ISRAEL
TECH POLICY INSTITUTE

November 17, 2021

Review of the Israeli Protection of Privacy Bill (Amendment 14), 2021

Adv. Rivki Dvash, Senior Fellow*

Introduction

Background

The Israeli Protection of Privacy Law was passed in 1981. Since 1996, no major amendments were made to it. The Israeli law has been widely criticized for being outdated, and for improperly regulating the right to privacy given current technological challenges. The entry into effect of the European General Data Protection Regulation (GDPR) in May 2018 only widened the gap between the current legal and regulatory situation in Israel, as opposed to Europe and other countries.

On November 7, 2021, the Israeli cabinet approved the government bill for amending the Protection of Privacy Law (Protection of Privacy Bill (Amendment 14), 2021). The following reviews the proposed amendment and explains it in layperson terms, for those interested in learning more about the key changes it promotes.

Previous recommendations and proposals for amendments

A proposal to amend the law, including recommendations to reduce the obligation of database registration and expand the enforcement powers of the Registrar of Databases, was proposed to Minister of Justice Tzipi Livni as early as in January 2007 by the Team for Reviewing Legislation in the Database Area (Schoffman Report).[1] Near the end of the team's work, it was decided to establish the Law, Information and Technology Authority (today, Privacy Protection Authority).

* Translated into English by Ami Asher.

[1] Full disclosure: the author coordinated the team and formulated its summary report.

In August 2012, the Ministry of Justice published a legal memorandum[2] for reducing the database registration duty,[3] and replacing it by a documentation requirement. This memo was not promoted as a government bill.

Regarding expanded enforcement powers, a government bill was twice proposed.[4] In November 2011, the bill was passed in the Knesset at first reading, and a single meeting was held to discuss it at the parliamentary Constitution, Law and Justice Committee (June 2012). In a subsequent Knesset, the bill was reintroduced in February 2018, and passed at first reading the following March. However, as the Knesset was disbanded and several elections were held in short sequence, the bill was no longer promoted.[5]

The present bill is based on the previous ones, with some changes. In addition, the Ministry of Justice declared in its annotation that it is currently working on an additional, substantial and comprehensive bill.

The Israel Tech Policy Institute's position

The position of the Israel Tech Policy Institute (ITPI) is that it is vitally important and urgent to update and adjust Israel's privacy protection regulations to current development and to the emerging global standard. The fact that Israel remains with an outdated law that is unsuited to the privacy protection challenges of the current era affects the protection given to its citizens, whose personal information is held by both the government and the private sector. It also affects the ability of Israeli corporations and businesses to operate in the global economic sphere, which requires meeting personal information protection requirements to enable the flow of private information between countries, including Israel.

The ITPI's recommendations for the required legislative arrangements are detailed in the response submitted by Managing Director Adv. Limor Shmerling Magazanik to the Ministry of Justice's call for comments (December 2020).

*

[2] A *legal memorandum* is a document distributed by the government to receive comments from the public, prior to formulating a government bill.
[3] Privacy Protection Legal Memorandum (Amendment No…) (Minimizing Registration Duty and Requiring Management Regulations and Working Procedure and their Documentation), 2012 (**all links herein are to Hebrew documents**).
[4] Protection of Privacy Bill (Amendment 12) (Enforcement Powers), 2011; and Protection of Privacy Bill (Amendment 13), 2018, respectively.
[5] According to Knesset rule of continuity, it is permissible to continue debating a bill only for two Knessets in a row. Thereafter, the government must reintroduce the bill.

The Proposed Amendments

Revised definitions

It is proposed to revise the definitions in the law, in a way that would better clarify the terms it uses. In some definitions, an attempt has been made to bring the terms in the Israeli law closer to those of the GDPR. The main revisions are as follows:

1. "Holder". The revised definition is designed, according to the annotation, to distinguish between those holding a database following a service provision contract and the owner of the database itself or any of the owner's employees. Note that according to the proposed formulation, it appears that the employees of the person's controlling the database may also be considered "holders".
2. Adding a definition of "database controller" (today there is no legal definition for the term "database owner", despite the common usage of this term) – the person who determines the database purposes (alone or with others), or who has been legally authorized to manage a database is considered the database controller.
3. Adding a definition for "biometric identifier".
4. Changing the definition of "information". This revision narrows the gap between the current formulation and the interpretation given to it in case law, and brings Israeli law to a closer match with the EU definition. From an outdated definition that referred to a list of ambiguous issues, it is proposed to define "information" as "data related to a person identified or identifiable, whether directly or indirectly, using reasonable measures, including a biometric identifier, an ID number, or any other unique identifier".
5. A list of issues considered "particularly sensitive information" (replacing the current definition of "sensitive information"). This definition is relevant for the purpose of database registration duties as well as for the purpose of the amount of the financial sanction that could be imposed on the controller in case of violation, as detailed below.

