ISSUE BRIEF

GLOBAL

Overview of Amendment No. 13 to the Israeli Privacy Law

Author: Rivki Dvash, Senior Fellow, FPF Israel

October/2024

FPF ISRAEL

TECH POLICY INSTITUTE

Overview of Amendment No. 13 to the Israeli Privacy Law

Adv. Rivki Dvash, Senior Fellow, FPF Israel

This analysis seeks to review the main points of Amendment No. 13 to the Israeli Privacy Protection Act, which was passed into law in August 2024. It is important to note that, according to representatives of the Ministry of Justice, another amendment to the Privacy Protection Law, which is expected to include substantial amendments to the provisions of the law, is in the advanced drafting stages and is planned to be published in the near future. The analysis will also consider the comparison of key aspects (even if not comprehensively) with two leading pieces of legislation in this field worldwide: the General Data Protection Regulation (GDPR) (EU) and the California Consumer Privacy Act (CCPA) (California).

A significant point to remember in relation to such a comparison is that there is a major difference as the EU and California regulations are extraterritorial. In other words, where a controller processes data about residents of the EU or California and meets the definitions of the normative arrangement, the law in that region will apply to them even if the business is not located in the relevant jurisdiction, unlike Israeli law and regulations that apply only to entities within the jurisdiction of Israel.

For the sake of convenience, the comparison with foreign law will be marked in a box.

1 - Background

On August 5, 2024, the Knesset plenum approved the proposed Privacy Law (Hebrew only) (Amendment No. 13), 5774-2024 (the Amendment), which will come into effect on August 14, 2025.

According to the explanatory notes, the legislative Amendment stems from establishing the Privacy Protection Authority (PPA) in 2006 and from the recommendations in the Schofman Report submitted in 2007, which dealt with necessary Amendments at the time regarding the arrangement relating to data protection. The bill that sought to advance the PPA's enforcement powers was first submitted in 2011 (Hebrew only), and then in 2018 (Hebrew only), and was not advanced due to political instability in Israel.

Despite the passage of time, the Amendments still focused on the enforcement powers of the PPA, while the long-awaited Amendment relating to substantive provisions of the law, including additional legal bases for processing data and the expansion of the rights of data subjects, remained outside the legislation. An exception was an arrangement established in the regulations under the Privacy law with respect to a database to which data from the European Economic Area is transferred, as detailed below:

In 2023, and in order to maintain recognition of the compliance of Israeli law with the GDPR, The Knesset approved the Privacy Regulations (Provisions Regarding Data Transferred to Israel from the European Economic Area), 5773-2023 (the Mediation Regulations) (Hebrew only). These regulations granted privileges to data subjects whose data is included in a database that also includes data originating from the European Economic Area (the EEA

Rothschild Boulevard 74-76, Tel Aviv-Yafo, 6521401
Offices: + 972 50 6217710
rdvash@techpolicy.org.il | www.techpolicy.org.il

Region). It should be emphasized that the distinction is not according to the identity or **nationality** of the data subject, but rather the **source** from which the data was obtained. In other words, the Mediation Regulations created two tiers of rights of data subjects: the first, the limited rights existing in the Israeli law that apply to all databases in Israel, and the second, which significantly expands the rights of data subjects compared to those provided by Israeli law and that applies to databases that contain data that came from the EEA Region – while the rights will apply to all data subjects in the database, regardless of the source from which the data came.

Even if the arrangement in the Mediation Regulations is partial and does not include all the balances in the GDPR, it created increased obligations regarding personal data processed in some databases in Israel.

For more information on the Mediation Regulations, read the ITPI's review on the subject (April 2023) (Hebrew only).

2 - Main Points of the Israeli Amendment to the Privacy Act

The Amendment includes several main issues:

- Changing legislative definitions (see Section 3 below);
- Reduction of registration obligations (Section 4);
- Adding the possibility of demanding compensation without proof of damage - an option that has so far been granted only for a breach of privacy and not for a violation of provisions relating to Data Protection (Section 5);
- The obligation to appoint a data privacy officer (Section 6);
- Regulating the status of PPA and its enforcement powers (Section 7);
- Determination of sanctions for administrative violation (Section 8); and
- Definition of criminal offenses in relation to Data Protection breaches (Section 9).

Furthermore, there are additional Amendments related to various issues. These include changing the wording related to the controller's obligation to process the data only in accordance with the purpose of the database, adding obligations to the notice given when collecting data, removing the limitation to file a suit (private right of action) under the Privacy Law, which previously stood for two years, and more. These Amendments will also be addressed in the review.

3 - Changing legislative definitions of key terms, such as "personal data" or "biometric data"

The definitions in the Privacy Law, 5741-1981 (the Law) are found over several Sections, including Sections 3, 7, and 17A. The Amendment moved the definitions applicable to the entire law to Section 3, updating and adding required definitions.

Below, we refer to some of the updated main definitions and compare them with the existing versions of the European and California arrangements. It should be noted that, as a rule, the definitions were not copied verbatim (where copied as stated, the wording is indicated in quotation marks). The reference relating to arrangements abroad is intended to present

significant gaps, if any, between the definition in Israel and the definition in the same place, and not necessarily to present the entire definition.

