STATE OF ISRAEL

Report on Developments in the Privacy and Personal Data Protection Regime in Israel

May 2019

Executive Summary

Following the request of the European Commission and upon the Commission's Decision of 31 January 2011 on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (the "Adequacy Decision"), Israel's Ministry of Justice is pleased to provide its report on significant changes and developments in the privacy and personal data legal protection regime in Israel. The Report provides information on the limitations and safeguards applicable to the access of public authorities to personal data.

The Report reviews the legal framework in Israel regarding the protection of privacy and personal data, access of authorities to such data, and significant legislative and case law developments in this field. As the Report underscores, Israel possesses a legal ecosystem that ensures the substantial and effective protection of human rights and includes a comprehensive privacy and personal data protection regime.

The main components of this regime include: (1) a sophisticated legal system based upon the rule of law and the protection of human rights, including the constitutional right to privacy enshrined in the Basic Law: Human Dignity and Liberty, and in the specific legal framework of the Privacy Protection Law and Regulations; (2) institutional mechanisms including a vibrant judiciary enabling the development of the law and judicial review by the Courts of all legislative and administrative measures; In addition, the unique institute of the Attorney General upholds the rule of law by providing valuable guidance and binding interpretation of the law to the executive branch; (3) the Privacy Protection Authority (PPA), which is a proactive and dynamic privacy regulator, with both regulation and enforcement powers which apply to all sectors, public and private, including security and law enforcement authorities.

The aim of this regime is, of course, to protect and promote the right to privacy in both the public and civil law, while balancing it against other rights and public interests such as protection of human life and public security. This balance is reflected, *inter alia*, in the relevant Israeli legal framework regarding access to personal data by enforcement and security authorities, whose activities are confined by their statutory powers as defined in specific laws. Furthermore, these authorities are subject to internal and external oversight mechanisms, amongst them are the internal comptroller and the legal

department of each authority, the Attorney General, the PPA, the State Comptroller and Parliament committees.

The Report elaborates on the main developments in the field of protection of privacy and personal data in Israel. Key among these are:

1) the coming into force in 2018, of the Privacy Protection (Data Security) Regulations, 2017, which aim to improve the level of data security across all sectors by setting general legally binding standards.
2) the passing of the first reading before the parliament of the Privacy Protection Bill (Enforcement Powers), which aims to enhance further the supervision and enforcement powers of the PPA.
3) the adoption of specific legislative texts that involve processing of personal data and provide customized privacy protection provisions, such as the Credit Data Law, 2016 and new regulations regarding the operation of cameras by local authorities.
4) an increase in the number of case law addressing the right to privacy, and a marked trend of the courts to interpret it in a broad manner, both in regard to the public and private sectors.
5) a significant expansion in the activities of the PPA, which has translated into an increase in the degree of supervision, enforcement and public awareness activities that have been undertaken over the last few years.

The above developments attest to the solid administrative and normative foundations on which Israel's privacy protection regime rests. To be sure, there remain challenges ahead which are indeed shared by democracies across the world – continuous technological developments, the ubiquitous use of internet-based services located abroad, and security concerns affecting all aspects of life. As the Report shows, a combination of strong institutional foundations and a forward-thinking approach have enabled Israel to address this challenge thus far. We are confident that through consistent, rigorous attention to the matter and ongoing governmental engagement, Israel will continue to effectively tackle these challenges to the right to privacy as they continue to evolve.

Table of Contents

5. **Access to personal data by public authorities for national security and law enforcement purposes**

5.1. Scope and background information

5.2. Rules, limitations and safeguards on collection and use of personal data for national security and law enforcement purposes

5.2.1. Authority to access data under specific laws

5.2.1.1. Law enforcement

5.2.1.2. National security

5.2.2. Application of the PPL in regard to data collected by security authorities

5.2.3. Transparency principles and the right to information

5.3. Oversight and supervision

5.3.1. General internal and external mechanisms

5.3.1.1. The police

5.3.1.2. The ISA

5.3.1.3. General supervision mechanisms that apply to all security authorities

5.3.2. Mechanisms under the PPL

5.3.2.1. Powers of the Registrar of Databases

5.3.2.2. Internal supervision model for security bodies under the Privacy Protection Bill

5.4. Judicial redress

5.4.1. Petitions for judicial review to the Supreme Court

5.4.2. Criminal proceedings

Introduction

Israel was invited to provide an update regarding significant changes and developments in the privacy and personal data protection regime in Israel, since the Commission Decision of 31 January 2011 on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (the "**Adequacy Decision**"). Further to discussions between the representatives of the Commission and the Israeli Government, we are pleased to submit this report detailing the significant changes and developments in Israel in this field.

In the past years, technological developments have brought about a sea of change in the way that personal data is collected and used by data controllers and processors. Governments around the world are looking into new ways and mechanisms to overcome the complex challenges in respect to the protection of privacy while enjoying the fruits of technology. A great effort is put into reviewing and updating legal frameworks regarding the right to privacy and protection of data.

The General Data Protection Regulations constitute perhaps the foremost example of modern privacy legislation, and its impact on the global discourse on privacy has been significant. Israel, too, has been proactive in its approach to privacy protection – laws and regulations have been revised, new laws have been adopted, its Privacy Protection Authority has been expanded, and courts have shown acute awareness of what privacy protection means in the 21st century.

This report summarizes the significant developments in the field of privacy protection law that have taken place since the Adequacy Decision in 2011. It is submitted as part of the Commission's review of adequacy-accredited countries. It describes the privacy landscape and ecosystem in Israel, focusing mainly on privacy regulation in the private sector, and it addresses the key issues raised by the Commission in its letter date January 25, 2017.

This report consists of the following parts: (1) an overview of the framework for the protection of the right to privacy and personal data in Israel; (2) a review of significant legislative and judicial developments concerning protection of privacy and personal data; (3) a more detailed analysis of developments regarding substantive rules for protection of personal data; (4) a review of developments regarding oversight and enforcement of the Privacy Protection Law by the Privacy Protection Authority; (5) a

review of the legal rules applicable to the access to personal data by public authorities for national security and law enforcement purposes; Additional case law, legislation, attorney general guidelines and other relevant documents are included in the appendix.

As this report underscores, Israel is committed to the protection of personal data, both for individuals in Israel and for individuals in the EU whose data is transferred to Israel, and has taken significant steps in recent years to further enhance such protection. Israel is confident that these steps, together with the privacy protection regime that has been in place, support a conclusion by the Commission that the Adequacy Decision should be maintained.

1. Framework for the protection of the right to privacy in Israeli law

1.1. Israel's legal system

As detailed in the documents submitted in support of the Adequacy Decision, Israel is a parliamentary democracy with characteristics similar to those of common law systems. As is known, in the common law tradition, courts play a central role in developing the law, and their decisions often complement legislation through interpretations and the setting of binding legal precedents. Thus, legislative texts do not necessarily reflect an exhaustive compendium of applicable rules, but rather must be read in conjunction with court decisions. In addition, the constitutional regime in Israel is not based on a single document which constitutes a formal and complete written constitution, but rather on several Basic Laws which are granted a superior normative status.[1]

The relevant normative and institutional components of the Israeli system that play a key role in the regime for the protection of privacy and personal data are described below.

1.2. Basic Law: Human Dignity and Liberty

Among the Israeli basic laws, the Basic Law: Human Dignity and Liberty of 1992 is the most relevant with respect to privacy protection. This law lists several of fundamental rights,[2] including the rights to dignity, liberty, privacy and property, and it provides that "each and every public authority is obliged to respect the rights in accordance with this Basic Law" (article 11). Article 7 of the Basic Law, which addresses privacy, provides as follows:

> "7. (a) Every person has a right to privacy and to intimacy in his life.
> (b) There shall be no entry into the private domain of a person, without his permission.
> (c) No search shall be held on the private domain of a person, upon his body, in his body, or among his private effects.
> (d) The confidentiality of conversation of a person, his writings or his records shall not be violated."

[1] CA 6821/93 Bank Hamizrahi Ha'Meuchad v. Migdal Kfar Shitufi 49(4) PD 221 (1995).
[2] In the context of these rights it is worth mentioning that in 1991 Israel ratified the International Covenant on Civil and Political Rights (ICCPR) in 1991. This step attests to Israel's commitment to human rights, amongst them the right to privacy.

This article has been interpreted by the Supreme Court and other courts as providing broad protection of the right to privacy and its various components, including the right to privacy of data – personal data protection.[3] As with other rights listed in the Basic Law, the right to privacy is not absolute; any violation thereof by a public authority is subject to the "limitation clause" (article 8) which provides as follows:

> "One is not to violate the rights accordance by this Basic Law save by means of a law that corresponds to the values of the State of Israel, which serves an appropriate purpose, and to an extent that does not exceed what is required, or on the basis of a law, as aforementioned, by force of an explicit authorization therein."

Pursuant to this article, the constitutionality of any legislative or administrative measures is determined based on the "appropriateness of the purpose" and its proportionality. The principle of proportionality consists of three cumulative subtests, as developed by the Supreme Court:[4] The **first** test is the "rational connection test", which examines the degree of compatibility between the legislation that infringes on the constitutional right and the purpose it is intended to realize.[5] The **second** test is "the test of the least harmful measure", according to which a legislative measure that infringes on constitutional human rights is only appropriate if the purpose cannot be achieved by another, less harmful measure. The **third** test, "proportionality in the narrow sense", evaluates the benefit derived from the measure as compared against the damage to the individual in its implementation. A proper balance between the measure and the purpose is therefore required.

A measure found to be unconstitutional based on the above principles and tests might be addressed in different ways by the court, depending on the severity of the violation and other considerations. Thus, for example, a finding of unconstitutionality in one decision might result in complete invalidation of a law, while in another case it might lead to a partial invalidation.

[3] A distinct example of the constitutional protection of the right to privacy of data - the right to personal data protection - may be seen within the Supreme Court's ruling in HCJ 8070/98 ACRI v. Minister of Interior 58(4) PD 842 (2004), in which the practice of providing financial entities, and other bodies with personal data listed in the Population Registry had been deemed unlawful.

[4] CA 6821/93 Bank Hamizrahi Ha'Meuchad v. Migdal Kfar Shitufi 49(4) PD 221 (1995).

[5] HCJ 2605/05 The Academic Center for Law and Business, Human Rights Division v. Minister of Finance, 63(2) PD 545 (2009). Hereinafter: The Academic Center for Law and Business case.

The Supreme Court has exercised its authority to invalidate legislation determined to be inconsistent with article 8 of the Basic Law in a diverse range of cases.

For example, in the **Academic Center for Law and Business** case[6] the Supreme Court annulled an amendment to the Prisons Order [New Version], 5732-1971[7] which enabled the privatization of prisons, ruling that it would be a disproportionate infringement of the constitutional rights to personal liberty and human dignity of prisoners to enable the prisons to be under private management. In the **Yekutieli** case, the Supreme Court annulled an income support payment for certain students in religious institutions and not to others enshrined in a provision in the Budget Foundations Law, 5745-1985,[8] on the grounds that the measure violated the right to equality in a disproportionate manner and therefore could not be included in the next budget law. The Court's analysis of the proportionality test is particularly relevant: in assessing whether the measure was "the least harmful measure" possible (the second test), the Court held that there are alternative measures that can achieve the purpose of economic assistance to the students with a lesser violation of the supra-legal right to equality.[9] With respect to the "proportionality test in the narrow sense" (the third test), the Court held that the violation of the right to equality was not proportional in relation to the social advantage arising from the measure. The Court established a guiding principle that pervades also in its privacy rulings, namely, that the greater the violation of a fundamental right, the stricter the test of proportionality will be.[10]

1.3. Fundamental Principles of administrative and constitutional law – reasonableness and proportionality

The principles of reasonableness and proportionality are key principles in the judicial review of government actions in Israel.[11]

Reasonableness: Lack of reasonableness of an administrative action has been recognized as grounds for judicial review,[12] and can lead to the quashing of an

[6] *Id*.
[7] Prisons Order [New Version], 5732-1971, SH No. 643 p. 22.
[8] Budget Foundations Law, 5745-1985, SH No. 1139, p. 60.
[9] The Academic Center for Law and Business Case, *supra* note *5*, at para. 47.
[10] HCJ 4124/00 Yekutieli v. Minister for Religious Affairs 64(1) PD 142 (2010), at para. 44 of the judgment of President Beinisch.
[11] 2 DAFNA BARAK-EREZ, ADMINISTRATIVE LAW, 725 (2010).
[12] HCJ 389/80 Yellow Pages Ltd. v. The Broadcasting Authority, 35(1) PD 421 (1980).

administrative measure. According to the Supreme Court, "the decision of an administrative authority will be disqualified due to unreasonableness, if the weight given to the various factors is not appropriate in the circumstances of the case. Indeed, this weighting and balancing are among the main tasks of the public authority, and the review of the manner in which they are carried out rests with the court".[13] Lack of reasonableness also includes cases in which a decision was influenced by improper or extraneous considerations.[14]

Proportionality: The principle of proportionality and its use as grounds for assessing the legality of administrative measures was developed in Israeli administrative law, in a sense, as an extension of the grounds of reasonableness.

As mentioned in part 1.1 above, the enactment of the Basic Law: Human Dignity and Liberty enshrined the principle in the limitation clause, as one of the conditions for the legality of violation of fundamental human rights.[15]

In practice, the grounds of reasonableness and proportionality are currently functioning as a central tool used by the courts in the exercise of judicial review in Israel. The example presented below illustrates the scope of judicial review applied to administrative decisions or legislation enacted by the Knesset, using the principles of reasonableness and proportionality.[16]

In the **Zidan** case[17] the court expanded the scope of judicial review by ruling that a provision of the Pension Regulations (Compensation for Delayed Payment) (Pension Fund from the National Insurance Institute of Israel), 5774-1984[18] enacted by the Minister of Labor and Social Affairs, was invalid even though the underlying decision was taken in a non-arbitrary manner after weighing all the relevant considerations.[19] The grounds for the disqualification of the provision rested on the fact that it

[13] See for example, HCJ 341/81 Beit Oved v. Traffic Controller, 36(3) PD 349,at para. 9.
[14] 2 BARAK-EREZ, *supra* note 11, at 726.
[15] See Basic Law: Freedom of Occupation, §4, 1454 (1994); Basic Law: Human Dignity and Liberty, §8, 1391 (1992).
[16] See appendix 1 for further, more detailed examples.
[17] HCJ 4769/90 Zidan v. Minister of Labor and Social Affairs (Apr. 14, 1993), Nevo Legal Database (by subscription, in Hebrew). Appendix 1 includes more details about this case.
[18] Pension Regulations (Compensation for Delayed Payment) (Pension Fund from the National Insurance Institute of Israel, 5774-1984, KT 4702 p. 2566.
[19] *Id.* at para. 31 & 33.

significantly deviated from the legislative purpose of the Pension Law, and was therefore manifestly unreasonable.[20]

1.4. The Privacy Protection Law

Beyond the constitutional and administrative law protections described above, the right to privacy has been granted explicit and substantial statutory protection under the Privacy Protection Law, 5741-1981 (hereinafter: PPL).[21] This law was, when first adopted in 1981, one of the first modern laws in the world to explicitly regulate protection of the right to privacy and its various components.

The PPL applies both to the public and private sectors. It establishes a civil tort and, under certain conditions, a criminal offense with a maximum term of imprisonment of five years for violation of privacy. Chapter A of the PPL prohibits the violation of the privacy of a person without that person's consent, and lists a series of typical situations that violate privacy concerning both the "classic" aspects of the right to privacy as well as the right to privacy of personal data. Chapter B of the law focuses on the protection of personal data and sets forth a regime of protecting privacy in databases, whilst appointing a Registrar of Databases with supervision and enforcement powers. Chapter C establishes defenses to violations of privacy, and addresses the applicability of the PPL to security authorities. Chapter D imposes limitations on the transfer of personal data by public bodies, and sets forth certain exceptions to those limitations. Chapter E contains various provisions concerning, *inter alia*, aspects of tort law, criminal law and law of evidence.

Further to the adoption of the PPL, regulations and orders have been enacted for various issues, including data security, personal data transfer outside of Israel, transfer of personal data between public bodies, and the transfer of personal data by public bodies to private bodies.

1.5. The Supreme Court of Israel

The Supreme Court of Israel is the country's highest judicial authority, upholding the rule of law, protecting fundamental rights and issuing definitive, binding rulings on the

[20] *Id.* at para. 28.
[21] Privacy Protection Law, 5741–1981, SH No. 1011 p. 128.

interpretation of the law. As will be elaborated below, public matters, including administrative matters which relate to disputes between a citizen and an authority exercising governmental powers, are generally dealt with directly by the Supreme Court in its capacity as a court of judicial review.[22] Due to high caseload, the authority to adjudicate on certain administrative matters has been transferred in recent years from the Supreme Court to district courts which will deal with the cases as a first instance. However, the Supreme Court continues to serve as a court of judicial review for the majority of administrative cases, whether as a first and only instance or as the last instance, and hears matters on a wide range of public and administrative matters, which raise the most sensitive and far-reaching issues of public interest.[23]

The powers of the Supreme Court are defined in the Basic Law: The Judiciary, in article 15. According to this article, the Supreme Court acts as an appellate court for the judicial decisions of the district courts in all matters (criminal, civil and public).[24] Furthermore, the Supreme Court is authorized to hear any matter in which it deems necessary to provide relief for the sake of justice and which is not within the jurisdiction of another court or tribunal.[25] In this capacity, the Supreme Court hears petitions filed against state authorities or against other bodies fulfilling public functions in the state, and exercises judicial review of the government authorities' activities. In addition, the Supreme Court serves as a constitutional court, disqualifying laws that violate the Basic Law: Human Dignity and Liberty.

A petition to the Supreme Court for judicial review may be filed against an act or omission of any of the state authorities (the government, government ministries, public officials, the Knesset, the IDF, the Israel Police etc.), which in the opinion of the petitioner violate the principles of justice or the laws of the state. As with other democratic countries, the power to exercise judicial review constitutes a restraining factor for the power of the executive and legislative authorities.

An important feature of the Supreme Court is the wide discretion given to the judges in deciding whether to hear a petition brought before them. For example, the right of

[22] Technically, the Supreme Court is said to be "sitting as the High Court of Justice".
[23] YOAV DOTAN, LAWYERING FOR THE RULE OF LAW: GOVERNMENT LAWYERS AND THE RISE OF JUDICIAL POWER IN ISRAEL 19 (2013).
[24] Note that the Supreme Court does not constitute an appellate court for decisions of courts outside the judicial hierarchy, such as the Rabbinical Court. However, it is possible to seek judicial review of such a decision if there have been fundamental flaws rending it unreasonable.
[25] Basic Law: The Judicature, §15(c), 1110 (1984).

standing has been extended so that even citizens and bodies not directly affected by the actions of the state can petition against it.[26]

Since the establishment of the State of Israel, the Supreme Court has been at the center of human rights discourse in Israel, interpreting and infusing concrete meaning to rights and freedoms and anchoring their status in the Israeli legal system. In addition, even before the enactment of the Basic Laws, and even with regard to freedoms and rights that have not yet been explicitly anchored therein, the Court recognized civil liberties as fundamental values of the legal system, and in its rulings created the status and protections which have since become entrenched in the Israeli legal system.[27]
The Supreme Court's powers, its functions and its accessibility to the average individual are among the unique characteristics of the Israeli legal system.

In addition, given that precedents and interpretation of case law play a central role in the Israeli legal system, Supreme Court rulings are a binding source of law. As such, the rulings of the Court contribute to the development of the law, thus playing a significant role in protecting human rights, including the constitutional right to privacy.

1.6. The Attorney General

The Attorney General of the State of Israel is the most senior legal authority within the executive branch, and as such he holds one of the most important and influential positions within the Israeli civil service. He is appointed by the government, based on a recommendation of a public professional committee headed by a former Supreme Court Judge and which comprises of members from the Knesset, Government, academia and the Israeli Bar Association. Moreover, the Attorney General is a professional impartial civil servant whose professional discretion is independent of governmental authorities.

The Attorney General performs several significant roles and duties. He is the chief prosecutor and head of the criminal prosecutorial system. In addition, he is the sole representative of the state in all judicial proceedings. As such, the Attorney General provides legal representation for the government, its policy, actions and resolutions.

[26] HCJ 651/03 The Association for Civil Rights in Israel v. Head of the Central Elections Committee of the Knesset 57(2) PD 62 (2003).
[27] RUTH GAVIZON, MORDECHAI KREMNITZER & YOAV DOTAN, JUDICIAL ACTIVISM: PROS AND CONS, 31 (2000).

Furthermore, the Attorney General serves as the chief legal counsel to the government, including the ministers and all governmental departments. In this capacity, he is entrusted with providing legal counsel to the entire executive branch, so as to assist the government in implementing its policy within the confines of the law and in accordance with constitutional principles. The Supreme Court has set forth the rule that the legal advice of the Attorney General and his legal interpretation of the law bind the government, as long as a court has not ruled otherwise.[28] An example of such interpretation given by the Attorney General in recent years in the field of protection of privacy, is a guideline concerning the taking of voice samples of prisoners and their retention in a database.[29]

More particularly, the Attorney General provides advice and assistance to the government with respect to bills presented by the government to the Knesset for legislation, in order to ensure compliance with constitutional principles. The Attorney General, through his representatives in the Office of Legal Counsel and Legislative Affairs, is involved in various stages of government legislation (including secondary legislation), from the initial drafting of the proposed bill to the submission of the bill to the legislature.

Considering that the Attorney General solely represents the government in judicial proceedings, and that his legal interpretations bind the government, the Supreme Court ruled that in the rare cases where the Attorney General concludes that the government's position is unlawful, he may decide not to represent or defend such position before the court.[30] This rule reflects the fundamental notion in Israel's legal tradition that in all its capacities, the Attorney General is entrusted with representing the broader interest of the general public and ensuring the rule of law.[31]

The Attorney General's advisory function also applies directly to privacy legislation, which is within the purview of the Minister of Justice, including, *inter-alia*, the

[28] HCJ 4247/97 "Meretz" Party in Jerusalem v. Minister of Religions 62(5) PD 241 (1998); HCJ 73/85 "Kach" Party v. Speaker of the Knesset – Shlomo Hillel 39(3) PD 141 (1985).
[29] For further elaboration regarding this Attorney General Guideline and other guidelines see appendix 1.
[30] HCJ 4287/93 Amitai – Citizens for Proper Administration and Integrity v. Yizhak Rabin, Prime Minister of Israel 57(5) PD 441 (1993).
[31] HCJ 3495/06 Chief Rabbi of Israel Rabbi Yona Metzger v. The Attorney General (Jul. 30, 2007), Nevo Legal Database (by subscription, in Hebrew).

formulation of legislative policy in this field, the promotion of amendments to the PPL and the promulgation of regulations thereunder.

Finally, the Attorney General is authorized to join any judicial proceedings, either at the request of a court or on his own initiative in significant cases in which he asserts that the right of the state, a public right or a public interest may be affected or is indeed affected in these proceedings.[32] In the context of the right to privacy, the Attorney General's submissions to courts with respect to the interpretation of laws have favored greater privacy protection. These positions have ultimately impacted court rulings.[33]

1.7. The Privacy Protection Authority

The PPL empowers the Registrar of Databases to enforce its provisions with regards to data protection, and provides the Registrar a variety of enforcement tools. The Registrar conducts criminal and administrative investigations and audits, imposes administrative fines and possesses the power to terminate or suspend activities of databases by suspending or erasing their registration. As mentioned above, the office of the Registrar, empowered with these authorities, works within the organizational framework of the Privacy Protection Authority (hereinafter: PPA).

The PPA regulates and enforces data protection across all sectors; private and public, according to the provisions of the PPL.

As an independent authority specializing in data protection, the PPA focuses on strengthening data protection and empowering individuals by promoting individual's control on personal data and by promoting processes of "Privacy by Design". The goal of the PPA is to reduce the risks for personal data, taking into consideration the frequent advancements in the digital environment.

As a civil rights gatekeeper in the field of data protection, the PPA monitors and promotes compliance with the provisions of the PPL on data protection among the private sector, NGOs and government authorities.

