Amendment 13 of Israel's Privacy Protection Law: A game-changer for data protection compliance?

Received (in revised form): 21st April, 2025

Dalit Ben-Israel
Partner and Chair of IT & Data Protection Practice and Co-Chair of AI, Naschitz Brandes Amir, Israel

Dalit Ben-Israel is a Partner and Chair of Naschitz Brandes Amir's IT, privacy and data protection practice and co-chair of the artificial intelligence (AI) practice. She specialises in the fields of computers, information technology, cyber, privacy and data protection law. Dalit has extensive experience in data protection regulatory compliance including Israeli law and General Data Protection Regulation (GDPR), providing assistance to clients in regulator audits, enforcement actions, drafting and negotiating cloud and data processing agreements, web and application terms of use, privacy notices, drafting and reviewing data security policies and procedures, handling international data breach cases and security incidents, spam issues and counselling insurance companies on cyber insurance coverage. Dalit renders services in these areas to diverse clients, *inter alia*, in the financial, insurance, transport and health sectors. She is also a frequent speaker and writer on various AI, privacy and cyber-related topics and offers training on Israeli privacy and European data privacy legislation compliance issues. Dalit is a member of the International Association of Privacy Professionals (IAPP), and during 2019–20 served as the co-chair for the Israeli KnowlegeNet chapter of IAPP. She is currently the chapter chair of the Tel-Aviv OneTrust PrivacyConnect and the Women in AI Governance for Israel.

Naschitz Brandes Amir, 5 Tuval Street, Tel-Aviv 6789717, Israel
E-mail: dbenisrael@nblaw.com

Abstract This paper explores Amendment 13 of Israel's Privacy Protection Law (PPL) and its potential impact on data protection in Israel. It examines how the amendment aligns Israeli privacy law with global privacy standards, particularly the General Data Protection Regulation (GDPR), and provides a framework for imposing new administrative fines. The paper discusses the broader implications of these changes for businesses and government entities, as well as the compliance challenges they present. Key reforms include stronger enforcement mechanisms, new criminal offences, and the introduction of the obligation to appoint data protection officers. The analysis includes actionable recommendations for policy makers, businesses and legal practitioners in adapting to these significant regulatory shifts. This paper is also included in **The Business & Management Collection** which can be accessed at https://hstalks.com/business/

KEYWORDS: Israel, Privacy Protection Law, information security, GDPR, data protection, privacy, controller, processor, consent, administrative fines, DPO

DOI: 10.69554/PEQP3161

BACKGROUND

The Israeli Privacy Protection Law, 5741-1981 (PPL) is the law governing data protection in Israel. It has not been substantially updated for many years, despite several unsuccessful attempts. Therefore, the Ministry of Justice has decided to amend it in several phases. The first phase, known as Amendment 13, was adopted by the Israeli Parliament in August 2024, after 20 lengthy

sessions at the Constitution, Law and Justice Committee.[1] Amendment 13 becomes effective on 14th August, 2025.[2]

The background to Amendment 13 primarily stemmed from the need to adapt to modern data protection laws, in particular the European Union (EU) General Data Protection Regulation (GDPR), and align Israeli law to similar terminology and principles — for example, the expansion of the definition of 'personal information' and the new definition of 'processing'. In this paper, all references to new provisions refer to the revised terminology, which will be further discussed in the first section.

The need to adapt to modern data protection laws also influenced changes made to certain key principles established in the PPL. Consent is one fundamental principle, as it serves as the primary legal basis for processing personal information, the sole alternative being legal obligation. To lawfully collect and process personal information based on consent, prior notice, including the relevant information required to formulate consent, must be provided.[3] This requirement was enhanced by the Amendment. Purpose limitation is another fundamental principle which was revised. In addition, the PPL was formed around the term 'database'[4] as a central component of the obligations of data protection and not the term 'personal information', as more commonly used in other data protection laws,[5] as well as established unique requirements such as database registration.[6] This concept of a legal database remains the cornerstone of Israeli data protection law even after the Amendment, but certain revisions were introduced towards a more modern approach. Revisions regarding these principles will be presented in detail in the second section.

Another reason leading to the Amendment was the clear indication in the decision of the EU Commission of January 2024 (the EU decision), reaffirming its recognition of the adequate level of data protection of the State of Israel to enshrine in legislation the protections developed at the sub-legislative level, specifically referring to Amendment 13:

> While the developments in terms of guidance, interpretation and case law … contribute to an increased level of data protection in Israel, codifying these developments in legislation would be important to enhance legal certainty and solidify the protection for Personal Information. The ongoing debate on a draft bill that would amend the PPL seems to offer such an opportunity.[7]

A further key driver was the need to improve meaningful sanctions for violations of certain regulations (secondary legislation) promulgated under the PPL, which the Privacy Protection Authority (PPA) did not have efficient means to enforce — specifically, the Protection of Privacy Regulations (Data Security), 5777-2017 (Data Security Regulations), which include detailed information security requirements for controllers and processors.[8] Changes regarding new enforcement abilities in response to different privacy violations, including sanctions, will be discussed in the third section of the paper.

There are limited data subject rights under the Israeli law in comparison to the GDPR.[9] The next phase of amendments to the PPL is expected to cover the more complex matters of legal bases of processing, extending the very limited data subject rights such as adding a right of erasure, adding statutory data minimisation requirements and more.[10] A draft bill of the additional amendment is yet to be revisited following changes required due to Amendment 13 and is expected to be published for public consultation thereafter.