Definition	The Israeli Arrangement	GDPR	CCPA
Personal data	"Data relating to an identified or identifiable person." "Identifiable person" means a person who can be identified with reasonable effort, directly or indirectly, including using an identifying individual or using one or more data relating to him.	The Israeli definition is similar to the European definition but for one difference – the GDPR does not use the term "reasonableness" in relation to the ability to identify a person, thus making it more stringent than the new definition in Israel (Art 4).	The definition in California is different in several ways – 1. It also refers to data associated with a household. 2. The setting lists examples of personal data (although the list is not closed). 3. The definition excludes publicly available information and truthful information that is a matter of public concern.. 4. The definition excludes deidentified or aggregated data (1798.140(v))
Particular sensitivity data	The definition is relevant concerning the obligation to notify, appoint a DPO (if the additional conditions are met), and raise the fine amount. It should be noted that in the first addition to the data security regulations, there is a list of types of data whose processing raises the database to a medium level of security, with the understanding that these categories are more sensitive. There is no correspondence between the two lists, which creates divergence in the normative	The essential difference between the two laws is that the reference to the term "special categories of personal data" is intended in the European regulation to limit the processing permitted in these categories while exacerbating the circumstances under which the data covered under one of the categories can be processed (Article 9). The type of data included in this category is more limited and overlaps only with the categories listed in paragraphs (1)-(4) and (7) of the definition in Israel, and	The essential difference between the arrangements is that the reference to "sensitive personal information" is intended to add special provisions regarding them, inter alia, in relation to the obligations of notice (1798.100) and the right of a data subject to restrict the use or disclosure of such data (1798.121). The categories of sensitive personal data are slightly different from those in Israel. In addition to definitions

Definition	The Israeli Arrangement	GDPR	CCPA
	perception and may mislead. Particularly sensitive data includes the following categories – 1. the privacy of a person's life and sexual orientation; 2. state of health of a person; 3. genetic information; 4. "A biometric identifier used or intended to be used to identify or verify an individual's identity by computer"; 5. origin of a person; 6. criminal record; 7. political opinions, human religious beliefs, and worldview; 8. personality assessment conducted on behalf of a professional; 9. location and traffic data generated by an authorized provider, and data about an individual's location that indicates data pursuant to paragraphs (1)-(7) and (10)-(11) of the definition; 10. payroll and financial activity data; 11. Personal data for which there is a legal obligation of confidentiality; 12. Additional data set forth by the Minister	trade union membership is added.	similar to the categories enumerated in paragraphs (1)-(7), there are also the following categories : 1. identification key (such as ID number, passport number); 2. data that allows login to a consumer's account; 3. precise geolocation information; 4. mail and message content, unless the business is the recipient; 5. Trade union membership. However, the right to limit the use or disclosure of sensitive personal information is limited only to information used to infer characteristics about an individual.

Definition	The Israeli Arrangement	GDPR	CCPA
	in the Second Addendum.		
Biometric identifier	"Biometric data used to identify or verify a person's identity, or a biometric device from which such data can be derived" " 'Biometric' – a unique human, physiological or behavioral characteristic that can be measured by computer."	The Israeli definition is similar to the European one (Article 4), although the GDPR definition distinguishes between the data itself and the data intended for identification of a person. The language used refers to the possibility of identification and not necessarily to the ability to do so, as can be seen from the language of the definition in Israel.	The definitions are similar, except that the California arrangement includes a biometric identifier that is used or is intended to be used for identification in conjunction with other data (and not just an identifier per se). (1798.140(c))
Database	"Collection of personal data processed by digital means, except" – 1. Collection for personal, non-business use; 2. A collection pertaining to less than 100,000 people, containing only a name, address, and contact information, for which there is no additional personal characteristic, and the controller does not have a collection that includes additional data about these people.	The European law applies to any processing of personal data which is done through automated means, regardless of whether such data is part of a filing system or not. The GDPR also applies to non-automated (manual) processing of personal data only as long as it is done in a filing system, defined in Article 4(6) as any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;	California law is essentially a consumer law. Therefore, the only relevant entity regarding accountability is the business that meets at least one of the following three – 1. Has an annual (gross) income over $M 25; 2. Annually buys, sells, or shares the personal data of 100,000 or more California residents or households; 3. 50% or more of annual income comes from selling personal data about California residents.
Processing, use	Any action performed on personal data.	There is some variation (the GDPR definition (Article 4(2)) explicitly refers to a set of data and processing by automated means), but it seems that the Israeli definition is, in any case,	The California definition is similar to the EU GDPR.

Definition	The Israeli Arrangement	GDPR	CCPA
		broader and includes those within it as well.	
Controller of a database	"A person who determines, alone or together with another, the purposes of data processing in the database or an entity in which he or an official authorized by legislation to process data in a database."	The Israeli definition corresponds to the European one (Article 4(7)).	The California equivalent is “Business” (see the definition above).
Holder	"An external party to the database controller that processes data for it."	The definition of “holder” in Israeli law is ambiguous when compared to the GDPR notions of “processor” and “third party”, but it is closer to the former. Under the GDPR, “processors” are any natural or legal persons who are processing personal data “on behalf of the controller”, while third parties are any natural or legal persons who are not data subjects, processors, or any other persons processing personal data under the authority of the controller (so they are external parties).	The equivalent definition is "Contractor," which includes limitations on the type of contract a business can make with someone acting on its behalf. (1798.140(j))
Data security	"Protecting the integrity of personal data or protecting personal data from processing, without lawful permission."	The GDPR does not define the term, but the obligation itself is defined more holistically than in the Israeli arrangement, with reference to various components that must be considered in adopting the appropriate security measures (Article 32). Data security obligation in the GDPR takes into account " the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying	The definition relates to security and integrity and includes three aspects: 1. The existence of networks or data systems to detect security incidents that jeopardize the availability, authenticity, integrity, and confidentiality of the personal data stored or transferred. 2. The ability to detect security incidents,

