Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

Israel: Law & Practice
Amit Dat and Omri Rachum-Twaig
FISCHER (FBC & Co.)

Israel: Trends & Developments
Amit Dat and Omri Rachum-Twaig
FISCHER (FBC & Co.)

practiceguides.chambers.com

ISRAEL

Law and Practice

Contributed by:
Amit Dat and Omri Rachum-Twaig
FISCHER (FBC & Co.) see p.13

Contents

1. Basic National Regime

1.1 Laws

Israel does not have a constitution, rather a set of "Basic Laws" that establish basic legal rights, including the right to privacy. The right to privacy is included in the Basic Law: Human Dignity and Freedom, 1992, which provides that "each person is entitled to privacy and seclusion".

The right to privacy is also established as a private cause of action in the Privacy Protection Law, 1981 (the "Privacy Law"). The Privacy Law provides the main general framework for privacy and data protection as private rights in Israel. It has two main parts: Part A which established a privacy violation tort, and Part B which provides data protection principles for the digital processing of personal data. The Privacy Law generally acknowledges only consent as a lawful basis for processing of personal data, with a general exemption for acts mandated or authorised by other laws.

1.2 Regulators

The key regulator overseeing privacy and data protection in Israel is the Data Protection Authority (PPA). The PPA has jurisdiction over any entity that processes personal data under the Privacy Law, which could be both private sector and governmental bodies. The PPA conducts several types of audits. It conducts self-initiated sector-wide audits, it conducts audits and inspections following notification of data breaches, and it conducts inspections based on individual reporting of potential violations.

1.3 Administration and Enforcement Process

The PPA's enforcement powers for administrative purposes (as opposed to its criminal prosecution powers) are established – but only vaguely – in the Privacy Law. The PPA has an explicit power to demand submission of documents, and has inspection rights including with respect to computer materials, potentially even without a court order. There is no structured process the PPA has to undertake to execute its powers or impose penalties, but it is customary that the PPA provides entities under inspection with a draft decision subject to a hearing before making a final administrative decision. Given that the PPA is part of the administrative branch, it is subject to general principles of administrative law, such as due process, explanation, reasonability and proportionality. Any act of the PPA is also subject to judicial review by petitions to Administrative Courts in Israel.

1.4 Multilateral and Subnational Issues

Israel is not part of the EU and therefore is not directly subject to EU regulations and directive. Israel is a party to Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data, but there is no other implementing act for this Convention other than the general provisions of the Privacy Law.

Israel currently enjoys an adequacy status acknowledged by the EU Commission. Israel's adequacy is currently being reviewed by the EU Commission and there is vivid debate between the governments in an attempt to preserve this status.

1.5 Major NGOs and Self-Regulatory Organisations

There are no NGOs specifically dealing with privacy and data protection in Israel. Some general NGOs that focus on the cyberspace are the Israeli Internet Association and the Israel Democratic Institute.

1.6 System Characteristics

Israel follows an EU omnibus model for privacy and data protection legislation in the sense that the Privacy Law is a general law applicable to all business sectors and governmental bodies in Israel. There are, however, some sectoral nuances, specifically in the field of information security but also from a data protection perspective, especially in the financial and medical sectors.

The Israeli Privacy Law is developing in the sense that it was first enacted in 1981, and the most recent material revision took place in 1996. There is a pending bill to amend the Privacy Law, and concurrently, Israeli courts face dozens of privacy and data protection-related cases focusing on modern data processing issues which have not been decided yet. Please refer to the Israeli Trends & Developments chapter in this guide for further discussion of potential reform to the Privacy Law and pending data protection-related cases.

Enforcement in Israel is relatively aggressive in the sense that the PPA attempts to oversee and inspect many data processing activities, both through individual inspection and through publication of guidelines and opinions. However, the enforcement powers of the PPA are relatively weak and do not include substantial administrative fines.

1.7 Key Developments

The Israeli Ministry of Justice has presented a bill to amend the Privacy Law, including substantial revisions in the enforcement powers of the PPA and broadened definitions – following those used in the EU's General Data Protection Regulation (GDPR) – for common terms such as "personal data", "processing", "controller" and "processor". The bill was approved in first reading in the Israeli Knesset and was discussed in several meetings of the parliamentary committee, but has not progressed since.