The PPA achieves its goals not only through enforcement, but also through a broad range of educational activities, by issuing interpretative guidelines, appearing before

[32] Procedures Order (Appearance of the Attorney General) [New Version], 5728-1968, §1.
[33] See, for example, the description of the Isakov and Kalanswa cases, in part 3.2, as well as other examples listed in appendix 2.

the Israeli Knesset and providing a professional opinion on privacy and data security in legislation processes, and advising the government in the creation and handling of major databases and digital projects.

In accordance with the PPL, The PPA reports annually to the Knesset on its activities, thus enhancing public accountability of its activities.

1.8. The Privacy Protection Council

The Privacy Protection Council is a statutory body[34] that was formed in 1986, and its members comprise of representatives from the academia, private sector and public sector, all having the relevant expertise in the field of privacy protection.

The main function of the Council is to advise the Minister of Justice on matters related to the protection of privacy. The Council expresses its opinion to the Knesset as well, with the aim of shaping policy and advocating for enhanced privacy protection in Israel. Thus, for example, the Council expressed its position in debates held in the Knesset concerning the Credit Data Law, 5776-2016.[35] Following the Council's suggestion, an article was added to the law regarding the appointment of a DPO at the Bank of Israel, which will be the controller of the credit database [36].

[34] See §10A of the PPL.
[35] Credit Data Law, 5776-2016, SH 2551 p. 838. Hereinafter: Credit Data Law.
[36] §17 of the Credit Data Law.

2. Significant updates - overview

2.1. Legislation regarding the protection of privacy and personal data

2.1.1. Privacy Protection Bill (Enforcement Powers)

As mentioned in part 1, the Registrar of Databases is entrusted with the protection of privacy of databases and ensuring compliance with the relevant provisions under Israeli law. The purpose of the bill is to enhance the supervision and enforcement capabilities and supervisory mechanisms of the Registrar, in order to address the contemporary risks to the right to privacy and personal data more effectively. The bill proposes to expand the authority given to the Registrar and to grant him the authority to conduct administrative inquiries into administrative violations and criminal enforcement. An important tool that the bill proposes to make available to the Registrar is the authority to impose financial monetary penalties. The expansion of the "toolbox" available to the regulator by way of establishing an alternative mechanism of the criminal procedure – a mechanism of imposing administrative monetary penalties for breach of the PPL – is intended to enable a quick, efficient and proportionate response to privacy violations thereunder.

The monetary penalties are based on a formula set out in the bill taking into account the severity of the violation, the number of data subjects and the sensitivity of the data. In severe cases the sanction could reach 3.2 million NIS for each violation.

The proposed bill would replace the term “Registrar of Databases” with the term “Director of Data Protection” in order to more accurately describe the role granted to the Registrar under Israeli law.

Regarding the supervision powers, the bill proposes, *inter alia*, to empower the Director’s officials to require that an individual identifies himself for the purpose of an investigation, as well as to require a copy of software and computer data that does not include personal data, or personal data samples, which would be collected in the required scope solely for the purpose of the supervision. The Director must delete the data when it is no longer reasonably required for the purpose it was obtained. It is further proposed to give the Director the authority to conduct administrative inquiries in cases where there are reasonable grounds to believe that provisions of the law have

been violated, as well as criminal investigative powers in cases where suspicion has been raised that an offense has been committed. The authority of the Director set forth in the bill is subject to certain listed limitations, including an explicit duty of confidentiality with respect to data so collected. It should be noted that even today the Registrar has the authority to conduct criminal investigations.[37]

The proposed bill contains provisions with respect to the unique manner of applying the supervisory and inquiry powers to security entities. The need for formulating a special model for these bodies derives from the fact that a significant part of their classified activities involves databases, and exposing these databases to external inspection could create a threat to national security. Recognizing the need to ensure that such databases nonetheless operate pursuant to the law and remain subject to supervision and enforcement, an internal supervision model is proposed for security bodies. According to this model, the supervision activities will be done by a Privacy Inspector according to the guidelines of the Director, and the findings of the Privacy Inspector will be reported to the Director. It should be noted that the regime enshrined in the new bill regards only to the aspects of supervision and enforcement pertaining to security bodies, and not to the substantive aspects of the PPL. For further explanation regarding the substantive aspects, see part 5.2.2.

Finally, violations of provisions of the bill will constitute offenses of the law under the PPL. The bill also establishes new offenses under the PPL. Particularly serious offenses will be defined as criminal offences and will be enforced as such.

The Committee of Ministers for Legislation Matters has approved the bill and it passed first reading in March 2018. The Plenary of the Knesset assigned the preparation of the bill for the second and third readings, to the Constitution, Law and Justice Committee of the Knesset.

2.1.2. **Privacy Protection (Data Security) Regulations, 5777-2017**

One of the most significant recent developments in data protection in Israel has been the publication of the Privacy Protection (Data Security) Regulations, 5777-2017

[37] Criminal Procedure Order (Testimony), 5688-1927, §2. See also part 4.1.3

(hereinafter: Data Security Regulations) in May 2017. The regulations came into effect in May 2018.

The regulations apply to both private and public sectors and establish mechanisms aimed at making data security part of the management routines of all organizations processing personal data. The regulations are a product of an in-depth study of legislation, standards and parallel Israeli and international guidelines. The regulations were enacted after extensive consultation with the Israeli public, and in particular with relevant stakeholders.

It is expected that the regulations will substantially improve the level of data security in Israel because they are simultaneously both flexible, concrete and specific to a degree that offer organizations both regulatory certainty and practical tools that are simple to implement. The entry into force of the regulations ushers in a new era for privacy protection in Israel.

The regulations classify databases into four groups according to the level of risk created by the processing activity in those databases: high, medium, basic and databases controlled by individuals that grant access to no more than three authorized individuals. The duties of the controllers are determined in accordance with the level of risk. The level of risk is defined by the data sensitivity, the number of data subjects and number of authorized access holders.

The regulations provide that, in specific circumstances, the PPA may impose certain additional requirements on a database in order to strengthen its security, or exempt certain databases from specific provisions. For example, the PPA may instruct that a low level risk database must comply with provisions that apply to medium risk databases.

Below are the main mechanisms in the regulations aimed at strengthening data security by creating awareness, accountability and working procedures.

1) Database Settings Document

The regulations require data controllers[38] to produce a "Database Settings Document" that will include the details of the data collection, processing and usages. The Document

[38] Throughout this Report, the terms "Controller" and "Processor" refer to the parallel terms of "owner of a database" and "holder of a database" under Israeli law.

must specifically address types of data being held, the scope of trans-border data transfers, types of processing activities by data processors, the main risks for data, means of mitigating the defined risks, contact details of the controller, processor and security officer.

The data controller must review and update the document annually or more frequently if needed (in the event of a data breach or where significant technological changes are made to the database). The annual review is also meant to prompt the controller to examine if it is holding excessive data.

2) Security Officer

The PPL requires that a Security Officer (SO) be assigned to public sector controllers, financial sector controllers, and substantive processors. The regulations define the position of SOs, their duties and their resources, whether the SO has been appointed voluntarily or because of legal obligation.

The SO reports to the controllers' manager or another senior manager. The roles of the SO include producing a draft of the organization's data security policy for the approval of the controller's authorized governing bodies, producing a plan for periodical audits in order to ensure the compliance with the regulations; executing the plan and reporting to the controller. The SO is not to fulfil additional roles if those could place him in a potential conflict of interest. Any additional role of the SO must be clearly defined. The controller must allocate appropriate resources required for the fulfilment of the SO's duties.

3) Data Security Policies

Controllers must keep documented data security policies. The policies include, *inter alia*, physical security measures, access authorizations, a description of protective measures and the way to operate them, instructions for authorizations' holders, risks for data and means to mitigate the risks, including encryption, means to handle security events, and a plan for managing mobile devices. For databases subject to medium and high security level the obligations include, in addition to those noted above, identification and verification measures, access controls including keeping records of access to systems, periodical reviews for security measure and for security procedures, and security data backup, use of data in development environment.

The procedures must be reviewed annually and more frequently if major changes have been made in the systems or in a case of new risks. The controller determines who in the organization is authorized to view the procedures or parts thereof, according to their roles in the organization.

The regulations require mapping the structure of the database and systems with security significance. The controller must keep documentation of the hardware and software systems with security significance detailing, *inter alia*, the types of infrastructure, communications systems, security systems and software that are connected to the data, software that is connected to the systems, network chart, and dates of updates. This documentation must only be accessible to relevant authorized individuals holding specific duties within the organization.

Databases to which high levels of security risk are assigned require data controllers to conduct risk assessments and penetration tests every eighteen months.

4) Physical Security

Systems are to be kept in protected spaces in order to avoid unauthorized access. In the case of databases to which medium or high levels of security risk are assigned, controllers must keep records of every access to the location of the systems.

5) Human Resources

Access to data is to be granted to an employee only after the employer took reasonable measures to ascertain the employee's suitability and only after the employee has received proper training with regards to data protection and security. In cases of databases involving medium and high levels of security risk, employees are to be trained periodically, and a least once every two years.

6) Access Authorizations

Access to data and systems is to be granted in accordance with the role of the employee in the organization and only when necessary to carry out their tasks. The controller must keep a list of employees with access rights and their roles in the organization.

In cases of databases involving medium and high levels of security risk, identification should, to the extent possible, be enabled through physical means that are in the sole control of the employee. The means of identification and the requisite strength of the password must be determined in the security procedures. In such cases, procedures will

address also the following: number of permitted password-based access attempts, frequency of password changes (a password must be valid for no more than 6 months), automatic disconnection following inactivity, etc.

7) Access Control

Medium and high levels of security require automatic recording of access including: user identity, date and time of access, which part of the system was accessed, type of access, whether the access succeeded or failed.

This control system must be able to give notifications about attempts to make alterations or deactivations of its functions.

8) Security Incidents and Data Breach Notification

The regulations define "severe data incidents" in various ways dependent upon the level of risk of the databases: in databases involving high levels of security risk, any unauthorized data usage or data infringement constitutes a severe data incident, and in databases involving medium risk, it is defined as the unauthorized data usage or data infringement of a substantial part of the database.

Controllers must notify the PPA about severe data incidents and about the measures that were taken in order to mitigate the risk. The PPA may instruct the controller to notify data subjects about the breach after consulting with the National Cyber Directorate.

Controllers are required to keep a record of every security incident, through an automatic mechanism if possible. Organizational security procedures must include instructions with regards to addressing security incidents in accordance with the severity of the incident and the sensitivity of the data. Such instructions must address, *inter alia* termination of access rights and, notifying the controller about the data breach and actions taken thereafter.

In cases of medium risk, the controller's management must conduct an annual review regarding the security incidents that occurred in the organization and must update the security procedures if necessary. In cases of high levels of risk, the management reviews must take place every three months.

9) Additional Provisions

The regulations include provisions on precautions that must be taken with regards to connecting systems to mobile devices, separating systems that enable access to personal data from other systems in the organization, avoiding connection of such systems to the internet or taking appropriate means when connecting the systems to the internet, encrypting data, and ensuring relevant authorization and authentication means for remote access.

10) Outsourcing

In outsourcing agreements, a controller must define the personal data the service provider may process, purposes of usage, systems that the service providers may access, period of the agreement, the means by which the data will be returned to the controller, deletion of the data, data security measures to be taken by the service provider, confidentiality agreements with the service providers and his employees, and annual reports from service provider to data controller. In addition, the controller must review and oversee the external party's compliance with the provisions of the agreement and the provisions of these regulations.

11) Periodical audits

Medium and high levels of security risk require conducting audits every two years, both internal and external, in order to ensure compliance with the regulations. The audit must indicate whether the security means comply with the regulations, identify inadequacies and suggest measures to amend them.

2.1.3. **Amendment of the Privacy Protection Regulations (Terms of Holding Data and Its Maintenance and Procedures for Transfer of Data between Public Bodies), 5746-1986**

Chapter D of the PPL addresses the limitations on the transfer of personal data by public bodies. The main provision under the chapter (article 23b) prohibits public bodies from transferring personal data unless the data has been lawfully disclosed or in cases where the data subject has given his consent to such transfer. In general, the transfer of personal data between public bodies is only permitted if it is needed for a cause within the framework of the authorizations or roles of the public body providing the data or

the public body receiving it, and provided that also not be prohibited under other legislation, regulations or professional ethics principles.[39]

In order to supplement the law, the Privacy Protection Regulations set forth a procedure for examining whether the conditions for transfer of personal data between public bodes are met. This procedure requires the establishment of a committee for the transfer of personal data by the general manager of any public body, headed by the general manager or a representative who reports directly to the manager. The members of the committee shall include the chief legal advisor of the public body or a representative thereof, as well as employees engaging in data management and security. The committee is required, *inter alia*, to discuss and pass a resolution regarding requests for providing personal data by such public body, and to examine incoming requests for personal data transfers issued by another public body. The regulations also include provisions concerning data security of the actual transfer and forms to be filled out by the requesting and disclosing bodies.

The method of examining requests for transfer of data by the committees in government ministries is regulated by guidelines given by the Deputy Attorney General. The guidelines refer to the Basic Law: Human Dignity and Liberty and instruct that the committees should examine the requests also in light of the of proportionality and reasonableness tests, while weighing carefully potential privacy violations.

In the course of 2016, the issue of transfer of data between government bodies was examined by an inter-ministerial team based, *inter alia*, on a comparative review of the laws in other countries. The report of the team, issued in July 2016, refers to various challenges and restrictions in sharing data between governmental bodies, including the

[39] §23C of the PPL states:
"Delivery of data shall be permitted despite the provisions of section 23B, where it is not prohibited by law or by principles of professional ethics –
(1) Among public bodies, where one of the following occurs:
(a) Delivery of the data within the capacity of authorities or functions of the person delivering the data and it is required for purpose of implementing a law or for a purpose within the capacity of the authority or the function of the person delivering or receiving the data;
(b) The delivery of data is to a public body which may request such data by law from any other source;
(2) From a public body to a Government unit or to another State institution, or between aforesaid units or institutions, if delivery of the data is required for the implementation of any law or for a purpose within the capacity of authorities or functions of the body delivering or receiving the data; however, no data shall be provided as aforesaid which was provided on condition that it shall not be delivered to others."

seemingly cumbersome process required by the current regulations. The report suggests maintaining the basic principles for inter-ministerial transfer of data, including the requirement that data be handled and stored in a compartmentalized manner and the requirement that any transfer of data be conditional upon a request by another government body. On this basis, the team recommended, *inter alia*, that the oversight of data transfers between the bodies should remain with the committees, and that clear guidelines regarding the frequency of meetings of the committee should be issued. In addition, a clear timeline would be established within relevant regulations, along with additional amendments designed to clarify the requirements for securing the data in the course of the transfer. The team's recommendations were adopted in Government Resolution 1933.[40]

Based on the report of the team, draft regulations have been prepared in order to streamline and clarify the process and the legal principles at play. These include substantive standards that will guide the committees in their examinations, some of them explicitly referring to the proportionality tests.

Comments from the public on the regulations have been received and processed, and the regulations are now in their final stage of approval at the government level.

2.2. Implementation of privacy and data protection principles in other legislation

In addition to the provisions under the Basic Law: Human Dignity and Liberty of 1992 and the PPL, the right to privacy is addressed through other legislative texts that involve processing of personal data by the private sector or by the government. For example, the Equal Rights for Law, 5758-1998,[41] the Income Tax Order [New Version],[42] and the Credit Data Law contain explicit privacy and personal data protection provisions.[43]

The provisions in these laws are intended to minimize to the extent possible the privacy risks involved in the regulated activity, with respect to the different aspects of processing the data such as the scope of permitted data processing, the planning and designing of the relevant technological system, the purpose of processing and the

[40] See further, part 3.1.1.
[41] Equal Rights for Law, 5758-1998, SH 1658 p. 152. Hereinafter: Equal Rights for Law.
[42] Income Tax Order [New Version], SH 339 p. 122.
[43] See appendix 2 for a more comprehensive list, which includes also relevant government resolutions.

security and deletion of the data. Such provisions implement the technological aspects of principle of "privacy by design", regarding the design of data systems and securing the data, and also implement other important data protection principles such as data minimization, purpose limitation, and storage limitation.[44]

As mentioned in part 1.6, the Office of Legal Counsel and Legislative Affairs, which is headed by the Attorney General, was involved with the shaping of these laws, and in particular with ensuring that they are drafted taking into account privacy and personal data protection considerations.

2.2.1. **The Credit Data Law, 5776-2016**

The Credit Data Law, 5776-2016 constitutes a comprehensive reform of the field of credit data in Israel, and is scheduled to go into effect in 2019. The law sets new rules for the collection and sharing of credit data, while protecting the privacy of the data subjects through various restrictions and purpose limitations. The new law is based on the recommendations of a government committee established to examine the issue of credit data sharing for public and economic purposes.

The committee found a link between the existing legal framework for credit data sharing and the lack of competition within the centralized retail credit market in Israel, and concluded that in order to increase competition in the credit market and enhance individuals' access to credit and minimize discrimination in this field, credit companies should be allowed to collect more complete credit data that indicates the probability of a person repaying his debts (combining positive and negative data). The committee was acutely aware of privacy concerns and proposed several mechanisms to allay such concerns and reduce the risks to privacy. Thus, for example, the committee found that privacy in this field would be better protected by having credit data collected and stored by the Bank of Israel, rather than by various private entities (as was the case prior to the entry into force of the new law), providing licensed private credit bureaus with access to the database while overseeing the transfer of data to credit providers.

Additionally, while the new law expands the scope of data collected by default regarding a customer, it simultaneously creates extensive mechanisms and restrictions

[44] As a rule, the provisions under such specific laws apply in addition to the PPL, unless the laws contain specific overriding provisions.

to protect privacy and personal data, thus minimizing privacy risks. First, the new law gives the data subject the possibility of objecting to the collection of his data, and when a person so objects, the law provides that identifiable data regarding him shall be deleted and only data clearly indicating that the individual does not repay debts can still be collected and stored. According to the previous law, the category of data that can be collected without consent is "data indicating that the data subject does not repay debts", while the new law is more restrictive regarding the scope of such data that can be collected without consent. Data that can be collected by default is also limited to data focused on credit extended to a customer or which a customer is entitled to borrow, and credit repayment, and does not include other economic or financial data.

The new law also requires that the technological system that will underpin the database be designed and updated in such a way as to minimize to the extent possible the risk of violating the customers' privacy. The law requires that the Registrar of Databases must be consulted and that the data be pseudonymised when stored. The law also provides for the appointment of a privacy protection officer at the Bank of Israel, and sets forth in detail his role and powers. In addition, it includes detailed provisions intended to ensure the quality of data and limits the scope of access to data and permitted processing purposes (which are more limited than those in the previous law), as well as provisions concerning data security, the period for retaining data and deletion of data. Moreover, the law allows access to identified data only with the consent of the data subject. It includes an explicit prohibition on any attempt to identify customers based on unidentified data. Finally, the law includes a comprehensive framework of supervision, administrative inquiry and enforcement powers, which may be exercised also with respect to third party entities that obtained data from the database. These powers are aimed at reducing possible concerns of violation of the provisions of the law and limiting further distribution of the data.

2.2.2. **Traffic Regulations (Operating Cameras by a Local Authority for Documenting Illegal Use of a Public Transportation Lane), 5776-2016**

A 2016 amendment to the Traffic Order [New Version][45] authorized local authorities to enforce traffic offenses regarding driving in a public transportation lane without

[45] Traffic Order [New Version], SH 352 p. 8.

authorization, by photographing or filming the public transportation lane and giving fines to those who have been filmed committing an offense. The order includes restrictions concerning protection of the privacy of the passengers and pedestrians, including the duty of maintaining the photographs in a manner that would not enable their identification, maintaining the data while reducing data security risks, and restricting the extent to which the photograph database can be connected to other databases beyond what is necessary for implementing the order.

The regulations enacted pursuant to the order[46] include detailed terms in respect of positioning cameras and their operation, notifying the public about the fact that photographs are being taken, the periods for retaining the film in the camera and in the central database at the local authority, as well as provisions regarding data security. The regulations further require the appointment of a senior officer within the local authorities who will be responsible for the implementation of the regulations, including the application of a mandatory annual compliance review.

2.3. Case law

Through a series of judgments in recent years, Israeli courts have taken an increasing role in protecting privacy as a constitutional right enshrined in the Basic Law: Human Dignity and Liberty. Below are some salient examples.[47]

2.3.1. Jane Doe v. Compensation Officer Case

In **Jane Doe v. Compensation Officer**[48]**,** the Supreme Court discussed the question whether a medical committee operating under the Persons with Disabilities Law (Compensation and Rehabilitation) [Combined Version] 5719-1959[49] is authorized to secretly investigate a subject in order to gather information about that person's medical condition or the level of his day-to-day functioning. In this case the Appellant was recognized as "disabled" within the meaning of the law. At a later stage, the Appellant

[46] Traffic Regulations (Operating Cameras by a Local Authority for Documenting Illegal Use of a Public Transportation Lane), 5776-2016, KT 7718 p. 2. Hereinafter: Traffic Regulations (Operating Cameras by a Local Authority for Documenting Illegal Use of a Public Transportation Lane).
[47] For further examples see appendix 2.
[48] PCA 2558/16 Jane Doe v. Compensation Officer - Ministry of Defense (Nov. 5, 2017), Nevo Legal Database (by subscription, in Hebrew).
[49] Persons with Disabilities Law (Compensation and Rehabilitation) [Combined Version] 5719-1959, SH 295 p. 276.

submitted an application to reconsider the level of disability that had been previously found, due to an aggravation in her medical condition. An investigator acting on behalf of the medical committee secretly followed and investigated her for four days, filming her during her everyday conduct in the public domain. Based on its investigation, the committee decided to reduce the Appellant's disability level.

In its judgment, the Court stressed that according to the principle of "legality of authority", each administrative authority must act solely within the powers vested in it by law. This principle is all the more important when the question of authority revolves around actions that involve infringement of basic rights. Accordingly, the Court emphasized that when the administrative act may lead to infringement of individual rights, there must be a clear, explicit and detailed legal authority in primary legislation allowing this act, and the legislative authority must itself comply with the limitation clause in the Basic law: Human Dignity and Liberty.

With respect to the case at hand, the Court indicated that a secret investigation in an individual's conduct infringes upon a protected basic right - the right to privacy. The violation was particularly problematic in that it related to matters of disability and health which belong to the core of an individual's personal life. The Court further noted that the fact that pictures of an individual were taken in the public domain, does not in and of itself nullify the privacy violation. The mere act of following a person without his knowledge, by entering the confines of that person's personal-private space, is an infringement of the individual's autonomy and dignity. Therefore, the medical committee's investigative actions were found to violate the appellant's right to privacy, and were held invalid since they were taken without explicit statutory authorization.

The Court indicated in this regard that if the legislator believes that there is need to allow secret investigations on behalf of the medical committee, it should explicitly anchor this authority in legislation, in a manner that complies with the principles of proportionality and reasonableness. In this context, the Court held that the exemption from liability provided in article 18 of the PPL could not apply in this case. The exemption in article 18 grants protection in a criminal or civil proceeding for infringement of privacy under certain circumstances (such as when the infringement was committed for the defense of a legitimate personal interest of the infringer, or there is public interest in the infringement which justified it under the circumstances). The

Court ruled that this article cannot legitimize, *ex-ante*, a general policy of an administrative authority that involves infringement of the right to privacy.

The Court thus granted the appeal and ordered that the Appellant's case be reconsidered by the medical committee without ascribing any weight to findings resulting from the investigation.

2.3.2. **Isakov Case**

The judgment in the **Isakov Inbar v. The State of Israel, the Commissioner for Women Labor Law**[50] case represents a significant development regarding employers' ability to monitor and read an employee's emails in the workplace.