Definition	The Israeli Arrangement	GDPR	CCPA
		likelihood and severity for the rights and freedoms of natural persons." Therefore, "appropriate technical and organisational measures to ensure a level of security appropriate to the risk" shall be implemented. Several measures that do not constitute an exhaustive list are mentioned: 1. pseudonymization and encryption; 2. ensuring the confidentiality, integrity, availability and robustness of systems and services; 3. the ability to restore availability and access in a physical or technical event; 4. Ongoing review process to evaluate technical and organizational measures to ensure security.	resist malicious, deceptive, fraudulent, or illegal actions, and help prosecute those responsible. 3. The ability to ensure physical safety for people. (1798.140(ac))
Direct marketing	"Personal appeal to a person, based on their belonging to a population group, determined according to one or more characteristics of persons whose names are included in a database."	There is no definition of the term. There is a reference to the right to object process for purposes of direct marketing including profiling, whether with regard to initial or further processing, at any time and free of charge. (Article 21)	"Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.
Direct marketing services	"Providing direct marketing services to others by transmitting	There is no unique reference to direct marketing services.	A data broker is required to register under California law. The

Definition	The Israeli Arrangement	GDPR	CCPA
	lists, stickers, or data by any means."		definition of a data broker is "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship" (1798.99.80(c)). There are exceptions to the definition for entities that have been obligated by law to act in this manner (such as credit rating companies).

4 - Reducing the Scope of the Registration Requirement

The Amendment seeks to reduce the existing registration requirement to two cases (Section 8A(a)(1)) –

1. Direct marketing services, if there are more than 10,000 people in the database.
2. A public authority, in relation to any database in its possession, unless the data concerns public authority employees only.

The outdated concept that exists in the law, which reflects a situation in which first there is registration, and only then is the use legal, is also preserved in the Amendment. However, the Amendment reduced the time between registering the database and the possibility of establishing it to 60 days (instead of 90) (Section 8A(a)(2)).

In an age when a database is established in a split second, this provision is not applicable in many cases. For example, suppose that a government authority organizes an awareness day for a population with special needs, who are not civil servants. The civil servant responsible for the day's organization requests to fill in the details of the participants (who are not employees of the public body) in an Excel table. According to the provisions of the amendment, if they have not submitted a request for registration and 60 days have passed or if they have not been given permission to establish the database (Excel table), he is not allowed to edit the list because it is a database whose controller is a public authority, and the data is not about its employees.

In addition to the registration requirement, a notification obligation applies to any particular sensitive database containing data of over 100,000 people. Such a database is required to send a notice to the Registrar within 30 days from the moment the condition for which it is obligated to notify is satisfied (Section 8A(a)(b)).

GDPR has no registration requirement at all. In the CPPA, there is a requirement to register businesses that act as data brokers. The arrangement stipulates that data brokers will be registered by January 31 of the year they became intermediaries with the California Privacy Protection Authority (Section 1798.99.82). Please note that this arrangement does not involve registration in the first place as a condition for establishing the database, as it is maintained in the Israeli arrangement.

For more information on registration arrangements worldwide, see a study conducted at the Institute on comparing arrangements in data protection legislation (January 2022) (Hebrew only).

5 - Compensation is Possible Without Proof of Damage

Under existing law, it is possible to file a civil suit and claim compensation without proof of damage (Section 29A(b)) for committing a civil tort of invasion of privacy. These torts relate to infringement of privacy according to one of the cases described in Section 2 of the law, all of which relate to the violation of "classic privacy" and not a violation of the provisions of the law relating to data protection. According to the ITPI's review of a decade of civil privacy rulings (January 2023), out of 293 judgments handed down for the tort of invasion of privacy, all but one of the plaintiffs sought damages without proof of damage. Therefore, it can be assumed that the Amendment is expected to encourage the filing of civil suits for violation of data protection provisions.

The Amendment allows claims of compensation in a civil proceeding, without proof of damage, in an amount not exceeding NIS 10,000 (approximately $ 2,700) per violation (Section 15A). The type of violations for which such a claim may be filed include:

1. Failure to register a database, provided that the claimant contacted the controller with a demand to register the database and 90 days have passed and the database has not been registered;
2. Failure to provide proper notice (the controller must be given the option to correct within 30 days);
3. Failure to exercise the right of review or correction; and
4. Failure to notify the head of PPA about the regular receipt of data between public authorities (30 days' notice must be given before the claim is submitted).

In the European and California laws, compensation is not possible without proof of damage.

6 - The Amendment mandates appointment of Data Protection Officers in specific cases

The Amendment mandates the appointment of a Data Protection Officer (DPO) in certain cases (Article 17B1). The obligation applies to the following entities:

1. registration receivables (data brokers and public bodies);
2. databases whose mode of activity is monitoring, such as cellular companies;
3. databases whose main occupation is processing data with special sensitivity, such as Health Management Organizations (HMO).

The role of the DPO is to act to "ensure compliance with the provisions of the law." This activity must be done by serving as a professional authority and knowledge center. In addition, the DPO must act to conduct training in the organization, set a control plan, give suggestions for correcting deficiencies in the field, and ensure the existence of a data security procedure and the database definitions document required by the Privacy Regulations (Data Security), 5777-2017 (the Data Security Regulations), act in the organization for the realization of the rights of data subjects, and be the organization's contact person with the PPA.

The DPO must report to the CEO or anyone acting on their behalf, and the organization must ensure that the DPO has the resources and involvement in the organization required to fulfill their duties.