The Ministry of Justice also published draft regulations to provide additional safeguards to personal data processed in Israel but originating in the EU, for the purpose of preserving Israel's adequacy status. This has not been approved yet, while the EU commission reviews Israel's adequacy status.

Please refer to the Israeli Trends & Developments chapter in this guide for further discussion.

1.8 Significant Pending Changes, Hot Topics and Issues

It is expected that in the next 12 months several of the pending class action litigations revolving around privacy and data protection issues will be decided, thus providing first judicial decisions on modern data protection questions which are highly awaited in Israel. It is also possible that the bill to amend the Privacy Law will further progress and perhaps even be enacted, thus materially changing the statutory framework for data processing in Israel and increasing the enforcement powers of the PPA.

Please refer to the Israeli Trends & Developments chapter in this guide for further discussion.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The Privacy Law has two main parts: Part A, which deals with violations of privacy, and Part B, which deals with data protection provisions for digital data.

Lawfulness of Processing

Section 2 of the Privacy Law, in Part A, sets forth 12 circumstances that constitute violation of privacy. Courts have already acknowledged that this is not a closed list, and that analogous circumstances would also violate privacy. Many of the statutory circumstances pertain to traditional privacy, such as violation of secrecy, surveillance, monitoring of bilateral communications, third-party viewing of mail and photography that intrudes upon a person's seclusion. However, one main circumstance focuses on the purpose limitation principles and provides that use of information on a person's private affairs for unauthorised purposes is a violation of privacy.

The term "information on a person's private affairs" is not defined in the Privacy Law, and courts, as well as the PPA, have gradually expanded its interpretation. Today, it is commonly understood as private information on an identified or reasonably identifiable person.

The basic premise under Part A of the Privacy Law is that violation of privacy is prohibited without a person's informed express or implied consent. There is no case law on what constitutes such consent in digital circumstances of data protection, and there are dozens of class actions pending in courts to review this standard in various contexts (consumer, children, etc).

Data Protection Provisions

Part B of the Privacy Law provides several data protection requirements and principles.

Database registration – the Privacy Law requires any digital collection of personal data to be registered with the PPA as a database. This is applicable either when the database includes sensitive data (which is broadly defined), or when non-sensitive personal data exists on over 10,000 data subjects. The registration requirement is mainly bureaucratic, and the PPA is advocating for its abolishment.

Data access right – the Privacy Law provides a data access right to data subjects, and requires a database owner to respond, within 30 days, to a data access request. The PPA has clarified in its guidelines that the response should be digital and secure to the extent possible, without placing an excessive burden on the data subject.

Data rectification/deletion – the Privacy Law allows data subjects to request rectification or deletion of their personal data only if it is inaccurate or incomplete, but does not provide a firm corresponding duty to grant such requests and actually rectify or delete the data.

Confidentiality – the Privacy Law provides that any personal data included in a database must remain confidential and only be used on a need-to-know basis with purpose limitation.

Information security – the Privacy Law and the Privacy Protection Regulations (Information Security), 2017, set forth a long list of technical and organisational measures required of any database owner, with a modular applicability based on three levels of security – basic, medium and high – depending on the sensitivity of the personal data and the number of data subjects and access holders.

Data protection officers – there is no statutory requirement to appoint data protection officers under the Privacy Law. Some sectoral regulations do require this position or a similar one, especially those applying to financial institutions. The PPA has issued opinions recommending the appointment of DPOs in certain cases and explaining what would be the relevant pro-

ficiency and duties of a DPO, mainly following the GDPR provisions.

Data protection impact assessment (DIPA) – there is no statutory duty to conduct a DPIA under the Privacy Law. Some sectoral regulations do require internal data protection assessments, especially in the financial institutions and medical sectors. The PPA has issued opinions recommending the adoption of DPIAs in certain cases and explaining the scope of such assessments, mainly following the GDPR provisions and guidelines.

Controller-processor relationships – the Privacy Law acknowledges the concepts of a database owner (controller) and a database holder (processor). The term database owner is not defined, and a database holder is defined as an entity holding a permanent copy of the database. The statutory language does not capture the entire concept of controller-processor relationships as depicted under the GDPR or the California Consumer Privacy Act (CCPA), but the PPA and the market generally follows these concepts, and the Information Security Regulations require certain legal provisions to be included in data transfer agreement, de facto substantiating the requirement for DPAs in such engagements.