AMENDED TERMINOLOGY

The PPL consists of two main chapters addressing different aspects of privacy protection. The first chapter addresses

traditional privacy, prohibiting violation of privacy of an individual without their consent and listing acts that are deemed as a violation of privacy:[11] ie use of a name or photograph of an individual for profit; publishing a photograph that can humiliate an individual; violating confidentiality obligations regarding the 'personal affairs' of an individual; use of information on the 'personal affairs' of an individual or providing such information to another person contrary to the purpose for which it was originally provided. The second chapter governs the regulation legal 'databases', which are now more accurately defined in Amendment 13 as a collection of personal information processed in digitised means, except: (1) if the collection is not for business purposes; or (2) if the collection includes only names, addresses and contact details of 100,000 individuals or fewer, provided the controller does not have another collection that includes additional personal information about the same data subjects.[12] The Amendment focuses mainly on the chapter governing databases, with a few changes in other provisions of the PPL.

Amended definitions mostly aligned with GDPR

The Amendment simplified and modernised some of the fundamental definitions of the PPL, mostly aligning them with the GDPR. While in some cases, the Amendment codified already enhanced and expanded meaning given to existing terms in case law and PPA guidelines,[13] some definitions differ in material aspects from the former definitions, requiring reassessing data protection practices in Israel in order to ensure compliance with the revised framework.

The first fundamental definition amended is 'personal information', which previously included a specific list of data items.[14] It is now a broad definition, including any data relating to an identified person or a person who can be identified, directly or indirectly, by reasonable efforts. The definition also lists examples of identifiable details, such as identification (ID) numbers, biometric identifiers or online identifiers.[15] While this new definition is very similar to the GDPR, the GDPR definition is broader, as it does not require the person to be identifiable by 'reasonable' efforts.[16]

Alongside the definition of personal information, the former, narrow, definition of 'sensitive information'[17] was replaced by a completely new definition of 'especially sensitive information'.[18] This definition includes a list of several types of personal information that are typically deemed sensitive, such as medical data, genetic data, biometric data, sexual orientation, racial or ethnic origin, criminal records, political opinions, religious beliefs and more. These types are comparable to the 'special categories of personal data' defined in the GDPR,[19] although there is no exact alignment, and the Israeli new definition includes a broader list.

These new definitions are complemented by a more extensive definition of 'use', which now explicitly includes new forms of use of personal information, extending to a wider array of activities.[20] The PPL formerly defined 'use' solely as disclosure, transfer and delivery.[21] The Amendment adds a modern definition of 'processing' or 'use' (which former definition was kept as an alternative) that is more extensive: any action performed on personal information, including receipt, collection, storage, copying, viewing, disclosure, revealing, transfer, delivery or granting access to personal information. The additional acts of erasure or destruction of personal information that are deemed processing under the GDPR[22] were intentionally not included in the definition.

Finally, definitions regarding the roles for determining the data processing activities and executing them were updated to reflect current standards and practices. The term 'controller of a database', previously undefined in the PPL, now has its own

definition as the entity that determines the purposes of processing.[23] The shift from the GDPR,[24] by not including reference to 'means of processing' in the definition, is intentional and reflects the intention for controllers to remain responsible for the database even if the means are determined by a processor. The example given during the hearings on the draft bill for this deviation from the GDPR was cloud computing or Software-as-a-Service (SaaS) services, where in many cases the provider (the processor) determines the means of processing. In addition, the concept of joint controllers was introduced for the first time.

Regarding the role of processor, the PPL uses a unique term and names it a 'holder of a database'. The former PPL definition referred to a holder as one who has permanent access to the database and is entitled to use it.[25] This definition raised many questions about the meaning of 'permanent access' and whether it included certain data processing operations, such as hosting (which does not necessarily entail access to personal information)[26] or remote access through one-time passwords. The new definition includes any external entity (to exclude employees of the controller) that processes personal information for the controller.[27]

Some implications of the amended definitions

The revised definition of personal information will require amendments of privacy notices and other acts of compliance, by expanding the scope of compliance and obligations under the PPL and regulations to a wider range of types of personal information. This is the first time that online identifiers, such as Internet protocol (IP) addresses, are formally deemed personal information under Israeli law, affecting the manner in which this type of information should be addressed in privacy and cookie policies and the way cookie banners are structured.

The new PPL definition of 'especially sensitive information' introduces some ambiguity, since it is not identical to the definition of sensitive information included in the Data Security Regulations (based on which a medium level of security of a database is determined).[28] This discrepancy is significant because the new PPL definition will form the basis for determining the amount of administrative fines imposed by the Amendment for breach of the Data Security Regulations. Therefore, an amendment is required to align the Data Security Regulations to the amended PPL in this and other areas to ensure consistency. It should be noted that until the Data Security Regulations are amended, the material obligations will continue to be based on the definitions in the Data Security Regulations. Administrative fines, however, will be imposed based on the definitions of Amendment 13.[29] In addition, the classification of personal information as especially sensitive information may have an impact on the imposition of additional obligations under the PPL, such as appointment of data protection officer (DPO), notice obligation to the PPA of databases and security level classification.

The amended definitions of processor and processing will encompass many more suppliers and service providers, which will be deemed as holders and, therefore, directly obligated to comply with many of the provisions of the PPL and with almost all the provisions of the Data Security Regulations that apply similarly to holders and controllers. Due to the expansion of the term 'holder', organisations need to review the list of third parties with whom data processing agreements have been signed and would probably need to enter into such agreements with additional suppliers and third parties. The term 'external factor' used in Regulation 15 of the Data Security Regulations as the entity with whom a controller needs to sign a data processing agreement (DPA), which has been clarified

in the past by the PPA to be broader than a holder,[30] remains unclear after the expansion of the term 'holder', and it is expected that this provision of the Data Security Regulations will also be amended and clarified in line with the amended PPL.