Reducing the scope of database registration duty

The recommendation to minimize the registration duty originates in the 2007 Schoffman Committee Report. Since then, and as also indicated in the bill's annotation, the database registration regime has been completely canceled in Europe. This is due to the understanding that this bureaucratic burden offers little benefit, if any, imposing on both the authorities and the database owners duties that divert resources from core activities designed to protect privacy. *Despite the above, the Ministry of Justice has decided not to revoke this duty*. The

partial explanation provided is that "According to the view of the professionals in the Privacy Protection Authority, it is important to retain said duty with regard to particularly large database that form the greatest risk to the privacy of personal information".

Also notable is the fact that the bill does not address the risk caused by creating such a registry. As opposed to the Israeli public, which apparently assumes that every entity and business known to it keeps a database, the existence of a registry that is supposed to contain all large and sensitive database may in itself be a key target for those seeking to identify high-quality databases for fraudulent or attack purposes, even if they are not too familiar with the Israeli market. It appears no appropriate attention has been devoted to this issue, also given the type of information required of controllers upon registering their database, as suggested by Article 9 of the law (the change proposed to which is minor).

Comparison between the current and proposed registration duty requirements

	The current requirement	***The proposed requirement***
Size	Every database on over 10,000 persons must be registered	Every database on over 100,000 persons must be registered, *only* if one of the following applies: 1. Data collected not from the individual, on their behalf or with their agreement 2. Public entity 3. Database whose main purpose is providing direct mailing services
Sensitivity	Every database containing sensitive information, as defined in the law, must be registered	Every database containing particularly sensitive information, as defined in the new law, and includes over 500,000 persons, must be registered Such a database on 100,000-500,000 persons will require reporting to the Database Officer – including both its very existence and the type of information in it.

Data collection method	A database whose information has not been submitted by the persons themselves, on their behalf or with their agreement must be registered	A database whose information has not been submitted by the persons themselves, on their behalf or with their agreement must be registered, but *only when containing more than 100,000 persons*
Public database	Every public body database, as defined in Article 23, must be registered	Every public entity database must be registered, so long as it is a public body subject to *Article 23(1)*, and so long as the information is about more than 100,000 persons Excluded from this requirement are entities defined as "public" in the Protection of Privacy Order (Determination of Public Bodies), 1986
Direct mailing services	Every database used for direct mailing services must be registered	A database whose *main purpose* is collecting information for delivery to another as an occupation (including also direct mailing services) and a database on *over 100,000 persons* must be registered
Reducing/ expanding registration duty	The Database Officer may *impose registration* also in the case of databases exempted from registration duty	The Database Officer may order a certain database to *register*, despite being exempted therefrom under the law. Conversely, it may *exempt* a certain database from registration despite a legal duty thereto.
Managing & maintaining the database	So long as 90 days have not passed since the registration request, using a database that requires registration is prohibited	The controller may not manage or maintain the database only if the Database Officer has informed them of refusing to register the database or of suspending registration, after having been given a hearing right. Therefore, once the registration request has been submitted, the database owner may continue managing and maintaining it.

Determination of violations and offenses

Defining new violations: Legal database management

The bill proposes to delete Article 8(b) that states that the usage of a database requiring registration will be limited strictly to the purpose for which the information has been provided in the first place. In lieu of this article, it proposes to impose several duties on the database owners, whose dereliction will constitute a violation:

1. *Adding Article 8A* – Managing and maintaining a database will be allowed only if the information it is included and managed in it subject to the provisions of the Protection of Privacy Law and the provisions of any law, independently of the database registration duty. Should the Database Officer find that legal provision have been violated, the Database Officer may notify the database controller or holder of the violation, and set a period within which the violation must be discontinued.
2. *Adding Article 10B* – Prohibiting a database controller or holder from using information or "data on a person's private affairs" for any purpose other than that for which it has been provided. Note that in view of the expansion of the definition of "information" it appears that the use of the ambiguous terminology "data on a person's private affairs" in Article 2(9) creates uncertainty, particularly as Article 10B is supposed to be the violation article, and as such should create certainty with regard to the causes of the violation.
3. *Adding Article 10C* – Prohibiting the use or holding of information or "data on a person's private affairs" (see above comment on this terminology) derived from a database without the controller's permission or in infringement thereof.