2.2 Sectoral and Special Issues

Sectoral Data

The Privacy Law does not treat many sectoral or special categories of personal data differently from other types of data, including financial data, health data, children's data, communications data, online identifiers, cookies, location data, social media data and political or religious data. These are all covered by the general requirements and prohibitions of the Privacy Law.

Some sectoral regulations such as banking and financial institutions regulations; healthcare provider regulations; and regulations pertaining to government-operated health, genetic, biometric or financial databases, treat these types of data with stricter purpose limitation provisions and information security standards.

Employment-related data is treated differently by courts, as explained in **2.4 Workplace Privacy**.

Browsing Data

It is an open question whether cookies and online identifiers fall with the scope of the Privacy Law, given the lack of definition for a "person's private affairs". Pending lawsuits allege that such data is reasonably identifiable and thus falls within the scope of the term, but courts have not yet decided this issue.

Children's Data

While children's data is not treated differently from the Privacy Law perspective, the Israeli Legal Capacity and Guardianship Law provides that minors under the age of 18 cannot validly take legal actions without their guardian's consent. This effectively means that the consent of children under the Privacy Law presumably require their parents' consent. However, the Guardianship Law also provides that minors are capable of taking independent valid legal actions which minors of their age typically take, or if the counterparty does not have a reason to believe they are minors. This makes things more difficult in online contexts, and raises questions such as whether teenagers, who commonly use online services, are capable of providing independent consent to personal data processing in such contexts. These questions remain unanswered, with several pending class actions challenging such practices.

Data Subject Rights
Data subject rights are fairly limited under the Privacy Law.

Data access right – the Privacy Law provides a data access right to data subjects, and requires a database owner to respond, within 30 days, to a data access request. The PPA has clarified in its guidelines that the response should be digital and secure to the extent possible, without placing an excessive burden on the data subject.

Data rectification/deletion – the Privacy Law allows data subject to request rectification or deletion of their personal data only if it is inaccurate or incomplete, but does not provide a firm corresponding duty to grant such requests and actually rectify or delete the data.

2.3 Online Marketing

Israeli law provides several restrictions pertaining to online marketing.

Anti-spam – the Israeli Communications Law (Telecommunications and Broadcasting), 1982, prohibits sending unsolicited advertisements via either SMS/MMS technologies or digital communications defined as any digital form that is retrievable. This typically includes email, direct messaging and inboxes. The law requires opt-in explicit consent for such digital advertising, except when the advertising is made to a pre-existing client or potential client who previously purchases or negotiated goods or services of the same type advertised, and provided that a clear opt-out option is provided.

Robocalls – the same Communications Law also prohibits pre-recorded telephone calls constituting advertisement, unless consent has been provided.

Marketing Calls – recently, an amendment to the Israeli Consumer Protection Law, 1981, constituted a statutory do-not-call-me data base, allowing consumers to register and refrain from unsolicited marketing calls. Businesses are now prohibited from making marketing calls to individuals who registered to the database, unless explicit separate consent was obtained or in pure call-back circumstances.

Direct Advertising – the Privacy Law prohibits approaching individuals with marketing efforts based on a profile of their personal attributes without the consent of such individuals and with a clear opt-out and deletion rights. The PPA clarified that when such direct marketing approaches are made as-a-service, or exceed the scope of expected business activity, a clear opt-in consent is required for such conduct.

2.4 Workplace Privacy

There is no statutory reference to workplace privacy in the Privacy Law. However, in several decisions, the National Labour Court has incorporated several principles applicable to the processing of personal data in employment contexts, and especially, adopted the principle of proportionality to such cases.

Specifically, the Court has set forth special rules for the processing of fingerprint data for time-clock purposes, and required opt-in explicit and transparent consent to collect and use such data. In addition, with respect to monitoring of work-related communications equipment, the Court required full transparency by employers; a published policy explaining such monitoring; and explicitly prohibited monitoring personal non-work-related communications, even if conducted on employer's equipment, without ad-hoc explicit consent of the data subject, or a judicial injunction allowing such conduct.

The PPA also published several guidelines on work-related privacy, including the collection and use of data from CCTV cameras in the workplace (requiring transparency and prohibiting cameras in private areas), processing of personal data in reliability tests, collection of location data related to employees (only when strictly required due to the nature of the work), and processing of health-related data as part of employment screening.