In addition to the effects described above, the primary impact of all the new definitions is the imposition of administrative fines, based on the broader definitions included in Amendment 13.

AMENDED PRINCIPLES AND OBLIGATIONS

Having clarified the updated definitions, this section examines the key principles and obligations that were amended and how they affect compliance.

Enhanced notice requirements

Consent under the PPL must be informed in order to ensure it is given based on true choice. Section 11 of the PPL requires that notification be provided to individuals when personal information is collected from them, which is typically delivered in the form of a privacy policy or consent form.[31] The notification may be provided prior to obtaining consent or simultaneously therewith, since other than legal obligation, consent is the only legal basis under Israeli privacy law and consent needs to be informed. The notification obligation when personal information (as previously defined) was collected from a data subject, prior to the Amendment, required the disclosure of the following: whether the provision of personal information is a legal obligation or based on the free will of the data subject, the type of personal information collected, the purposes of its use, the third parties with whom the personal information would be shared and the purposes thereof. Section 11 was amended and now includes additional requirements: detailing the consequences of lack of consent, the name and contact information of the controller and referencing data subject rights (access, rectification and deletion in specific cases). These new requirements must be addressed in privacy policies and notices.

The Amendment also introduced a new obligation to appoint a DPO in certain cases and stipulates that the manner of communication with the DPO should be published in an accessible and clear manner.[32] In practical terms, this means that these details would most likely appear in the privacy policy or other notifications.

Purpose limitation principle

The purpose limitation principle in the PPL includes two provisions, originally referring to the previous definitions: (1) a prohibition to use information about 'personal affairs' of a person (narrower term than personal information) for purposes other than those for which it was provided; and (2) prohibition to use personal information in a database for purposes other than those for which the database was registered.[33] Since Amendment 13 cancelled the unique obligation under the PPL to register databases with the PPA for most databases (except public entities and data brokers processing personal information of more than 10,000 data subjects), a new purpose limitation principle was established regarding personal information, complementing the existing prohibition on using information about 'personal affairs' of a person other than for the original purpose.

The new principle prohibits the processing of personal information for a purpose that is contrary to the lawfully compliant purposes established for the relevant database to which the personal information pertains.[34] Lawfully compliant purposes may include, for example, any purposes set forth in a privacy notice or in the internal Database Definitions Document[35] (internal mapping document similar to a GDPR Records of Processing) or for a processor — included in the DPA with the controller. It should be noted that 'processing' for this purpose does not include

storing personal information randomly and in good faith.[36] Organisations will need to review their policies and procedures in light of this updated principle to ensure compliance with the law; it is therefore advisable to list the purposes of processing both in privacy policies and in Database Definitions Documents in a more detailed manner.

New requirements for lawful processing

The Amendment added a prohibition to process personal information without authorisation from the controller, or in excess of the scope of authorisation from the controller, except if the violation is insignificant under the circumstances.[37] This provision will most probably cause processors to try and broaden the permitted processing activities in their agreements with controllers in order to avoid a breach (ie any lawful purposes required to perform the services), and controllers, on the other hand, will tend to limit those purposes.

The Amendment also added that a controller shall not process, or permit processing of, personal information collected, created or received in violation of the PPL or any other law governing data processing. Notwithstanding, the controller will be exempt from liability if the personal information was provided by another person acting unlawfully, under the conditions that the controller did not have knowledge about it and was not expected to have such knowledge, before the processing was carried out.[38] Processors will most likely request to add to data processing agreements representations by controllers that the personal information was collected and received without violation of any applicable law.

It should be noted that breach of these new provisions, including the purpose limitation principle, entails administrative fines and may be subject to a court order to stop processing activities and even to delete personal information.[39] Processing personal information in a database without authorisation from the controller is also a criminal offence, punishable by up to three years' imprisonment.[40]

Database registration

In addition to the changes in definitions outlined above regarding databases, the Amendment also introduced a shift by minimising the requirements for database registration, thus placing greater emphasis on material compliance and internal policies and documentation regarding databases. The unique obligation to register databases, which previously applied to all databases, was not enforced *per se* by the PPA, focusing enforcement efforts on material compliance. This requirement was cancelled through the Amendment, except for public entities and data brokers with 10,000 data subjects or more.[41]

According to the amended PPL, some databases are subject to a milder notification obligation to the PPA, ie databases of especially sensitive data of 100,000 data subjects or more.[42] The remainder of the databases are exempt from registration or notification, but not from compliance with all other provisions of the PPL and regulations. While this change has the potential to reduce administrative burdens, especially for smaller businesses, organisations should evaluate whether the amended registration or the new notification obligations apply to their databases and ensure compliance.

Key roles in data protection under the PPL

The statutory obligation to appoint an information security officer is not a new provision under the PPL;[43] however, the threshold for such appointment was amended to apply to controllers or processors of at least five registered or notifiable databases (see above). Previously, this requirement

applied only to processors of five databases that required registration. Information security officers also need to be appointed by certain specific entities (this has not been changed): banks, insurers, public entities and credit scoring or rating providers.[44]

Under the Data Security Regulations, information security officers cannot perform an additional role within the organisation that may put them at risk of conflict of interest. [45]