In this judgment, the National Labor Tribunal held that the virtual sphere is equivalent in terms of the right to privacy in the physical space, such that an employer's invasion of this virtual space is equivalent to prying into a person's personal belongings, in a manner constituting an infringement of the constitutional right to privacy.[51]

In the judgment, the Tribunal laid out several principles to balance between the employer's ability to supervise its employees' activity, and the need to protect the employee's privacy: the employer must act in good faith, and the principles of proportionality, transparency, legitimacy, and purpose limitation apply. Thus, for example, in accordance with the principle of proportionality, the employer must examine alternative technologies for tracking that are less damaging to the employee's rights. Furthermore, in accordance with the principle of purpose limitation, the collection of the employee's personal data must be for a specific, pre-defined purpose. Likewise, pursuant to the transparency principle, the employer must inform the employees of the policy of the workplace in all matters pertaining to the uses of the computer and the circumstances in which it is possible to monitor the employee.

The judgment is also significant in that it emphasizes the necessity, as a prerequisite condition for monitoring, of obtaining the employee's free and informed consent as to the infringement of privacy. The employee must be provided with all relevant information required to fully understand the employer's intention. In this context, it was

[50] National Labor Court 8/90 Tali Isakov Inbar v. The State of Israel, the Commissioner for Women Labor Law, (Feb. 8, 2011), Nevo Legal Database (by subscription, in Hebrew).
[51] *Id.* at para. 6.

held that a high threshold should be set so as to ensure that the employee's consent is explicit, informed and given freely. The Tribunal emphasized that, beyond the employee's general prior consent to the employer's monitoring policy, the employer must also receive the employee's consent to any specific tracking activity or specific access to the employee's personal correspondence.

In light of the above principles, the Tribunal distinguished between "professional accounts" intended solely for work purposes, "mixed accounts" and "external-private accounts". Thus, for example, in all matters pertaining to the employee's external-private account (for example, a Gmail account), the tribunal held that this account was owned exclusively by the employee such that the employer is not entitled to monitor this account except pursuant to a court order (the conditions for which are defined restrictively and in detail in the judgment).[52] The Tribunal emphasized that even if the employee's consent had been given to the monitoring of the external email account, in view of the inherent power asymmetry in the employer-employee relationship, there was a presumption that this consent had not been given freely, such that the employer's monitoring activities based upon such consent should not be allowed.[53]

This judgment is considered authoritative and seminal, placing special emphasis on the importance of ensuring the protection of the employee's privacy in the employee-employer relationship, and imposing stringent requirements that an employer must comply with in this context.[54]

2.3.3. **Facebook Case**

In the judgement of **Facebook Inc. v. Ohad Ben Chamo**,[55] an appeal on a class action of Facebook users against Facebook, the Supreme Court dealt mainly with a choice of jurisdiction clause according to which disputes between a user and Facebook were to be referred to the courts of California, and pursuant to U.S. law.

[52] *Id.*at para. 50.
[53] *Id.* at para. 45-50.
[54] See also the Kalansuwa Municipality case, discussed in depth in part 3.2.
[55] CA 5860/16 Facebook Inc. v. Ohad Ben Chamo (May 31, 2018), Nevo Legal Database (by subscription, in Hebrew).

The plaintiffs claimed that Facebook's collection of personal data contravened the provisions of the PPL which require notification, informed consent and registration of the database. In

At the Court's request, the Attorney General submitted his position on the matter, to the effect that Facebook's terms of use constituted a standard form contract. As such, the Attorney General argued that the choice of jurisdiction clause was presumptively invalid, given the inequality in the balance of power between the company and the users, leading to the conclusion that the case should be litigated in the Israeli Court rather than in California.

The Attorney General further submitted that in the circumstances of the case, the choice of law clause was also invalid, such that Israeli law should apply. The Court partially agreed with this position, stating that the interest of Facebook's users in Israel prevails over Facebook's interest to centralize all causes of action against it in one place.

The Court thus held that Israeli courts have jurisdiction over the claim. However, it found that the claimants had not provided compelling evidence with respect to the claim that the choice of law clause should be invalidated as well, though it left open the possibility of ruling otherwise should such evidence be adduced.

2.4. International Updates

In 2018 Israel became an observing state in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), and joined the first meeting which preceded the adoption of the amended Convention in May, 2018. As was mentioned in the meeting, it is believed that participation in the meetings of the Convention will strengthen Israel's cooperation with other countries for the benefit of increasing data protection worldwide.

3. Developments regarding substantive rules for the processing of personal data

3.1. Concepts

3.1.1. Interpretation of the concept of "data"

The scope of protection the PPL provides for personal data is delimited by several terms.

The main operative term in the PPL is the definitions of “data” (article 7 of the PPL) - "data on a person's personality, personal status, intimate affairs, state of health, economic status, professional training, opinions and belief."

In addition, the law includes a broader term – "data on a person's private affairs" which applies to the purpose limitation principle embedded in chapter A of the law (article 2(9)), to the provisions regarding direct mailing and to chapter D (data transfers between public bodies).

Additionally, chapter A of the law includes other terms of data such as "a matter that relates to a persons' intimate life" (article 2(11)), or “other data obtained in a way which infringes privacy under the provisions of the article” (2(10)).

Major privacy case law turns to the interpretation of these terms, and as discussed below, Israeli courts have tended to interpret them broadly.

1) In the **Manna** case,[56] the Supreme Court discussed the legality of a practice of collecting tax debts from individuals at a road block set up by the police, in which ID numbers of those individuals were transferred between the police and tax authorities. The Court rejected the claim that ID numbers do not constitute "private data" as defined by the PPL, and ruled that the identity number is not just a " sequence of numbers", but rather an identifier that, in combination with additional data, can be used to conclude more personal data such that "the person and the ID number becomes identical". The court ruled that granting control over the ID number to someone other than the data subject, integrating

[56] HCJ 6824/07Dr. Adel Manna v. Tax Authority (Dec. 20, 2010), Nevo Legal Database (by subscription, in Hebrew) .

of the number with other data, and transferring the number to third parties, infringes the right to privacy of the data subject.

2) In the **Gotesman** case,[57] a client refused to give his architect permission to publicize pictures of his house, which the architect had planned, on the architect's website. Nevertheless, the architect published the images on his website though without including the client's identifying details. The client sued the architect, claiming that the images fall within the scope of the term "a matter that relates to a person's intimate life" such that their publication infringed his right of privacy under article 2(11) of the PPL. The Supreme Court ultimately concluded that the publication of an image of the interior of the client's home violates his privacy. It held that article 2(11) of the PPL does not refer solely to the most intimate aspects of an individual's personal life, and that disclosure of other aspects of his personal affairs could trigger a violation under that article. The Court further held that the article applies where a reasonable person can infer the identity of the data subject through the published data. As to the degree of identifiability, it held that the examination should be substantive and not technical: even if a person's actual name is not published, the potential of re-identification leading to linking the data to a particular person suffices. The Court also established an even lower threshold where the data is of particularly high level of sensitivity to an individual, holding that disclosure of such data would constitute a privacy violation even in the rare case where there is no potential to link the data to an individual, if the individual were to feel that his privacy had been severely violated.

3) In the **IDI** case,[58] a financial services company had been granted a foreclosure order against an individual in order to seize his funds in the company's possession, and later used the data pertaining to the foreclosure for another purpose, namely to assess entitlement to insurance of the individual that was the subject of the order. The District Court ruled that in the digital age which

[57] CA1697/11 Gotesman Architecture Ltd. v. Arie Vardi (Jan. 23, 2013), Nevo Legal Database (by subscription, in Hebrew).
[58] AdminC (TA) 24867-02-11 I.D.I. Insurance Company Ltd. v. Ministry of Justice the Israeli Law, PPA – the Registrar of Databases, (Jul. 7, 2012), Nevo Legal Database (by subscription).

enables enhanced searches of data and cross-referencing, the definition of private data must be interpreted more broadly. The court rejected the claim that foreclosure orders are not private data. The Supreme Court upheld the decision and noted its approval of the merits of the District Court's decision. [59]

4) In the **Freedom of Information** case,[60] the Supreme Court interpreted the term "data on a person's private affairs" as including the names of persons who have reached plea deals with the tax authorities, as well as the names of persons who applied for positions within the civil service and the reasons for disqualifying their candidacy. The Court's ruling in this case relied on previous case law in which it had interpreted broadly the term "data on a person's private affairs", stating that "a person's private affairs are any data related to their private life, e.g. name, address, telephone number, place of work, identity, friends, relations with spouse and family, etc.[61]".

5) In the **Shenrom** case,[62] the Supreme Court ruled that a list of property holders which includes details regarding the size of the property, for taxation purposes, is protected under the term "data on a person's private affairs" because it may reveal data about one's economic condition. Similar to its ruling in the **Freedom of Information** case, the court adopted an approach which relied on the constitutional status of the right to privacy and on previous case law, to interpret "data about a person's private affairs" broadly and in a flexible manner based on the circumstances.

Regarding the aspect of identifiability of the data, the broad approach adopted in the **Gotesman** case is also reflected in resent relevant government resolutions, which are binding on all government entities:

1) **Government Resolution 1933 regarding "open data" of the government's databases (30.8.16) –** This resolution requires public service bodies to grant

[59] AdminA 7043/12 I.D.I. Insurance Company Ltd. v. Ministry of Justice the Israeli Law, PPA – the Registrar of Databases (Jan. 15, 2014), Nevo Legal Database (by subscription, in Hebrew).
[60] AdminA 398/07 The Movement for Freedom of Information v. The State of Israel – Tax Authority 63(1) PD 284 (2008); AdminA 9341/05 The Movement for Freedom of Information v. the Governmental Companies Authority (May 5, 2009), Nevo Legal Database (by subscription, in Hebrew).
[61] CA 439/88 Registrar of Databases v. Moshe Ventura 48(3) PD 808 (1994).
[62] AdminA Municipality of Hadera v. Shenrom ltd. (Jul. 16, 2012), Nevo Legal Database (by subscription, in Hebrew).

access to their databases to the public, excluding personal "identifiable data", defined broadly to include un-identified data that can be potentially identifiable if integrated with additional data. The resolution provides that a determination of whether data may be identifiable is to be made upon receiving the input of a technical expert, a data security consultant and legal counsel.

2) **Government Resolution 2733 regarding the promotion of "Digital Health" (25.3.18) –** In order to promote the field of digital health and create an ecosystem for big data research and medical development, the resolution requires that the Minister of Health, with the consent of the Ministry of Justice and the Ministry of Finance, issue legislation or regulations regarding secondary use of health data, *inter alia,* for purposes of medical research. According to the resolution, these future regulations must implement recommendations of a committee that examined the subject, and must be based on principles of privacy protection and medical secrecy. The resolution requires several levels of protection including adequate pseudonymisation of the data, mechanisms for prior approval of specific uses of the data, organizational requirements regarding who can process the data, supervision and data security measures regarding the processing of data, and mechanisms to enable the data subject to opt in or out of such processing based on the level of identifiability of the data and the purposes of the processing. [63]

3.1.2. **Interpretation of the term of "sensitive data"**

Article 7 of the PPL includes definitions both for "data" and "sensitive data".[64] "Sensitive data" is defined as "data on a person's personality, personal status, intimate affairs, state of health, economic status, opinions and beliefs".[65]

The main direct statutory implication of the difference between the two terms is that a database containing sensitive data must be registered as such, regardless of other conditions which are required by the law for registration.[66] The Privacy Protection

[63] For further elaboration on both resolutions, see appendix 1.
[64] For the interpretation of the term "data" see part 3.1.1.
[65] The definition of "sensitive data" also allows the Minister of Justice to issue a decree, with authorization by the Knesset Constitution, Law and Justice Committee, defining more kinds of data as sensitive data. No such decree has been issued thus far.
[66] §8(c)(2) of the PPL.

Regulations (Data Security), 5777-2017[67] also provide for an increased level of data security requirements when the database includes "sensitive data". Moreover, the Privacy Protection Bill (Enforcement Powers) provides for increased fines when the privacy violation involves "sensitive data", defined, *inter alia*, as data regarding an individual's personal affairs, medical data or mental health, genetic data, data regarding opinions and beliefs, criminal record, biometric data, communications data and economic data.

Alongside the general provisions of the PPL and the various Privacy Protection Regulations Israel has specific topical legislation regulating the handling of particularly sensitive data. For example:

1) **Genetic Data Law, 5761-2000[68]** – In light of the heightened sensitivity and uniqueness of genetic data, the law includes specific provisions regarding the data, intended to enable medical treatment and research while protecting individuals' right to privacy.
2) **Rights of Patient Law, 5756-1996**[69] – The law regulates several aspects of the rights of patients, including the right to medical secrecy, setting forth specific conditions under which a caretaker or medical institution are allowed to transfer medical data.
3) **Credit Data Law** – As mentioned in part 2.2.1, this law constitutes a comprehensive reform within the field of credit data, establishing a new system for processing credit data subject to limitations and restrictions regarding the collection, transmission and purposes of processing of such data, all of which are intended to protect the privacy of the data subject and prevent undue infringements of privacy.

Additional specific frameworks of legislation regulating databases containing sensitive data include: the Criminal Registry Database, which is run by the police under the Crime Register and Rehabilitation of Offenders Law, 5741-1981[70]; the biometric

[67] Privacy Protection Regulations (Data Security), 5777-2017, KT 7809 p. 1022. Hereinafter: Data Security Regulations.
[68] Genetic Data Law, 5761-2000, SH 1766 p. 62. Hereinafter: Genetic Data Law.
[69] Rights of Patient Law, 5756-1996, SH 1591 p. 327.
[70] Crime Register and Rehabilitation of Offenders Law, 5741-1981, SH 1031 p. 322. Hereinafter: Crime Register and Rehabilitation of Offenders Law. Hereinafter: Crime Register and Rehabilitation of Offenders Law.

identification of suspects, defendants, detainees and prisoners database, regulated under the Criminal Procedure Law (Enforcement Authorities – Body Searches and Collecting Means of Identification) 5756-1996;[71] Communication data, regulated under the Criminal Procedure Law (Enforcement Powers - Communication Data), 5768-2007,[72] and wiretapping data, regulated under the Wiretapping Law, 5739-1979.[73]

These specific pieces of legislation serve as additional protection for sensitive data, beyond the protection afforded by the provisions of Basic Law: Human Dignity and Liberty, and by the PPL.

Moreover, there is ample case law dealing with the need to extend broader privacy protections when the data at stake is sensitive personal data. Below are some examples.

1) In the **Garayes** case,[74] a couple was followed and photographed without their knowledge in an intimate situation, in a forest, and the pictures had been shown to their family members and acquaintances. The Court ruled that the appellant's actions constituted a violation of article 2(3) of the PPL even though this article refers to photographing a person "in a private domain" and the photographs were taken in the "public domain". The Court explained that the term "private domain" should be interpreted with reference to the specific context, in light of the provisions of Basic Law: Human Dignity and Liberty, and should not be reduced, in this context, to its technical definition in property law. As such, in this particular case, the parties were in fact in a private domain.

2) In the **John Doe** case,[75] the question was whether photographs taken by one party for the purpose of a divorce claim, in which the other party had been documented having sexual relations with a third party, are admissible in court procedures under the provision of article 32 of the PPL. According to this article, data obtained by committing an infringement of privacy is inadmissible

[71] Criminal Procedure Law (Enforcement Authorities – Body Searches and Collecting Means of Identification) 5756-1996, SH 1573 p. 136. Hereinafter: Criminal Procedure Law (Enforcement Authorities – Body Searches and Collecting Means of Identification).
[72] Criminal Procedure Law (Enforcement Powers - Communication Data), 5768-2007, SH 2122 p. 72. Hereinafter: Telecommunication Data Law.
[73] Wiretapping Law, 5739-1979, SH 938 p. 118. Hereinafter: Wiretapping Law.
[74] CA 2126/05 Garayes v. State of Israel (Jun. 26, 2006), Nevo Legal Database (by subscription, in Hebrew).
[75] HCJ 6650/04 John Doe v. Netanya District Rabbinical Court (May 14, 2006), Nevo Legal Database (by subscription, in Hebrew).

as evidence in Court unless the data subject consents, the court allows it on specific grounds, or the infringer has a defense under article 18 of the law.[76] The Supreme Court ruled that the greater the violation of privacy is, the greater the weight that ought to be given to privacy considerations and that, in the present circumstances, in light of the sensitivity of the data, the infringement on privacy was severe and extreme. The Court also rejected the article 18 defense, given the severity and disproportionality of the violation.

3) In the **Jane Doe** case,[77] regarding the publication of a book detailing the intimate relationship between the author and his former spouse, the Supreme Court decided that intimate details of the relationship should be granted strong protection, and under the circumstances of the case, in the balance between freedom of speech and the right to privacy, the latter should prevail. In light of the excessive infringement of privacy in this particular case, the Supreme Court approved the District Court's injunction prohibiting the publication of the book.

4) In the **Kalanswa** case, the National Labor Tribunal ruled that biometric fingerprints data taken in workplaces constitute sensitive personal data, and therefore the employer cannot obtain these without the employee's consent, and must protect the data accordingly. The case is discussed in greater detail in part 3.2 in connection with the concept of "informed consent".

5) In the **Singer** case,[78] the Supreme Court dealt with the issue of whether the content of private email correspondence left on a computer screen can be copied by an employer without the consent of the data subject, and whether the copied emails are admissible in court procedures under the provision of article 32 to the PPL. The Supreme Court ruled that the act of copying private emails violated article 2(5) of the PPL, noting that leaving the correspondence accessible on a computer screen cannot be taken as consent to reading or copying it. The Court also emphasized that "in our time the private virtual space

[76] For further elaboration regarding §18 of the PPL, see part 3.4.
[77] CA 8954/11 Jane Doe v. John Doe (Apr. 4, 2014), Nevo Legal Database, (by subscription, in Hebrew). See also appendix 2.
[78] PCA 2552/16 Singer v. Yahav Nahmias Technologies (1990) Ltd. (May 10, 2016), Nevo Legal Database (by subscription, in Hebrew).

- the e-mail box, Facebook account etc. contains data that is extremely private and sensitive."

3.2. Grounds for lawful processing – consent of the data subject

According to article 1 of the PPL, it is prohibited to infringe a person's privacy without that person's informed consent. Regarding computerized processing of personal data, article 11 requires that any request for such data from individuals for the purpose of processing via a database be accompanied by a notice that informs the data subject as to whether the data is being collected pursuant to a legal obligation or is dependent upon the data subject's consent, the purpose for which the data is collected, the intended recipients of the data and the purpose for which they are to receive it.

Following are few examples of courts decisions from recent years emphasizing the importance of the principle of informed consent:

1) **Milgam Cellular Car Parking** case[79] was a District Court case which dealt with the collection of data from individuals as part of a car parking payment cell phone service operated by a private company (Milgam). The data was collected by Milgam pursuant to an arrangement with the Coalition of Local Authorities (which consisted of various cities and towns in Israel). The main dispute concerned the personal data collected from data subjects by Milgam under the arrangement between the company and the Coalition, and what may be done with the personal data collected after the arrangement terminates.

   The question was complicated since, on the one hand, the contract between the bodies and the nature of their relationship, the database controller was the Coalition, such that the Coalition should receive the data once the contract terminates. On the other hand, the notice to the data subjects prior to the collection of data was vague and did not clarify that the data was collected on behalf of the Coalition. In an opinion submitted at the Court's request, the Attorney General emphasized central principles enshrined in the PPL that should be applied to the circumstances of the case – the principle of **informed consent** and the principle of **purpose limitation**.

[79] Originating Motion 60239-03-15 The Local Government Economic Services Co. Ltd. v. Milgam Cellular Car Parking Ltd. et. al. (Oct. 27, 2015), Nevo Legal Database (by subscription, in Hebrew).

The Attorney General explained that in his view, one of the underlying values of the PPL – and indeed, of the right to privacy in Israel law – is the data subject's control over his data. This applies to the delivery of the data, the permissible recipients of such data and the permissible uses of it. Thus, the data subject must be informed clearly and in advance regarding the entire relevant aspects of the data processing, including the identity of the database controller and processor, and his consent must pertain to all these aspects. Similarly, the Attorney General stressed that given the importance of informed consent, in cases where the data is collected from the data subject by a processor on behalf of a controller and there is no direct contact between the data subject and the controller, it becomes all the more important to inform the individual of the identity of the database controller and to be obtain his informed consent.

Finally, the Attorney General addressed the respective duties of the database controller and processor, stressing that the obligations and liabilities imposed upon a database controller apply regardless of whether the controller has outsourced the data processing to a processor. In addition, certain obligations under the PPL apply to the database processor in the same way as they apply to the controller, including with regard to data security, determining rules of day to day operation etc. The Attorney General noted that all of the abovementioned aspects, regarding informed consent of the data subject and the respective duties of the database controller and processor, are also emphasized in guidelines issued previously by the PPA regarding the use of outsourcing for the processing of personal data.

The Court adopted the principles set forth in the opinion of the Attorney General in its judgment and ruled that the Coalition may not receive or use data of the data subjects, and may not transfer it to third parties, unless it receives their active, specific and informed consent. If such informed consent is not given, the data must be deleted from the existing database.

2) The **Kalanswa** case[80] raised the question of whether an employer is entitled to compel employees to provide and enter their fingerprints for a biometric

[80] Collective Dispute Appeal 7541-04-14 The New Workers' General Federation v. the Kalansawa Municipality (May 5, 2017), Nevo Legal Database (by subscription, in Hebrew).

timekeeping clock, as the sole means for maintaining timekeeping data in the work place. Here too, the Attorney General submitted the government's position on this question, further to the National Labor Tribunal's request. The Attorney General noted that forcing an employee to give a biometric sample involves an infringement of two basic rights - the right to privacy and the right to autonomy. Given that the sole purpose of the fingerprint requirement was to register attendance at the workplace, the Attorney General was of the opinion that this infringement did not withstand the constitutional tests.

The National Labor Tribunal's' judgment adopted the Attorney General's position. In the judgment, the Tribunal emphasized the importance of the right to privacy both for the individual and for society as a whole, and the necessity of interpreting this right broadly. It also stressed the ever-increasing necessity of protecting this right and the need to establish stable safeguards.[81]

Likewise, it was held that the very act of transferring fingerprint data to a third party infringes upon the right to privacy and autonomy. Another separate infringement is caused as a result of the significant risk of abuse of the fingerprint.[82] In light of this the Tribunal held that an employer is not entitled to compel the obtaining of fingerprints for the purpose of use in a biometric attendance system.

In order to determine whether the biometric fingerprint data is collected or according to the employee's informed and freely-given consent, the judgment established criteria which take into consideration the asymmetric nature of the employer-employee relationship. Regarding the concept of **freely-given consent**, the tribunal stressed that every case must be evaluated separately, and that if there exist any coercion, whether direct or indirect, such as sanctioning an employee who refuses to give his consent, then the employee's consent will not be considered having been given freely. Regarding the aspect of **informing**, it was held that the employer must convey the employees a clear and proportionate policy regarding the biometric system, including the entire relevant details, *inter alia* the nature of data that is collected, whether and where it will be stored, who will grant access to the data, how it will be secured, the

[81] *Id.* at para. 101-107.
[82] *Id.* at para. 113.

relevant risks, when it will be deleted, and the official who will be responsible for all of these aspects. In the absence of one of the abovementioned terms, the employee's consent will not be considered informed.

3.3. The purpose limitation principle

The basic principle of purpose limitation is embedded in article 2(9) of the PPL regarding any "data of a person's private affairs", and also in article 8(b) regarding data processed in a database.

The main case that focused upon the purpose limitation principle in recent years was the **IDI** Case, in which a District Court ruled that data obtained by a company in connection with a foreclosure could not be used for the purpose of assessing the individual's eligibility for car insurance, since this violated the purpose limitation provisions of the PPL. The court also emphasizes in its judgment the great importance of the right to privacy and the broad interpretation that should be applied to the PPL (see part 3.1 above).

Finally, most legislation that regulates processing of personal data in specific fields includes provisions that limit the use of the data to specific purposes and prohibits its use for other purposes. For example, the Credit Data Law (see part 2.2.1),[83] includes a provision that limits the use and transmission of credit data only to those explicitly permitted by the law or by a court order. Many other laws that apply to processing of sensitive personal data include similar provisions.[84]

3.4. Proportionality principle applied in the field of data protection

While the proportionality principle is rooted in constitutional and administrative law, the concept of proportionality has also informed court decisions with respect to data protection in the private sector. Specifically, the principle of proportionality affects the "good faith" defense under article 18(2) of the PPL, according to which in limited, enumerated circumstances, a person who infringes the right to privacy can be exempt from civil or criminal liability if the violations were carried out in good faith. These

[83] See further part 2.1.2.