2.5 Enforcement and Litigation

From an administrative regulatory perspective, the PPA is very active in inspecting and enforcing the Privacy Law, despite its relatively weak enforcement powers. It conducts self-initiated sectoral audits over several hundred organisations per year, conducts specific investigations and inspections during and after security breaches, and in extreme cases initiates criminal investigations and indictments.

The PPA's general statutory authority is to "oversee the execution of the Privacy Law". From this, the PPA with some supporting obiter dictum statements of courts, has expanded its enforcement powers to conduct investigations of potential administrative violations of the Privacy Law, and, in the absence of substantial statutory administrative fines, to publicly disclose its finding of violations of the Privacy Law. In some specific cases there may be an administrative fine of up to ILS25,000 for violations of the Privacy Law. There is a pending bill to amend the Privacy Law to allow for administrative fines of up to ILS3.2 million.

From a civil litigation perspective, the Privacy Law allows statutory damages of up to ILS60,000 in private lawsuits for privacy violations under Part A of the law.

Israel also has class action proceedings. The Class Action Law, 2006 does not allow filing class actions merely due to violation of privacy. However, in consumer-related or financial services relationships, class actions are allowed regardless of the cause of action, giving rise to dozens of motions to certify class actions for privacy violations filed in the past five years. Most of these motions focus on financial institutions, large retailers and multinational online platforms. None, however, have yielded final written court decisions, and most are still pending. There have been some settlements approved by courts, but it is not yet possible to estimate what would be the monetary risk in privacy class actions, given the relatively strict requirement to prove damages that are common to the entire class of plaintiffs at hand.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Israel has three main legal standards pertaining to law enforcement access to data in cases of serious crimes: the Wiretapping Law, the Search Ordinance and the Communications Data Law.

The Wiretapping Law

The Wiretapping Law allows law enforcement agencies to seek an order from a District Court President, to allow monitoring of conversation content, including through digital means. In extremely urgent cases, such wiretapping is allowed with an administrative order of the supervising minister, but only for a period of 48 hours. Courts have generally interpreted this law to allow monitoring of data-in-transit, as opposed to data at rest. However, due to journalistic exposures published recently, it appears

that the Israeli Police have used such orders to allow remote monitoring of data-at-rest through sophisticated "zero click" spyware.

The Search Ordinance

The Criminal Procedure Ordinance (Arrest and Searches) allows law enforcement agencies to seek a Magistrate Court Judge's order to search content stored in computers. This has been interpreted to only include searches for data-at-rest in a device physically seized by the agency, and restricted to such types of content set forth in the order.

The Communications Data Law

The Criminal Procedure Law (Communications Data) allows certain law enforcement agencies to seek orders to obtain communications data directly from communication service providers in Israel, including identity of the parties to the communications, location data, and other meta-data, but excluding the content of the communications.

All such laws are generally understood to apply only with the borders of the state of Israel, and raise complex questions when the data searched for resided outside of Israel, especially in the context of cross-border communications and cloud storage.

3.2 Laws and Standards for Access to Data for National Security Purposes

The provisions discussed in **3.1 Laws and Standards for Access to Data for Serious Crimes** generally also apply to national security purposes. In cases of national security, such wiretapping or communications data disclosures are not subject to judicial review and are granted based on an order by Head of the General Security Service for a period of up to three months (which is extendable to additional periods).

3.3 Invoking Foreign Government Obligations

Israeli organisations cannot invoke a foreign government access request as a legitimate basis for data processing and transfer. There is no publicly disclosed Cloud Act agreement between Israel and the USA.

3.4 Key Privacy Issues, Conflicts and Public Debates

In recent years, there have been two types of debate revolving government access to personal data: those to do with public interest legislation and those to do with investigations of crimes and national security.

Public Interest Legislation

Beginning with legislation related to COVID-19, which allowed contact tracing efforts, there has been a movement of objection to governmental surveillance, ranging also to new efforts pertaining to biometric surveillance and road monitoring for traffic violations. These have been mainly attacked through petitions filed with the High Court of Justice based on the constitutional right to privacy, and in some cases, the Court determined that certain governmental practices were unlawful.