In addition, a new mandatory DPO appointment was introduced,[46] replacing the recommendation of the PPA to appoint DPOs.[47] Under the amended PPL, it is required to appoint a DPO in four cases: (1) public entities; (2) data brokers processing personal information about 10,000 data subjects or more; (3) core activities consisting of or involved with processing operations, which require ongoing and systematic monitoring of data subjects on a large scale, with specific examples, such as Internet providers, cellular providers or online search engines; and (4) core activities consisting of processing of especially sensitive data on a large scale, with specific examples, such as hospitals, health maintenance organisations (HMOs), banks or insurers. The obligation applies to both controllers and processors, except data brokers where the obligation only applies to controllers. The Amendment further defined the DPO qualifications and major roles[48] and stipulated that the DPO will not be in a potential conflict of interest.[49]

Since the introduction of the DPO role as mandatory is novel, organisations are struggling with the question of who should be appointed as a DPO, specifically since in-depth knowledge of Israeli data protection law is required. In particular, many organisations are considering the appointment of their information security officer (ISO) or chief information security officer (CISO) also as DPO. The PPA has previously clarified that the DPO cannot also serve as the ISO because the role of the DPO is broader, and includes, *inter alia*, professional guidance to the ISO on how to implement the information security requirements in order to serve the purposes of data protection laws and to ensure optimal protection of the right to privacy.[50]

While these key principles and obligations provide the foundation for privacy protection, effective enforcement is essential to ensure these principles are upheld in practice. This will be discussed in the following section.

ADDRESSING PRIVACY VIOLATIONS

PPA independence

The independence of the PPA is essential for impartial enforcement of privacy laws, ensuring fair and effective application of sanctions and supervision. As part of the efforts to reaffirm Israel's adequacy by the EU, a historic decision was adopted by the Israeli Government on 2nd October, 2022 substantiating the independence of the PPA in the exercise of its authorities.[51] This decision also defined the criteria for appointment of the head of the PPA and instructed on the separate management of the PPA budget within the Ministry of Justice budget. This government decision, which was mentioned in the EU decision to reaffirm Israel's adequacy, was adopted into Amendment 13,[52] enhancing the status of the PPA in primary legislation.

Administrative fines

The primary tool for deterring privacy violations is the imposition of administrative fines, which also serve as means to hold organisations accountable for their failure to protect personal information. Prior to the Amendment, the PPA was authorised to impose very limited and low fines for breaches of a limited number of specific provisions of the PPL itself, and not for breaches of the Data Security Regulations. The Amendment granted the PPA the right

to impose new administrative fines, which may be substantial, depending on the nature of the breach and other circumstances, such as the size of the database and sensitivity of personal information affected. The fines are predefined fixed sums for each type of breach and apply to a list of specific sections of the PPL and of the Data Security Regulations.

In addition, there are predefined fixed fines for breaches of the Protection of Privacy Regulations (Provisions Regarding Information Transferred to Israel from the European Economic Area), 5782-2023 (European Economic Area [EEA] Regulations), which apply to personal information transferred from the EEA to Israel by a third party (not the data subject itself).[53] These EEA Regulations were adopted at the request of the EU to enable reaffirmation of Israel's adequacy. As of 1st January, 2025, the EEA Regulations apply also to any personal information in the same database as personal information originating from the EEA.

The PPA has no discretion to determine the amount of the fine if a specified breach occurs (subject to the reduction options detailed below).

It should be noted that there are no fines for breaches of the cross-border requirements under the Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761-2001 (Cross Border Regulations), since these regulations need to be amended and adapted to modern cross-border mechanisms. They are subject to certain clarifications by the PPA (one still in draft form).[54] The lack of clarity regarding the actual requirements prevented inclusion of the Cross Border Regulations in the sanctions part of the Amendment.

Under the amended PPL, the fines are classified into several categories, varying per category. The tiered structure of fines ensures proportional penalties according to the severity of the breach and the potential harm to data subjects. This classification is carved to determine the appropriate response to each violation.

One category involves violations concerning database registration and notification. For example, failure to register a database or to notify the PPA of a database (as applicable), or failure to update the PPA on the database details, may lead to fines in the amount of NIS 150,000 (approx. €37,000) and NIS 300,000 (approx. €74,000) in a database with more than 1 million data subjects.[55]

The second category involves violations concerning data subject rights and carries fines in the amount of NIS 15,000 (approx. €3,700), unrelated to the database size. The violations include failing to grant access to personal information upon request; failing to notify the data subject about refusal to rectify or delete personal information; failing to rectify personal information by a processor despite the consent of the controller or contrary to a court order.[56] This category reflects the importance of the rights of individuals regarding their personal information, despite the limited data subject rights under the PPL compared to the GDPR, by ensuring the relevant obligations are fulfilled.

Fines for failing to notify data subjects prior to collecting personal information are imposed for each data subject that was contacted, with a higher amount regarding especially sensitive data. These fines are in the amount of NIS 50 (approx. €12) per data subject, with a minimum of NIS 30,000 (approx. €7,300),[57] and they reinforce the fundamental principle of informed consent.

In addition, further categories of fines are calculated based on the size of the database in the amount of NIS 2 (approx. €0.5) for each data subject in the database, or NIS 4 (approx. €1) for each data subject if it contains especially sensitive data. Violations under this category include contacting an unspecified group of people for collection of personal information without proper notification; failing to appoint an ISO; failing to appoint a DPO by public entities or data brokers. Fines for DPO appointments in

the private sector will be postponed until such time that the Minister of Justice issues an order, approved by the Constitution Committee, applying the sanctions also to such appointment. This is due to the novelty of the DPO appointment requirement in Israel and the need of the market to implement it and train DPOs. Violation of provisions regarding the DPO, despite a PPA order to cease the violation, also falls under this category. A minimum amount is also set for these violations of NIS 20,000 (approx. €5,000) and no less than NIS 40,000 (approx. €10,000) in a database with especially sensitive data.[58]

