those for which it was provided, granting the right of access, correction, and deletion to data subjects, and maintaining confidentiality concerning data received by an individual in connection with his/her position.

Additionally, the agreement must address aspects of data security. In that context, it is possible to include a commitment by the data recipient to fulfill the material obligations stipulated in the Privacy Protection Regulations (Data Security), 5777-2017 (the “**Data Security Regulations**”). Alternatively, the agreement can include a declaration that the data recipient has obtained ISO/IEC 27001 certification and complies with it, as well as with the requirements stipulated under the [Guideline of the Database Registrar No. 3/2018](#) (link in Hebrew) regarding the application of the Data Security Regulations in the case of such certification.

If the database in Israel also contains information transferred from the European Economic Area, the data recipient will also be required to comply with the material provisions stipulated under the Privacy Protection Regulations (Instructions Regarding Data Transfers from the European Economic Area to Israel), 5783-2023 (for more information on those regulations, [see here](#)).

### **What are companies required to do?**

In light of the Opinion, companies are required to review their agreements governing the transfer of personal data abroad (for example, SaaS service agreements that involve the processing of personal data). Even where such agreements do not contain an explicit undertaking to comply with the Israeli Privacy Protection Law, they may nonetheless be regarded as meeting the requirements of the Regulations. This may be the case, for example, where personal data is transferred to jurisdictions within the European Union, or where the agreement implements provisions that are substantially similar to those applicable under Israeli law.

Please do not hesitate to contact us with any questions and/or advice regarding the above.

---

This update is intended to provide general and concise information only. It does not constitute a full or complete analysis, legal opinion, or legal advice and should not be relied upon as such.

## Key Contacts



**Assaf Harel**  
Partner



**Rebecca Genis Shepetovsky**  
Partner