Investigations of Crimes and National Security

As discussed in **3.1 Laws and Standards for Access to Data for Serious Crimes**, there has been significant debate on the enforcement powers of agencies in Israel with respect to alleged use of sophisticated zero-click spyware for criminal investigations. Such tools that were previously reserved for national security purposes, were allegedly used in civil circumstances, which led to public outrage and several internal reports issued by the Attorney General and the Israeli Police. This has not been resolved, and

allegedly, Israeli law as it is today does not allow the use of such tools for criminal investigations.

4. International Considerations

4.1 Restrictions on International Data Issues

The Privacy Protection Regulations (Transfer of Data from Databases Outside the Country Borders), 2001, generally restrict the transfer of personal data to a country that does not provide data protection standard equivalent to those provided under Israeli law.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

There are several statutory derogations from the general restriction on international data transfers, the most important of which are:

- transferring data to EU members states or to jurisdictions to which such members states allow the transfer of data;
- with the consent of the data subject; and
- to an "inadequate" jurisdiction, subject to a contractual undertaking of the recipient party to substantially comply with Israeli data protection and information security requirements.

4.3 Government Notifications and Approvals

There are no governmental notifications or approvals required for international personal data transfers.

4.4 Data Localisation Requirements

There are no data localisation requirements in Israel.

4.5 Sharing Technical Details

There are no general requirements to share technical information such as software code, algorithms or otherwise with the Israeli government. There are some limitations and restrictions on the use of encryption technology in Israel, and the government has an option to intervene in patent applications including technology deemed to have a significant effect on national security.

4.6 Limitations and Considerations

There are no specific exemptions under the Privacy Laws for collecting and transferring personal data in connection with government data requests, foreign litigation proceedings (eg, civil discovery) or internal investigations. There is, however, a general defence for organisations acting in good faith based on personal legitimate interest, which may serve as a basis for courts to acknowledge such external requirements as mandating the processing of personal data even without consent as a lawful basis.

4.7 "Blocking" Statutes

There are no blocking statutes in the context of Israeli data protection and privacy.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

There are no explicit laws or statutory references pertaining to the following:

- big data analytics;
- automated decision-making;
- profiling or microtargeting;
- artificial intelligence (including machine learning);
- internet of things (IoT) or ubiquitous sensors;

- autonomous decision-making (including autonomous vehicles);
- facial recognition; or
- disinformation, deepfakes, or other online harms.

The PPA has published some guidance on privacy-related issues pertaining to deepfakes and collection of data from drones. Some courts have treated geolocation as private affairs of a person for the purpose of privacy violations, but only in specific cases and on an ad hoc basis. See **2.4 Workplace Privacy** for discussion of the treatment of biometric information by the National Labour Court.

The Ministry of Justice recently published a draft opinion on its view of AI-related regulation, explaining that Israeli will not have a general AI law or regulation, rather sector specific treatment of the issue pertaining to explainability, privacy, automated decision-making, discrimination and other legal considerations on a risk-based approach given the specific sector and industry.

The Consumer Protection Authority recently published guidelines on the unlawfulness of opt-out consent practices in consumer-related online activity, as a first attempt to restrict dark patterns based on the general "unfairness" doctrine in the Consumer Protection Law. This may also apply to personal data processing activities aimed at consumers as well as to online marketing efforts requiring consent.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Internal digital governance is not common in Israeli organisations. This could be found in incumbent organisations in the financial sector that have large compliance departments and some sectoral duties pertaining to data protection and information security.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

From an administrative regulatory perspective, the PPA is very active in inspecting and enforcing the Privacy Law, despite its relatively weak enforcement powers. It conducts self-initiated sectoral audits over several hundred organisations per year, conducts specific investigations and inspections during and after security breaches, and in extreme cases initiates criminal investigations and indictments.

From a civil litigation perspective, the most noticeable trend is filing motions to certify class actions including claims for violation of privacy under the Privacy Law. The Class Action Law, 2006 does not allow filing class actions merely due to violation of privacy. However, in consumer-related or financial services relationships, class actions are allowed regardless of the cause of action, giving rise to dozens of motions to certify class actions for privacy violations filed in the past five years. Most of these motions focus on financial institutions, large retailers and multinational online platforms. None, however, have yielded final written court decisions, and most are still pending. There have been some settlements approved by courts, but it is not yet possible to estimate what would be the monetary risk in privacy class actions, given the relatively strict requirement to prove damages that are common to the entire class of plaintiffs at hand.