As noted, the role of Data Protection Officer also exists in the GDPR, which stipulates the obligation to appoint a DPO in several scenarios, similar to the obligation existing in the Amendment (except in relation to data merchants).

However, there are several substantial changes between the two laws –

1. The GDPR provides for the DPO's professional independence and determines that the DPO will not accept any instructions regarding the fulfillment of tasks and that it is forbidden to dismiss or punish the DPO for performing their duties (Article 38(3));
2. The DPO also advises on the Data Protection Impact Assessment when introducing new components that may violate privacy and supervises the implementation of the privacy assessment (Section 39(1)(c)). In Israel, there is still no obligation to conduct such an assessment, but the variance sharpens the difference between a DPO who assists in implementing legal provisions that contain substantive provisions that define the professional framework and a DPO whose professional content is ultimately very limited (consent, giving notice, registration where applicable, and granting the right of review and correction);
3. In the GDPR, the DPO is not only a liaison with the Privacy Authority but is obligated to cooperate with it (Article 39(1)(d)).

In the California law, there is no similar function.

7 - The Privacy Protection Authority's (PPA) competences and powers are significantly modified

7.1 - Definition of PPA and its Functions

The Privacy Protection Authority (PPA) was established by a government decision in January 2006, in which it was determined that a legal authority for data technology and privacy protection would be established, which would unite the Registrar of Databases, the Registrar of Credit Data, and the Registrar of Electronic Signature under one body. It was also determined through the appointment of the head of the authority, who would be responsible for managing the system of registration, supervision, and administrative enforcement of the three registrars (Resolution No.4660) (Hebrew only).

As part of Israel's attempt to maintain the status of EU adequate jurisdiction under the GDPR (accountability), and after its promises to the EU to anchor the status of the authority in the legislation were not fulfilled, it was decided to regulate the status of the authority in a government decision (executive action) of October 2022 (decision number 1890) (Hebrew only).

In this decision, it was determined that the PPA would be independent in fulfilling its duties and that the PPA's budget would be managed separately within the Ministry of Justice budget (Section 1(b) of the government decision). In addition, conditions of eligibility for those who may be the head of the authority have been established, which do not involve concrete experience or education in the field of privacy, data protection, or technology (Section 3 of the government decision).

The decision states that the functions of the PPA will include the following (Section 2 of the government decision):

1. Supervision of compliance with the provisions of the law in relation to databases;
2. Investigation of suspicions of committing offenses under the law in relation to databases following the PPA's powers;
3. Raising awareness through education, training, and advocacy;
4. Handling public inquiries;
5. Development and implementation of "professional programs and training in its areas of activity;"
6. Promoting ties on the international level with parallel bodies; and
7. Execution of the powers of the Registrar of Approving Bodies according to the Israeli Electronic signature law.

The text of the bill, as submitted by the government, did not propose to regulate the PPA's status but only proposed changing the regulator's name. The desire to regulate the definition of the PPA and its role arose during the discussions on the proposal. It was determined that the definition of the PPA would refer to the four relevant government decisions when the text of the 1890 resolution was presented in the First Appendix.

This is a way of wording that is generally not accepted in Israeli legislation, both because in regulating the status of a public authority, it is customary to define it in law and because it is not customary to take government decisions and copy them verbatim into law. At the substantive level, a situation has arisen in which ostensibly the law relies on a government decision (executive action), but in practice, if the government seeks to change the decision, a parallel legislative Amendment will be required, and as long as it is not amended, the law will prevail.

7.2 - Powers of the Authority

The essence of the law deals with the powers granted to the PPA to fulfill its duties. These powers include the following:

1. *Preliminary opinion* – the possibility of a controller or "holder" (processor) to request a pre-ruling opinion. The PPA may publish these opinions identifying the requesting

entity by name (with the consent of the applicant) or anonymously (without their consent) (Section 17I2);

2. *Lateral supervision* — The Authority may carry out lateral supervision by sending questionnaires to relevant parties. In carrying out lateral supervision, a person who is not a civil servant ("external expert") can assist, but the discretion will remain only with a civil servant (Section 23Q). The external expert may also require documents and information, provided that prior approval of a supervisor is given (Section 23R(f)).
3. *Supervisory powers* (Section 23J) — Under the Amendment, the powers require the supervised body to identify themselves in front of the supervisor, provide the supervisor with any requested document or information, allow the entry of the supervisor to any place other than a private home, and hand the supervisor system data (such as logs) or sample personal data. Concerning the last two data, the PPA must delete them as soon as they are not required, and no later than seven years for system data and three years for sample personal data, unless they are required to conduct proceedings.
4. *Administrative inquiry* (Section 23L) — Where there is suspicion that a violation has been committed under the law, the supervisor should be given additional powers, including the possibility of requesting a search warrant, seizure, and warrant for computer penetration (Section 23N).
5. *Investigative powers* — The head of the PPA may appoint civil servants as investigators of criminal offenses on behalf of the authority. Investigators shall have the authority to interrogate relevant persons, seize an object related to the offense, request a court order to seize and penetrate computer material, detain a person, require them to accompany the investigator, or summon them for interrogation at the PPA's offices (Sections 23AX-23AY).