[84] For other examples see: Traffic Regulations (Operating Cameras by a Local Authority for Documenting Illegal Use of a Public Transportation Lane) mentioned in part 2.2.2; Emergency Call Centers Law 5776-2016, mentioned in part 3.5; Supervision over Financial Services Law (Regulated Financial Services), 5776-2016, SH 2570 p.1098, mentioned in part 4.4 (hereinafter: Supervision over Financial Services Law (Regulated Financial Services)).

circumstances include the case where the infringer did not know nor should have known of the possibility of infringement of privacy; the infringer acted pursuant to a legal, moral, social or professional obligation or for the defense of a legitimate personal interest; and in the case of a publication protected under the Defamation Prohibition Law, 5725-1965.[85] Notwithstanding the foregoing, article 20(2) of the law denies the good faith defense if the infringement of privacy was "greater than was reasonably necessary for the interests that are protected in article 18(2)".[86] It should be noted that in the absence of an additional basis for the processing of personal data in Israeli law, apart from data subject's consent or statutory authorization, the defense clause is of significant importance for processing of data that does not fall under these *ex ante* formal bases.

The proportionality principle is also reflected in Regulation 2(e) of the Data Security Regulations**,** which entered into force in May 2018, and which applies to both public and private sectors. It requires database controllers, *inter alia*, to ascertain, once a year, whether the personal data kept in the database is not excessive in relation to the purpose of the database.

Following are few examples of courts decisions from recent years in the field of labor law, emphasizing the importance of the principle of proportionality:

1) The **Isakov** case, mentioned in above part 2.3.2, explicitly stated that the employer is subject to the principle of proportionality when collecting and processing employee's data.
2) In the **Kalanswa** case, mentioned above in part 3.2, the National Labor Tribunal relied, inter alia, on the principle of proportionality in ruling that the employer could not compel employees to provide their fingerprints in order to include them in the biometric timekeeping system.

In addition, several guidelines issued by the PPA, reflecting the Registrar's interpretation of the law, apply the proportionality principle in various fields.[87]

[85] Defamation Prohibition Law, 5725-1965, SH 464 p. 240.
[86] An example of implementation of these provisions, see HCJ 6650/04 John Doe v. Netanya District Rabbinical Court (May 14, 2006), Nevo Legal Database (by subscription, in Hebrew).
[87] For further elaboration regarding the PPA's guidelines, please see part 4.3.

1) **The PPA's guidelines regarding screening procedures for employment and the activities of employment screening agencies** emphasizes the proportionality principle to the use of diagnostic data, in addition to other data protection principles described further in part 4.2.
2) **The PPA's guidelines on Workplace Surveillance** are new guidelines which apply to all workplaces, including the private sector. The guidelines elaborate on the employer's obligation to act proportionately regarding the use of surveillance cameras and the collection of visual data about employees.
3) **The PPA's guidelines on the use of surveillance cameras in the public space,** published in 2012, apply to all database controllers that operate surveillance cameras in public spaces, including in private bodies. The guidelines elaborate on the obligations derived from the PPL including the obligation to act proportionately regarding the use of cameras, both while planning their coverage, installing them, and using them.

3.5. Data retention principle

According to article 14 of the PPL, a data subject may request deletion or rectification of data which is incorrect, incomplete, unclear or not up to date.

In addition, article 2(C) of the new Data Security Regulations provides that controllers must annually examine if the data stored in their databases is excessive for the purpose of each database. Legislation from the last years regulating specific activities involving the processing of sensitive personal data includes provisions requiring the deletion of the data. For example, article 23 of the Credit Data Law provides that data may be retained for a maximum of three years, after which it must be stored for up to seven years, and used only for specific purposes: use in legal proceedings, inspection or supervision according to the law, or another purpose that can be determined in regulations approved by a Knesset committee. After these periods, any identifying data must be deleted, and the rest of the data can be retained, but only in a manner that no longer enables the identification of data subjects.

Another example is a new amendment of the law regulating the activity of public emergency call centers[88]. This amendment was adopted in order to allow for timely

[88] Supervision over Financial Services Law (Regulated Financial Services).

responses to urgent calls or requests to the centers, while including provisions preventing disproportionate infringement upon the privacy of the callers. According to the amendment, communication companies must provide the emergency centers automatically with data regarding the location of each caller. However, the location data is to be stored in a separate database, which will be accessible to a worker of the center only for the purpose of attending urgent requests, or for making an *ex post* inquiry approved by a senior ranked official, regarding the manner in which a specific call was handled by the call center. Otherwise, data stored in the database can only be accessed pursuant to a court order, where the court is convinced that the data is necessary, and that the benefits of such access outweigh the privacy harm. Location data that was not accessed for these purposes must be deleted from the database after 3 hours, and in the case of the Police emergency service center, after 14 days.

3.6. Security principle – the newly enacted privacy protection Data Security Regulations

In May 2017, the Constitution, Law and Justice Committee of the Knesset approved the Data Security Regulations. These regulations are intended to provide a clear and detailed implementation framework in the field of data security and set forth, among other things, the obligation that applies to databases owners to report substantial data security breaches to the PPA.[89]

3.7. Restrictions on data transfers – the Privacy Protection Regulations (Transfer of Data Abroad)

The Privacy Protection Regulations (Transfer of Data Abroad), 5761-2001[90] prohibit transfer of personal data from a database in Israel outside its borders, unless the law in the destination state provides level of protection which is not less than the level of protection provided by Israeli law. However, the regulations include exceptions, and the transfer of data is permitted in other circumstances detailed in the regulations, amongst them that the data subject gave his consent to the transfer. The regulations also provide that in any case of transfer of personal data abroad, the receiver of the data must

[89] For further elaboration regarding the new Data Security Regulations please see part 2.1.2.
[90] Privacy Protection Regulations (Transfer of Data Abroad), 5761-2001, KT 6113 p. 900.

undertake in writing to apply sufficient measures in order to protect the privacy of the data subjects, and that it will not transfer the data to any other party.

3.8. The right of access

Article 13 of the PPL establishes the data subject's right of access to his personal data. In the PPA's guidelines regarding the right of access,[91] issued in 2017, the PPA interpreted this right as including data in any format or file type including video, text messaging and voice recordings, and as applying to customers who want to access data collected or stored by their service provider. According to the guidelines, the right to access data means that data subjects should receive the data in digital format that may be read, heard or viewed by publicly available software, via email, secure website or any other digital mean. The service provider should authenticate the identity of the data subject and ensure that the applicant will not receive data about other data subjects.

3.9. Automated-decision making

Israeli law enables the data subject to object to the adoption of a decision regarding him based on automated means, both on the general principles of administrative law and in several cases on the base of specific provisions in the law.

Under Israeli administrative law, a public authority is required to guarantee the right to a hearing, which is derived from natural justice. This right is considered fulfilled so long as the relevant authority that makes a decision concerning a person enables the person to voice his claims and arguments against the decision in the presence of the authority. In the absence of fulfillment of this obligation by the authority, its decision is void.[92]

In addition to the general principle mentioned above, an example from the criminal sphere can be found in the provisions regarding financial penalties of criminal offenses,

[91] See also part 4.2.

[92] HCJ 654/78 Riva Gringold v. The National Labor Tribunal 35(2) PD 649 (1979): "a basic right under the Israeli law is that a public authority which harms the stand of a person, will not do so prior to allowing the person harmed the opportunity to voice his claim. In the fulfillment of this right, there is no difference whether the public authority operates on the basis of the law, or on the basis of an internal resolution or agreement. Furthermore, there is no significance to the question whether the authority applied is a judicial, semi-judicial or administrative, if the consideration given to the authority is wide or narrow. In any case where a public authority seeks to change the status of a person, it must operate in fairness, and grant him the opportunity to voice his claim."

among them traffic reports which are given based on an automated decisions of speed cameras. According to article 229 to the Criminal Procedure Law, 5742-1982 [Combined Version][93] a person who received a financial penalty notice is entitled to issue a request for its cancellation. A prosecutor appointed by the Attorney General is authorized to cancel the financial penalty notice if he is convinced that the traffic violation was not committed, or committed by a person other than the one who received the notice, or if he determines that the circumstances as a whole do not merit the continuation of the proceedings. According to regulation 42A of the Criminal Procedure Regulations, 5734-1974,[94] the request of cancellation should be submitted to the prosecutor and should include explanation regarding the request. Attorney General Guideline 4.3040 specifies the considerations which the prosecutor should take into account while considering the request. The use of this provision is common in appeals concerning financial penalty notices given on the basis of speed cameras and public transport route cameras.

Another example is the Traffic Regulations (Operating Cameras by a Local Authority for Documenting Illegal Use of a Public Transportation Lane), (see part 2.2.2). According to these regulations, the enforcement of offenses related to the illegal use of a public transportation lane is based on the use of cameras, but the issuance of a financial penalty notice is conditional upon examination of the film by a human inspector.

An example from the academic sphere can be found in the rules and practices regarding acceptance to higher education institutes. According to a decision of the CFHE (Council for Higher Education), the institutes are allowed to accept up to 10% of the number of students who do not meet the terms of acceptance that the institutes have set, for purposes such as enhancement of the accessibility of higher education in Israel and special academic and personal data which justify exceptional acceptance. Most of the decision-making process is automated, but a candidate who was not accepted can appeal to an exceptions committee or to another specific official in the relevant institution, which will reconsider the candidate's specific case.

[93] Criminal Procedure Law, 5742-1982 [Combined Version] SH 1043 p.43.
[94] Criminal Procedure Regulations, 5734-1974, SH 3172 p. 1200.

In the field of insurance, article 35(19) of the Equal Rights for Law provides that a disabled person whose request to be insured was rejected or was discriminated against by an insurance provider, can lodge a complaint to the Commissioner of Capital Markets, Insurance and Savings, or to a special committee, in addition to his right to apply to a court of law.

3.10. Non-Automated Processing of Personal Data - Privacy Protections

The provisions of the Basic Law: Human Dignity and Liberty provide protection to all aspects of the right to privacy and to personal data, regarding both automated and non-automated data processing. In addition, the general provisions of chapter A of the PPL, apply equally to automated and non-automated data processing. This includes protection from the main types of violations of the "classic" right to privacy, including the purpose limitation principle and prohibition of onward transmission without consent, and protection against surveillance, photographing and publication of personal data under the terms of the chapter. The Law includes a variety of remedies for privacy violations including civil damages, criminal proceedings and court orders ordering the removal or destruction of privacy violating content and data (as demonstrated by the **Jane Doe** case regarding the publishing of a book revealing intimate data).[95]

Furthermore, other provisions of the PPL apply too to non-automated processing – the provisions regarding Direct Mail and those regarding data transfer between public bodies. In addition, other specific legal frameworks, regarding specific sensitive types of personal data, applies to non-automated processing as well. For example, the Genetic Data Law and the regulations that were published under the law, establish a comprehensive framework for regulating genetics, and include provisions regarding protection of non-automated data and biological samples.[96]

[95] See further part 3.1.

[96] The Genetic Data Regulations require that laboratories conducting genetic tests will appoint a DPO (which could be the manager of the lab or an employee appointed by the manager). The data (biological sample, medical opinion etc.) must be kept in a secure site and the access to identifiable data is limited. The regulations require that the data be deleted after 7 years from the date the examination was conducted and that biological samples will be destroyed.

Non-digital data that is scanned and stored is considered automatically processed and therefore subject to the enforcement powers of the Registrar.

4. General review and developments regarding oversight and enforcement of the PPL

4.1. The PPA is adapting to future changes

4.1.1. Establishment of two new departments in the PPA

In order to advance and improve capabilities of the PPA in coping with future challenges to data protection, and in order to strengthen the PPA and enable it to fulfill its tasks in an environment that is exposed to far-reaching and ongoing developments in the digital space, in the year 2016 the PPA went through a significant strategic change that includes re-organization of its structure and modifying and re-prioritizing its aims. The strategic change was completed in 2018, and it included the creation of two new departments: a Department for Strategic Alliances and a Department for Innovation and Policy Development.

The main purpose of the Department for Strategic Alliances is to raise awareness about privacy protection and its significant role in the digital economy through educational, informational and training programs and activities. In addition, the department aims to raise awareness regarding the rights of the public and relevant actors protected in the PPL, and to the various roles and responsibilities under the law of entities controlling or processing personal data, and of their employees. Another mission of this new department is to create a community of experts in the field of data protection that will receive appropriate training and acquire relevant skills in order to strengthen data protection across the country.

The main tasks of the Innovation and Policy Development Department are identifying emerging trends in the fields of technology, business and social privacy, conducting research and initiating innovative regulatory solutions to data protection suited for today's digital economy.

Amongst its many projects, the new department is developing a guide for smart cities in order to assist municipalities to comply with the PPL. The PPA hired a consulting company in order to map the numerous digital activities of municipalities, and created the guide with the aim of educating and assisting all the relevant stakeholders to implement their legal obligations.

After finalizing the guide, the PPA will engage in educational and media activities in order to raise awareness amongst the relevant stakeholders in municipalities across the country.

4.1.2. **Merger of the criminal and the administrative enforcement departments**

Until recently the Criminal Investigations Department and the Administrative Supervision Department operated separately. Following the re-organizational change, the two departments were merged into one. The goal of the merger is to establish an effective and focused enforcement policy that will promote effective compliance.

Enforcement and guidance activities will expand and focus on cases that involve particularly sensitive data or large amounts of data, and on cases in which individuals or disadvantaged sectors in society lacking sufficient tools and skills face large and powerful organizations processing their personal data. The PPA intends to investigate and supervise more sectors and companies by increasing its enforcement department and staff.

4.1.3. **New audit mechanism**

The PPA established an innovative auditing mechanism as part of the Enforcement Department that is carried out with the assist of outsourced audit professionals, and helps the PPA in identifying and narrow the gaps between data protection laws and their actual implementation by organizations throughout the country. The audits are aimed at creating awareness and incentivizing organizations to comply with the legislation and regulations. As more audits are conducted, awareness will increase, leading in turn to increased self-regulation and implementation of accepted privacy protection standards.

The audits are thematic and are carried out amongst pre-identified sectors in which relevant controllers or processors are identified.

Audits are to be completed in 3 months, based on questionnaires distributed to hundreds of organizations. The audits assess organizational control and governance with regards to data management and protection, data transfers, data security and more. The outsourced teams which assist the audit mechanism are leading accounting

firms, including experts in the area of IT audit and data security. The teams distribute the questionnaires, summarize the findings and submit them to the PPA which will draw conclusions from the findings.

The goals of the audit system are divided into three main objectives:

1) Promoting and implementing the guidelines of the PPA amongst data controllers and processors;

2) Reducing gaps between privacy regulation and its implementation by organizations, by identifying such gaps through the audits, correcting deficiencies by guidelines, and enforcing guidelines and corrections by follow up and repeat audits.
   Increasing awareness by broad media exposure of sectorial aggregated findings.

It is expected that the findings of the new audit mechanism will lead to regulatory adjustments and guidance when needed, initiating administrative or criminal investigations following the audits (when required), and producing sectorial privacy compliance key performance indicator.

4.1.4. **Significant increase in the PPA's budget**

Until 2016, the budget of the PPA was approximately 10 million NIS and had not gone through significant changes over the years. Following the strategic change the PPA described above in part 4.1.1, its budget has increased by 50% increase in 2016, reaching 15 million NIS. In 2018, the PPA's budget is expected to increase by an additional 10% and will reach 16.5 million NIS (total increase of 65%).

In terms of personnel, as of the date of this report, the PPA's staff includes 51 employees. It consists of lawyers, technical experts, administrative staff, interns, national service volunteers and students. Between 2016 and 2018, the PPA was granted 10 additional professional positions of full-time public service employees and 10 part-time non-permanent employees. This represents an increase of 25% in the PPA’s staff.

4.2. Guidelines and draft guidelines published by the PPA

In the dynamic reality of the digital economy, guidelines are a significant tool for the promotion and enforcement of data protection. Therefore, guidelines are one of the most effective methods for soft regulation in the PPA's regulatory toolkit. These guidelines reflect the way the PPA interprets the PPL when exercising its enforcement powers. They promote compliance and awareness, provide clarifications as to how the law and regulations will be interpreted by the PPA, and direct organizations in the manner in which they are expected to manage their data.

The judgment in the **IDI** case, discussed in detail in part 3.1,[97] clarified the Registrar's powers to publish guidelines and enforce them, stressing that they are to be construed broadly and not limited only to the sanctions set forth explicitly in the law. The Registrar is entitled to exercise its discretion in an individual case or according to a general policy determined in accordance with the professional interpretation of the PPL. Thus, it is within the authority of the Registrar to issue guidelines and corrective orders to database controllers, processors and managers, reflecting the Registrar's interpretation to the provisions of the law.[98] The Supreme Court adopted the abovementioned decision of the District Court and the reasoning on which the judgment was based.[99]

The PPA publishes its guidelines after public consultations with relevant stakeholder. Some recently published guidelines and draft guidelines issued by the PPA are summarized below.

1) Data Security Regulations Guidelines

As mentioned in part 3.6, the new Data Security Regulations entered into force in May 2018. The regulations were published in April 2017 in order to enable organizations to prepare themselves and make the necessary adjustments to the new requirements. The guidelines address the fact that some organizations already adhere to existing international data security standards like IS27001/27002, or to data security

[97] See further part 3.1.

[98] AdminC (TA) 24867-02-11 I.D.I. Insurance Company Ltd. v. Ministry of Justice the Israeli Law, Information and Technology Authority – the Registrar of Databases, (Jul. 7, 2012), Nevo Legal Database (by subscription), at para. 3 of the judgment of Judge Agmon-Gonen.

[99] AdminA 7043/12 I.D.I. Insurance Company Ltd. v. Ministry of Justice the Israeli Law, Information and Technology Authority – the Registrar of Databases (Jan. 15, 2014), Nevo Legal Database (by subscription, in Hebrew).

requirements that were issued by domestic regulators (e.g. the Financial Conduct Authority under the Bank of Israel, the Insurance Supervisor), by clarifying the gaps between the existing data security frameworks and the Data Security Regulations.

2) Right to access guidelines

As explained in part 3.8, The PPL grants data subjects the right to access their personal data. In its new guidelines, the PPA clarified that the right to access includes personal data in any format or file type. This guideline was very well received by Israeli public, since it empowers individuals not only as data subjects but also as consumers to whom providers often have refused to supply recordings of phone calls or other kind of negotiations.

3) Surveillance Cameras Guidelines

In 2012, the PPA published general guidelines concerning the use of surveillance cameras in the public domain. The guidelines aim to ensure proportionality and transparency with regards to the use of surveillance cameras. The guidelines include provisions with regards to Privacy by Design, transparency, right to access, and accountability principles that are linked to the decision to use surveillance cameras, and to the way they collect data and process it.

Due to technological and economical developments such as widespread drone use, wearable cameras, improvements in automatic face recognition, and general increase of surveillance cameras usages in all sectors, the PPA is routinely updating its guidelines in this context.

4) Guidelines on Workplace Surveillance

In October 2017, the PPA published its Workplace Camera Surveillance Guidelines. Workplace surveillance is becoming a common practice and it raises difficult questions with regards to privacy and employees' rights. Given the subordinate status of employees' vis-à-vis their employers, their apparent consent regarding the use of surveillance cameras might not have been given freely and in a fully informed manner. The guidelines recall and elaborate upon the employer’s legal obligations in these cases including the duty to act in a reasonable, fair and proportional manner, and in good faith. The guidelines establish criteria for assessing the legality of the use of surveillance cameras, namely: they are for a legitimate purpose which is essential to the

employer’s interests, or are necessary to fulfill a legal obligation (such as Police demand to apply CCTV in banks and gas stations). Prior to the installation of surveillance cameras, the employer must establish a clear and detailed policy with regards to the manner and the extent of the usage, and its purposes. This policy should be presented to the employees. The guidelines emphasize the purpose limitation principle.

5) Use of outsourcing services for personal data processing guidelines

The guidelines provide organizations with guidance for protecting privacy in connection with data processed via outsourcing services. Accordingly, the guidelines elaborate on the obligations of data controllers and processors when designing a data processing service to be outsourced, with special regard to organizational accountability, controls and procedures.

The principles set forth in the guidelines apply to private sector organizations as well as public ones. Their purpose is to reflect the principle that the controller remains ultimately responsible for compliance with the law even if the processing was outsourced to a third party, and to prompt data controllers to ensure that contracting for data processing services with a third party will not reduce their obligation to comply with data protection law or breach data subject's right to privacy.

The basic principles outlined in the guidelines, which must be addressed prior to outsourcing a processing activity, are as follows:

a) Preliminary examination of the legitimacy and appropriateness of outsourcing the intended processing activity;

b) Clear and detailed definition of the type of service to be performed via outsourcing services, and a precise specification of the purpose of the intended processing, so that no further processing and use will take place, and in order to avoid processing which is incompatible with the specified purpose;

c) Definition of data security and confidentiality provisions to prevent security breaches;

d) Provisions and procedures with regards to the fulfillment of the data subjects' reviewing and rectification rights;

e) Criteria for choosing an outsourcing contractor, e.g. previous experience in processing personal data and avoiding risk for conflict of interests;

f) Integration and instruction mechanisms to ensure that personal data protection principles are incorporated by the contractor's employees;

g) Defining means to perform follow-ups and supervisions of the contractor's fulfillment of legal obligations (provisions of the law and contract);

h) Duration of retention period of the data by the contractor and deletion of data upon conclusion of the contractual engagement.

It should be noted that the 2017 Data Security Regulations (see part 2.1.2) contain some of the provisions of these guidelines as well.

6) Guidelines on Privacy Protection During Recruitment Procedures and Privacy Protection by Recruitment Agencies

The process of recruiting employees involves collection of large amounts of data about candidates. This data includes *inter alia* prior employment experience, education, skills, health condition, family status and more.

The guidelines clarify that in these scenarios, potential employers are data controllers, while recruitment agencies act as processors. Therefore, the recruitment agencies are not permitted to use and process the data for purposes other than the ones of the potential employer.

According to the guidelines, the consent of a candidate to additional uses of the data (i.e. for purposes other than completing the hiring process) given on or before the day on which he was tested - shall be presumed to be given without free choice and therefore invalid. The consent of the candidate is only likely to be valid and based on genuine freedom of choice if it was given after receiving an acceptance or rejection notification in respect of the position for which he was originally tested.

The guidelines also emphasize the importance of candidates' right to access the results of the compatibility tests, including their personality profile.

7) Direct Mailing Guidelines

The PPL contains detailed provisions regarding direct mailing, defined broadly in article 17C of the PPL, to refer to contacting a person, via any type of communication,

"based on their belonging to a group of the population that is determined by one or more characteristics" which are protected data according to the PPL.

Article 17C of the law also defines "'direct-mailing services" as "…providing direct-mailing services to others by way of transferring lists, labels or data by any means".[100] According to the PPL, operation and holding of a database for the purpose of direct mailing and direct mailing services triggers stricter regulation than a "regular" database. Thus, in addition to the duties imposed on "regular" databases, a database created for direct mailing **services** must comply with the following requirements:

a) The database must be registered with the PPA, no matter how many data subjects are listed, and whether or not the data is sensitive.

b) The database "owner" (*i.e.*, controller) and/or "holder" (*i.e.*, processor) of such a database must maintain a log of the sources of data and of third parties to whom the data was transferred (sec. 17E)

c) Data subjects may request that the data be deleted from the specific database or that it shall not be transferred to a specific third party or specific types of third parties.

Databases for purposes of either direct mailing or direct mailing services are also subject to additional specific duties towards the data subject regarding the content and format of notice

In light of technological developments and the multiplicity of media platforms in recent years, there as been a significant rise in the number of marketing messages sent to individuals as well as a diversification in the form and means by which the public is being thus contacted and harassed.

