TABLE OF CONTENTS

March 2024

1. GOVERNING TEXTS

1.1. Legislation

There is no equivalent legislation in Israel for the Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) ('the ePrivacy Directive') that establishes specific obligations regarding the collection of data from terminal equipment via cookies or similar technologies.

However, it has been argued that the Protection of Privacy Law, 5741-1981 (unofficial translation) ('PPL') requires informed express or implied consent for some uses of cookies, especially where they involve the transfer of personal information to third parties.

1.2. Regulatory Authority Guidance

There is no general guidance, but in the context of digital wallets, the Privacy Protection Authority ('PPA') recommended obtaining consent for collecting data from mobile phones.

2. DEFINITIONS

Cookies & similar technologies: There is no definition of 'cookies' in the Israeli law.

Consent: The PPL defines 'consent' as informed, express, or implied consent. In some instances, however, including a controller to controller transfer, the PPA suggests express consent is needed.

Personal data: At the time of writing, the PPL defines the term 'data' as information on a person's personality, personal status, intimate affairs, state of health, economic status, vocational qualifications, opinions, and beliefs, but the law also protects 'personal affairs,' a term that the law does not define and that courts have interpreted broadly.

An amendment under debate in the Israeli Parliament would, if enacted, define 'personal data' as follows: 'information relating to an identified or identifiable person; an identifiable person is someone who can be reasonably identified, either directly or indirectly, including by identifiers such as a name, an identification number, biometric data, location data, online identifiers, or other data related to the physical, health, economic, cultural, or social context of that person.'

Data processing: The PPL defines 'use' as including disclosure, transfer, and delivery. An amendment under debate in the Israeli Parliament would, if enacted, define 'processing' to cover any transaction or transfer involving personal data, including receiving, collecting, storing, copying, using, browsing, disclosing, transferring, submitting, or granting access.

Online identifiers: There is no definition of the term 'online identifiers' in Israeli law.

3. CONSENT MANAGEMENT

3.1. Is consent required?

There is no need for consent for the mere placing or reading of cookies. However, if cookies are used as a mechanism for processing personal information, especially when sharing it with third parties, consent may be required as a matter of the PPL. In several pending cases it is alleged that explicit consent is required for the use of cookies, especially when using the services of third parties, but the question remains unsettled.

3.2. Conditions for valid consent

If needed, consent should be informed (which requires notice), but consent may be express or implied. Guidance by the PPA recommends explicit opt in consent in some circumstances, but strictly speaking this is not statutorily required.

3.3. Analytics and audience measurement cookies

There are no specific requirements or guidance regarding consent for analytics and audience measurement cookies in the Israeli law. If measurement involves the transfer of personal data to third parties as controllers, especially out of the country, this may require obtaining consent (in the broad sense as defined under Israeli law).

3.4. Exemptions

As mentioned, there is no specific law addressing obligations related to cookies as such. Thus, there are no exemptions for these requirements in Israel. However, it is likely reasonable to assume that collecting information via cookies and similar tools for necessary operational purposes does not require explicit consent in Israel, as such a choice is not feasible in this case.

3.5. Cookie information requirements

There is no specific law in Israel that explicitly requires notification for the use of cookies. However, if cookies are used to collect personal information, there is an obligation to inform users in connection with the collection of such data. This requirement is typically reflected in the privacy policy. These requirements come on top of any contractual requirements imposed by some companies.

3.6. Cookie consent mechanism

There are no specific requirements in Israeli law at the moment. There are a few pending proceedings in courts that may lead to clearer determinations regarding this subject.

3.7. Cookie walls

There are no specific requirements regarding cookie walls in Israeli law.

3.8. Consent duration

There are no provisions on this matter.

4. COOKIES & THIRD PARTIES

There are no specific requirements in Israeli law regarding cookies/similar technologies third party access. However, in some cases, providing access to third parties can raise privacy issues and therefore privacy laws will apply.

4.1. Conditions for placement of third-party cookies

The placement of third-party cookies may require consent if they serve as a mechanism for transferring personal information between controllers. In several pending cases in Israel, it is alleged that explicit consent is required for the use of cookies, especially when using the services of third parties, but the question remains unsettled. Consent is not required for the mere placement of cookies (or third-party cookies), but rather their use which may result in personal data reaching third parties. Additionally, we note that in general, the transfer of personal information to a third party for the purpose of providing their services (for example, transferring information to a supplier acting as processor) is usually possible based on notification and implied consent.

