

March 8, 2026

Israeli Privacy Protection Authority Publishes New Guidance on Obtaining Consent

Client Updates

On February 25, 2026, the Israeli Privacy Protection Authority (the "**Authority**") published a comprehensive [position paper](#) (link in Hebrew) on the implementation of the the principle of consent under the Privacy Protection Law 5741-1981 (the "**Position Paper**," and the "**Law**," respectively). In the Position Paper, the Authority seeks to clarify its position regarding the manner in which valid consent should be obtained in the digital age, and to outline the conditions and criteria by which the validity of such consent will be assessed.

The Position Paper reflects the legal interpretation that will guide the Authority in exercising its supervisory and enforcement powers, including its authority to impose monetary sanctions. Below is our summary of the key points and their practical implications for organizations.

Elements of Consent: Informed and Freely Given

Under the Law, consent to a violation of privacy must be informed, meaning consent given when the individual is aware of the purposes of data collection, how the information will be used, and the implications of their decision. According to the Authority, compliance with the formal notice requirement under Section 11 of the Law constitutes only a minimum standard, and **the validity of consent depends on the information actually provided** and how it is presented. Accordingly, broad or vague wording - such as using phrases like "including" in relation to the types of data collected or the purposes of use - may not meet this requirement. Similarly, where information may be transferred to additional parties, the nature of such use should be clarified, for example, by identifying the types of entities to which the information may be transferred (e.g., "advertising companies").

In addition, consent must be given freely. It may be considered not freely given where it is provided in circumstances of dependency or where no real alternative exists. For example, in employment relationships, when essential services are provided, or where a service is conditioned on consent to collect information not necessary for providing the service. In such cases, the burden may shift to the party seeking consent to demonstrate that it was given voluntarily. The Authority suggests mitigating this risk by offering **reasonable alternatives, avoiding conditioning services** for the collection of non-essential information, and preferring **explicit and active consent mechanisms**.

Secondary Uses of Information and Increased Disclosure Requirements

Where information is used for purposes that exceed the purpose for which it was originally collected, or where circumstances increase the risk of violation of privacy - such as power imbalances between the parties, the provision of essential services (e.g., healthcare or transportation), or the use of new technologies - organizations may be required to provide a higher level of disclosure and accessibility. In such cases, it is not sufficient to rely on general language in terms of use or privacy policies; instead, the information relevant to the individual's decision should be presented clearly and prominently, and in some cases, separate consent should be obtained, for example, through a dedicated notice during the registration process.

Obtaining Consent: Active and Passive Mechanisms

Under the Law, consent to a violation of privacy may be given explicitly (for example, by signing a contract or actively clicking an "I agree" button to accept terms of use) or implied from conduct. For instance, according to the Authority, continued browsing of a website after the user has been presented with the information required to obtain informed consent to the collection of their data will generally be considered implied consent to the collection and use of that information. However, such consent will be valid only where there is a reasonable connection between the purposes of data collection and use and the nature of the service. By contrast, where personal data is used for purposes not necessary for providing the service, or for purposes that materially differ from the purpose of the engagement, **explicit and active consent (Opt-in)** should be preferred over implied or passive consent (Opt-out).

Withdrawal of Consent

The Authority recognizes that in certain cases, consent to a violation of privacy may also include the possibility of withdrawing that consent and requesting that the use of personal information be discontinued, even though this right is not expressly anchored in the Law. Accordingly, when an individual seeks to withdraw their consent - or when their conduct indicates such intent - the Authority recommends examining whether the consent remains valid and considering requests to cease the use of the information. This is particularly relevant if the consent was given for a specific purpose or limited period.

Practical Recommendations - How Should Consent for Data Collection and Use Be Obtained?

Based on the Position Paper, below we outline several key recommendations for obtaining consent:

- **Clear and prominent presentation of the consent request:** The key aspects of data collection and use should be clearly highlighted, particularly where the use may exceed the user's reasonable expectations.

- **Accessible and simple consent process:** Organizations should use clear and user-friendly tools to present the information required for informed consent- for example, pop-up notices, banners, and interactive tools - and avoid misleading design practices or "dark patterns" that may obscure the meaning of the consent.
- **Increased transparency in complex situations:** Where new technologies are used that may affect privacy, or where there are power imbalances between the parties, the relevant information should be presented clearly and prominently.
- **Renewed consent where purposes change:** If the purposes for which the information is used change, additional consent should be obtained, either explicitly or in another manner demonstrating that users are aware of the change.
- **Providing alternatives:** In situations where consent may be considered "suspicious," reasonable alternatives should be offered, services should not be conditioned on the collection of unnecessary information, and users should be allowed to choose which types of data are collected and for what purposes.
- **Documenting consent:** As consent may need to be demonstrated, organizations should retain documentation of consent, particularly where it is obtained orally or by phone (for example, through call recordings), and especially where sensitive information is collected or power imbalances exist.
- **Preference for Opt-in mechanisms:** Where the use of information is not necessary for providing the service (for example, advertising based on profiling), separate active consent should be obtained.
- **Possibility of withdrawing consent:** Organizations should consider implementing mechanisms that allow users to withdraw their consent and discontinue the use of their information and should examine such requests on a case-by-case basis.

The Position Paper outlines the Authority's position regarding how consent for the use of personal information should be obtained, and it is expected to guide the Authority's approach in enforcement proceedings. This position may also be considered by courts when adjudicating claims relating to violations of privacy. In light of this, it is important that each organization review how it collects consent in light of the Authority's position, and take steps to mitigate the risks of claims and enforcement actions in this context.

Please feel free to reach out to us should you have any questions.

*This update was prepared with the assistance of Rona Tal.

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