For this reason, following a period of public consultation in June 2017, the PPA published guidelines on the interpretation and implementation of the PPL provisions with regard to direct mailing and direct mailing services.

The guidelines detail the cases in which contacting an individual will be considered direct mailing (including in the context of a consumer- service provider relationship), and where selling individuals' personal data will be considered as direct mailing

[100] Note that this definition excludes bulk, impersonal direct marketing via unsolicited mail and other forms of communications (i.e. "spam mail"), which is primarily regulated under the Communications Law (Bezek and Broadcasts) 5742-1982, KT 2153 (2008-2009) (as amended).

services. They also outline the conditions and the form of consent that a company is required to obtain from customers, in order to use their personal data for the purpose of direct mailing services (usually "opt-in") or direct mailing.

Furthermore, the guidelines specify the obligations of those making contact by direct mailing, as well as the rights of the recipients of such contacts (including the scope and manner of exercising the recipients' right to have their personal data deleted from a direct mailing database).

The guidelines include a list of "Dos and Don'ts" for organizations considering purchase of direct mailing lists, in order to ensure that the data sources they acquire were lawfully obtained. The guidelines stress that unlawful uses of personal data expose both data traders and buyers to enforcement actions and, where appropriate, to the imposition of sanctions by the PPA. They can also be ground for a civil claim in a court of law.

8) Guidelines on the Prohibition on the Use of Data Regarding the Imposition of Foreclosure

As noted above regarding the IDI Case, the PPA published guidelines after imposing an administrative fine on IDI Insurance Company Ltd, in connection with the company's unlawful use of personal data received in connection with foreclosure proceedings, in order to assess that person's eligibility for insurance (see part 3.1).

The guidelines, the validity of which was upheld by the Supreme Court in the IDI case, clarify that data regarding foreclosure is provided to a third party only to carry out the foreclosure registration and that the third party is not allowed to use this data for any other purpose.

The main principles in the guidelines are as follows:

a) The data included in the foreclosure order must be given to the third party **only** for the purpose of implementing the order. In other words: locating the debtor's assets, freezing the assets and passing to execution, in case of a "freezing order". Accordingly, the third party is allowed to keep the data about the debtor only for the purpose of fulfilling the court order.

b) Hence, a third party is not allowed to use data for any purpose other than the purpose of the order, including purposes of the third party itself. Thus, a

bank or an insurance company that receives registered liens on assets of a policyholder is not allowed to process the personal data in order to decide whether to give them services or credit.

c) The legal framework for receiving credit data is the Credit Data Law, according to which only special regulated license holders may provide credit data services.

9) Guidelines on the use of voter register during elections

Prior to the municipal elections which will take place in October 2018, the PPA issued guidelines to the local municipalities, political parties and contestants in order to raise awareness to the limitations and obligations that apply to the use of personal data during campaign and emphasize them, especially the restrictions on the use of voters' data transferred to candidates under election laws.

10) Personal health applications guidelines

In 2018, the PPA published a guide for consumers on the use of personal health applications for the purpose of assisting the public to use the smart gadgets apps safely and wisely in a manner that reduces risks to their privacy. In recent years, health, fitness and clothing applications have become very popular. There are many different applications on the market that offer users the ability to follow their physical training routines, monitor their nutritional habits, sleeping habits, etc. The applications are easy to download and are user friendly and convenient. Wearable means are user-worn accessories that seek to collect physiological data such as blood pressure, step count, and data related to the quality of the user's sleeping habits using special sensors. Therefore, the recommendations presented in this document are also relevant to the use of wearable means. Since these applications typically collect a significant amount of sensitive data, the main concern is that insufficient data security or its transfer to third parties seeking data may harm consumer privacy. In addition, data collected by these applications can be cross-linked with personal data from other sources, such as pharmaceutical companies, thus resulting in a violation of consumer privacy. Therefore, the guide outlines the possible risks to user privacy inherent in the use of these means and suggests best practice recommendations to address these risks.

4.3. Prominent enforcement actions

The Registrar, acting under the framework of the PPA, holds a broad range of enforcement powers, including criminal investigations and administrative penalties.[101] These are expected to be further expanded upon the adoption of the bill regarding enforcement powers.[102] As mentioned above, the bill has passed the first reading in the Knesset in March 2018.

4.3.1. Cooperation of the PPA with other enforcement and investigation authorities

The PPA maintains a continuous dialogue with parallel authorities and bodies, including law enforcement and security agencies (the Israeli Police, the Israel Security Agency, the National Cyber Directorate, the General Director of Biometrics, etc.). The PPA engages these agencies in order to share knowledge and contribute to the ways in which the right to privacy is balanced with security considerations within these agencies. In particular, the PPA is a meaningful source of knowledge to those authorities regarding lawful collection and use of citizens' data to these authorities.

The PPA provides these authorities with training activities in order to promote compliance with and awareness to the PPL and its regulations. The PPA also receives information from these authorities with regards to data breaches in other organizations, which the PPA then examines to determine whether a violation of the PPL might have occurred.

In cases involving criminal offences deriving from the PPL and other acts, the PPA and the police investigate the case together, forming joint teams aiming to increase the outcomes of the enforcement action.

4.3.2. Criminal investigations and proceedings

The PPA has powers to conduct criminal investigations which can result in indictments. Following is a short description of the most prominent criminal investigations the PPA conducted in the past year:

[101] See further part 1.7.
[102] See further part 2.1.2.

1) Investigation of communications services provider

The PPA investigated suspicions regarding offenses under the PPL carried out by employees and managers of a virtual cellular operator. The suspicions focused on the prohibited use of personal data collected in the company's data systems about its customers for the personal and business purposes of the suspects. The investigation was carried out by a joint investigation team together with the central unit of the Jerusalem District Police, and the findings of the investigation were transferred to the Office of the Jerusalem District Attorney for review and consideration for indictment.

2) Investigation against health service providers and data traders

The PPA completed an investigation about extensive trade in sensitive health data of patients. The PPA investigated social workers, nurses in hospitals, employees of healthcare services suppliers, managers and agents of private nursing services providers and telemedicine services and data traders.

The findings of the PPA were sent to the Cyber Department in the State Attorney's Office for review and consideration for indictment.

Treatment in medical institutions generates sensitive personal data about patients including name, contact data, department where treatment was received, the healthcare service provider that the patients received services from, the scope of the patients' health insurance, age, details of the hospitalization and treatment provided, the type of surgery the patient has gone through and more.

This data is of great economic value for companies offering nursing services for the elderly after surgery. Patients are eligible for free care (from the National Insurance Institute of Israel), resulting in competition between the nursing services providers to be the first to reach the patient and reach a profitable deal.

According to the allegations, employees of the hospital and other healthcare organizations with access to data systems gave confidential and private data about elderly patients to middle men, who in turn transferred contact information of patients to nursing service providers and telemedicine service providers, as leads for potential customers. In many cases data was transferred when a data subject was scheduled for

treatment, before being hospitalized and before receiving medical treatment and therefore was most susceptible to agree rashly to the offered services.

Following receipt of the data, nursing services providers approached the patients in order to sell them their services, while exploiting sensitive medical data about them.

The parties involved in this case had been conducting these actions for three years before they were discovered by the PPA's enforcement team. Two of the companies that purchased the data were fined 400,000 NIS and 150,000 NIS. Hospital employees were fired and sentenced to prison doing community service and fines.

3) Enforcement against significant breach of Population Registry Database

The **Population Registry Database** case involves a third party contractor who stole the Population Registry Database from a government ministry. The database contained dozens of fields of personal data about all residents of the State of Israel (including minors and deceased). The investigation was conducted by the Criminal Investigations Unit of the PPA. It revealed that the database was passed on from one defendant to another, and one of them also developed an application that enabled easy and efficient queries and report generation (hereinafter: "The distributor").

The distributor had made the data accessible to the entire public by uploading links and a 30 page manual, encouraging the public to use the application. He disguised his identity using proxies and inaccessible servers. After realizing the strong digital evidence against him, he confessed in court about his role in the case.

The Israeli Magistrate Court in Tel Aviv found the contractor guilty for invasion of privacy and (due to special personal circumstances) sentenced him to only 1 year imprisonment, and a fine of 100,000 NIS. The Court found the distributor guilty for invasion of privacy and obstruction of justice offences, and sentenced him to 18 months imprisonment, a fine of 100,000 NIS (approximately 20,000 Euros) and 6 months probation.

In addition, other 4 defendants were charged with invasion of privacy and other crimes. 3 of them have already been sentenced to community service and imprisonment, and another defendant was sentenced to 10 months imprisonment. The sixth defendant was sentence to jail after a long brake in his trial due to his health condition. This defendant was a DBA in the ministry of social affairs who illegally copied the database after he got fired. In the verdict, the court ruled that this defendant should have been sentenced

to 25 months in prison, but due to personal circumstances he imposed a year's imprisonment and a fine of NIS 100,000.

The case received high attention from the Israeli media.

4) More enforcement activities

Two other cases were investigated and are now at the district attorney office:

a) Medical data: A secretary who worked in an abortion clinic gave detailed and highly privet data about patients to a religious organization that opposes abortions.
b) Insurance data: An employee in an insurance company took a 20,000 records database and sold it to a call center.

4.3.3. **Administrative enforcement actions**

The Registrar's enforcement powers include the power to impose administrative fines following specific infringements of chapter B of the PPL. Fines in the amount of NIS 2,000 to NIS 5,000 may be imposed for a violation by an individual, and five times this amount on an infringing corporation. In order to enhance data protection, and in order to be able to impose meaningful fines, the Registrar often increases the sanctions by imposing a fine on multiple violations derived from the same case. A person who contests a fine is entitled to request to be indicted by a criminal court.

1) Actions taken by the PPA against data traders and their clients

The abovementioned breach of the Population Registry Database lead not only to criminal indictments against the main perpetrators, but also to robust administrative actions against other parties that got hold of the data and integrated it with other sources of data, some of which were illegally obtained as well. In a complex forensic investigation, which took place in 2016, the PPA found a company that obtained the illegal data and sold it to third parties. The PPA conducted a search and seizure of computer materials in simultaneous on-site inspections at 4 sites and seized documents of the orders and payments.

The PPA found that the company obtained the illegal data and integrated it with other data sources, such as data given to the parties and candidates running for election to the

parliament for the purpose of contacting the voters, online phone directories and statistical data from the Central Bureau of Statistics.

The customer database of the offenders included over 1,000 companies from various market sectors including banks, insurance companies, health services organizations, newspaper publishers, charity organizations, law firms and research institutions.

Following the investigation, the PPA determined that the activity of the company was illegal, and thus deleted the database from the database registry, effectively closing the company's business. The PPA followed the data and identified more than 1,000 clients who bought the data, instructed them to delete the data and sign an affidavit stating that the data was destroyed. The PPA investigated some of the clients and found that one of them did not delete the data. This client was fined as well.

This case shows how the PPA acts against all the data chain components, and how it leverages administrative supervision, inquiries, instructions, audits, administrative enforcement and criminal prosecutions. It further indicates how a proactive policy that involves the integration of various regulatory tools, can tackle severe privacy violations.

2) Investigation concerning misuse of personal data by a political party

In Israel there are several non-profit organizations that provide assistance to Holocaust survivors. These associations hold personal details of the survivors who receive assistance from them and they operate under the "Organization for Aid to Holocaust Survivors" (hereinafter "the Organization"). In 2017, the Chairwoman of the Organization was asked by a representative of a large political party ("Yesh Atid") to send him files containing records of sensitive and identifiable personal data about Holocaust survivors. These files were then transferred without the consent of the survivors, in violation of their privacy and the PPL. Later on, the party used the data for publicity and direct mailing to survivors prior to the elections for the 20th Knesset.

In a hearing held by the PPA, representatives of the party and the Organization were invited to respond to the allegations against them. After the completion of this procedure, the Organization, the chairwoman and the political party admitted to having acted in violation of the law, and administrative fined were imposed on them.

3) Leumi Card Data Breach

Leumi Card is the largest credit card company in Israel. In 2014, a former employee stole extensive and sensitive data and tried to extort the company.

This prompted an investigation by the PPA into the level of data security in the company's systems and its compatibility with the PPL's obligations to secure personal data. The PPA concluded the company did not sufficiently restrict access to the data and that the data was unnecessarily accessible to more than 100 employees that did not need to be exposed to the data, in violation of the PPL.

In addition, the PPA found that the company did not implement basic data security principles in its systems with regards to access authorizations, and did not implement relevant mechanisms to monitor employees' retrieval activities and logins, such that the company had become aware of the data theft only after the former employee began to extort the company.

Finally, the PPA assisted the Israeli Bank Supervisor, who investigated this case as well.

4.3.4. **Data breaches and leakages**

Following is a description of a few cases in which the PPA's team identified data leakages and instructed organizations to secure their data.[103]

1) "TAF's" data leakage

A severe data security flaw was discovered on the computer server of "TAF" which is an NGO that operates as an intermediary and consultant in adoption procedures. The security flaw allowed the leakage of particularly sensitive personal data of adopting families and of adopted children.

The PPA issued an immediate demand to address the problem, but due to slow and unsatisfactory response from the NGO, inspectors of the PPA raided the offices of the NGO and found many physical and logical data security failures in its systems. The relevant officials regulating the NGO in the Ministry of Welfare were updated with the

[103] These cases occurred before the breach notification duty came into force on May 2018 in the new data security regulations.

findings of the inspection, due to the fact that the Adoption Law, 5741-1981,[104] imposes heightened obligations on confidentiality.

Due to the severity of the findings, the PPA suspended the NGO's database's registration (which means that the database was not allowed to function) until the failures were corrected, so that the NGO or anyone acting on its behalf was prohibited from making any use of the registered database files and its derivatives or copies without obtaining the Registrar's approval.

2) Data leakage exposing data of political party's members

The PPA detected an Excel file that included thousands of records revealing personal data of the Labor Party's members. A name search of a member in Google exposed the sensitive file. The file was stored in the Kibbutz Movement website, an association affiliated with the Labor Party.

The PPA instructed the Kibbutz Movement to investigate the incident, and to conduct the following: a risk assessment to its systems, penetration testing with the assistance of security experts, implement protection systems, for monitoring, control and warnings regarding data security breaches, for all its systems and servers, with an emphasis on systems that allow access to personal data in order to prevent future breaches. The Kibbutz Movement will have to report to the PPA about the implementation of its instructions.

3) Miscellaneous

Similarly, the PPA has also found data security deficiencies in other organizations such as the Prisoner Rehabilitation Authority and Employees Fund (exposing sensitive data about employees).

4.4. Involvement of the PPA in legislative processes and in the initiation and development of governmental digital projects

The PPA is involved in complex legislative processes with privacy and data security implications. In addition, the PPA ensures that certain legislation involving sensitive

[104] Adoption Law, 5741-1981, SH 1028 p. 293.

digital projects empowers the PPA to act as an advisory agency or as a certification authority.

In addition, the PPA is involved in the initiation and development of broad and sensitive digital national governmental projects that affect national digital infrastructure and the national economy.

Following is a list of examples of legislation processes and government activities that the PPA is involved in:

1) **The Credit Data Law:** the PPA advised with regards to the identity of the body that will hold the central database and inserted Privacy by Design mechanisms to the systems. In addition, the PPA advocated for heavy data security mechanisms, which were incorporated into the law. Notably, the PPA's input lead to the inclusion of a requirement to appoint a data protection officer for the project, as mentioned in part 2.2.1.

2) **The Committee for Increasing Competition in the Banking Services Market:** During 2015-2016 the Israeli Government appointed a committee to explore the lack of sufficient competition in the Banking sector. The committee issued various recommendations aimed at promoting competition in the Banking Services Market, in order to bring consumers better services and lower their costs. One of the recommendations was focused on Personal Data, as a facilitator of increased competition. The Committee recommended forcing financial institutions to open their API's in a way that exposes online customer accounts, subject to customer consent, so that Fintech initiatives may arise to offer customers "comparison services ", that will inform them if they can receive better terms in other banks. Since this prospect holds privacy risks to individuals that require mitigation, the PPA presented it's professional opinion and recommendations for Privacy risk assessment and Privacy by Design to the committee. The recommendations were adopted by the Israeli government, and are in the process of being legislated. The PPA

3) **The Supervision of Financial Services Law (Regulated Financial Services)** is a law concerning services of financial costs comparison. The provisions under the law require a financial entity to enable the customer or a service provider on his behalf to view online financial data regarding the customer held by the

financial entity. The law was formulated based on the recommendations of the committee for Increasing Competition in the Banking Services Market, detailed above.[105] The PPA continues to support strong mechanisms of Privacy by Design and enhanced data security during the governmental work over formulating the required regulations. For example the PPA validated the customer identification processes of the framework in order to protect people's privacy and minimize the risk of false identification resulting in data breaches. The PPA also made sure that a Risk Assessment of the process defined in the legislation be conducted by a professional in data security.

4) **The Inclusion of Biometric Methods of Identification and Biometric Identification Data in Identification Documents and Databases, 5770-2009**[106]: The State of Israel has been working on a smart identity card project for many years, to replace the simple paper ID card, and the plan included the establishment of a Biometric Data Base.

   The PPA was involved in different stages of the project from concept to legislation and to the planning of a trial period to examine the necessity of the Biometric Database. Also during the two and a half year trial period, the PPA was a member of the oversight committee over the Ministry of Interior who carries out the project.

   Through all this, the PPA was instrumental in introducing Privacy by Design and privacy-default measures to the project, and advocated for strong privacy protection vis-à-vis the needs of the government.

   For example, at the legislative stage, there were several mechanisms implemented, to limit the potential of mission creep, including specific purpose limitations for use of the data. There were articles specifying a robust security regime, creating regulation and supervision within the government over the project by an independent regulator, appointment of a Data Protection officer in the project and mandatory Privacy & Security Risk Assessments.

[105] See appendix 2 for further details.
[106] The Inclusion of Biometric Methods of Identification and Biometric Identification Data in Identification Documents and Databases, 5770-2009, SH 2217 p. 256.

The trial period was designed to test whether a biometric database is essential to the project and reach a decision on the amount and type of biometric data to be included in the database, in order to apply the minimization principal and collect only what is essential.

5) **Smart cards for public transportation**: The Israeli Ministry of Transportation initiated a national project in which all public transportation will be operated by smart cards. The PPA advised and issued specific guidelines for the public transportation operators in order to ensure that citizens' privacy risks are mitigated in the systems. The PPA also conducted security audits on all operators and gave instructions to improve security. The PPA continues to advise the ministry during the legislation process.

6) **Income Tax Regulations (Regulations Regarding Currency Service Providers) (Temporary Provision), 5779-2018:** [107] The PPA advised the Minister of Finance on the manner in which data should be collected, managed and stored with regards to reports that currency service providers are required to issue to the Tax Authority).[108]

7) **Draft Regulations on Equality for People with Disabilities**: The PPA advised on necessary privacy controls with regards to new regulations enacted to maintain equal rights for people with disabilities. The draft regulations contemplated by the law aim to ensure that people with disabilities receive proper representation as public servants in public work places. The PPA advised with regards to the manner in which data will be stored, managed and collected during the time it is needed for examining the rate of employment of people with disabilities in the relevant workplaces.

8) **Opinion of the PPA submitted to the National Academy of Science**: The National Academy of Science has initiated a national project for the establishment of a large database in the education sector which aims to use big data analysis in order to improve education services based on statistical

[107]Income Tax Regulations (Regulations Regarding Currency Service Providers) (Temporary Provision), 5779-2018.
[108] See appendix 2 for further details.

conclusions. The PPA was asked to opine on the privacy implications and legal requirements with regards to personal data in this project.

9) **Government Cloud Computing Committee:** The PPA collaborated with the Israeli Government ICT Authority in developing a policy for the use of cloud computing services (locally and abroad) within the Israeli government. The policy includes privacy and security considerations. Furthermore, the PPA is a member of the committee that examines each request of a government body to use cloud services.

10) **Re-use of public service data (open data):** The PPA was a member in the advising committee on the Re-use of public service data and gave its opinion with regards to principles of privacy, Privacy by Design, anonymization as a "Privacy by Design" mechanism and more. Some of these principles were embedded in Government Resolution1933.[109]

11) **The Committee for Data Transfers within the Government:** The PPA, alongside the Office of Legal Counsel and Legislative Affairs, was a member of the Committee on Data Transfers within the Government that aimed to review access mechanisms of public sector organizations to data. Government Resolution 1933 was formulated on the basis of the work of this committee.

12) **Steering Committee for the Improvement of the Government Real Estate Database:** The PPA is a member of the Steering Committee whose role is to establish a national infrastructures database in order to make geographic data available to all ministries.

13) **International agreements:** The PPA advises on international trade agreements that involve data transfers.

14) **Knesset Committee on Science and Technology**: The PPA advises the Knesset Committee on Science and Technology on a variety of subjects including data collection by drones, smart cities, and databases used to combat car accidents, regulation of internet companies, managing government data and more.

[109] See further part 3.1.1.

4.4.1. **Public awareness activities and cooperation within the government**

The Strategic Alliances Department at the PPA was established in order to create and promote alliances with strategic partners in order to promote data protection in additional ways to enforcement and deterrence. This conclusion stems from an understanding, within the PPA, that the challenges of regulating hundreds of thousands of data controllers requires a wide outreach that cannot be sufficient only in enforcement actions.

Furthermore, the PPA realized that complying with privacy principles is not sufficiently clear to data Controllers, and while many wish to comply, they lack the tools and guidance how to do so.

The PPA has thus identified several strategic partners, first of which is the public itself. The PPA aims to engage the public in a meaningful discourse on privacy and promote it to be aware of privacy rights and exercise them with organizations. Its aim is also to deliver policy in a way that provides tools for private sector organizations, business and public bodies, to comply with data protection requirements, since we have recognized a gap between regulations and implementation.

Since its establishment in mid 2016, the department has achieved a prominent and constant presence in national media and social media, and Israel has seen a lively debate over privacy issues and incidents.

The PPA's Facebook page has gained almost 5000 followers, and PPA staff have been interviewed and cited in hundreds of occasions.

Furthermore, in order to better communicate the PPA's policy to organizations, a new Internet site was created, along with many new materials including implementation guides, Q&A, tips and articles. These were focused on taking PPA guidelines and policy, and mitigating them to the public in clearer simpler and practical ways. Special attention was dedicated to the new Data Security regulations, for which many content was created.

The site also includes a transparent report of all PPA enforcement activity (criminal, administrative and audit), as well as all guidelines and hearing procedures.

The PPA also started sending a monthly newsletter that has reached over 3,000 subscribers, including law specialists, IT specialists, Academia, Managers and public

officials, who receive notice of new content published, new enforcement activities published and invitation to events that are open to the public.

A further outreach to the public was achieved in an abundance of sessions and events providing information and guidance by PPA staff, accumulating to over 150 appearances since the starting of the activity.

In the government sector, the PPA established a forum for privacy awareness and training, which currently includes 150 members, from both legal and technological background and positions. The forum holds meetings, receives a monthly newsletter and gives officials who deal with privacy issues in their roles in government a group of peers to consult with and a link to the PPA, which they use frequently.

The PPA re-branded its name and logo after a process of consultations and a government resolution, in a decision to focus and dedicate the resources to privacy protection. The authority changed its name from the Israeli Law Information and Technology Authority- ILITA- to the Privacy Protection Authority, in order to better reflect its activities and increase public awareness as to its mission and the services it provides.

Another strategic relation that was fostered is its amplified presence in Parliament committees and hearings, where the PPA presents its contribution to data protection efforts and providing data and professional insights to parliament members as they consider legislation and supervise the work of government.

Lastly, in June 2018 the PPA, held the first Annual Privacy Protection Conference - entitled "Privacy. The Next Generation." Over 580 participants attended the event, including senior public officials from central and local government, senior private sector managers in both legal and IT fields, and academia. The speakers included the Minister of Justice, the Director General of the Ministry of Justice and Head of the PPA. Other prominent speakers gave talks on various topics including the economics of data, differential privacy, privacy of children, the future of privacy and privacy and the media.