4.2. Roles and responsibilities

Israeli law does not impose specific requirements regarding the mere placement of cookies, including third-party cookies. However, when third-party cookies are used as a means of transferring personal information between controllers, consent may be required. In several pending cases, it is alleged that explicit consent is required for the use of cookies, especially when using the services of third parties, but the question remains unsettled.

When cookies are used to collect personal information, there is an obligation to inform users about the collection and uses of such data. This requirement is typically reflected in the privacy policy.

4.3. International data transfers

The Privacy Protection (Transfer of Information to Databases Abroad) Regulations, 5761-2001 ('the Regulations') restrict data exports. According to those regulations, personal data can be exported out of Israel through one of the following ways:

- data may be transferred to a country whose laws guarantee a level of data protection equivalent to that prescribed by Israeli law; or
- data may be transferred under specific conditions, including:
    - when the data subject has consented to the transferring of personal data out of Israel;
    - if obtaining consent from the data subject is impossible and the transfer is crucial for their health or physical well-being;
    - when data is transferred to a subsidiary of the Israeli controller;
    - when the data is transferred to a person bound by an agreement with the controller of the database from which the data is transferred, to comply with the conditions for the ownership and use of the data applying to a database in Israel;
    - if the data was publicly accessible or inspected by legal authority;
    - when data transfer is vital for public safety or security;
    - when the transfer of data is mandatory according to Israeli law;
    - when the data is transferred to a country that is part of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108');
    - when the data is transferred to a country that receives data from European Member States, under the same terms of acceptance; or
    - when the data is transferred to a country that the Registrar of Databases announced that it has an authority for the protection of privacy, after reaching an

arrangement for cooperation with the said authority.

The Regulations also require data exporters to ensure, in writing, that the importer takes sufficient measures to protect the privacy of the individuals whose information was provided. Additionally, the data exporter must ensure that the data will not be transferred to any other third party. The PPA recently clarified that the meaning of 'will not be transferred to any other third party' is 'will not be transferred to any other third party without the prior consent of the data exporter' (which can be more convenient for situations such as transferring of personal data to a data processor or subprocessor).

Israeli law does not specifically refer to the export of data in the context of cookies.

5. COOKIE RETENTION

Cookies are not explicitly regulated by Israeli law, but their use may be subject to other rules that limit the retention of data. For instance, if cookies collect personal information, the data minimization principle should be followed. This principle is not directly stated in the PPL, but is provided for under the PPA guidelines on data minimization (only available in Hebrew here). Moreover, Section 2(c) of the Protection of Privacy Regulations (Data Security) 5777-2017 ('the Data Security Regulations') requires an annual review of the data stored in the controller's systems and whether it exceeds the database purposes. Furthermore, if the personal data collected by cookies falls under the Data Security Regulations that govern the data transfer from the EEA to Israel, the retention rules in those regulations will apply.

6. ADDITIONAL INFORMATION

Not applicable.

7. CASE LAW & ENFORCEMENT DECISIONS

There are several ongoing legal proceedings in Israel related to cookies, including civil lawsuits and applications for class action against a wide range of defendants (such as banks, financial institutions, credit card companies, and insurance companies). Other proceedings that were included in claims regarding the use of cookies came to their end.

With this regard, recently a settlement was reached in one of these cases. The lawsuit was filed against the Israel Electric Corporation (IEC) and Israel Railways on different legal bases, claiming that the defendants violated their customers' privacy by collecting data through cookies and sharing data with third parties without any consent from the customers. As part of the settlement, which was signed with IEC, the IEC has committed to placing a cookie banner on its website by the end of 2024. This banner will include an opt-in consent for using such cookies. Additionally, the settlement involves payment of remuneration and legal fees totaling NIS 140,000 (approx $38,150).

It is important to note that the circumstances in the above-mentioned IEC case are unique and are not identical to the circumstances which are in the other proceedings. That is why the ability to infer from the IEC settlement to other cases is limited and it does not necessarily reflect the upcoming requirements in Israel regarding the placing of cookies and other similar technologies.

8. PENALTIES

There are no specific sanctions applying to cookies, but sanctions apply to a breach of the PPL. Currently, sanctions include modest administrative fines, however, the Israeli Parliament ('the Knesset') is preparing an extensive revision of the law would substantially increase fines.

Criminal sanction may apply to offenses such as failure to give notice, but such enforcement is rare. Breaches are also civil torts, which, in the context of consumer relations, can be pursued as class actions.