Another category of fines which are calculated based on the size of the database includes violations, such as using information about private affairs of a person for a purpose other than the one for which it was provided, despite an order issued by the PPA to cease the violation; processing personal information for a purpose that violates privacy under Section 2 of the PPL, despite the PPA's order to cease the violation; processing personal information in a database for an illegal purpose; processing personal information in a database in which the information was created, received, accumulated or collected in violation of the PPL or any other law on data processing, despite the PPA's order to cease the violation; processing without authorisation by the controller or exceeding its authorisation. Under this category, the fines are in the amount of NIS 4 (approx. €1) for each data subject in the database, or NIS 8 (approx. €2) for each data subject if it contains especially sensitive data, with a minimum amount of NIS 200,000 (approx. €50,000).[59]

Additional fines may be imposed for failing to deliver a document or a copy of computer material to the PPA in the amount of NIS 300,000 (approx. €73,600).[60]

Regarding violations of the Data Security Regulations, the fines vary depending on the severity of the violation and the level of security assigned to the database according to the criteria in the Data Security Regulations (basic, medium or high); the highest amount is doubled if the database contains more than 1 million data subjects.[61] The security level assigned to the database is determined by the Data Security Regulations and varies depending on the type of personal information in the database, the number of data subjects and the number of personnel within the organisation authorised to access the database.[62]

Severe violations, such as failure to immediately report to the PPA a severe data breach, to perform a vulnerability survey or penetration test, or rectify the required findings as required, are met with significant fines, of NIS 80,000 (approx. €20,000) for medium security level databases and NIS 320,000 (approx. €80,000) for high security level databases.[63] These substantial fines underscore the importance of immediate and proactive security measures in mitigating risks related to personal information breaches.

For most violations, however, the fines are NIS 40,000 (approx. €10,000) for medium security level databases and NIS 160,000 (approx. €40,000) for high security level databases. These violations include, among others, failure to prepare or update the database definitions document, failure to conduct an annual review of excess personal information (data minimisation), or failure to prepare information security procedures.[64]

Finally, minor violations are still addressed yet subject to lower fines of NIS 20,000 (approx. €5,000) for medium security level databases and NIS 80,000 (approx. €20,000) for high security level databases. These violations include failure to conduct bi-annual privacy training to employees, failure to maintain access logs, or failure to separate systems with personal information from other systems.[65]

Additionally, fines for violation of obligations under the EEA Regulations further emphasise the importance of compliance with data protection standards across jurisdictions.[66] For example, failure to

notify a data subject of a decision on a data deletion request may result in a fine of NIS 15,000 (approx. €3,700).

Violation of some of the EEA Regulations may trigger imposition of a direct fine in the amount of NIS 2 (approx. €0.5) for each data subject in database and NIS 4 (approx. €1) for each data subject if it contains especially sensitive data. Such violations include failure to implement a mechanism to ensure that personal information that is no longer required for the original purpose or for another lawful purpose is no longer processed (excess personal information); failure to implement a mechanism to ensure that personal information is correct, complete, clear and up-to-date; failure to employ reasonable measures under the circumstances to rectify or delete personal information that is incorrect, incomplete, unclear or outdated.

Furthermore, there are instances where a preliminary order to cease the violation of the EEA Regulations is required prior to imposing the fine, and in such event the fine is in the amount of NIS 4 (approx. €1) for each data subject in the database and NIS 8 (approx. €2) for each data subject if it contains especially sensitive data. This applies to violations such as failure to delete or anonymise personal information upon a data subject request; failure to delete or anonymise excess personal information; failure to inform a data subject whose personal information is transferred from the EEA of the processing and failure to notify of further processing.

Administrative warning and obligation to refrain from a breach

The PPA may issue an administrative warning in lieu of imposing sanctions, informing the violator to cease the breach and that if the breach continues or is repeated, an administrative fine will be imposed. Alternatively, the PPA may instruct the violator to submit an undertaking according to which the violator will undertake to cease the breach, refrain from further breach in the future and pay a security deposit to the PPA in the amount of the administrative fine that could have been imposed, which may be forfeited if the violator does not meet the conditions.[67] Should the violator continue to commit the breach after an administrative notice has been given or a letter of undertaking has been submitted, the continuation of the breach will be considered a 'continuous violation', adding to the amount of fine one-hundredth part for each day the breach continues.[68]

An administrative warning cannot be issued for every sanctionable breach. Regulations determining the provisions of the PPL whose breach may lead to the issuance of an administrative warning in lieu of the imposition of administrative fines are expected to be published in the near future.

In addition, the Amendment introduced the concept of a 'repeat breach', defined as a breach of the same provision for which the violator was sanctioned which is committed within two years of a previous breach.[69] In this case, the administrative fine imposed for the repeat breach will be doubled, thereby encouraging organisations to take corrective action following their initial violation to avoid more severe financial consequences.

Reduction of administrative fines

While warnings can be issued in lieu of immediate fines, if a financial sanction has already been imposed, the PPA may reduce administrative fines, based on certain considerations defined in the Amendment, with a predefined percentage of deduction matched per circumstance.[70] For example, when no fine was imposed for violation of the same provision in the last five years; if the violator implemented measures to correct the breach; if a controller or processor who are obligated to appoint a DPO when an entity systematically monitors data subjects

on a large scale or when the core business includes processing especially sensitive data on a large scale, actually appointed the DPO prior to imposition of the fines; or personal circumstances when the violator is an individual. The maximum reduction possible is 70 per cent of the fines imposed.[71]

