

January 2, 2024

PPA Publishes Guidance on IoT Products and Smart Homes

Client Updates

The Israeli Privacy Protection Authority (the "PPA") recently [published](#) a guidance paper on privacy aspects of Internet of Things (IoT) products and smart homes (the "Guidance").

This Guidance follows a [draft guidance paper](#) issued in August 2022 by the Commissioner of the Consumer Protection and Fair Trade Authority together with the Cyber Directorate.

IoT devices collect significant amounts of personal information, including sensitive personal information. Therefore companies that supply IoT products and services are subject to the provisions of the Protection of Privacy Law, 1981 and the regulations promulgated thereunder, including the Protection of Privacy Regulations (Data Security), 2017 (the "**Data Security Regulations**"). Below is a summary of key guidelines included in the Guidance for companies offering IoT or smart home products or services:

- **Data Protection.** There are significant concerns surrounding the potential misuse of IoT products and the threats to cyber security and privacy that companies should be aware of. In order to mitigate these risks, the Guidance suggests implementing various procedures and mechanisms, including the following:

o Taking appropriate security and data protection measures, as required under the Data Security Regulations;

o Implementation of Privacy by Design and by Privacy by Default principles while developing the IoT product – meaning, building the system in a manner that would provide optimal protection for the privacy of data subjects and would allow the collection and processing of the minimal personal information necessary to achieve the purpose for which it was collected.

- **Notice and Informed Consent.** Companies must ensure they provide adequate notices and obtain informed consent from users and potential users of IoT devices. Accordingly, companies should:

o provide a clear and easily understandable notice to users and potential users regarding the collection of their personal information. The notice shall indicate whether that person is legally obligated to provide that information (or whether its provision is subject to his own free will and consent), the purpose for which the information is requested and to whom it will be disclosed and for which purposes. The scope and content of

the notice varies depending on the context and the type of information collected;

oensure that any personal information collected through IoT devices is used solely for the purposes for which the consent was obtained;

oensure that the collection and use of personal information for AI-based decision-making systems fully conforms with the legal standards for notification, despite the intrinsic difficulty of allowing full transparency as to how such systems reach decisions; and

oallow individuals to revoke their consent for the collection and utilization of their personal information in a simple manner.

- **Data Minimization, Deletion and the Right to Access Information.** To address privacy concerns associated with the potential gathering of excessive data through IoT devices, companies should conduct annual reviews of their data collection practices. Additionally, given the possibility that some of the collected information may be inaccurate or outdated, companies should honor users' requests to delete their personal information, especially in the case of minors.

The PPA also provides guidelines for users of IoT products. It emphasizes the importance of informing household members and guests about the use of IoT products that may record or monitor them, and avoiding placing such products in sensitive areas like bedrooms or bathrooms. Users are advised to use strong passwords and regularly change them, update their systems as recommended by the manufacturer, limit the information collected and transferred to the manufacturer, and avoid connecting the systems to social media accounts. Additionally, the PPA highlights certain features that users should consider when purchasing IoT products, such as cyber security features.

As the IoT market expands, it becomes essential for businesses and organizations operating within the IoT ecosystem to implement privacy and data protection requirements and standards and to remain vigilant in their adherence to them.

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.

This client update is designed to provide general information only, is not a full or complete analysis of the matters presented, and may not be relied upon as legal advice.

Key Contacts



Assaf Harel
Partner



Rebecca Genis Shepetovsky
Senior Associate