Defining new offenses

In Chapter D(4), the bill defines several new criminal offenses:

1. Disrupting the work of the Database Officer, an inspector or an investigator operating by force of law (§23/45)
2. Deceiving the Database Officer or an inspector operating on their behalf (§23/46)
3. Seeking to store or use fraudulently obtained information in a database (§23/47)
4. Using information from the database for a purpose other than that for which it has been provided (§23/48)
5. Using or holding information without legal authorization (§23/49)
6. Divulging information by a public body without authority (§23/50)

Note that apart for the deception and fraudulence offenses (2 & 3), in the other cases it is not stated that *criminal forethought* is required. Thus, the list includes *negligent* acts as criminal offenses publishable by six months to five years' imprisonment, depending on the offense.

New administrative sanctions

The bill expands the administrative enforcement measures available to the Privacy Protection Authority, including financial sanctions, administrative warnings, and undertakings to avoid violations, as follows.

Financial sanctions

According to the proposed arrangement, the basic amount of financial sanctions will be affected by the size of the database and the type of information in it. This amount may be doubled according to the type of violation. Note that at this time, the amount of administrative fines the Authority may impose, subject to the Administrative Offenses Regulations (Administrative Fine – Protection of Privacy), 2004, is limited to NIS 2,000-5,000 per individual and NIS 10,000-25,000 per corporation.

The following are the basic fines stipulated in §23/22(a):

No of individuals	*Ordinary information (NIS)*	*Particularly sensitive information (NIS)*
Up to 1,000	5,000	50,000
1,001-10,000	10,000	100,000
10,001-100,000	20,000	200,000
100,001 - 1,000,000	40,000	400,000
Over 1,000,000	80,000	800,000

The basic amount is imposed on violations listed in §23/22(b) and includes, for example, violations of registration duty, failing to inform of regularly receiving information between public databases, failing to submit a document or a computerized copy thereof to an inspector, etc.

An amount double the basic amount may be imposed only on an individual, including a corporation (but not a public body) for violations listed in §23/22(c), such as denying the right of review stipulated in §13, not appointing an officer in charge of protecting personal information, and addressing an individual by direct mailing in violation of the law.

An amount quadruple the basic amount may be imposed on "anyone" (be they an individual or a public body) who has violated §23/22(d), which refers to the use of information for a purpose other than for which it has been provided, such that the violation has been made by the database controller, holder or manager (the manager is excluded from the violation of §§(1)).

In addition, financial sanctions that may be imposed for violating regulations determined under this law have been added. The main implication of this is with regard to violating the Protection of Privacy Regulations (Information Security), 2017; from now on, several violations can lead to administrative sanctions. The amounts stipulated in this addition range from NIS 1,000-160,000, and unlike the provisions of the main text of the law, there is a distinction between a database held by an individual and one held by a corporation.

The proposed law stipulates the procedures for imposing financial sanctions, including the right of hearing and the Database Officer's power to reduce or revoke the sanction, the punitive implication of ongoing or recurring violation (within two years), etc. It is also proposed that for a single act that involves several violations, no more than one financial sanction will be imposed (§23/40), and in general, that both a criminal and an administrative procedure may not be initiated with regard to the same violation (§23/43). The bill also stipulates the Database Officer to publicize all administrative sanctions imposed for violations on the Authority's website (§23/42).

Administrative notice

The Database Officer may replace the financial sanction with an administrative notice, according to procedures to be determined thereby, subject to approval by the Attorney General or a deputy authorized thereby for this purpose (§23/32-34).

Undertaking to avoid a violation

The Database Officer may replace the financial sanction with an undertaking to avoid a violation, according to procedures to be determined thereby, subject to approval by the Attorney General or a deputy authorized thereby for this purpose. The violator will attach to said undertaking – for a predefined period that will not exceed two years – a collateral at the amount of the financial sanction. The Database Officer may forego the deposit of the collateral or reduce its amount (§23/35-39).

*

Enforcement powers

Administrative oversight powers

In order to implement the oversight powers of the Privacy Protection Authority, broad powers are proposed for inspectors, including those stipulated in §23/10(a):

1. Demand that any person identify themselves, including by presenting official ID documents, and including that person's address;
2. Demand any data or document (including "output" as defined in the Computer Law, 1995;
3. Obtain a copy of computer materials that include system data or sample information *to the minimal extent required to accomplish the purpose of supervision* (this provision is unique to administrative oversight powers in terms of its caution, given the fear lest the Authority collect too much private information). Sample information collected subject to this provision will be erased to the extent it is no longer required for oversight procedures and within three years at the most, unless it is required for the purpose of procedural management (§23/10(b));
4. Enter premises where there is reason to believe a database is used,[6] unless these are residential premises, in which case a court order is required.