In addition, the administrative fines are capped at 5 per cent of the annual turnover of the violator.[72] The amended PPL also differentiates between types of businesses, considering their size and annual turnover, enabling smaller businesses to enjoy lower caps. Caps are set for micro businesses (annual turnover up to NIS 4m) and small businesses (annual turnover between NIS 4m–10m) depending on the nature of the violation (caps vary between NIS 20,000–70,000 for micro business (approx. €5,000–17,500) and between NIS 40,000–140,000 for small business (approx. €10,000–35,000).[73] This differentiation enables to take account of the financial capabilities of businesses, ensuring a more equitable approach to enforcement. A violator requesting any kind of reduction needs to provide the PPA with documentation proving the relevant turnover.[74]

Appeal on the imposition of fines

The PPA decisions to impose fines, issue administrative warnings and require undertakings to refrain from further breach may be appealed to the Magistrate Court within 45 days. Filing an appeal, however, does not delay the execution of the decision (unless the PPA agrees to a delay, or the court orders a delay).[75]

Publishing the fines to the public

After enabling the violators to present their claims, the PPA will publish on its website the names and details of violators who have been instructed to pay administrative fines, including certain details on the nature and circumstances of the breach, the amount of the fine and the identity of the breaching controller or processor, as well as details of an appeal if submitted.[76] Certain exceptions, however, apply to the publication of the names of the violators, particularly when the violator is a corporation or an individual, and the breach is deemed insignificant. The PPA will not publish the name of a corporation if the breach is insignificant, unless publication is needed to warn the data subjects in the relevant database, and will not publish the name of an individual violator unless publication is needed to warn the public.[77] The publication will remain on the PPA website for four years for corporations and two years for individuals.[78]

Some practical aspects of the new sanctions in controller — processor relationships

Due to the possible imposition of administrative fines, controllers will need to review their data processing agreements with processors to verify if they are well adapted to the new risks and consequences of the Amendment. For example, the PPA may notify a controller that its processor has violated the PPL and order the controller to instruct the processor to correct the violation, and that if such violation remains unremedied, impose sanctions on the controller.[79] It would be therefore advisable for controllers to include specific provisions in their agreements with processors, obligating processors to comply with such PPA instructions, authorising the controller to terminate the agreement if the violation is not satisfactory remedied and including specific indemnification provisions for PPA monetary sanctions, if imposed. Limitation of liability provisions should also be revisited to determine if indemnification for PPA monetary sanctions is excluded or not from processors' liability and if the contractual liability ceiling is sufficient due to the possibility of hefty PPA monetary sanctions.

PPA investigative, audit and enforcement authorities

Prior to the Amendment, the powers of the PPA were limited, and some were not formally enacted in the PPL, despite the importance of ensuring compliance. The Amendment enshrined the ongoing audit powers of the PPA regarding compliance with the PPL and added an authority to order the cessation of a breach.[80] When the PPA orders a cessation of a breach, administrative fines can be imposed only if the breach did not stop. The PPA was also granted new powers of administrative enquiry if the PPA has reasonable grounds to believe that a violation of certain provisions of the PPL or of the instructions of the PPA has occurred.[81]

In addition, the PPA may request an administrative court (which is part of the district court) to issue an order to a controller or processor to cease processing activities that cause or may cause a violation in certain severe cases listed in the Amendment. In such cases, the court may also order the deletion of personal information in the database.[82]

The PPA has been conducting sectorial audits for a few years as part of its general enforcement powers, auditing compliance with the PPL and Data Security Regulations in various market sectors. The amended PPL includes the sectorial audit procedure formally.[83]

Criminal offences

The Amendment codified the criminal enforcement powers of the PPA and added new criminal offences, by replacing the list of the PPL provisions whose breach is a criminal offence with new offences, including: disturbance to performance of the PPA's duties according to the PPL; providing data subjects a notification on collection of personal information with erroneous information intending to mislead data subjects to provide personal information; processing personal information without authorisation from the controller; including erroneous information in a request to register a database or a notification to the PPA of a database with especially sensitive information with an intent to mislead the PPA. The imprisonment varies from six months to three years depending on the offence committed.[84]

Legal remedies and law enforcement agencies

In addition to the means described above, legal remedies in private actions play a significant role in addressing privacy violations as they ensure individuals have easy access to courts and violators face legal consequences. The Amendment introduced additional statutory damages. Under the existing PPL provisions, in a tort claim for breach of privacy the court can award statutory damages without need to prove actual damages amounting to NIS 50,000 (approx. €12,500) or NIS 100,000 if the breach was intentional (approx. €25,000).[85] The Amendment added a new right to claim statutory damages without need to prove actual damages amounting to NIS 10,000 (approx. €2,500) in a civil claim for breach by a controller or processor of certain provisions of the PPL relating to databases.[86]

In addition to expanding statutory damages, the Amendment also extended the limitation period. The two-year limitation period for civil claims under the PPL[87] was cancelled, aligning the limitation period to the seven years of general law.

Furthermore, the amended PPL includes specific provisions regarding law enforcement and national security agencies, exempting them from some of the PPA's oversight powers due to their unique nature, mandating appointment of internal privacy inspectors similar to DPOs, who will liaise with the PPA.[88]

FINAL WORDS

Amendment 13 is a landmark for Israeli privacy and a long-awaited game changer,

positioning Israel in the first tier of countries with modern privacy laws based on similar principles and terminology.

This is achieved by limiting the database registration requirement to two specific scenarios only and the enabling enhanced enforcement mechanisms, including the imposition of monetary sanctions in an administrative procedure, varying according to the severity of the violation or the number of data subjects affected. This reflects a shift towards broader accountability and risk-based approach to data protection.