Despite the broad supervisory powers of the Authority, there are several exceptional cases regarding how supervision is carried out by the Authority:

1. *Supervision of entities subject to security directives of the Cyber Directorate* shall be carried out following a procedure to be formulated between the PPA and the National Cyber Directorate (Section 23S);
2. *For authorities dedicated to security*, such as the Police, IDF, Shin Bet, Mossad and some more security authorities that are detailed in the section, the method of supervision will be different. In these authorities, a privacy supervisor will be appointed from among the employees, who will report to the head of the security authority and will be guided by the head of the PPA (Section 23U). The supervisor in that authority shall carry out activities according to an annual plan approved by the head of the security body and the head of the PPA and shall have the same powers as the supervisor of the PPA (Sections 23V-23W). The head of the authority may instruct the supervisor to carry out actions on their behalf, or employ administrative or criminal enforcement measures where suspicions of a violation or offense have arisen (Section 23X);
3. *Special arrangement for an election period* – The exercise of PPA's powers in relation to databases of parties or candidates for elections in local authorities during an election period can be carried out only if preliminary approval is obtained from the

chairman of the Central or Regional Elections Committee, as the case may be (Section 23BG).

In addition to the PPA's powers, it must submit an annual report to the Constitution, Law, and Justice Committee (Section 17I3). The law specifies the report's content while requiring that the report include segmentation by governmental, public, and private bodies. About each of them, the PPA must report on the number of pre-rulings, registration, notices, complaints, supervision actions, administrative inquiries, search and seizure warrants, complaints about an external expert, instructions for stopping infringement, administrative notices, commitment or guarantee required, sanctions, exercise of the right to plea, notice of charge without sanction, reduction of sanction, repeated violations, ongoing violations, appeals to the head of the authority to impose financial sanctions, criminal enforcement proceedings, request for a party investigation, and file data for compensation without proof of damage.

The GDPR requires that the "supervisory authority" be an independent entity (Article. 4(21)) and Article 52). It is interesting to note that European legislation emphasizes that the role of the supervisory authority is to enforce the provisions of the legislation both to protect the rights of data subjects and to enable the free flow of data (article 51(1)). The need to create a legal regime that allows the free flow of data while preserving basic rights is interwoven throughout European legislation and its absence is conspicuous in the Israeli Amendment. This means that even in implementing the enforcement tools in the hands of PPA, it is not committed to the balance in which a European authority is obligated to allow the free flow of personal data as a value that must be protected if it exists within the established frameworks.

The European law enumerates the tasks assigned to the supervisory authority (Article 57) and its powers (Article 58). It is noteworthy that the following functions assigned to the supervisory authority in the GDPR are absent from Amendment 13:

1. To be an advisory body to the government and other public institutions in relation to legislation and administrative decisions in the field of personal data protection;
2. Provide data to each data subject, upon request, about their rights;
3. Monitor relevant developments, in particular on issues of data and communication technology development, and commercial practices;
4. To encourage the formulation of codes of conduct in accordance with the European Regulation (Article 40), and to examine such codes with an opinion on them.

Regarding the powers conferred to European supervisory authorities compared to those of the Israeli PPA, note that the authority to conduct criminal proceedings is absent from the GDPR. In this regard, it should be noted that the GDPR does not determine offenses in the Regulation and leaves their determination to the states (Article 84). In addition, the Israeli law lacks details of the powers granted to the supervisory authority to assist controllers in complying with the provisions of the law (not as punishment but as preliminary assistive actions), such as drafting ethics rules, customary clauses for standard contracts, etc. (Article 58(3)).

The California Personal Data Protection Agency (the Agency) was established by an Amendment to California law in 2020. The Agency is administered by a 5-member board. Board members must have expertise in privacy, technology, and consumer protection (Section 1798.199.10) and are appointed by four different bodies (one appoints two representatives, and the rest appoint one representative each). The functions of the Agency are similar to those of the EU supervisory authorities, with minor modifications, with the addition of an obligation to establish regulations required by legislation (Section 1798.199.40(d)), as well as the review and distribution of grants from a designated fund established for data protection under the law (Section 1798.199.40(k)). The Agency also cannot conduct criminal investigations.

The California Attorney General is separately empowered to enforce the Act.

7.3 - Administrative means of enforcement

The law detailed several administrative enforcement measures granted to the head of PPA or a person authorized on their behalf that can be imposed on an entity that violated the law's provisions regarding data protection.

A preliminary note regarding the legislative practice created by the Amendment: Regulation requires the normative determination of appropriate behavior in order to regulate the desired behavior. The legislature customarily attaches punishment (administrative, or criminal) to certain provisions or to allow the filing of a civil suit for violating them. That is, after the obligation in an Article has been clearly formulated, the legislature will indicate that violation of provisions from that Article may lead to administrative or criminal sanctions. It is not customary in Israeli law to determine violations in another separate Section.

In the 13th Amendment, and unlike the customary practice, the legislature decided to re-list all violations. Beyond the awkwardness and difficulty in understanding the provisions of the law, this may create gaps between the various versions, especially where there will be future legislative Amendments, and there will be no care to amend all the places required by the law. It should be noted that there are already discrepancies between certain provisions and the violations that have been redefined. For example, the data security regulations require preservation logs for two years (Regulation 17), but the violation defined in item (25) of the Third Appendix allows for the imposition of a fine if the logs are not kept for only a year. In other words, a person who kept logs for 18 months violated the provisions of the regulations but cannot be subject to a sanction. This encourages controllers to converge for a year of preservation. If the legislature believes that the substantive requirement is erroneous, it is recommended to propose an Amendment to the provision for legal certainty.