Wishing to promote privacy enhancing technologies out of Israel's vibrant start up community, there were also presentations by five Israeli start-ups and a selection of creative campaigns created by students promoting awareness to the importance of the right to privacy. Two short videos were produced for the conference and later promoted

on the internet, and a media campaign with additional content was started after the conference on social media and the radio.

All talks and videos are available on the PPA's YouTube channel.[110]

4.4.2. **Activities of the PPA in the international arena**

In the digital economy, data protection is a global mission. Data processed in one jurisdiction may affect data subjects in other jurisdictions. Given the global nature of such activities, jurisdictions need to cooperate in order to mitigate risks. Cooperation may take effect in joint enforcement activities, sharing best practices and harmonizing standards and working procedures.

PPA is a member of the following organizations:

1) **The International Conference for Data Protection and Privacy Commissioners** (Israel hosted the conference in 2010);
2) **The Global Privacy Enforcement Network** – the PPA is a member of the GPEN committee together with ICO (UK), FTC (USA), OPC (Canada) and PCPD (Hong Kong). The PPA is very active in GPEN and has spearheaded a variety of tasks and projects including preparing its Annual Report, chairing quarterly meetings, preparing a comparative report about enforcement powers of members, and more.
3) In June 2018 the PPA, hosted the second annual GPEN Enforcement Practitioners' Workshop, themed "Practical Solutions for Enforcement in a Global Digital World" in Tel Aviv.

More than 40 experienced investigators and case handlers from North America, Europe, Asia, Africa and Australia from privacy enforcement and other regulatory sectors, attended the event and shared their techniques and practical experiences in relation to case handling, investigation and enforcement.

The agenda for this event included panel discussions about practical solutions to common enforcement challenges, such as implementing new enforcement powers due to new or amended privacy legislation, applying alternative soft enforcement strategies

[110] https://www.youtube.com/channel/UCDck9TllW8iFQfds8-cZSPg/featured?disable_polymer=1.

to achieve compliance, handling mandatory breach notifications from receipt to action, considering the perspectives of regulated parties in enforcement, using innovative strategies to achieve positive enforcement outcomes, leveraging technology in evidence gathering, and international enforcement cooperation.

During the event, the PPA's delegation presented its new audit mechanism, advanced forensic technologies used in its investigations, case studies and more.

1) **OECD's Working Party on Security and Privacy in the Digital Economy**: the working party operates under the Committee for Digital Economy Policy;
2) **The International Working Group on Data protection in Telecommunications (the "Berlin Group"):** The PPA joined the working group in 2016. Currently the PPA took the lead on drafting a working paper about the Protection of Children in Online Services. The PPA was also asked to participate as a speaker about this topic on a workshop held by OECD. In addition, the Berlin Group will hold its spring meeting of 2019 in Israel.
3) **The Digital Clearing House Network:** The network brings together authorities who are responsible for regulation of the digital sector. The PPA joined the network and participated in its first meeting in May 2017.

4.4.3. Preparations of the PPA towards the entry into force of the new Data Security Regulations

The entry into force of the Data Security Regulations in May 2018 was one of the most significant events in the activities of the PPA in the past year, in light of their potential for widespread effect on the Israeli economy.

In order to prepare for, the PPA created a detailed program to carry out the complex tasks that were required to implement the regulations.

The program included several pillars: legal infrastructure (see part 2.1.2), public relations and education activities, enforcement policy, the formulation of guidelines and procedures and the recruitment and training of personnel with relevant skills.

Preparation activities included the following:

a) Publication of guides for the public on the PPAs' website which clarify how to implement the regulations, including a guide for small businesses. These guides

also include explanations regarding the new breach notification obligation established in the regulations.

b) QA section in the PPA's website which addresses questions raised by the public regarding the implementation of the regulations including the breach notification obligation.

c) The creation of a guide presenting a variety of types of incidents that require (or do not require) breach notification.

d) An Internet campaign, media publications, dozens of lectures and training sessions for the public, both in the public sector and in the private sector, regarding the manner in which the regulations should be implemented.

e) On the technological level, the PPA has developed an online reporting infrastructure in order to make it easier for the public to fulfill the breach notification obligation. In addition, a self-assessment simulator was developed to assist the public to examine the level of security and reporting requirements applicable to the databases they control. The PPA is about to publish a call for the public to develop technological means to improve the accessibility and effectiveness of the simulator.

f) Regarding personnel, the PPA recruited and trained four new data security professionals who are part of a new technology unit in the Enforcement Department, which will deal, among other things, with the technological aspects of breaches and will assist the PPA to improve the departments' enforcement capabilities.

g) The PPA’s policy for breach notification: In 2017, a year before the regulations came into effect, the PPA conducted consultations with data security experts and various stakeholders about the breach notification obligation. Controllers expressed their concerns regarding civil actions and the PPAs' enforcement actions that may follow breach notifications. In order to address the concerns, the PPA published its enforcement policy, aiming to encourage a positive "notification culture" across all sectors of the economy and to increase certainty regarding cases requiring notification. The policy established a transitional period for the implementation of the regulations, in which the PPA will adopt a more lenient enforcement approach towards organizations that fulfill their notification obligation, as opposed to a strict approach with regards to imposition of administrative penalties.

5. Access to personal data by public authorities for national security and law enforcement purposes

This part elaborates on the legal framework applicable in Israel as regards access to personal data by public authorities for national security and law enforcement purposes. It is divided in four parts: part 5.1 discusses the scope of the analysis and provides some important background information; part 5.2 provides an overview of specific laws that enable access by public authorities for national security and law enforcement purposes; part 5.3 addresses the applicable oversight mechanisms; part 5.4 elaborates on the subject of judicial redress.

5.1. Scope and background information

The State of Israel has been facing security threats since the day it was established. The rules, limitations and safeguards elaborated in this part reflect the Israeli legal system's approach to the balance required between the substantial public interest of security and protecting human life, on the one hand, and the protection of the human right to privacy on the other – a challenge faced these days by all democracies worldwide.

This challenge impacts different aspects of national security and law enforcement. Taking into account the purpose of this document in the context of the Adequacy Decision, this part focuses on Israel’s legal framework as it relates to possible access by law enforcement and national security authorities to personal data transferred to Israel from the EU pursuant to the Adequacy Decision.

In light of this context, laws that grant public authorities access to personal economic data in accordance with common international standards, such as tax laws, anti-money laundering laws, etc. are excluded from the scope of this review. Similarly in July 2018, the draft bill on Cybersecurity and the National Cyber Directorate (INCD) was published for comments. Such publication is the first stage of the adoption of legislation, and is intended to complement the deployment of Israel's domestic cybersecurity strategy, approved in 2015. Under this strategy the INCD regulates Israel’s critical infrastructures and operates a national CERT. The draft bill aims to define the INCD's powers to deal with cyber attacks, whilst distinguishing it from law enforcement or other national security authorities, and without empowering it to conduct criminal investigations. The draft bill also sets up a national cybersecurity

regulatory scheme, defining the INCD as a regulatory body. The draft bill is currently in the process of inter-governmental deliberations.

Turning now to the legal background for collection of personal data by law enforcement and national security authorities, it is important to keep in mind that the foundations of Israel's legal ecosystem contains certain elements, discussed in preceding parts, which play a key role in the protection of the right to privacy and personal data in general, and apply all the more so to address the security-privacy balance required in a democratic society. Such elements include a firm constitutional framework and specific additional legal protection of the right to privacy, the basic principles of administrative law, and the existence of several institutions in charge of protection of human rights, including the right to privacy (see part 1). One such foundational principle is the requirement that administrative authorities act solely within the confines of their statutory powers, especially in relation to activities that might infringe upon basic rights (see part 2.3).

Additionally, any authority whose mandate involves the collection and processing of personal data is subject to the provisions of the PPL. Furthermore, in many instances, such security authorities are subject to a specific law or specific regulations, which include specific restrictions and safeguards, discussed in greater detail in the following part.

In addition to legal regimes granting an administrative authority the ability to collect specific kinds of personal data, it may also receive personal data from another public body pursuant to chapter D of the PPL and subject to the restrictions therein and in the regulations (see part 2.1.3). Regarding "security authorities" as defined under the law,[111]it provides that such authority may receive and transfer data in order to fulfill its functions so long as such receipt or transfer is not prohibited by legislation.[112]

The abovementioned legal framework, together with the underpinning constitutional and administrative principles, form an ecosystem intended to address the challenge of balancing between the protection of the right to privacy and the interest of public and national security. In this process take part all the relevant agencies: the Knesset, the Attorney General, the PPA, courts and in particular the Supreme Court.

[111] The term "security authority" is defined in §19 and comprises the following authorities: the Israel Police, the Intelligence Branch of the General Staff of the Israel Defense Forces the Military Police, the Israeli Security Agency (ISA), the Institute for Intelligence and Special Operations (Mossad) and the Witness Protection Agency.
[112] See Privacy Protection Law, 5741–1981, §23B(b), KT 1011 p.128 (1981).

5.2. Rules, limitations and safeguards on the collection and use of personal data for national security and law enforcement purposes

This part elaborates upon the various legal frameworks in Israel under which access to personal data by law enforcement and national security authorities is authorized. It sets forth various data access laws under specific law enforcement and national security regimes, including limitations and safeguards, as well as general relevant administrative law principles and applying provisions the PPL.

5.2.1. Authority to access data under specific laws

5.2.1.1. Law enforcement

The Israel Police (the "**IP**") is the main law enforcement authority in Israel.[113]

The IP controls different databases that include personal data for operational, investigative or administrative purposes. In general, the IP obtains personal data for the purpose of fulfilling its functions, by virtue of the Police Order [New Version], 5731-1971[114] and the Criminal Procedure Order (Arrest and Search) [New Version], 5731-1969.[115] In addition, all procedures in connection with the collection and storage of certain types of sensitive data are regulated in specific legislation: the management of the Crime Register Database is governed by the Crime Register and Rehabilitation of Offenders Law; the biometric identification database of suspects, defendants, detainees and prisoners is regulated by the Criminal Procedure Law (Enforcement Authorities – Body Searches and Collecting Means of Identification); the receipt and use of communications data is regulated by the Telecommunication Data Law; and wiretapping is regulated under the Wiretapping Law.

As further detailed below, these laws relate to the processing of types of sensitive data and include, *inter alia*, provisions on the authority to obtain the data, the permitted purposes for obtaining it and its permitted purposes of use, the persons authorized to access the data, restrictions on transfer of the data to a third party, and in some cases

[113] Some regulatory authorities with unique specialties such as the Israel Securities Authority, the Israel Antitrust Authority and the Israel Tax Authority, are also entrusted with the power to conduct criminal investigations.

[114] Police Order [New Version], 5731-1971, SH 643 p. 22.

[115] Criminal Procedure Order (Arrest and Search) [New Version], 5731-1969, SH 580 p. 16. Hereinafter: Criminal Procedure Order (Arrest and Search).

specific provisions regarding data security, deletion of data and the right to access the data.

Furthermore, each of the above laws includes internal and external supervision and control mechanisms such as reporting duties to external bodies and other regulatory requirements. These are described more fully in part 5.3.

In addition to the provisions of the specific laws regarding specific types of data abovementioned, and in addition to the general provisions of the PPL, additional instructions apply to some of the databases and the types of data controlled by the Police, such as the Attorney General Guidelines and the State's Attorney Guidelines (for example, instructions pertaining to communication of data from investigation cases or publications from an investigation). Finally, parts of the databases are governed by internal Police circulars such as those that regulate the supervision of police emails or data regarding travel routes of police vehicles.

The Telecommunication Data Law regulates the access by the IP and a few other investigating authorities to telecommunication data from telecommunication companies. "Telecommunication data" is defined as including subscriber data, location data and communication traffic data, excluding the content of the communication. The law provides that an investigating authority seeking access to such data must petition the relevant District Court with a request to gain access to the data. The court will only grant an order permitting such access if it is satisfied that the conditions provided for in the law have been met, namely, that giving the authority access to the data does not harm the privacy of the data subject in an excessive manner, and that the collection of data is done only for one of the following purposes: saving the life of a person or protection of such life, investigating or preventing of offences, determining the identity of offenders and bringing legal action against them, or forfeiture of property according to law.

Where the circumstances do not allow time for petitioning the court, the law allows the authority to gain access to such data in cases where the data is urgently needed in order to save a person's life or in order to prevent a serious crime, after receiving a special permit from a designated officer. The permit is valid for 24 hours.

Regarding identifying details of subscribers, telephone numbers and other identifying numbers of telephones or their components, and data regarding locations of antennas,

the head of the Investigations and Intelligence Division in the IP is authorized to request from telecommunication companies an up-to-date file that includes such data.

The law includes other rules regarding, *inter alia*, confidentiality, data security, periodical obligation to report to the Attorney General regarding the abovementioned permits, and an annual obligation to report to the Constitution, Law and Justice Committee of the Knesset.

As will be elaborated in part 5.4.1 in the case of **The Association for Civil Rights in Israel**,[116] the Supreme Court examined the constitutionality of the provisions of the law. It held that, in order to ensure the correct balance between fulfilling the purposes of the law and the protection of the right to privacy, and in order for the law to withstand the constitutional tests, a narrow interpretation of the arrangements prescribed in the law should be adopted. Thus, for example, it concluded that the law should be interpreted as allowing the authorities to apply to the court with a request to receive an order solely for the purpose of investigating or preventing specific offenses or offenders, and not for general intelligence activity purposes relating to offenses or offenders.

The Wiretapping Law imposes a criminal prohibition on wiretapping of a conversation – whether oral or by telecommunications, including by communications between computers – and on use of such wiretapping. However, the law contains two exceptions: wiretapping for national security purposes (addressed below) and wiretapping for preventing offenses and identifying criminals. Concerning the latter purpose, wiretapping requires prior authorization by the Chief Justice of a District Court or a Deputy Chief Justice of the District Court. The order can be issued only if they are "convinced, after considering the measure of violation of privacy, that such a measure is required for identification, investigation or prevention of criminal offenses defined as "severe", that is, punishable by a prison term of over than three years . The order must state the identity of the person who is the subject of the wiretapping, or the phone line on which wiretapping is being permitted, if they are known in advance, and must detail the manners of wiretapping that are permitted. The validity of the order is limited to three months, though it is renewable, based on the same criteria as the initial order.

[116] HCJ 3809/08 The Association for Civil Rights in Israel v. the Israel Police (May 28, 2012), Nevo Legal Database, (by subscription, in Hebrew).

In urgent cases, the Israeli Police General Commissioner can order the wiretap for a maximum period of 48 hours; however the Court is authorized to permit it for a longer term pursuant to the process described above.

The law includes a provision regarding deletion and elimination of wiretapping data which an authorized Police officer has determined is not required for preventing offenses or identifying criminals.[117]

Finally, the law provides for reporting mechanisms - a monthly inter-governmental report to the Attorney General, as well as an annual report to the Constitution, Law and Justice Committee of the Knesset. These reports detail the scope of the permits that were issued and the number of people, lines and facilities in respect of which wiretapping had been allowed.

The Wiretapping Regulations 5746-1986,[118] include specific provisions regarding the abovementioned conditions and, *inter alia*, requires that the use of data collected pursuant to the law must be according to a specific permit issued by the Head of the ISA or the General Commissioner of the IP, such that only the relevant agents can be privy to it. In addition, the regulations require that wiretapping data be stored and deleted in accordance with the provisions of the Archives Law, 5715-1955,[119] unless an authorized IP officer determines the data is not required for the purposes mentioned previously –in which case the data is to be deleted within 10 days.

The Criminal Procedure Order (Arrest and Search) regulates the activity of the IP regarding arrests and searches in the context of a criminal investigation. Article 23A regulates the access of the IP to computer data, irrespective of the kind of hardware in which it is stored, including smartphones etc. It provides that such access is permitted only after receiving a court order "that details the objectives of the search and its conditions that will be determined in a manner that will not harm the privacy of a person in an excessive manner."

Currently, the government is promoting a bill that will eventually replace this order and will regulate the various aspects of searches. The bill contains further clarifications regarding the conditions in which the court may issue an order. In particular, it

[117] Wiretapping Law, 5739-1979, KT 938, §9B(c). See also: Wiretapping Regulations, 5746-1986, KT 4949 p. 1118, §7.
[118] Wiretapping Regulations 5746-1986, KT 4949 p. 1118. Hereinafter: Wiretapping Regulations.
[119] Archives Law, 5715-1955, SH 171 p. 14.

emphasizes the principle of proportionality, by providing that in cases where access to partial data would be sufficient to achieve the objectives of the search, the court must prefer to grant orders that permit only such partial access to the data. Additionally, the bill includes a new provision authorizing the chief justice of a District Court or his deputy to issue an order approving an undercover search in a computer, only for certain limited circumstances,[120] and only if conducting the search openly would undermine the very purpose of the search.

5.2.1.2. National security

The Israel Security Agency ("**ISA**") is Israel's principal national security authority.

According to article 7 of the Israel Security Agency Law, 5762-2002,[121] the ISA is in charge of the "protection of State security and the order and institutions of the democratic regime against threats of terrorism, sabotage, subversion, espionage, and disclosure of State secrets, and to safeguard and promote other State interests vital for national State security, all as prescribed by the Government and subject to every law". For the purpose of the above, section 7(b) of the ISA law details the specific functions that the ISA must perform.

The powers and activities of the agency, including powers to obtain data, are regulated by the ISA Law. In addition, certain specific powers to obtain data by the ISA are regulated by other laws, for example the Wiretapping Law.

As mentioned previously, the Wiretapping Law provides two exceptions to the general prohibition on wiretapping: wiretapping for national security purposes and wiretapping for preventing offenses and identifying criminals. Regarding the national security exception, the Wiretapping Law provides that wiretapping requires the approval of the Prime Minister or the Minister of Defense, further to a request by the Security Agency Director, but only after giving consideration to the degree of violation of privacy. The law further provides that a wiretapping permit must describe the identity of the person or the line to which the wiretapping has been approved, if their identity is known in

[120] Specifically, the undercover search order can be granted only for those grounds set forth in the Wiretapping law in connection with law enforcement authorizations.
[121] Israel Security Agency Law,5762-2002, SH 1832 p. 179. Hereinafter: ISA Law.

advance, as well as the permitted manners of wiretapping. The permit is valid for a maximum period of three months.[122]

Other relevant provisions of the Wiretapping Law and regulations including with regards to storage of wiretapping data, deletion of the data, authorization of specific agents and police officers to it, and reporting mechanisms were described previously in this part.

Access of the ISA to telecommunication data is regulated under the ISA Law. Section 11 of the law states that telecommunications companies, which are licensed by virtue of the Communications Law (Telecommunications and Broadcast), 5742-1982,[123] must transmit to the ISA certain categories of data found in their databases that are needed for the fulfillment of the functions of the ISA, and specified in rules issued by the Prime Minister. "Data" is defined under this section as including telecommunication data, but excluding content of a conversation within the meaning of the Wiretapping Law.

The law also requires that the use of relevant data will be according to a specific permit issued by the Head of the ISA, such that only relevant agents can have access to the data. The permit can be granted by the Head of the ISA "after he has been convinced that it is required by the agency to fulfill its functions under this law". The law also requires that "the permit specify particulars, wherever possible, about the data required, the purpose for which it is required and the particulars of the database in which it is found." The permit is valid for a maximum period of six months, but the Head of the ISA is entitled to extend it in accordance with the provisions set forth in that section.[124]

[122]Another type of wiretapping permitted under the law for purpose of protecting national security, is wiretapping to a worker in a classified position, for prevention or detection of a leak of confidential data that might cause severe damage to national security. According to the law, such wiretapping requires a permission issued by the Prime Minister or the Minister of Defense, further to a request by the Security Agency Director. The permission can be issued only after considering other measures that are less harmful, and must describe the identity of the persons, lines or devices to which the wiretapping has been approved. The permission is valid for a maximum period of 15 days, and its extension for a period longer than 30 days requires an approval by the Attorney General. The law also sets forth a mechanism for notifying workers in the relevant positions annually, regarding [the exercise of] this authority.

[123] Communications Law (Telecommunications and Broadcast), 5742-1982. SH 1060 p. 218.

[124] The ISA Law includes also specific provisions regarding the ISA's authority to conduct a search at a border station (§9), and to conduct an undercover search of vehicles and domains (§10), under the conditions specified in those articles.

5.2.2. **Application of the PPL in regard to data collected by security authorities**

The PPL sets forth a general legal framework, which applies to data collection and processing both by the private and public sector, including security authorities as defined by the law - the Israel Police; the Intelligence Branch of the General Staff of the Israel Defense Forces, and the Military Police; Israeli Security Agency (ISA); the Institute for Intelligence and Special Operations (Mossad) and The Witness Protection Agency (article 19). However, security authorities and those working on their behalf are subject to several unique provisions of the law, as will be elaborated below. In addition, as a general rule, processing activities are subject to the general provisions of the PPL, unless there is a specific legislative provision regulating directly the processing activity.

As a result of the above, the obligations included in chapter B of the PPL regarding database registration, management and data security, apply to security authorities databases, unless there is another specific provision in legislation regulating their activity.

Data transfers between public bodies – regulated under chapter D of the PPL – involving security authorities, are subject to article 23B(b) of the PPL, which states that security authorities are not prevented from receiving or providing data in order to fulfill their duties, provided that the delivery or receipt is not prohibited by legislation. In addition, in some cases, data transfers from security authorities are subject to specific rules that are stricter (such data transfers are only permitted to certain authorities under certain conditions). As an example, data that is included in databases regulated under Crime Register and Rehabilitation of Offenders Law and Criminal Procedure Law (Enforcement Authorities – Body Searches and Collecting Means of Identification) is subject to the stricter regime of these laws with respect to how personal data may be shared.

As noted in part 2.1.3, the Privacy Protection Regulations of 1986[125] provide a procedural mechanism for authorizing and supervising the sharing of the data between public bodies under chapter D of the law, so as to ensure that only data that complies

[125] Privacy Protection Regulations (Terms of Holding Data and its Maintenance and Procedures for Transfer of Data between Public Entities), 5746 – 1986, KT 4931 p. 858 (1986).

with the statutory requirements, including the proportionality requirement, can be transferred in this framework. Regarding data sharing which is not regulated under a specific law, the security authorities' act according to the provisions of these regulations when requesting data from other public bodies. In the working process on the updated draft of the new amendment to these regulations, specific provisions regarding the examination of a request for data by a security authority were included.

In addition, the security authorities are subject to chapter A of the PPL, which broadly defines a wide range of conducts as an infringement of privacy, which are both a criminal offense and a civil tort. However, article 19 of the PPL exempts certain security authorities from such liability if the infringement was reasonably committed within the scope of their functions and for the purpose of fulfilling those functions. Article 19's liability exemption is not frequently referred to in case law. However, in significant cases where it was deliberated by the Supreme Court, it was interpreted narrowly, in a manner that emphasized the limitations embedded in the article. In the relevant precedents,[126] before the enactment of the specific law regulating police authority to conduct body searches, the Supreme Court examined the legality of a specific method conducted by the petitioner's investigators (coercing him to drink salt water without his consent in order to induce vomiting, and thus extracting bags of drugs that he was suspected of having swallowed). The Court ruled that this activity was considered "other harassment" which violates article 2(1) of the PPL, and was not "reasonably committed". Therefore, the investigators were not exempt from liability under the PPL. In 2012, the Supreme Court examined the provisions of the Telecommunication Data Law in the case of **the Association for Civil Rights in Israel**. In the judgement, the Court pointed out that the provisions of the PPL stress the importance of the protection of the right to privacy. The Court emphasized that although the law includes liability exemption for security authorities, it is limited to acts that were "reasonably committed" within the scope of the authority's functions and "for the purpose of fulfilling such functions".[127]

[126] HCJ 249/82 Moshe Vaknin V. The Military Court of Appeal 37(2) PD 393 (1983); Further Hearing 9/83 The Military Court of Appeal v. Mosh Vaknin 42(3) PD 837 (1988).
[127] HCJ 3809/08 The Association for Civil Rights in Israel v. the Israel Police (May 28, 2012), Nevo Legal Database, (by subscription, in Hebrew), at para. 6. see also part 5.4.1.