The Amendment encourages organisations to focus on ensuring data protection through internal structures and policies, other than through regulatory oversight and reporting. It also places greater responsibility on organisations to ensure that privacy risks are identified and mitigated, thereby necessitating more accurate internal policies and expert advice. This enhances the importance of the DPO and privacy counsel for organisations, especially if they process personal information on a large scale and process sensitive personal information (especially sensitive information).

The Amendment is a reform affecting all businesses operating in Israel, as well as foreign entities doing business in Israel and collecting or processing personal information of Israeli data subjects. It is expected to foreground the rights of privacy in Israel and push entities to prioritise allocation of resources for privacy compliance in light of the increased regulatory, civil and criminal risks.

Nevertheless, while the Amendment introduced a significant shift, the PPL remains incomplete compared to other privacy laws, particularly in aspects such as legal bases for processing and data subjects rights, and it is expected to be subject to future amendments. The Data Security Regulations will need to be amended to match the new definitions of the PPL and ensure consistency. Furthermore, the PPL still contains provisions concerning databases, a concept not addressed in other privacy laws.

Nonetheless, the changes introduced by the Amendment require organisations operating under Israeli law to re-evaluate their compliance strategies. Recommended actions to be taken in response, in addition to those referenced throughout the paper, are mainly the following:

- To begin with, organisations should conduct a comprehensive compliance review to assess their current practices and identify any gaps in relation to the updated requirements, based on the new definitions, enhanced principles of notification and consent, purpose limitation and lawful processing. This process should include a gap analysis to identify areas where current policies, procedures or data processing agreements do not align with the new requirements. Based on the findings, organisations should take corrective measures to address any identified deficiencies, such as revising policies, updating procedures or implementing new ones.
- Existing data processing agreements should be reviewed in light of the Amendment, specifically, regarding limitation of liability provisions that may exclude indemnification for the new financial sanctions.
- Continued database registration or substituting it with the new notification obligation should be evaluated when the Amendment takes effect.
- Organisations should review whether the new obligation to appoint a DPO applies to them according to the requirements detailed in the Amendment and based on their data processing activities and scope.
- Finally, organisations should adopt a risk-based approach to data processing, considering the potential sanctions and their severity, as well as factors such as the sensitivity of the personal information, the scope and nature of the processing and

the amount of data subjects, all of which may result in more severe sanctions and therefore necessitate greater focus on data protection measures and compliance.

References

1. Privacy Protection Bill (Amendment No. 13), 5722-2022 (Israel) was submitted to the Knesset in 2022. In May 2023, the Parliament decided to apply the rule of continuity for advancement of the Bill in the newly elected parliament, which was then discussed in the Constitution Law and Justice Committee from December 2023 to July 2024 and was officially published on 14th August, 2024, available at Government of Israel, https://fs.knesset.gov.il/25/law/25_lsr_4810658.pdf (accessed 21st April, 2025). (Hebrew.)
2. *Ibid*., Art. 74(a).
3. Government of Israel, 'Protection of Privacy Law 5741-1981', Art. 11, available at https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf (accessed 21st April, 2025).
4. 'Database' is defined in the amendment as a collection of personal information processed by digital means (subject to certain exclusions).
5. Birnhack M. D. (2025), 'Constitutional Privacy', in Barak, A., Medina, B. and Roznai, Y. (eds), *Oxford Handbook on The Israeli Constitution*, Oxford University Press, Oxford, pp. 134–136.
6. Government of Israel, ref. 3 above, Art. 8.
7. European Commission (EC) (2024), 'Commission Staff Working Document – Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC', available at https://commission.europa.eu/document/download/f8229eb2-1a36-4cf5-a099-1cd001664bff_en?filename=JUST_template_comingsoon_Commission%20Staff%20Working%20Document%20-%20Report%20on%20the%20first%20review%20of%20the%20functioning.pdf (accessed 21st April, 2025).
8. The Government of Israel (April 2017), 'Privacy Protection (Data Security) Regulations, 5777-2017', available at https://www.gov.il/BlobFolder/legalinfo/data_security_regulation/en/PROTECTION%20OF%20PRIVACY%20REGULATIONS.pdf (accessed 21st April, 2025).
9. Government of Israel, ref. 3 above, Art. 13–14.
10. The Government of Israel (2023), 'Privacy Protection Authority Annual Report – 2023', available at https://www.gov.il/BlobFolder/reports/ann2023/he/my_privacy_anual_report_Mo.pdf (accessed 21st April, 2025).
11. Government of Israel, ref. 3 above, Art. 1 and 2.
12. Government of Israel, ref. 1 above, Art. 3.
13. Privacy Protection Authority (PPA) (December 2022), 'Opinion on the Interpretation of the Terms "Information" and "Information about an individual's Private Affairs" in the Privacy Protection Law', Government of Israel available at, https://www.gov.il/BlobFolder/reports/legat_terms2022/he/Legal%20Terms.pdf (accessed 21st April, 2025).
14. Government of Israel, ref. 3 above, Art. 7.
15. Government of Israel, ref. 1 above, Art. 3.
16. European Union (EU), 'General Data protection Regulation (GDPR), Art. 4(1), available at https://gdpr.eu/tag/gdpr/ (accessed 21st April, 2025).
17. Government of Israel, ref. 3 above, Art. 7.
18. Government of Israel, ref. 1 above, Art. 3.
19. European Union (EU), Art. 9.
20. Government of Israel, ref. 1 above, Art. 3.
21. Government of Israel, ref. 3 above, Art. 3.
22. European Union (EU), Art. 4(2).
23. Government of Israel, ref. 1 above, Art. 3.
24. European Union (EU), Art. 4(7).
25. Government of Israel, ref. 3 above, Art. 3.
26. Privacy Protection Authority (PPA) (2020), 'Audit on Data Storage Services and Database Processing in Israel', The Government of Israel, available at https://www.gov.il/BlobFolder/dynamiccollectorresultitem/ppa-report13/he/dtatbase%20compeny.pdf (accessed 21st April, 2025).
27. Government of Israel, ref. 1 above, Art. 3.
28. Government of Israel, 'Protection of Privacy Regulation (Data Security) 5777-2017', Art. 1(3) First Schedule, available at https://www.gov.il/BlobFolder/legalinfo/data_security_regulation/en/PROTECTION%20OF%20PRIVACY%20REGULATIONS.pdf (accessed 21st April, 2025).
29. Government of Israel, ref. 1 above, Third Schedule referring to sanctions under Article 23Kf(h).
30. See QA at the PPA website on the Data Security Regulations, Privacy Protection Authority (PPA), 'What is the difference between 'External Factor' according to Regulation 15 of the Data Security Regulations and 'Holder' according to the PPL?', available at https://www.gov.il/he/pages/data_security_fqa?chapterIndex=5 (accessed 21st April, 2025).
31. Government of Israel, ref. 3 above, Art. 11.
32. Government of Israel, ref. 1 above, Art. 17B2(b).
33. Government of Israel, ref. 3 above, Art. 2(9) and 8(b).
34. Government of Israel, ref. 1 above, Art. 8(b).
35. Government of Israel, ref. 28 above, Regulation 2.
36. Government of Israel, ref. 1 above, Art. 8(a).
37. Government of Israel, ref. 1 above, Art. 8(c).
38. Government of Israel, ref. 1 above, Art. 8(d).
39. Government of Israel, ref. 1 above, Art. 23MI(a).
40. Government of Israel, ref. 1 above, Art. 23NE.
41. Government of Israel, ref. 1 above, Art. 8A(a).
42. Government of Israel, ref. 1 above, Art. 8A(b)(1).
43. Government of Israel, ref. 3 above, Art. 17B.
44. Government of Israel, ref. 1 above, Art. 17B(a).
45. Government of Israel, ref. 28 above, Regulation 3(4).
46. Government of Israel, ref. 1 above, Art. 17B1.
47. Privacy Protection Authority (PPA) (2022), 'Opinion on Data Protection Officer Appointment', available at https://www.gov.il/BlobFolder/reports/dpo_doc_kit/he/dpo_doc.pdf (accessed 21st April, 2025).