The following are the enforcement powers granted to the PPA:

1. *Termination of a violation* – a notice by the head of the PPA, after a hearing, that a violation has been committed and that it must be corrected. The violations against which termination of infringement may be determined related to the following violations: use of data not for the purpose for which it was provided, unlawful processing of data, processing not in accordance with the Mediation Regulations, and deficiencies in the appointment or functioning of the DPO (Article 23Y).
2. *Financial sanctions (fines)* – The head of the authority or anyone acting on their behalf may order the imposition of financial sanctions by administrative decision due to violation of the provisions of the law (Section 23Z). In contrast to the government bill, which established a certain schematic level of punishment regarding the size of the database, the degree of sensitivity of the data, and the type of violation, the law approved by the Knesset created a division into nine different calculations regarding

the amount of the monetary sanction. For details of the said division into the nine different calculations, See the document's Appendix.

3. *Administrative warning* – The head of the authority may issue an administrative warning in lieu of a monetary sanction. The warning should indicate the nature of the violation and warn that failure to correct it may lead to the imposition of a financial penalty for a repeated or ongoing violation (Section 23AK). A request to cancel the notice may be submitted within 45 days (Section 23AL).
4. *Obligation to refrain from infringement* – The head of PPA may demand a commitment to refrain from the identified violation, as an alternative to a monetary sanction. The violator will deposit guaranty and undertake not to commit the breach within a period to be determined, not exceeding two years. The head of the PPA may add additional conditions to the commitment period to reduce the damage caused by the breach or prevent its recurrence (Section 23AM-23AN). Breach of obligation shall be deemed to be a repeated or continuing breach (Section 23AQ).
5. *Judicial Termination Order (Section 23AX)* – The head of the PPA may apply to the Administrative Affairs Court to request an order for the cessation of processing or the deletion of data where there are reasonable grounds to believe that a violation has been committed or that a violation is about to be committed in one of the following cases:

I. Use of data other than for the purpose for which it was provided;
II. Use of data other than for the lawful purposes of the database or exceeding the permissions of the controller;
III. Data security breach; or
IV. Unlawful provision of data from a public authority.

To issue the order, the Court must be convinced that —

I. A violation is or is about to be committed and is of sufficient severity justifying the issuance of an order;
II. There is no means of lesser harm to prevent the violation; and
III. The damage that may be caused by the violation is greater than the damage that may be caused by the issuance of the judicial order.

Insofar as the order is issued ex parte, it shall not exceed 48 hours and shall not include an order to delete data.

7.4 - Procedural provisions regarding the imposition of monetary sanctions

The Amendment also regulates the procedure for imposing the monetary sanction. Among other things, it was determined that:

1. The head of the PPA is required to announce the intention to charge (Section 23AA) and to give the right of defense before imposing the sanction (Section 23AB).
2. The head of the PPA may reduce the amount of the sanction (Section 23AC) for reasons specified in the Fifth appendix (such as the non-existence of previous violations, taking actions to recur the violation, appointing a DPO where necessary, personal circumstances, etc.) and this shall not exceed 70% unless the amount of the sanction exceeds 5% of the turnover of transactions. In any case, the decision of the head of the authority will be given in writing and in a reasoned manner.

3. In a continuing violation, one-hundredth of the amount imposed will be added for every additional day the violation is committed. In a repeat violation committed within two years of the first violation, the amount will be doubled (Article 23AD).

The Amendment also relates to updating the sanction amounts (Section 23AF), paying the sanction within 45 days from the date of delivery of the demand for payment (Section 23AG), paying additional interest and arrears fees (Section 23AH), and the procedure for collecting debts (Article 23AI).

In addition, the following provisions are prescribed -

1. It is forbidden to impose more than one monetary sanction on one action (Section 23AS).
2. An appeal against enforcement proceedings may be submitted to the Magistrate's Court within 45 days (Section 23AT).
3. The head of the authority must publish, after allowing the violator to present their claims, the financial sanction imposed and details pertaining to it (including the name of the violator). The publication in the PPA's website shall remain for two years for the individual and four years for the corporation (Article 23AU).

The GDPR specifies that each supervisory authority must have the power, provided for in national legislation, to impose monetary penalties. These sanctions are limited in certain violations enumerated in the Regulation to 10 million euros or 2 percent of the total turnover of the previous fiscal year and in other offenses to 20 million euros or 4 percent of the total turnover of the previous fiscal year (whichever is higher) (Article 83). The provision to sanction violations in Israeli law with 5% of turnover does not differentiate based on the type of violation and exceeds the maximum European ceiling.

The California law stipulates an administrative penalty of $2,500 for each violation. If the violation was committed with malicious intent or involves known minors, the penalty increases to $7,500 (Section 1798.155). These funds are transferred to the Consumer Privacy Fund to strengthen privacy protection. The agency considers the level of cooperation received from the violator when determining the amount of the sanction (Section 1798.199.100).

8 - The Amendments introduces criminal offenses related to processing of personal data

The Amendment stipulates that certain actions will be defined as criminal offenses, which the PPA will be authorized to investigate. The new offenses in the Amendment include the following:

1. Interfering with the head of PPA, an investigator, or a supervisor acting on their behalf in the performance of their duties (six months' imprisonment) (Section 23BA).
2. Providing false information in an application for database registration, in a notice of a change in details, or in response to a supervisor and an external expert on behalf of

the authority, with the intention of deceiving them (imprisonment for two years) (Section 23BB).

3. Processing data without permission from the controller (Article 23N).
4. Providing incorrect information in a notification under Section 11 to mislead the person regarding the provision of personal data (3 years) (Article 23BC).
5. Unlawful disclosure of personal data from a public authority to another party (3 years) (Section 23BD).

As mentioned, the European and Californian regulations do not include criminal provisions, although the GDPR expects that each state will define offenses.

