SmartSuite

Framework / Privacy / Global Privacy Regulations

Protection of Privacy Law, 5741-1981 (Israel)

Israel's Protection of Privacy Law, 5741-1981, adopted by the Knesset and enforced by the Privacy Protection Authority, as amended by Amendment No. 13 (in force August 14, 2025).



What it is

The Protection of Privacy Law, 5741-1981 is Israel's statute on privacy and personal data: Chapter A makes infringement of privacy a civil wrong and a criminal offense, and Chapter B regulates databases of personal data. The Knesset adopted it on March 11, 1981, and the Privacy Protection Authority (PPA), a unit of the Ministry of Justice, enforces it. Amendment No. 13, approved by the Knesset on August 5, 2024 and in force since August 14, 2025, is described by the PPA as the most comprehensive reform of Israeli privacy law since the original statute.

According to the PPA's guide, Amendment No. 13 updated the Law's definitions (section 3 now defines personal data and twelve categories of data of special sensitivity), replaced the broad duty to register databases with registration for data-broker and public-body databases and notification for very large special-sensitivity databases (section 8A), and added a duty to appoint a data protection officer (sections 17B1 to 17B3). It also introduced monetary sanctions of up to millions of shekels per violation (Chapter D3), new criminal offenses, wider court power to award damages without proof of harm and the end of the shortened limitation period for civil claims.

At a glance

PUBLISHER The Knesset (enforced by the Privacy Protection Authority, Ministry of Justice)	TYPE Regulation	VERSION Protection of Privacy Law, 5741-1981, as amended by Amendment No. 13 (5784-2024)
EFFECTIVE August 14, 2025 (Amendment No. 13); law adopted March 11, 1981	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION Israel	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: gov.il/BlobFolder/legalinfo/legislation/en/Protection-of-Privacy-Law57411981unofficialtranslatioup.pdf

Why it matters

- **Defined terms that set the scope** Section 3 defines personal data, data of special sensitivity, database, processing, controller and processor.
- **Registration only where it matters** Section 8A requires registration for data-broker databases above 10,000 individuals and for public bodies, and notification above 100,000 individuals with special-sensitivity data.
- **Named security duties** Section 17 makes controller and processor each responsible for data security, and the 2017 Regulations set the measures by security level.
- **A privacy officer with standing** Section 17B1 requires a data protection officer in public bodies, data brokers and large-scale monitoring or special-sensitivity processors, reporting to the general manager (17B2(c)).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Israel PPL 5741-1981

Database Inventory and Registration Status

Keep each database with its purpose, number of individuals and special-sensitivity data in Privacy Management, and record whether section 8A requires registration or notification.

Access and Rectification Requests

Log requests under sections 13 and 14 in Privacy Management with owner, response and outcome.

Security Level Measures

Track the Data Security Regulations measures that apply to each database's security level in Cyber & IT Risk, with evidence.

Security Incident Handling

Manage security incidents in IT Service Management (ITSM) and attach the immediate notice to the Registrar required after a severe incident (regulation 11(d)).

Processor and Provider Oversight

Assess and monitor processors and external service providers that reach a database in Third Party Risk Management (regulation 15).

Data Security Audit Program

Schedule the audits of regulation 16 in Internal Audit Management and track findings to closure.

Common framework mappings

APEC PF | CCPA/CPRA | GDPR | HIPAA | ISO 27001:2022 | ISO 27701 | NIST Privacy Framework v1.0 | OECD Privacy Guidelines

Official resources

Israel Protection of Privacy Law — 5741-1981

Defines legal requirements for data protection and privacy in Israel, enforced by the Privacy Protection Authority.

gov.il/en/departments/privacy_protection_authority

Privacy Protection Regulations

Outlines regulations related to data security measures under the Israel Protection of Privacy Law.

gov.il/en/service/privacy_protection_regulations

Guidelines for Data Controllers

Provides guidance for data controllers on complying with the Privacy Protection Law requirements.

gov.il/en/service/data_controller_guidelines

Breach Notification Guidelines

The Privacy Protection Authority's guidance on reporting serious security incidents under the Protection of Privacy Law.

gov.il/en/service/breach_notification_guidelines

Frequently asked questions

Who must appoint a data protection officer under the Law?

Section 17B1(a) requires an officer for a public body, for a controller whose main purpose is collecting personal data to give to others for consideration with data on more than 10,000 individuals, for controllers or processors whose core activity involves regular and systematic monitoring of individuals on a significant scale, and for those whose main activity is processing special-sensitivity data on a significant scale, such as banks, insurers, general hospitals and health maintenance organizations. The officer may be a non-employee, reports to the general manager and must not hold a role that creates a conflict of interest (17B2(c), 17B3).

When must a database be registered or notified?

Section 8A(a) requires registration of a database held by a public body, unless it holds only employee data, and of a database whose main purpose is collecting personal data to give to another for consideration, including direct mailing, with data on more than 10,000 individuals. Under 8A(b), a controller of any other database that holds special-sensitivity data on more than 100,000 individuals must notify the Authority within 30 days, with the officer's details and a database definitions document.

 © 2026 SmartSuite Inc. All rights reserved.

What must a controller do after a security breach?

The Data Security Regulations, 5777-2017, require the controller to document security incidents (regulation 11) and, after a severe security incident, to notify the Registrar immediately and report the measures taken (11(d)). A severe incident is defined by security level: at the high level, use of data without authorization or damage to integrity; at the medium level, the same affecting a substantial part of the database. The Law itself has no separate breach-notification section.

What are the sanctions for violating the Law?

The Head of the Authority can impose monetary sanctions under section 23KF, for example NIS 150,000 for processing personal data in a database that is subject to registration but unregistered, doubled for databases on 1,000,000 individuals or more, and fixed amounts by security level for Regulations violations. Courts can award exemplary damages up to NIS 10,000 without proof of loss for specified database violations (15A) and statutory damages up to NIS 50,000 for a privacy infringement, doubled if the intent was to harm (29A). Appeals against sanctions are filed within 45 days.

When did Amendment No. 13 take effect, and is Israel still adequate for EU transfers?

The Knesset approved Amendment No. 13 on August 5, 2024, and it took effect on August 14, 2025, according to the PPA. The European Commission adopted Decision 2011/61/EU on Israeli adequacy on January 31, 2011, and its January 15, 2024 review concluded that Israel continues to provide an adequate level of protection. The Commission also recommended enshrining protections now found in sub-legislative rules and case law in legislation.

License included / downloadable: Yes The Law is an Israeli statute. The Privacy Protection Authority publishes an unofficial English translation updated after Amendment No. 13 on gov.il, and the platform links to it.

Full framework page and mappings: smartsuite.com/frameworks/israel-protection-of-privacy-law-5741-1981

© 2026 SmartSuite Inc. All rights reserved.