5.2.3. **Transparency principles and the right to require information from security authorities**

Article 13 of the PPL exempts "security authorities" (as defined in article 19) from the data subject's right to access. Similarly, the Freedom of Information Law, 5758-1998,[128] exempts information held by security authorities, as defined under the law, from the provisions of the law.

Nevertheless, even though these laws seem to exclude security authorities completely from the right to information, there are other norms in Israeli law regarding transparency and the right to information, which apply to security authorities.

According to precedents of the Supreme Court (summarized below), the principle of transparency and the right to information are part of the foundations of the Israeli democratic regime and derive, *inter alia*, from the right to be heard by an administrative authority, and from the principle that information possessed by authorities is held "in trust" on behalf of the public.

Due to its significance, the right of individuals to access personal information about themselves has been recognized in Israeli case law as a constitutional right.

Therefore, even in the absence of a specific arrangement that regulates the right to access or review information (such as article 13 of the PPL) or the arrangement provided for in the Freedom of Information Law, and even when the said specific arrangement sets restrictions on the scope of the right to access information (such as those listed in the Freedom of Information Law), the principle of transparency of government activity continues to apply. Two Supreme Court judgments on this topic shed light on the contours of the right to information under Israel law:

1) In the **Fried** case,[129] the question was whether an individual has a right to review his criminal investigation file. The Supreme Court determined that the right of a person to review all the material in the possession of the authority derives from Israeli administrative law, and is closely related to the right to be heard by an administrative authority. In view of its importance to protect other procedural

[128] Freedom of Information Law, 5758-1998, SH 1667 p. 226. Hereinafter: Freedom of Information Law.
[129] HCJ 10271/02 Avraham Fried v. Israel Police (Jerusalem District), 62(1) PD 106 (2006).

rights of the individual, protecting this right is necessary in light of the rules of natural justice, in the relationship between individuals and authorities. In addition, when an individual has a direct and special interest in the information requested, the exemption from disclosure of information under the Freedom of Information Law does not necessarily prevent the right of the individual to review the information. When the special interest exists, the starting point of the legal analysis should be disclosure, and confidentiality should be the exception to the rule. Therefore, in such cases, the onus is on the administrative authority to show sufficient grounds for refusing to disclose the information. The Court also determined that since the general rule is disclosure, the authority must examine, in each case, the extent of the individual's interest in obtaining the information against the conflicting interests of non-disclosure, and must balance those interests in order to decide which of the interests will prevail. The scope of the right to review depends on the circumstances of the case and the extent of the anticipated damage to the applicant that will be caused by the refusal to disclose the information. As a general rule, it can be said that the more severe the expected damage from the refusal to disclose the information, the broader the right to access the information will be.

2) In the **Segal** case,[130] the Supreme Court recognized the possibility that the right of individuals to review information about themselves, outside the limitations of the Freedom of Information Law, would be broad, since in these cases "the fate of the data subject asking access to the information is at stake".

This principle is also reflected in the State Attorney's guidelines regarding handling requests to review investigation files (Guideline N. 14.8). In accordance with the guidelines, and although the Freedom of Information Law does not apply to this information, it is possible to review an investigation file in appropriate cases when there is a legitimate interest to be examined, taking into account the identity of the person seeking the information, their link to the information and the purpose for which they wish to review the information. The authority must take into account, when deciding whether to reveal the information, the prevention of misuse of investigation

[130] AdminA (Jerusalem Administrative Court) 814/07 Elitzur Segal v. State of Israel – Ministry of Justice (Feb. 2, 2018), Nevo Legal Database, (by subscription, in Hebrew).

proceedings and the prevention of disproportionate infringement upon the right to privacy.

5.3. Oversight and supervision

5.3.1. General internal and external mechanisms

5.3.1.1. The police

The activities of the police in the field of access to personal data and use thereof is subject to internal and external control and oversight mechanisms, intended to ensure conformity with the statutory powers vested in the police and subject to specific permissions granted to access the data. The main control and oversight mechanisms are as follows:

Internal Supervision and Control:

1) **The Data Security Unit**: A police unit whose function is to supervise the classification of the organizational data and its proper use. The unit is responsible for issuing instructions regarding the protection of data and databases. With respect to the activities of police personnel, the unit conducts different investigations and inquiries to detect any irregularity or deviation from the instructions, unlawful use of data or use of data without permission. Any irregular event is treated immediately with administrative, disciplinary or criminal proceedings.
2) **Data Security Division**: This division is part of the Technology Administration of the Israel Police and is responsible for the security of its computerized databases. All police data is managed, supervised and monitored in the police computer center, which applies monitoring systems that can detect and monitor immediately any unauthorized access or the use of unauthorized media in a manner that is not according to internal instructions. In addition, the unit is responsible for the operation of technological tools that ensure that the data is accessible only to people that have the authorized access clearance with respect of any action of each of the users of the police network.
3) **Additional police units**: Additional units in the police that engage in these fields include the Review Unit of the Police and the Legal Department that accompanies the activities of the Police in this field. These units provide

guidance to the professional entities and headquarter entities regarding the actions that are permitted and prohibited with respect to access to data, the use of data and disclosure of data.

External supervision and control

As mentioned in part 5.2.1.1, some of the specific legislative texts noted above include built-in monitoring and control mechanisms, such as the monthly reporting requirement to the Attorney General and annual reporting requirement to the Constitution, Law and Justice Committee of the Knesset according to the Wiretapping Law and the respective reporting mechanisms under the Telecommunications Data Law.

In addition, the police are subject to all of the external and general monitoring mechanisms that will be detailed below in part 5.3.1.3.

5.3.1.2. The ISA

In order to ensure the proper balance between protection of human rights in general, and the right to privacy in particular, with the goal of protecting national security, the ISA Law sets out several internal and external mechanisms of checks and balances, especially with relation to personal data, as will be elaborated below.

Regarding the internal supervision and control mechanisms, and conditions for exercising authority:

As noted above, article 11 of the ISA Law that deals with communication data, as well as the Wiretapping Regulations, prescribe the use of the data upon issuance of a permit by the Head of the ISA such that only relevant agents shall be granted access to the data. The Service is particularly cautious with respect to the protection of the data in its possession, *inter alia*, by setting out strict and specific data security arrangements, providing specific training to the ISA personnel regarding the use of data, regulating the manner of its storage and security and constant supervision of the use of sensitive data.

In light of the sensitivity of data, even within the Service itself, staff members are compartmentalized in their access to the data and they are granted personal permissions according to their functions and the needs of their work. In addition, according to article 19(A)(2) of the ISA Law, an employee or former employee of the ISA is forbidden to give information which he received in the course of his service in the ISA to anyone

who is not authorized to receive such information, except as required by law or pursuant to written permission.

In addition to the above, the internal control mechanisms also include administrative and legal supervision, and oversight by the internal comptroller of the organization. The ISA comptroller conducts audits from time to time that pertain, *inter alia*, to the conduct of the ISA with respect to the data it possesses for security purposes.

The external supervision and control mechanisms include:

1) Periodic reports to the Attorney General:
    a) **Reporting pursuant to article 11 of the ISA Law**: reporting about permits issued under that section, with respect to communication data and the manner of use of the data. The Head of the Service is obligated to deliver this detailed report to the Prime Minister and the Attorney General every three months.
    b) **Reporting pursuant to article 4(d) of the Wiretapping Law:** the Service provides to the Attorney General data regarding permits for wiretapping that were issued under chapter B of the Law for national security purposes.

    Based on this report, the Attorney General examines, together with the ISA, specific issues, for the purpose of ensuring that the data is used in a restrained and proportionate manner and solely for security purposes in accordance with the provisions set forth in the law. The issues discussed during these examinations may concern specific cases or broader trends, and from time to time leads to changes of internal procedures.
2) Parliamentary supervision – the ISA Law and the Wiretapping Law require that periodic reports be submitted to the Knesset Foreign Affairs and Defense Subcommittee and to a joint committee of the Knesset Foreign Affairs and Defense Subcommittee and the Constitution, Law and Justice Committee.

5.3.1.3. General supervision mechanisms that apply to all security authorities

General institutional supervision mechanisms apply to all government bodies including security authorities. As mentioned in part 1, the Supreme Court has the power to overturn laws, regulations and administrative decisions on grounds of constitutional or administrative law. In addition, various Knesset committees exercise important oversight functions and are authorized, as part of their constitutional role, to require from every governmental entity, including the security authorities, any information regarding their activities (additionally to their review of periodic reports by virtue of specific laws). The State Comptroller conducts periodic inspections of the different State authorities including the security agencies, and he is empowered to conduct in-depth investigations on a variety of issues including data security and protection of privacy. Finally, there is the Attorney General, the most senior legal entity in the executive branch, whose interpretation of the law is binding upon the government and its agencies. As part of his activities, the Attorney General guides the said agencies regarding different issues that arise in the course of their work and also as part of the periodic statutory reports specified above.

5.3.2. **Mechanisms under the PPL**

5.3.2.1. Powers of the Registrar of Databases

According to the PPL, the current powers of the Registrar of Databases with respect to Israeli public authorities for national security and law enforcement purposes are not different than its powers regarding other public and private sectors,[131] except for specific procedures regarding entry in a military base or facilities of a security authority.[132] .

Thus, the PPA has conducted several investigations with respect to law enforcement and national security authorities. Below are some examples of instances in which the Registrar executed his enforcement powers involving, *inter alia*, the collection of data from those authorities and the collection of testimonies from high level

[131] Regarding the powers of the Registrar, please see part 4.1 of this report.
[132] See Privacy Protection Law, 5741–1981, §10(e1)(2), KT 1011 p.128 (1981).

commanders..[133] Those examples reflect the Registrar's independence and autonomy vis-a-vis national security authorities.

1) **Lack of access controls and data minimization mechanisms within the IDF with regards to data-transfers from the Ministry of Interior to the IDF:** the PPA investigated data transfers from the Population Registry, which is managed by the Ministry of Interior, to the Ministry of Defense. The PPA found that exposure to data about civilians received from the Population Registry by the Ministry of Defense was too broad, and that the Ministry of Defense did not adequately manage its permissions and controls and did not act to implement data minimization mechanisms as required.

   The PPA instructed the Ministry of Defense to map the needs and usages of data by its various divisions and to determine profiles of access permissions according to professional necessities. In addition, the PPA ordered the Ministry of Defense to submit an updated application, in accordance to chapter D of the PPL, for the approval of the committee in the Population Authority for transferring data from the Population Registry and the Ministry of Defense based on the necessity of the data to each department (rehabilitation, recruitment and national security).

2) **Malfunction in IDF drafting system:** an update of an IDF drafting website caused a malfunction which resulted in the exposure of personal data, about data subjects who were in the process of recruitment to the army.

   The data included an evaluation of skills and psychogenic abilities of the data subjects. The breach was discovered following public complaints, several hours after the breach happened. The authority opened an investigation against the IDF. During the investigation of the incident the authority received the report of the internal investigation of the incident that was conducted by the IDF and about corrective measures that the IDF took following the incident.

3) **Data Theft from Military Data Bases:** The PPA is conducting an ongoing investigation against soldiers (who have completed their service by now) and against two data traders.

[133] For further examples see appendix 5.

The investigation was initiated following many complaints from soldiers who had completed their service, regarding telemarketing phone calls they received based on the fact that they completed their service. The findings of the investigation revealed that the data traders conspired with soldiers who had access to the military systems and received lists of personal data of hundreds of thousands of soldiers, including data about their life before their service in the army.

The PPA investigated several suspects and collected a large quantity of testimonies. The PPA seized computers and cell phones, and will soon transfer its findings to the State Attorney's Office for review and examination towards indictment.

5.3.2.2. Internal supervision model for security bodies under the Privacy Protection Bill

As mentioned in part 5.3.2.1, the Registrar's supervisory powers under the PPL are valid also in relation to security bodies. However, the new model proposed by the Privacy Protection Bill is more adapted to the special characteristics of databases controlled by security bodies. The model relates only to the manner in which security bodies are supervised, and not to the substantive law norms that continue to apply.

According to the proposed model, the Registrar's supervision in a security body will be carried out through an internal supervisor within the organization who must act in accordance with and be bound by the instructions of the Registrar. The internal supervisor will be required to act in accordance with an annual work plan to be approved in advance by the Registrar and the head of the security body, and to follow any supplementary instructions and corrective orders issued by the Registrar. The internal supervisor will be required to report his findings directly to the Registrar.

The powers of the internal supervisor will be similar to those of an inspector appointed by the Registrar, including powers to demand information, documents and access data. Based on the findings received from the internal inspector, the Registrar may impose on the security body or its employee's sanctions, or refer the findings to a criminal investigation under the PPL or to another authority's investigation. The internal

supervisor will be appointed by the head of the security body after consulting the Registrar and subject to qualifications determined by the Registrar.

The dismissal of the internal supervisor also requires a prior consultation with the Registrar. The internal supervisor will be a senior member of the security establishment's management and will receive sufficient resources and budgets to carry out its tasks.

5.4. Judicial redress

As elaborated in part 1, no administrative action in Israel by any public authority, including security authorities, is immune from judicial review.

In addition to filling a petition for judicial review to the Supreme Court, there are other means to challenge in court surveillance measures for national security or law enforcement purposes, mainly within the framework of criminal proceedings.

Below are summaries of relevant court cases concerning activities involving access to personal data for national security and law enforcement purposes.

5.4.1. Petitions for judicial review to the Supreme Court

1) **The Association for Civil Rights in Israel case:**[134] In this case, the Supreme Court examined the constitutionality of the Telecommunication Data Law that, as mentioned in part 5.2.1.1, allows the investigative authorities in Israel to obtain communications data from telecommunication companies under conditions specified in the law. In the judgment, the Court focused on the need for a balance between the constitutional right to privacy and the concern of excess government interference in the life of the individual on the one hand, and on the other hand the need to provide the investigative authorities with effective tools to maintain security and the public order. The Court emphasized that in light of the potential for significant privacy harm, the law should include complex arrangements which give appropriate consideration to the range of the relevant interests. In order to assure the correct balance between fulfilling the purposes of the law and the protection of the right to privacy and in order for the law to withstand the constitutional tests, the Court held that a narrow

[134] HCJ 3809/08 The Association for Civil Rights in Israel v. the Israel Police (May 28, 2012), Nevo Legal Database, (by subscription, in Hebrew), see para. 60 in our report from June 2017.

interpretation of the arrangements prescribed in the Telecommunication Data Law should be adopted. Thus, for example, in all matters pertaining to the arrangement in the law allowing the investigative authority to receive communications data via a request to the Court, it was held that the law should be interpreted as allowing the authorities to apply to the court with a request to receive an order solely for the purpose of investigating concrete offenses or offenders, and the law should not be interpreted as allowing the issuance of an order for the purposes of general intelligence activity relating to offenses or offenders. This is despite the language of the law that *prima facie* may allow this broader interpretation.

Likewise, for the purpose of assuring the protection of the right to privacy, the Court emphasized in its judgment that it is mandatory for the enforcement authorities to properly exercise the powers granted to them, while exercising cautious discretion that the powers in the law be exercised only on the scale and to the extent required. Furthermore, the Court noted that the Knesset and the Attorney General form an additional mechanism prescribed in the law, the purpose of which is to ensure ongoing scrutiny over the scale of the usage of the authorities granted by the law. Finally, the Court held that the law is constitutional, but emphasized that the powers given in the law should be given a narrow interpretation and its authorities should be exercised only to the extent necessary.

2) The **Academic Center of Law and Business case:**[135] This case involved a petition contesting the introduction of a new telephone system in the Israel Prison Service which enabled the collection of a voice sample from some prison inmates that agreed to do so, as a means of biometric identification. The petitioners argued that implementing the system constitutes a prohibited violation of the prison inmates' right to privacy. In order to protect the privacy of the prison inmates, the Attorney General formulated a guideline designed to regulate all of the aspects concerning obtaining a voice sample from prison inmates, as an interim measure that will apply until the matter will be legislated.

[135] HCJ 2779/13 The Academic Center of Law and Business, the Criminal Law and Criminology Division, the Prison Inmates and Detainees' Rights Workshop v. the Israel Prison Service (Dec. 24, 2013), Nevo Legal Database (by subscription, in Hebrew).

A bill to this effect, regulating the different aspects of obtaining voice samples from prison inmates, and other relevant aspects, passed the first reading in the Knesset.

5.4.2. **Criminal proceedings**

A suspect in criminal proceedings may request the court to exclude evidence against him.

1) According to the judgment of the Supreme Court in the **Isascharov** case,[136] a court may exclude such evidence if the following two conditions are fulfilled: Firstly, the evidence was seized in an unlawful manner. Evidence that was collected using unlawful investigation techniques or evidence seized in a manner that was unfair, or that harmed a protected basic right of the suspect. Secondly, accepting the evidence in court will substantially harm the right of the suspect to a fair trial, in an excessive manner and for an unworthy purpose.

2) The **Eliezer Philosof** case:[137] In this case, the defendant requested to exclude evidence that was found in an email account of the defendant pursuant to a search order issued by the court per the request of the police. The police was conducting an investigation against the defendants, and requested the order according to article 43 of the Criminal Procedure Order (Arrest and Search), which regulates "an order to seize an object". The defendants argued that access to email accounts should have been requested according to the Wiretapping Law and not through a search warrant issued according to the Criminal Procedure Order (Arrest and Search). The argument was accepted by the court and the evidence was excluded. The Court decided that the correct way to balance between the right to privacy of the individual and the public interest in investigation and prevention of offences is through the mechanism set forth in the Wiretapping Law, which includes more checks and balances, and therefore, a Wiretapping Order should be used to gain access to email accounts.

[136] CrimA 5121/98 Private Raphael Isascharov v. The Military Prosecutor 61(1) PD 461 (2006).
[137] CrimC (TA) 40206/05 State of Israel V. Elierzer Philosof (Feb. 5, 2007), Nevo Legal Database (by subscription, in Hebrew).

3) The **Corporal Sigawi** case:[138] The Military Court of Appeals issued a ruling regarding a search of the contents of mobile phone of a defendant. The court differentiated between a manual search in the presence of a suspect and a search done in a laboratory, without the presence of the suspect, for which the investigative authorities must issue a court order. The Court emphasized the significance of the right of the defendant to privacy, and determined that in the case at hand the defendant did not give lawful consent to the search. The request to appeal this decision submitted by the military prosecutor was denied by the Supreme Court.

4) The **Military Police** case:[139] During the investigation of a suspect, the military police requested and received orders to search the computer and cell phone of the suspect. The suspect petitioned to the Supreme Court and requested a hearing in the presence of both sides. Although the order was legally obtained, the Supreme Court ordered to delay the search order until the Magistrate Court, which issued the order, conducts a hearing with the presence of both sides. During the hearing, the suspect claimed that conducting the search would harm his right to privacy in an excessive manner and asked that restrictions be imposed on the search. Considering the suspect's claims, the Magistrate Court examined the principle of proportionality in regard to the search orders given. It confirmed the legality of the orders while setting forth conditions for retention of the data and limiting the exposure of the data to a specific investigator, a decision which reflects the importance of proportionality.

[138] Military Appeal 24/15 Corporal Jone Doe v. The Military Prosecutor (Nov. 6. 2016), Nevo Legal Database (by subscription, in Hebrew).
[139] HCJ 8183/17 John Doe v. State of Israel (Oct. 24, 2017), Nevo Legal Database (by subscription, in Hebrew).

Appendix 1 – Framework for the protection of the right to privacy under Israeli law

Part 1.3 – Fundamental Principles of administrative and constitutional law – reasonableness and proportionality

The examples presented below illustrate further the scope of judicial review applied to administrative decisions or legislation enacted by the Knesset, using the principles of reasonableness and proportionality

1) The **Juamis** case[140] discussed the reasonableness of the Minister of the Interior's decision to revoke the appointment of members of the Zarzir Local Council, that were appointed by an order issued by the previous Minister of the Interior. The court held that although the Minister of the Interior had the power to remove a member of the Council from office, the exercise of this power, like any other administrative decision, is subject to the rules of discretion and must be made on the basis of reasonable considerations and due exercise of discretion.[141] The court added that weighing all relevant considerations is insufficient, and that in order to pass the test of reasonableness, the administrative decision must express a proper balance between the various considerations, while giving appropriate weight to each of them. In the circumstances of the case in question, the court held that the Minister of the Interior did not ascribe sufficient weight to certain considerations, and therefore his decision deviates from the scope of reasonableness granted to the authority, and it cannot stand.[142] Accordingly, it was decided that the members of the Local Council should be convened in its composition as determined by the previous Minister of the Interior.

2) The **Zidan**[143] case involved the validity of regulation 5(2) of the Pension Regulations (Compensation for Delayed Payment) (Pension Fund from the National Insurance Institute of Israel), 5774-1984, enacted by the Minister of Labor and Social Affairs. According to this regulation, the entitlement to a grant

[140] HCJ 5240/96 Juamis v. Minister of the Interior (Mar. 3, 1997), Nevo Legal Database (by subscription, in Hebrew.
[141] *Id*, p. 298.
[142] *Id*, p. 304.
[143] HCJ 4769/90 Zidan v. Minister of Labor and Social Affairs (Apr. 14, 1993), Nevo Legal Database (by subscription, in Hebrew).

for a person who became disabled while working was limited to a certain period of time after the person becomes disabled. The petitioners argued that the regulation was extremely unreasonable, to the extent that justified its invalidation. The court held that even in cases where an administrative decision is non-arbitrary and made in "good faith", the decision could still be invalidated if it is a "manifestly unreasonable" decision. Furthermore, this principle applies also to disqualification of secondary legislation involving extreme unreasonableness. The bases for this are the rules of administrative law, which obligate the administrative authority to exercise its discretion reasonably and fairly. In the circumstances of the case, the court ruled that limiting the period of entitlement to compensation, significantly deviates from the legislative purpose of the Pensions Law and is therefore manifestly unreasonable. Accordingly, the court ruled that the regulation should be repealed.

3) Regarding the application of the principle of proportionality, in the **Hassan** case,[144] a petition was filed against a provision of the Income Support Law, 5741-1980, which categorically denied income support to a person who uses or owns a private vehicle. The court held that the provision violates the right to minimal human dignity, which is a basic constitutional right, and that this provision does not pass the second test of proportionality. The court emphasized that the presumption that a person who owns a private vehicle is not entitled to income support is disproportional, in that it denies the income support from persons who require it for minimum dignified existence.[145] Furthermore, the court held that it is possible to point to a number of reasonable alternatives, causing less harm or no harm at all, but still capable of realizing the legislative purpose underlying the provision in question and the constitutional right to a minimal and dignified existence.[146] As a result, the petition was granted and the court ordered the cancellation of the statutory provision.

[144] HCJ 10662/04 Hassan v. National Insurance Institute 65(1) PD 782, para. 58 of the judgment of President Beinisch (2012).
[145] *Id*, para. 62.
[146] *Id*, para. 64.

Part 1.6 – The Attorney General

As noted in the report, the Attorney General has the authority to set forth legal guidelines that bind the government in its activities. Below are examples of such guidelines in the field of privacy and data protection.

Attorney General Guideline No. 3.1103 - **"**Obtaining a Voice Sample from Prison Inmates and Maintaining It in a Database**"** (2015)

An example of implementing the privacy protection principles as part of the Israeli protection of privacy and personal data regime may be seen in the Attorney General Guidelines with respect to obtaining a voice sample from prison inmates and maintaining it in a database. The guidelines were adopted following the submission of a petition to the Supreme Court, objecting to the implementation of a new telephone system, arguing that the system constitutes a prohibited violation of the prison inmates' right to privacy.[147] In order to protect the privacy of the prison inmates, the Attorney General formulated guidelines designed to regulate all aspects concerning the obtainment of a voice sample from prison inmates, as an interim stage until the matter is legislated.[148] A bill to this effect passed the first reading in the Knesset.