9 - Miscellaneous Amendments: From tweaking purpose limitation, to expanding the Notice requirement

9.1 - Purpose limitation

The Amendment sought to "tighten" the provisions of the law that require the use of data only for the purpose for which the data was provided. The amended version states that "no person shall process personal data in a database except for the purpose of the database duly determined for him" (Section 8(b)). The law does not specify where such a determination is made or who determines the relevant law when the only legal anchor for the use of data is consent.

In addition, it is clarified that no person shall process personal data without permission from the controller and must be acted upon within it (Section 8(c)), and that data received in violation of the provisions of the law, or any other law cannot be processed (Section 8(d)(1)).

The European Regulation is different from the Israeli law. The GDPR establishes legal bases for processing data (Article 6), which list several alternatives, including consent, the need to fulfill a contract, a legal obligation, public interest, and more. Hence, the law regarding lawful data processing purposes is clearer in the GDPR. In addition, the general principles of data processing enumerated in Article 5 of GDPR stipulate, inter alia, that the data must be collected for defined purposes, explicit and legitimate, and the processing must be compliant with these purposes unless the processing is carried out for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

In other words, in contrast to the vague wording chosen in the Amendment, EU regulation lays out the legal framework for the type of purposes for which data processing may be permitted, defines that the purposes must be explicitly determined and acted upon, and even lists cases in which it is permitted to process data outside the framework of the objectives. It should be noted that the GDPR stipulates that state legislation must address several issues and determine the clearer frameworks regarding them, among them in relation to the purpose limitation) (Section 6(3)(b)).

The CCPA requires that each business determines its business purpose ("Business purpose") (Section 1798.140(e)). The law states that the use of personal data must be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed or for another disclosed purpose that is compatible with the context in which the personal information was collected..." The California law establishes business purposes that enable the processing of personal data, including auditing consumer interactions, security, debugging, etc. The Agency's regulations created heightened data minimization requirements, providing that collection and use of data should be consistent with the "reasonable expectations" of users (CPPA Regulations, § 7002).

The fact that in Israeli law the only anchor for processing data remains consent, without defining legal purposes for processing information, is set to create difficulties in practice for lawfully processing personal data for legitimate interests, like ensuring security of systems, or combating fraud, as it does not consider legitimate processing as is customary in other legal regimes. As of this date, the Amendment did not grant the authority to impose an administrative sanction for a violation of Section 8(b) referring to purpose limitation. The sanctioning authority is granted only when there is a deviation from the authorization granted or when the data is used for a purpose other than the one for which it was provided (this relates to a violation of Section 2(9) which deals with the limitation of purpose regarding infringement of the "classic" privacy).

9.2 - Notice

The current legal requirement for notifying individuals when their data is being collected (Section 11) will be expanded to include the obligation to provide the following details to the individual from whom the data is requested:

1. The consequences of their refusal to provide information;
2. The name of the controller and ways of communicating with him; and
3. The existence of the right to review and erasure. In this regard, it is notable that the Amendment did not require that the controller specify all the rights of the data subject, which would have ensured that the data subject was informed of the rights available to him by the Mediation Regulations. This issue is even more important because the data subject cannot have knowledge of whether a database is subject to the Mediation Regulations, and therefore, their ability to exercise their rights decreases.

The wording of the Israeli law does not distinguish between a notice given to a person about whom data is requested and a person from whom data is requested.

The European regulations make a distinction between contacting a person directly (Article 13) and collecting data from a third party. When data is collected from another party, the data subject must be notified about the collection of their data (Article 14). In addition to the information required by Israeli law to be provided in a notice to the data subject under Article 13 of the GDPR (equivalent to the Israeli law), the following details must also be provided:

1. Contact details of the DPO;
2. The legitimate interests of the data controller insofar as the data is required for their realization;
3. Recipients to whom data are transferred or categories of such recipient, if any;
4. Whether the data is intended for transfer to a third country or international organization and what mechanism allows such transfer;
5. The retention period of the data or criteria according to which the retention period is determined; and
6. Use of automated decision-making, the meaning and consequences of such use.

In addition, the controller is required to give advance notice before processing data for another purpose, while under Israeli law, the notice is given only upon the initial collection of information.

The CCPA notification requirement requires that the business informs the data subject at or before collecting the personal information. In other words, it is assumed that data cannot be collected from the person directly or from another party without giving notice (Section 1798.100). The business must include the following information in the message: the categories of data collected (regular or sensitive), the purpose for collecting these categories, whether the data is sold or transferred to a third party, the length of time during which the data will be retained, and in the absence of a defined time, the circumstances under which the data will still be kept.

Therefore, despite the expansion of the Israeli law to include additional information added to the provision of notice, other legal regimes still create greater transparency for the data subject. In addition, both the GDPR and CCPA take into account the current reality in which data is often not collected from the data subject. In the Israeli data protection framework, which is based entirely on consent, such a situation creates a paradox: how can consent be obtained if the person concerned is not aware that their data is collected?. However, it is clear that, in reality, such situations where processing of personal data occurs without the consent of the data subject exist (for example, peer feedback at work or a teacher's report on student behavior in a computerized system).

9.3 - Obsolescence

The Amendment revokes the special rule that set the statute of limitations for violations of the Privacy Act at two years (Section 26). Instead, the standard statute of limitations in Israeli law, which is currently set at 7 years, will apply.

9.4 - Strict liability

The Amendment eliminates the criminal offenses prescribed in Section 31A of the Law, which do not require proof of intention ("strict liability").