5.4 Due Diligence

Privacy and data protection due diligence processes in corporate transactions in Israel typically revolve around key legal issues:

- Lawfulness of processing – reviewing the privacy disclosures and consent mechanisms of the organisation to ensure that informed consent was obtained for all types of processing of personal data.
- Data protection undertakings – reviewing the database registrations of the organisation, its internal data protection practices and its compliance with data subject rights.
- Information security – reviewing the organisation's compliance with the Information Security Regulations.
- Legal proceedings – Reviewing any administrative inspections or proceedings conducted by the PPA, and any pending or past lawsuits filed against the organisation.

5.5 Public Disclosure

Publicly traded companies are required to include in their quarterly and yearly statements risk factors pertaining to cybersecurity risk and privacy risks. The Israeli Securities Authority also requires such companies to issue immediate notifications when a cybersecurity-related event materially affects the business of the company.

Privately held companies are generally not required to publicly disclose such risks, however some sectoral regulations such as banking guidelines, require notification of risks that materialise to regulators, who may, in extreme cases, communicate them to the public.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws

There is no statutory reference to the intersection between privacy, competition and consumer protection laws. In 2021, a joint white paper by the PPA, the Competition Authority and the Consumer Protection Authority was published with respect to potential guidelines regarding data portability, but this has not yet progressed.

The Consumer Protection Law, 1981 applies to any consumer-related acts and thus may impact some data processing activities. Certain pending class actions attempt to combine consumer protection and standard form contracts provisions with the Privacy Law to establish unlawful data processing, but these have not yet been decided.

5.7 Other Significant Issues

There are no significant issues not already covered in this article.

FISCHER (FBC & Co.) was founded in 1958 and is one of Israel's premier full-service law firms and among the largest in the country, providing high-quality, diverse and multidisciplinary legal services in a wide range of practice areas Over more than half a century, the firm has acquired a distinguished reputation, while championing its core values of excellence, professionalism and integrity. The firm's multidisciplinary approach enables it to provide clients with legal services tailored to its needs. Having worked at top-tier international law firms, many of FISCHER's associates have foreign legal education and practice experience. The firm benefits from an outstanding reputation among leading legal professionals in numerous countries. The firm is regularly involved in a broad range of transactions and litigation at the centre of Israel's legal, economic and public agenda, and represents local and international clients in a long list of practice areas.

Authors

Amit Dat concentrates his practice on technology-oriented legal matters. He provides legal counsel to individuals, private and public companies (local and multinational) with respect to IP, IT, privacy, data protection, information security, commercial activities in cyberspace, internet law, gaming, and media and entertainment law. Mr Dat has extensive experience in advising clients on various types of IP transactions, including investment in IP companies, development agreements, purchasing and licensing of IP, content and data transfers, as well as services in the arena of big data, the web intelligence industry and information-oriented transactions. He is a member of the AIPPI.

Omri Rachum-Twaig concentrates his practice on IP, privacy and data protection, information security, artificial intelligence, technology regulation and commercial cyber issues, technology and information-oriented transactions. He provides legal counsel to individuals, private and public companies with respect to internet law, artificial intelligence and media, entertainment law, patents, trade marks, copyrights and trade secrets, commercial cyber issues and the export of dual-use technologies. Dr Rachum-Twaig obtained a PhD in law from Tel-Aviv University, and has published books and articles in leading publications and journals worldwide, some of which have been cited by the Israeli Supreme Court. He teaches information technology law at Tel Aviv University and has CISSP certification.

FISCHER (FBC & Co.)

146 Menachem Begin Rd
Tel Aviv
Israel

Tel: 972 3 6944111
Fax: 972 3 609 1116
Email: fbc@fbclawyers.com
Web: www.fbclawyers.com

Trends and Developments

Contributed by:
Amit Dat and Omri Rachum-Twaig
FISCHER (FBC & Co.) **see p.18**

Israel's Outdated Privacy Laws and Legislative, Regulatory and Judicial Attempts to Modernise

Israel's privacy laws are outdated. The Privacy Protection Law, 1981, which is the main omnibus privacy and data protection law, was enacted over 40 years ago, with one significant amendment in 1996. The statutory language is not up to date and has not kept up with digital data processing as it is known today.

