ISRAEL
TECH POLICY INSTITUTE

Reducing the gap between Israel's Data Protection regime and the GDPR – A governmental proposal

By: Adv. Rivki Dvash

It was recently published that the Israel Ministry of Justice (MoJ; through the Privacy Protection Authority and the Department of Advisory and Legislation) seeks to promote an amendment to the Israeli Privacy Protection Regulation, for assimilating several of the General Data Protection Regulation (GDPR) principles into the Israeli legal framework. This advancement of legislation stems from an attempt to maintain the European Union (EU) recognition in Israel as an adequate country that Israel received in 2011, in accordance with the conditions of former Directive 95/46/EC (article 25).[1]

In this review, we shall briefly present the background to this Initiative and the difficulties it raises.

The EU adequacy in Israel – background

On January 31, 2011, following the establishment of ILITA – The Information, Law and Technology Authority in 2006 (the former name of the Israeli Data Protection Authority), and following the MoJ's commitment to promote legislative amendments which will narrow the gaps between Israeli Law and the EU regime on data protection issues, Israel was recognized as an adequate third country.

However, since 2007, the provisions of Israeli law have not undergone far-reaching changes to ensure a data protection regime that complies with EU principles, except for the enactment of the Privacy Protection Regulations (Data Security) 5757-2017.

Such modifications to the Israeli data protection regulation are essential, due to key differences between the two regimes, such as –

- Consent is the single legal basis under Israeli regulation;

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

- There is no designated directive for protecting sensitive data (except for the obligation to register a database, which remains a broad obligation in Israel);
- Under Israeli law, data subjects are merely entitled few rights, which, are not always protected, in practice in the field (such as the duty to notify data subject when collecting data from him and the right to correct and review information).

In 2016, the EU has enacted the GDPR . The regulations, which came into force in May 2018, extended the available protections for personal data and transformed the data protection regime in Europe, in a way that dramatically affected data protection regimes outside the EU, as well.

Article 45 of the GDPR stipulates the adequacy mechanism with certain changes from Directive 95/46/EC, including the need to conduct an examination of the compliance of adequate countries, at least once every four years. The European Data Protection Board (EDPB) is currently examining the compatibility of a number of countries, including Israel.

In examining the adequacy of a third country (a country that is not part of the EU), an identity between the arrangements is not necessary, but it is required, however, that core principles of the GDPR are manifested in the latter's regulation. The EU is also required to examine the existence of –

1. A national commitment to human rights;
2. The existence of an independent and functioning authority;
3. A commitment to international organizations;
4. A suitable protection from public authorities' access to personal data in the context of individual surveillance.

Adequacy principles

In a paper by the Article 29 Data Protection Working Party that, consolidating the principles according to which the Commission shall examine the adequacy of third countries, the following issues are referred to -

1. Basic data protection concepts or principles should be in place. In Israel, there are few gaps, especially concerning definition of terms, such as "data" and "sensitive data"; and there is no definition in place for "processing". Furthermore, the arrangement of the Israeli Privacy Protection Law is based on the regulation of "databases" rather than "data processing".

2. Data must be processed in a lawful, fair and legitimate manner.

3. Data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of the processing.

4. Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are processed. There is currently no provision in Israeli law regarding an obligation for the information to be accurate and up-to-date, however, the database controller is required to inspect excess data, annually, according to article 2(c) of the Data Security Regulation (DSR).

5. Data should be kept, generally, for no longer than is necessary for the purposes for which the personal data is processed. There is currently no similar provision under Israeli law.

6. Any entity processing personal data should ensure that the data is processed in a manner that ensures security of the personal data. Israeli law meets this requirement in light of the DSR directive.

7. Individuals should be informed of all the main elements of the processing of their personal data in a clear, easily accessible, concise, transparent and intelligible form. There is currently no similar provision under Israeli law, although there is a more limited notification obligation when data is collected from the data subjects (article 11 of the Privacy Protection Act – PPA).

8. The data subject maintains rights of access, rectification, erasure and objection. The exercise of those rights should not be excessively cumbersome for the data subject. There is currently no similar provision in place, under Israeli law, although such (related) rights of access and rectification, are in place (article 13-14 of PPA).

9. Further transfers of personal data should be permitted only where the recipient is also subject to rules affording an adequate level of protection.

10. Specific safeguards should be in place where 'special' categories of data are involved. There is currently no similar provision in the Israeli law.

11. Where data is processed for the purposes of direct marketing, the data subject should be able to object. Israeli law complies with this requirement in light of articles 17F(b)-(c) of the PPA.

12. Decisions based solely on automated processing (automated individual decision-making), including profiling, which produce legal effects or significantly affect the data subject, can take place only under certain conditions established in the third country legal framework. There is currently no similar provision in the Israeli law.

13. As per procedural and enforcement mechanisms:
    13.1 A supervisory authority, tasked with monitoring, ensuring and enforcing compliance with data protection and privacy provisions should exist. Since 2006, there is a DPA in Israel;
    13.2 A high degree of accountability and of awareness among data controllers and those processing personal data on their behalf, for their obligations, tasks and responsibilities; And a high degree of accountability and of awareness among data subjects for their rights and the means of exercising them;
    13.3 Data controllers and those processing personal data on their behalf must comply and be able to demonstrate such compliance in particular to the competent supervisory authority. Israeli law meets this requirement in light of the DSR directive.

13.4 The data protection system must provide support and assistance to individual data subjects in exercising their rights, as well as appropriate redress mechanisms.