9.5 - Elimination of database registration fees

The Amendment cancels the provisions in the main law authorizing the Minister to regulate the fees involved in registering a database (Section 36A). It should be noted that, in practice, no such fees have been collected since 2017, when the Privacy Protection Regulations (Fees) were abolished. The Amendment is intended to adapt the arrangement in the main legislation to the policy implemented by the Authority upon repealing the aforementioned regulations.

Registration is not required in the GDPR, and a fee of $400 is charged in the CCPA for registration of data brokers, which is intended to finance the cost of operating the database of such information intermediaries.

10 – Conclusion

The comprehensive legislative Amendment, which was passed on August 5, 2024 and will come into effect in a year after its publication (on August 14), significantly increased the risk of controllers engaging in unlawful processing of personal data in Israel. Considering the gaps between Israeli legislation and other leading privacy and data protection legal frameworks worldwide, it seems that even those who have put in place compliance programs for the strict rules of the GDPR may find themselves at risk of non-compliance with the new Israeli privacy law.

At the substantive level, due to the only legal anchor of consent for lawfully processing personal data, the PPA seemingly has ample scope for guidance and legal interpretation when it applies the law. This creates a certain degree of legal uncertainty and raises a question about the effectiveness of increasing compliance with the law. It can be assumed that, at least regarding the imposition of the high monetary sanctions, and considering that the substantive law mostly remains as originally written in the 1980s, Courts will be called to provide clarity.

Appendix

Below are details of the different levels of monetary sanctions that can be imposed for the various violations by law. The breakdown is according to the lower to higher amount and not according to the order in which the sanctions appear in the legislation.

I. A multiple of NIS 2 (approximately 0.5$) for each person in the database, and if in a database with special sensitivity, NIS 4. (Approximately 1.1$) If the amount is less than NIS 20,000 (approximately 5,400$) and in an especially sensitive database of NIS 40,000 (approximately 10'800$), the amount may be increased up to this amount (Section 23Z(d)). Following are details of the violations for which this sanction may be imposed:

1. an unspecified addressing to a group without giving notice under Section 11;
2. failure to appoint a DPO;
3. processing personal data in the database for direct marketing services without registering the source of the data, the date of its receipt, and registration to whom the data collection was provided;
4. a public authority that has not registered the personal data provided;
5. The database controller who is liable for registration has not corrected a relevant violation ordered by the head of PPA.

II. A multiple of NIS 4 (approximately 1.1$) for each person in the database, and if in a database with special sensitivity, NIS 8 (approximately 2.2$). If the amount is less than NIS 200,000 (approximately 54,000$), the amount may be increased up to this amount (Section 23Z(e)). Following are details of the violations for which this sanction may be imposed:

1. has not stopped committing a declared breach of unlawful processing of data, or not for the purpose for which it was provided;
2. processed data without permission from the controller;
3. Disclosure of data from a public authority outside the framework of the arrangement in Chapter IV for the transfer of data between public bodies.

III. A multiple of NIS 50 (approximately 13.5$) for each person to whom the request was made, and if data is of special sensitivity - NIS 100 (approximately 27$). If the amount is less than NIS 30,000 (approximately 8,100$), it may be increased up to this amount (Section 23Z(c)). Following are details of the violations for which this sanction may be imposed:

1. failure to give notice under Section 11 (request for data);
2. Failure to provide notice when contacting direct marketing following the provisions of Section 17F(a);
3. A public authority that has not announced that it regularly discloses data.

IV. Processing data for purposes other than those of the database may constitute a breach, resulting in a sanction ranging from NIS 2,000 to NIS 160,000 (approximately between 540$ - 46,000$), according to the security levels classification of the database stated by the security regulations (note: it is not clear what the connection between the breach and the classification determined in the security regulations) is (Section 23Z(f)).

V. A monetary penalty in the amount of NIS 15,000 may be imposed for the following violations (Section236(b)) –

1. failure to exercise the right of review;
2. correction of data without notification to anyone who has received data from it;
3. failure to provide notice of non-correction of data;
4. non-correction of data;
5. Failure to delete from a database used for direct marketing (Note: This is a problematic provision because the source of data may beused for a legitimate businessand the direct marketing was carried out as part of the management of the business. The breach should have been defined as such when a referral was made where the data subject requested not to be contacted again);
6. We will not respond to the demand of a database for direct marketing services not to transfer to another.

VI. A monetary penalty in the amount of NIS 150,000 (if more thanone millionpeoplethe fine is NIS 300,000) may be imposed for the following violations (Section236(a)) –

1. Non-registration (only if trading information)
2. Include incorrect details in the application (allegedly also a public body), or did not announce a change in details.
3. Failure to provide notice or change details required in the notice
4. Process personal data for direct marketing services without one of the purposes being written as such.
5. A public body that has not informed the head of the authority that it receives data on a regular basis from another body

Failure to provide information, documents, or computer material to PPA's Supervisor may result in the imposition of a financial sanction of NIS 300,000 (approximately 809,000$) (Section 23Z(g)). It should be noted that this is one of the highest sanctions, regardless of the database's size, the data's sensitivity, or other relevant circumstances.

VII. Violation of the Data Security Regulations (Third Appendix) will result in financial sanctions ranging from NIS 1,000 to NIS 640,000 (approximately $270 to $173,000), depending on the required level of security in the database as specified in the Data Security Regulations.

VIII. For violating the provisions of the Mediation Regulations, monetary sanctions may be imposed in varying amounts (Fourth appendix) (Section 23Z(i)). These amounts correspond to the violation of rights under the law and the scales prescribed in the subSections of Section 23Z of the Law.

Washington, DC | Brussels | Singapore | Tel Aviv

info@fpf.org

FPF.org