Current trends and developments in Israeli privacy and data protection laws could be generally divided as follows: draft bills to amend privacy laws, self-initiated regulatory guidelines and litigation aiming for judicial interpretation of the law.

Bills to amend the Privacy Law

The Ministry of Justice has been working on several bills to amend the Privacy Law for several years now. In 2022, the Bill to Amend the Privacy Protection Law (Amendment 14), 2022 was approved in the Israeli Knesset at first hearing, and proceeded to the legislative committee for further discussions. The political instability and the fact that the Israeli government has dissolved the Knesset, interrupted the process and Amendment 14 is still pending for future review.

Amendment 14 seeks to substantially change the Privacy Law in two main ways. First, it provides a new set of terms and definitions to keep the Privacy Law on a par with its modern counterparts such as the EU's General Data Protection Regulation (GDPR). Terms such as controller, "processor", "personal data", and "processing", which are currently left undefined in the Privacy Law will be statutorily defined under a modern understanding of data protection.

Second, Amendment 14 proposes new regulatory powers for the Privacy Protection Authority (PPA), increasing the administrative fines from ILS25,000 to up to ILS3.2 million, which would be a dramatic change in enforcement of the Privacy Law.

The Ministry of Justice has also declared that it is working on another bill to amend the Privacy Law, which will include a new set of data subject rights, reference to the appointment of data protection officers and data protection impact analyses, and provide a new set of lawful grounds for processing of personal data, other than consent (which is the only lawful basis today). This bill has not been published yet.

In the background of these legislative initiatives, lies a current review of Israel's adequacy status by the EU Commission. Israel was acknowledged as an adequate country in 2011, and given the provisions of the GDPR, such status is currently under periodic review. Given certain concerns that Israeli privacy laws today are not on a par with the GDPR, the Ministry of Justice published draft regulations proposing to grant additional data protection rights to personal data transferred from the EU to Israel. These now have to be approved by the Minister of Justice and then by the legislative committee.

It is noteworthy that other non-privacy related legislative and regulatory efforts may have an

effect on privacy and data protection issues. These include an overarching initiative of the Ministry of Justice to offer a framework for regulations concerning artificial intelligence in various sectors, with a focus on privacy concerns and automated decision-making, as well as initiatives of the Consumer Protection Authority to tackle "dark patterns" in online consumer activities, including consent mechanisms.

Regulatory developments

The PPA does not currently have extensive enforcement powers under the Privacy Law, and its fines are limited to ILS25,000 per violation. Given the statutory limitations, the PPA is very active in publishing guidelines and opinions on current data protection questions, in an attempt to interpret the Privacy Law and bring it closer to modern data protection standards.

The guidelines and opinions of the PPA do not have binding legal effect and they are more of a recommendation. However, these have a signalling effect on the market, and potentially on courts dealing with new privacy and data protection cases where there are not clear precedents.

In recent years, the PPA has published guidelines and opinions on what constitutes personal data under the Privacy Law, on employment-related processing of personal data, on the role of data protection officers and the structure of data protection impact assessments, and other relevant data protection issues.

For example, the PPA published an amendment to the policy for reporting information security incidents. The policy concerns the legal obligation imposed on the owner, manager or holder of a database with a high or medium security level, to submit an immediate report of a serious information security incident to the PPA. The amendment tightens the reporting obligation and stipulates that the report must be submitted immediately, upon discovery or concern about a serious information security incident, without specifying the previously established time frame (ie, to report within 72 hours).

In addition, the PPA published a statement regarding the obligation to notify data subjects of the collection and use of personal data as part of the consent procedure, which refers, among other things, to the collection and processing of personal data using decision-making systems based on algorithms or artificial intelligence (AI). The PPA also published for public comments a recommendation document regarding privacy aspects of signing a medical confidentiality waiver and disclosing potential employee's medical data during the hiring processes. The document highlights that medical data is considered extremely sensitive information, and accordingly lists recommendations for potential employers, such as to obtain a prior consent to the disclosure of medical data, to avoid the collection of irrelevant data, to limit its retention period and to reduce excess information.

Furthermore, in the past year the PPA reviewed the risks to patients' privacy in the provision of remote medical services (including applications for virtual encounters between therapist and patient; services for monitoring, collecting and transferring health data from patient to caregiver; and primary diagnostic services based on artificial intelligence), and lists duties in the field of privacy and data protection imposed on health organisations, caregivers and external technology providers involved in the provision of remote medical services.