Further provisions proposed for the purpose of administrative oversight:

1. The inspector must be identified, unless such identification could prevent them from performing their duty or threaten their safety (§23/11).
2. The inspector must be a public servant (the proposed §10(e)), but a contractor employee with relevant experience and expertise may be employed, under the conditions stipulated in §23/12.
3. Wherever an authorized and qualified inspector has reason to believe that legal previsions have been violated, they have the power to issue a search and seizure order, as well as a computer material access order (§23/13).

Criminal investigation powers

Whenever a criminal offense is suspected, an *investigator* acting on the Authority's behalf is authorized to perform the following (§23/15):

1. Investigate an individual. The investigator will also be authorized to detain an individual and investigate them on site (§23/15(c)-(d));
2. Seize every object the is cause to believe may be related to the offense;

[6] The proposed article also includes entry into premises "that contain a database" (§23/10(a)(4)), however, given the broad definition of "use", this appears to be redundant.

3. Request a search and seize order, or a computer material access order.

Whenever acting on their criminal enforcement authorities, the investigator must be identified, apart for the exceptions made in the case of inspectors. Moreover, the investigator must wear a uniform, as instructed by the Database Officer, so long as that uniform does not appear to be that of a police officer (§23/16).

Note that during the Knesset voting on the Privacy Bill in 2011, Chair of the Science Committee MK Meir Shitrit questioned the scope of powers the law sought to provide the Authority, saying that "*it's [like] creating another police force. I'm not sure it's the right thing, I think it needs to be examined, and with all due respect to the Ministry of Justice's enthusiasm – it's a unit within the ministry – the measures must be attenuated*". We believe it is worthy of serious consideration whether the Authority's powers should not remain within the strict administrative scope, while leaving criminal enforcement in the hands of the entities specializing in it.

Enforcement in security organizations

The law stipulates special arrangements with regard to its enforcement in security organizations, as defined in the bill (§23/17(a)(1)-(9)),[7] plants defined as such by the Minister of Defense (§23/17(10)), and bodies determined in an order by the Minister of Defense, with the Minister of Justice's consent (§23/17(11)). Orders applying to security organizations may include organizations concealed from public review (§23/17(c)).

For the organizations listed in the fifth addendum to the Regulation of Security in Public Bodies Law, 1998,[8] these powers will not be implemented until such time as a procedure governing such supervision is determined jointly by the Privacy Protection Authorities and the Cyber Authority (§23/17(b)).

In every security organization, a privacy inspector will be appointed for a period of no more than seven years, and will be subordinated to the head of that organization or to another senior employee subordinated to the head of that organization. The internal inspector's term in office will not be suspended, and they will not be removed from office other than in consultation with the Database Officer (§23/18).

The internal inspector will be made responsible for inspection activities and for ensuring compliance with the law in the organization in question. The inspector will report to the Database Officer about the findings of their inspection and review, subject to classification

[7] Israel Police, the IDF, the ISA (*Shabak*), the Mossad, the Cyber Directorate, the Witness Protection Authority, the Israel Prison Service, the Ministry of Defense and its dependent units, state-owned corporations, and public and private infrastructure companies.
[8] Note that the law applies to a long list of bodies, which also includes government ministries and their dependent units, state-owned corporations, and public and private infrastructure companies.

limits (§23/19). The Database Officer may instruct the inspector to perform complementary actions and to impose administrative measures subject to Section D3 of the law, or pursue criminal investigation procedures subject to their authorities and to the extent no other authority has the power to investigate the organization in question (§23/21).

In addition, the inspector will make sure all faults have been corrected, will provide training and guidance on privacy protection, and submit an annual report on their activities to the head of the organization and to the Database Officer (§23/19).

Finally, the internal inspector will have the authorities given to Authority supervisors, mutatis mutandis (§23/20).

Information Security

Adding an article that authorizes the Minister of Justice to determine provisions in the information security area (adding §17(b)). The regulations subject to this addendum require the Prime Minister's Agreement, and for certain organizations (listed in items 2-3 under the first addendum), consulting with the Minister of Defense is also required.

Conclusion

We hope that the promotion of this bill by the Minister of Justice will lead the Knesset to initiate a professional dialogue with all relevant stakeholders in order to formulate a legal arrangement that appropriately deals with the current challenges to privacy. The approval of the law memorandum in the Ministerial Legislation Committee is a welcome first step essential for moving forward.