14. In addition, the Commission is to examine in third countries the existence of protections limiting the intervention of law enforcement and national security authorities in the protection of fundamental rights. Among other things, it will examine whether –
    14.1 Processing is based on clear, precise and accessible rules (legal basis);
    14.2 Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated;
    14.3 The processing is subject to independent oversight; and
    14.4 Effective remedies are available to individuals.

Hence, under the current Israeli data protection regime, there are still gaps to be filled between the former and the minimum GDPR principles required for preserving the Israeli adequacy.

The Israeli MoJ proposed amendments

As noted, on July 5, 2022 the MoJ presented its proposal for reducing the gap between the local data protection regime and the EU, in order to preserve the EU adequacy, before a group of private market lawyers. There is still no official wording for the new proposed regulation; however, it seems likely that it will be published soon.

The proposal seeks to amend the regulations established by article 36(2) of PPA, the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001. In the proposal laid out at that meeting, the MoJ advised imposing additional obligations on data controllers with regard to data transfers from the EU, unless the data came from the data subject itself.

According to a document presented to the participants in the meeting, the MoJ considers adding four main obligations to the currently existing ones –

1. **Deletion of data upon request** – a controller will be required to delete data at the request of the data subject to the extent that the source of the data or its

continued use is contrary to the provisions of the law or to the extent that the information is no longer needed for the original purposes. The deletion obligation is proposed to include a number of exceptions, such as freedom of expression, another obligation under the law, protection of public interest (including for archiving and research purposes), protection of a legitimate agreement, or implementation of an international agreement to which Israel is a party.

2. **Data retention** – a controller will be required to implement mechanisms that will ensure the deletion of data from the moment the data is no longer required for the original purpose. Such deletion is not required where the information was anonymized, or if the data is required for one of the exceptions mentioned in relation to deletion of data.

3. **Data accuracy** – a controller will be required to produce mechanisms that will ensure that the data in the database is correct, complete, clear and up-to-date. Where it is found that the information is inaccurate, the controller must act to correct, or delete the information.

4. **Notification** – The controller will be required to inform the data subject soon after receiving the data, and no later than one month thereof, of the controller's identity and his contact details; the purpose for which the data was transferred; the type of data transferred; and the data subject rights. Insofar as there is an intention to transfer the data to a third party, the controller is required to inform the data subject the same information in relation to that third party.
   There are exceptions to this section, such as, where it is reasonable that the data subject is aware of the details of the data transfer; the controller does not know the contact details; there is a legal obligation of confidentiality on the disclosure of information; the notification may harm a person's living or well-being.

In addition, the Israeli MoJ proposes to extend the definition of "sensitive data" so that it also includes information about a person's origin, or membership in a workers' union. The proposal is to extend the definition only in relation to data transferred from the EU, unless the data were received from the person himself.

Difficulties with the Israeli proposal

The MoJ's proposal raises a number of difficulties, which we shall briefly review:

1. **The ability to presently amend legislation** – it is doubtful whether under the current political situation in Israel, where elections have been decided, the MoJ will be able to pass amendments to regulations that also require the approval of the Israeli parliament's (the Knesset) Constitution, Law and Justice Committee.

2. **Other crucial gaps** – as the review of EU requirements shows, it is clear that the proposed amendment improves the Israeli regime in a way that reduces the gap between the EU and Israel regime, but not entirely.

3. **Unnecessary and unreasonable regulatory burden** – the proposed amendments distinguish between rights associated with data originating in the EU, and data originating in Israel or other countries. It should be clarified that this is not a distinction between the rights of Union citizen and other citizens, but a distinction relating to the source from which the data was obtained. For example, an Israeli citizen whose data is transferred from an educational institution located in one of the EU countries will be entitled to data protection privileges, while an EU citizen whose data is transferred from an educational institution located in Israel will not enjoy such privileges. Incidentally, given the increasing use of cloud storage, the question of the geographic source of data becomes even more complex and uncertain.
   It should be emphasized that such a distinction, even if possible in terms of legislation, is more complex on a practical level when a data controller is required to comply with different sets of provisions, according to the source of the data at his disposal. The difficulty is particularly exacerbated given the fact that the MoJ is in the process of amending the principal privacy protection legislation, which contains additional adjustments to be imposed on data controllers in the future.

4. **Discrimination** – the proposed amendments potentially discriminate, by creating a parallel system of rights. Anyone whose data came from the EU will enjoy greater protection than those whose data originated outside the EU. To

the extent that the obligations mentioned in the proposal can be embedded in regulation, it is suggested that these rights apply to all data subjects – regardless of the geographic origin of the data.

5. **Transfer of additional information** – it should be borne in mind that the proposed arrangement potentially creates a way around it. According to the requirements of the EU, the transfer of additional information should also be subject to the minimum rules required by the Union. Hence, according to the proposal, the data controller will be able to receive data from the EU, keep it in Israel in a way that requires the protection of additional rights, but upon transfer to another controller, similarly situated in Israel, the original controller will be "released" of his obligations.

In conclusion

Following the timetable set by the EU, and the fact that the MoJ is delayed in finding a comprehensive and appropriate responses to the gaps that opened up between the Israeli and European arrangements, the MoJ opted to examine the advancement of a partial arrangement, which, in itself, raises many difficulties.

Despite the critical need to preserve EU-Israel adequacy, and the broad implications of removing the adequacy, especially for small businesses, it is proposed that Israel considers promoting a comprehensive and appropriate legislative amendment as necessary, and examines, in the interim, the creation of similar agreements with the United States.

In the meantime, and if the acknowledgment in Israel as an adequate country is removed, it is proposed that the PPA assists small and medium-sized businesses in creating templates for potential agreements that will make it easier for them to sign individually with European companies, where applicable.