The PPA further published a position paper regarding privacy and information security using

deepfake technologies, in which it formulated a series of recommendations for the public and database owners using such technology. It was emphasised, among other things, that photos or videos that have been digitally edited and may be perceived as authentic must be secured according to the law as if they were real personal data, and that the distribution of fake data that presents humiliating content or that concerns the data subject's personal life without their consent violates their privacy.

In addition, the PPA engages in self-initiated audits and inspections and reviews the data protection status of hundreds of organisations each year. In addition, the PPA is becoming more active in inspecting data breaches, not only after-the-fact, but also during information security incidents involving potential personal data breaches. In this context, the breach notification duty has been shortened to several hours from becoming aware of an incident.

Privacy litigation

One key direction from which privacy law is expected to develop in Israel is private litigation. Israel is characterised by high rates of litigation per capita, especially in the context of consumer related class actions. These have expanded, in recent years, to privacy and data protection as well.

Israel follows a semi-common law system with case law having a binding precedent effect. Coupled with an inclination towards legal activism, courts tend to interpret statutory texts in a manner allowing the development of the law, especially in the context of older, outdated legislations. Given that the Privacy Law was enacted in 1981, it would be no surprise to see judicial interpretation applying newer concepts of data protection to the statutory language of the law.

Israeli law allows class action litigation. The Class Action Law, 2006, allows bringing class actions in any cause of action related to consumer relationships. This has led, in recent years, to the filing of dozens of motions to certify class actions based on privacy and data protection causes of action. Pending case law is mainly divided into post-data breach cases and core privacy and data protection cases.

Given that the lifecycle of an average class action, before appeal, could be four to five years, most of these class actions are still pending and none has yielded final decisions on the merits. Some actions end in consensual dismissals that do not shed any light on how the court viewed the matter at hand. A handful of such class actions ended in settlements, most of which did not yield significant compensation to the class members. It is thus still to be seen how courts will view such issues in final decisions, especially given the difficulty of proving and calculating damages, which is a prerequisite both in the Class Action Law, and in the Privacy Law.

FISCHER (FBC & Co.) was founded in 1958 and is one of Israel's premier full-service law firms and among the largest in the country, providing high-quality, diverse and multidisciplinary legal services in a wide range of practice areas Over more than half a century, the firm has acquired a distinguished reputation, while championing its core values of excellence, professionalism and integrity. The firm's multidisciplinary approach enables it to provide clients with legal services tailored to its needs. Having worked at top-tier international law firms, many of FISCHER's associates have foreign legal education and practice experience. The firm benefits from an outstanding reputation among leading legal professionals in numerous countries. The firm is regularly involved in a broad range of transactions and litigation at the centre of Israel's legal, economic and public agenda, and represents local and international clients in a long list of practice areas.

Authors

Amit Dat concentrates his practice on technology-oriented legal matters. He provides legal counsel to individuals, private and public companies (local and multinational) with respect to IP, IT, privacy, data protection, information security, commercial activities in cyberspace, internet law, gaming, and media and entertainment law. Mr Dat has extensive experience in advising clients on various types of IP transactions, including investment in IP companies, development agreements, purchasing and licensing of IP, content and data transfers, as well as services in the arena of big data, the web intelligence industry and information-oriented transactions. He is a member of the AIPPI.

Omri Rachum-Twaig concentrates his practice on IP, privacy and data protection, information security, artificial intelligence, technology regulation and commercial cyber issues, technology and information-oriented transactions. He provides legal counsel to individuals, private and public companies with respect to internet law, artificial intelligence and media, entertainment law, patents, trade marks, copyrights and trade secrets, commercial cyber issues and the export of dual-use technologies. Dr Rachum-Twaig obtained a PhD in law from Tel-Aviv University, and has published books and articles in leading publications and journals worldwide, some of which have been cited by the Israeli Supreme Court. He teaches information technology law at Tel Aviv University and has CISSP certification.

FISCHER (FBC & Co.)

146 Menachem Begin Rd
Tel Aviv
Israel

Tel: 972 3 6944111
Fax: 972 3 609 1116
Email: fbc@fbclawyers.com
Web: www.fbclawyers.com

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com