48. Government of Israel, ref. 1 above, Art. 17B2(a) and 17B3(a).
49. Government of Israel, ref. 1 above, Art. 17B3(c).
50. Privacy Protection Authority, ref. 47 above.
51. The Government of Israel (October 2022), 'Government Resolution No. 1890, Independence of the Privacy Protection Authority and Amendment of Government Decision', available at https://www.gov.il/he/pages/dec1890-2022 (accessed 21st April, 2025).
52. Government of Israel, ref. 1 above, First Schedule.
53. Privacy Protection Authority (PPA) 'Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023', available at https://www.gov.il/en/pages/datatransferredisrael2023 (accessed 21st April, 2025).
54. Ministry of Justice (September 2024), 'Draft Statement of Opinion on the Transfer of Information Outside of Israel – Interpretation of Regulation 2(4)' available at https://www.gov.il/he/pages/regulation_2_4 (accessed 21st April, 2025).
55. Government of Israel, ref. 1 above, Art. 23KF(a).
56. Government of Israel, ref. 1 above, Art. 23KF(b).
57. Government of Israel, ref. 1 above, Art. 23KF(c).
58. Government of Israel, ref. 1 above, Art. 23KF(d).
59. Government of Israel, ref. 1 above, Art. 23KF(e).
60. Government of Israel, ref. 1 above, Art. 23KF(g).
61. Government of Israel, ref. 1 above, Art. 23KF(h).
62. Government of Israel, ref. 1 above, First Schedule.
63. Government of Israel, ref. 1 above, Third Schedule.
64. *Ibid*.
65. *Ibid*.
66. Government of Israel, ref. 1 above, Fourth Schedule.
67. Government of Israel, ref. 1 above, Art. 23LF.
68. Government of Israel, ref. 1 above, Art. 23LH(a).
69. Government of Israel, ref. 1 above, Art. 23LH(b).
70. Government of Israel, ref. 1 above, Art. 23LA and Fifth Schedule.
71. Government of Israel, ref. 1 above, Art. 5 of the Fifth Schedule.
72. Government of Israel, ref. 1 above, Art. 7(a) of the Fifth Schedule.
73. Government of Israel, ref. 1 above, Art. 1 of the Fifth Schedule.
74. Government of Israel, ref. 1 above, Art. 7(b) of the Fifth Schedule.
75. Government of Israel, ref. 1 above, Art. 23ME.
76. Government of Israel, ref. 1 above, Art. 23MF(a) and 23MF(b).
77. Government of Israel, ref. 1 above, Art. 23ME(d).
78. Government of Israel, ref. 1 above, Art. 23ME(f).
79. Government of Israel, ref. 1 above, Art. 23KF(j).
80. Government of Israel, ref. 1 above, Art. 23J.
81. Government of Israel, ref. 1 above, Art. 23JB.
82. Government of Israel, ref. 1 above, Art. 23MI.
83. Government of Israel, ref. 1 above, Subchapter D.
84. Government of Israel, ref. 1 above, Subchapter B.
85. Government of Israel, ref. 3 above, Art. 29A.
86. Government of Israel, ref. 1 above, Art. 15A.
87. Government of Israel, ref. 3 above, Art. 26.
88. Government of Israel, ref. 1 above, Art. D2.