The Attorney General Guidelines condition the implementation of the telephone system upon the safeguard of basic principles of data protection. First, the inmate must have provided informed and free consent, after having been notified of: (1) the existence of a true alternative telephone system with no need to obtain a voice sample; (2) the purposes and implications of obtaining the voice sample and maintaining it in a database and (3) the option to withdraw the inmate's consent at any given time.[149] Second, the guidelines require the implementation of additional basic principles concerning, *inter alia*, the scope, use and storage of data that will be collected. For example, the establishment of the database must be carried out in accordance with the "Privacy by Design" approach, so as to ensure that personally identifiable data is used

[147] HCJ 2779/13 The Academic Center of Law and Business, the Criminal Law and Criminology Division, the Prison Inmates and Detainees' Rights Workshop v. the Israel Prison Service (Dec. 24, 2013), Nevo Legal Database (by subscription, in Hebrew).
[148] Attorney General Directive No. 3.1103, "Obtaining a Voice Sample from Prison Inmates and Maintaining it in a Database" (2015).
[149] *Id*, p. 2.

only for lawful purposes and in accordance with the Attorney General Guidelines.[150] Furthermore, pursuant to the control of data principle, data stored in the database must be deleted if the inmate so requests or upon termination of his prison term, and the inmate must be granted the right to refer to the Israel Prison Service to inquire as to whether the identifying data regarding him had been duly deleted. Additionally, the Attorney General Guidelines emphasize the purpose limitation principle and defines the restricted use that may be made with the database.[151]

[150] *Id*, p. 3.
[151] See also part 3.3.

Appendix 2 – Significant updates – overview

Part 2.2 – Implementation of privacy and data protection principles in other legislation

The following is a brief overview of relevant legislation from recent years which includes embedded privacy and data protection principles.

Laws and Regulations

1) Financial Legislation

Supervision of Financial Services Law (Regulated Financial Services), 5776-2016:[152] This new law includes provisions requiring a financial entity to enable a customer or a service provider on his behalf to access online financial data held by the financial entity regarding the customer. Along with this duty[153], the provisions include checks and balances intended to mitigate privacy risks to the customer, arising from the sensitivity of the data, the online access to it, and its disclosure to a third party - the service provider. The provisions include restrictions on access to the data and security requirements and a finite list of the specific purposes for which the service provider is allowed to make use of such data. In addition, the law authorizes the Minister of Finance to prescribe regulations, after receiving the consent of the Minister of Justice, intended to ensure the rights of customers and emphasize protection of the customer's privacy and security of data. Governmental work is currently being carried out for the formulation of these regulations, and after those are instituted, the arrangement under the law will take effect.

2) Tax Legislation

The Income Tax Ordinace [New Version]:[154] Under the 2013 amendment of the Income Tax Ordinance, a temporary order has been adopted, imposing a duty on currency service providers to report to the Tax Authority on any financial action they carried out in the sum of NIS 50,000 or above, including identification details of the

[152] Supervision over Financial Services Law (Regulated Financial Services), 5776-2016, SH 2570 p.1098. Hereinafter: Supervision over Financial Services Law (Regulated Financial Services).
[153] The general right of access is enshrined in the PPL (see part 3.8). Nevertheless, the provisions of the Supervision of Financial Services Law (Regulated Financial Services) regulate specifically the right of access in the online financial data context.
[154] Income Tax Order [New Version], SH 339 p. 122.

customer. This order was put in place due to the phenomenon of money laundering and tax offences related to foreign currency traders, as an interim order until a new regulator is established under the Financial Service Providers Law (Regulated Financial Services). Along with this temporary order, a list of detailed restrictions has been set forth. These include the duty to maintain the data in a segregated database; to delete a customer's data after three years; to design the database and the system for collecting the reports in a manner that will minimize the risk of violating the privacy of the data subjects, and to consult with the Registrar of Databases for this purpose. The order restricts the individuals that are allowed access to the database, and sets detailed provisions concerning the entities entitled to obtain data from the database, as well as the terms and purposes for obtaining such data. The order also includes an explicit confidentiality duty, and it empowers the Minister of Finance, after receiving the consent of the Minister of Justice, to enact additional regulations, including regulations regarding the scope of the data held by the Tax Authority that can be cross-referenced with data obtained in accordance with these provisions.

3) Equality Legislation

The Equal Rights for People with Disabilities Law, 5758–1998:[155] The 2015 amendment of the law requires that 5% of employees of a large public employer will be employees with disabilities, in order to reach proper representation of that population among the employees. In order to monitor compliance with this provision, the law requires that several public entities provide the National Insurance Institute with data regarding the number of employees with disabilities, on an annual basis, including their details. The law provides that the data collected thereunder should be retained in a designated database separated from any other data, and that the Minister in charge must enact regulations regarding the disclosure, processing, maintenance, securing and deletion of such data, for the purpose of protection of privacy.

4) Political Parties Legislation

The Political Parties Regulations (Update and Verification of Identifying data of Political Parties' Members out of the Population Registry in Primaries), 5775-

[155] Equal Rights for Law, 5758-1998, SH 1658 p. 152.

2014:[156] The regulations were enacted pursuant to a 2012 amendment of the Political Parties Law, 5752-1992.[157] The amendment enabled the political parties to update and verify identifying data regarding the party's members, in order to enhance the contacting of party members and managing of the primaries. The regulations set forth a mechanism of cross-referencing between the party members' data file and the Population Registry file for the verification and update of the party members data. The mechanism aims to reach this goal along with preventing any data leakage or exposure of the party members' identities. The regulations state that the cross-reference can only be conducted in a computerized manner at the Population Registry, on a designated computer that is not connected to the database of the Population Registry and does not enable data retention. The regulations set additional provisions concerning the terms for conducting cross-reference, and the deletion of all data from the designated computer once the process is completed.

5) Biometric Identification

The Inclusion of Biometric Methods of Identification and Biometric Identification Data in Identification Documents and Databases (Amendment and Transitional Provisions) Law, 5777-2017:[158] With the aim of dealing with attempts to use fake identities and in order to ensure that every resident of the State of Israel holds one genuine identity card, an arrangement has recently been enacted, ordering the establishment of a biometric database. This arrangement includes restrictions and conditions which are noted below, that are designed to ensure the protection of the right to privacy. Naturally, this is a sensitive and complex question that involves considerations of national and public security together with the protection of privacy. Therefore, the law was enacted after extensive consultations within the government, and with professionals and the general public. Moreover, the law was constructed in such a way that it was applied gradually, setting a trial period in order to examine the necessity of maintaining a biometric database, the method of using it, the data that should be kept in it and the existence of other alternatives to the database. Likewise, a

[156] Political Parties Regulations (Update and Verification of Identifying data of Political Parties' Members out of the Population Registry in Primaries), 5775- 2014, KT 7429 p. 6.
[157] Political Parties Law, 5752-1992, SH 1395, p. 190.
[158] The Inclusion of Biometric Methods of Identification and Biometric Identification Data in Identification Documents and Databases (Amendment and Transitional Provisions) Law, 5777-2017, SH 2607 p. 434.

multi-disciplinary advisory committee was formed in order to oversee the process during the trial period as well as examine its results. After the examination process was completed, the Minister of Interior was convinced that it was necessary to maintain a biometric database and that this would fulfil the purpose for which the law had been enacted. However, in light of privacy and security considerations, and pursuant to the recommendations of the committee, the law contains a number of safeguards and revisions which differ from the original arrangement. Thus, for example, the biometric database may contain only photographs of facial features and two fingerprints. Unlike the inclusion of facial photographs, which is mandatory, the collection of the fingerprints is conditioned upon the resident's expressed and written consent**.** The provisions relating the two fingerprints, were prescribed as transitional, namely as a temporary arrangement only, valid for five years, with the possibility of reducing this period of time. During the course of this period, a periodical examination would be conducted to examine whether there are existing technological means which provide an appropriate solution for the purposes of the law, instead of including fingerprints in the database. Likewise, the law and regulations contain extremely stringent data security arrangements, including encrypting the data kept in the database; determining control and monitoring mechanism; restricting access to authorized persons; and designating two employees with a significant function in the protection of privacy, the Data Security Director and the Privacy Protection Director, whose function it is to prevent any leak of data and ensure the protection of the right to privacy. Following the enactment of the law, a petition which claimed that the law was unconstitutional was filed to the Supreme Court. The most recent verbal hearing of the petition took place in February 2019 and the case is still pending.

6) Preventing Sexual Harassment - Publishing Sexual Content

The legislative amendment described below is different from the examples provided thus far in that it does not concern the regulation of governmental activities, but rather the protection of privacy within the private sector. This amendment was initiated in light of the spreading social phenomenon of distributing videos and photos of a sexual nature on social networks, as detailed below.

The Prevention of Sexual Harassment Law, 5758-1998:[159] As part of a 2014 amendment, the definition of sexual harassment under article 3 of the law was changed in order to include, in addition to the existing list of activities enumerated in the law, the act of "publishing a photo, video or recording of a person, focusing on his sexuality, under circumstances where such release may degrade that person or humiliate him, where his consent had not been given for its release". The law also added protection for such publication in the context of criminal or civil law proceedings similar to the protection in the PPL, which due to the extensive applicability of the law, intended to balance between protecting the victim on the one hand, and other interests and rights on the other hand, particularly the right to freedom of speech.

The behavior defined as part of the amendment to the Prevention of Sexual Harassment Law was already at the time of amending (and still to this day), viewed as a violation of privacy pursuant to article 2(4) of the PPL.[160] Even so, defining the distribution of photos that focus on the sexuality of a person as sexual harassment under this law was mainly intended to characterize such behavior as being prohibited because of being "sexual harassment". Such characterization includes public implications, and it grants those harmed by such behavior an additional channel for suitable remedies.

Implementation of privacy and data protection principles in government resolutions and central general director circular

The need for protection of the right to privacy and establishing specific mechanisms designed to protect this right is expressed also within government resolutions and procedures set forth by various government ministries. The two resolutions below reflect this:

1) Government Resolution No. 1933 dated 30.8.16, regarding the improvement of the transfer of government data and granting the public access to government data bases

The first part of this resolution discusses the transfer of data between government offices in order to improve government services provided to the public. This is balanced against robust privacy protections. The resolution provides that data can be transferred

[159] Prevention of Sexual Harassment Law, 5758-1998, SH 1661 p. 166.
[160] The article concerns: “releasing to the public a photo of a person under circumstances where such release may degrade or humiliate him”.

between government offices only if the intended transfer is approved by the Inter-Ministerial Committee for Transfer of Data[161]. The committee's task is to ensure that the transfer of data is carried out as authorized and only to the extent that is proportional to the purpose of the transfer, including, in the appropriate cases, conditioning the transfer upon consent given by the data subject. The resolution further states that sharing data can only be carried out after examining, *inter alia*, the sensitivity of the transferred personal data, the scope of the data, and the benefits of such transfer to the public.

The second part of the resolution concerns the access to governmental databases. It authorizes government ministries to provide access to the databases they are responsible for, provided that the data therein does not constitute "identified personal data".[162] "Identified personal data" is defined broadly, and includes "data as its definition under the PPL, including data concerning a person's private matters, and including data that is not identified data, but could be identifiable, in itself or together with additional data. The decision of whether data is identifiable, in itself or together with additional data, shall be made by an expert in the technology industry, accompanied by legal advice and data security advice".

2) Government Resolution no. 2733 dated 11.6.17 regarding the promotion of the national project "Digital Israel"

This government decision encourages the public sector to implement innovative technologies through digital tools. The resolution refers to the principles of the protection of the right to privacy. For example, it states that as part of implementing the government resolution, the governmental bodies must consider whether the programs promoted by them entail collection of identified or identifiable personal data, and if so they must take into account privacy and data protection considerations as early as at the stage of formulating the program. The relevant bodies are required to set forth mechanisms for protecting privacy and personal data, whilst implementing the principles of data security.

[161] For further elaboration regarding data transfer between public bodies, see part 2.1.3 of the report.
[162] Government Resolution No. 1933, "Improvement of the Transfer of Government Data and Granting the Public Access to Government Data bases (30.8.16).

An additional example of safeguarding privacy protection aspects as part of government resolutions or procedures may be seen in the Director General Circular issued by the Ministry of Education, as detailed below. A Director General Circular is a document which the Director General of the government office publishes. The circular binds all employees and it expresses the principles of the office's policy on certain matters. The circular usually contains guidance and regulations concerning continuous work procedures of the office and of all its regulated bodies.

3) The Ministry of Education Director General Circular no. 5775/9(a) regarding operation of cameras in educational institutions

In May 2015, a Director General Circular issued by the Ministry of Education was published, concerning cameras in education institutions. It regulates the installation and use of such cameras and strikes a balance between the students' right to privacy on the one hand, and maintaining security and protection in schools on the other hand. The Circular states that "continuous use of the cameras is considered to be a last resort",[163] given that it entails violation of students' privacy. The Circular emphasizes that the use of cameras must be carefully considered and should be implemented only to the extent that is strictly required. According to the Circular, the decision to place cameras in a school must be stated in writing, and signed by the director of the education institute. Furthermore, the Circular establishes various mechanisms designed to reduce violation of privacy, in the event that the school decides to install cameras. For example, the cameras should be placed so that they will film only the "public area", which serves all of those visiting the school (such as the school yard, sports fields, etc.); No camera may be placed or operated in a manner that enables photographing personal space or a place within the public area where private and quasi-private activities take place (such as bathrooms, counselor's room and infirmary); The cameras should not be placed in classrooms. Further, the Circular includes instructions with respect to notifications and posting signs on the placement of the cameras the level of data security that must be used, access restrictions and restrictions on the permissible uses of films` confidentiality, and deletion of the recorded material.

[163] The Ministry of Education Director General Circular no. 5775/9(a), "Operation of Cameras in Educational Institutions" (3.5.2015).

Part 2.3 – Case law updates

Judicial review of legislative and administrative powers

Alongside the case law elaborated in the report, judgments from recent years illustrate their involvement with privacy protection in the public sector. These judgments embody the judicial authority's significant oversight role over the legislative and executive branches and its sensitivity to privacy concerns.

For example, the **Jane Doe v. the National Insurance Institute** deals with the permitted scope of an investigation to assess an individual's entitlement to National Insurance benefits. In the case at hand, an investigator at the National Insurance Institute had conducted an undercover investigation in the plaintiff's home, in the course of which, he filmed the plaintiff without her knowledge, while hiding his identity.[164] The Labor Tribunal held that the use of deception for the purpose of investigation constitutes an invasion of privacy, and this invasion is reinforced when the investigation is conducted in the home of the person being investigated. In this context the Tribunal emphasized the importance of the right to privacy as allowing a person to have control over the course of his life and the data pertaining to him. The Tribunal held that it would have been possible to conduct the investigation outside the home of the plaintiff, and there was no need for such a severe invasion of her privacy. The Tribunal also held that the invasion was not proportional under the circumstances of the case and therefore the video recorded was inadmissible. An important determination in this context is that the investigator's entering into the plaintiff's home under a false pretense constitutes a severe infringement of the right to privacy.

The Tribunal emphasized the necessity of acting with great caution when using such methods of investigation, paying attention, *inter alia*, to the infringement of the constitutional right to privacy.[165]

Protection of privacy balanced against freedom of information

[164] NI (Tel Aviv) 59213-01-12 *Jane Doe* v. the National Insurance Institute (Mar. 3, 2014), Nevo Legal Database (by subscription, in Hebrew).
[165] *Id.*, at para. 13-16.

The Freedom of Information Law, 5758-1998:[166] The law enshrines the right of every Israeli citizen or resident to receive information from a public authority. The law makes this right subject to reservations and outlines that create a balance between the right to information and other various rights and interests. In the context of the right to privacy, article 9(a)(3) of the law prohibits a public authority to disclose "information of which disclosure constitutes an infringement of privacy, within the meaning of the PPL, unless the disclosure is permitted by law". It should also be noted that the law includes provisions protecting a third party that is likely to be hurt as a result of the delivery of the information. *Inter alia*, the law regulates the right of a third party to object to the disclosure of the information (article 13), and his right to have his arguments heard before the Court (article 17(c)).

An overview of the Supreme Court's decisions in recent years indicates that the right to privacy has often prevailed over the right to freedom of information.

1) In the **Shenrom** case[167] the Court dealt with a request by a private company to receive details from a municipality about certain properties. The data requested was generic (the size and classification of the properties), but combined with data regarding the names and addresses of the people occupying the properties, it would allow conclusions to be drawn concerning the type of use of the property and therefore data about its owners. The company claimed that the data requested would enhance the ability of the public to observe the municipality's activity. The Supreme Court held that the possibility of drawing conclusions regarding the owners through cross-referencing of the data unlawfully violates the privacy of those individuals.[168] Therefore, the Court held that the disclosure of the requested data could only apply with regard to property owners who had provided explicit consent on their own initiative. The importance of the judgment lies in its emphasis of the importance of protecting the constitutional right to privacy within the framework of the freedom of information requests. The judgment explains that the public authority must act with caution and precision when it considers providing data of which disclosure is likely to

[166] Freedom of Information Law, 5758-1998, SH 1667 p. 226. Hereinafter: Freedom of Information Law.
[167] AdminA Municipality of Hadera v. Shenrom ltd. (Jul. 16, 2012), Nevo Legal Database (by subscription, in Hebrew).
[168] *Id.*, at para. 11.

infringe a person's privacy. The judgment also stresses that in the absence of the data subject's explicit consent, the authority that considers providing the data must assume that he or she objects. This derogates from the general principle which stands at the base of freedom of information requests, according to which a third party should actively and explicitly express his objection in order for him to be considered as objecting to the disclosure of data regarding him (opt-out mechanism). In effect, in freedom of information cases which involve privacy concerns, the Supreme Court interpreted the law as requiring a unique mechanism, according to which a data subject's silence is deemed to constitute his objection to the disclosure (opt-in mechanism).

2) In the **Rosenberg** case,[169] which concerned a request to disclose personal data regarding sides to procedures in the Law Enforcement and Collection System Office,[170] the Court upheld the rule that was set in the **Shenrom** case and approved the decision to reject the request, emphasizing that in the balance between the right to privacy and the right to freedom of information – the legislator chose to give priority to the right to privacy. The Court mentioned that in previous cases where considerable public importance was attached to the delivery of the data, it did not rule to disclose the requested data immediately, but rather it ruled that the relevant data would be disclosed only in the future, regarding future data subjects, after they will be notified in advance that the relevant data in their matter might be exposed in freedom of information procedures.[171]

[169] AA 2820/13 Raz Rosenberg v. the Law Enforcement and Collection System Authority (Jun. 6, 2014), Nevo Legal Database (by subscription, in Hebrew).

[170] The Execution Office is the governmental authority in charge of enforcement of judicial decisions on debt collection.

[171] The court was referring to previous cases that dealt with the exposure of the names of tax offenders who came to a settlement with the Taxes Authority to pay an amount of money in order not to be charged with criminal procedures , and also in the matter of the exposure of candidates for the position of director in government companies, who had been disqualified by the appointments Committee. See respectively, AdminA 398/07 The Movement for Freedom of Information v. The State of Israel – Tax Authority 63(1) PD 284 (2008); AdminA 9341/05 The Movement for Freedom of Information v. the Governmental Companies Authority (May 5, 2009), Nevo Legal Database (by subscription, in Hebrew).

Protection of the right to privacy in the digital space

As the examples below demonstrate, Israeli courts are keenly aware of the need to safeguard the right to privacy in the digital sphere, taking into account the significant challenges that threaten this right, especially given technological advances and more specifically the ubiquity of computers and other connected devices.

1) In the **Ezra** case,[172] the Supreme Court discussed a criminal appeal filed by the State, after the accused had been acquitted of hacking-related offenses. In an *obiter dictum* the Court stressed the need to reexamine and update traditional legal frameworks in light of technological changes, and in particular the transfer of increasing amounts of personal data in digital format and the urgent public interest to ensure adequate protection to such data.[173] The court interpreted the term "unlawful" circumstance[174] that constitutes part of the definition of the offense "penetration into computer material", by focusing on the principle of consent, and held that the offence relates to any penetration to a computer without the consent of its owner (whether the computer was protected by a password or not).[175] The Court clarified that penetration into a computer constitutes, inherently, an infringement of the privacy of its owner, in a similar manner to entering into a person's physical home without his consent.

2) In the **Dvir** case,[176] the Supreme Court heard an appeal against the decision of the District Court to convict the accused for stealing mobile telephones, and on the severity of his punishment. In its judgment, the Court emphasized that the very fact of the theft of a mobile telephone constitutes a violation of a person's innermost privacy, being that it's an entry point to the entire range of the person's personal data. Due to that, the court held that the stealing of the mobile

[172] CA 8464/14 State of Israel v. Nir Ezra (Dec. 15, 2015), Nevo Legal Database (by subscription, in Hebrew).
[173] *Id*., para. 10 of the judgment of Justice Rubinstein
[174] *Id*.., Justice Rubinstein relied upon the determination\s of the learned Kerr, however contrary to the aforesaid words, expands the definition of "unlawful". For Kerr's article see: Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1641 (2003).
[175] §4 of the Computers Law, 5755-1995, SH 1534 p. 366.
[176] CrimA 8627/14 **Natan Dvir v. the State of Israel** (Jul. 14, 2015), Nevo Legal Database (by subscription, in Hebrew).

telephone is "a damage multiplier" and an aggravating circumstance in the offense.[177]

3) The **Rihani** case[178] concerned the legal status of e-mail account. The appellant, who acted as the receiver of the respondent's assets in bankruptcy proceedings, petitioned to receive a copy of the debtor's e-mail account. The appellant was denied access despite his suspicions that the concealed e-mail account was being used for managing income in an illegal manner. The appellant argued that his appeal should be accepted since the statutory provisions pertaining to bankruptcy regulate the authority of the Court to order, under specified conditions, that items of mail that were addressed to the debtor be sent to the receiver. Nevertheless, in its judgment the Court emphasized the unique characteristics of the e-mail account and the significant differences regarding the infringement of privacy between reviewing letters and reviewing the content of an email account. Since allowing access to the debtor's email account constitutes a greater infringement of the right to privacy,[179] the Court gave priority to the right to privacy over the purposes of the bankruptcy laws, and ruled that the email account constitutes the individual's personal space. These determinations exemplify the importance of the protection of the constitutional right to privacy by means of giving a narrow interpretation to the statutory provisions whenever their implementation might lead to an increased infringement of privacy. The judgment clarifies that in view of the changing times and technical advancements, the Court must take into account the potential effects on privacy while interpreting the terms of the law and their application to the virtual world.[180]

4) The status of the right to privacy in the digital sphere was also debated in the **Savir** case,[181] in which Google was required by the Court to remove a harmful

[177] *Id.*, para. 7 of the judgment of Justice Amit.
[178] CA 129/17 Rihani v. Strikovsky (Jul, 4, 2017), Nevo Legal Database (by subscription, in Hebrew).
[179] *Id.*, Para. 24 of the judgment of Justice Solberg.
[180] In the words of the Court: "the wooden desktop has become the desktop on the computer screen, the geographical site has become an Internet site, and also the post box has become a 'e-mail' box. Notwithstanding that sometimes the terms are identical; the meanings are likely to be different". *Id.*,, in Para, 11-14 of the judgment of Justice Solberg.
[181] CA (Tel Aviv) 44711-11-14 Ami Savir Adv. v. Shaul Bar Noy, para. 7 of the judgment of Judge Cohen (Jun, 22, 2015), Nevo Legal Database (by subscription, in Hebrew).

publication after a third party that published it refused to cooperate and remove it. The Court held that whenever search results in a search engine are entirely erroneous, the right to privacy prevails over the rights embodied in the publication appearing on the Internet. As a result, the search engine must remove the harmful publication, even if the third party, the original publisher, refuses to do so.[182]

5) An additional issue that was brought before the Supreme Court and raises complex questions in the interplay between law and technology is the judgement in the **Hashavim** case.[183] In this matter the Court addressed the question of whether it should be allowed to prohibit a commercial company from indexing court judgments, in a manner that would prevent its finding through Internet search engines, as a requirement for granting access to the judgment database maintained by the Israeli Judicial Authority. The intention of the prohibition was to protect the privacy of data subjects mentioned in the judgements, by limiting the availability of the content of the judgements through random search in the general search engines. The Court acknowledged the importance of protecting the privacy of the parties and the third parties mentioned in the judgments, while noting that in light of the new technological era, which places new challenges in the context of the right to privacy, a balance must be maintained between enjoying the fruits of technology and minimizing violation of the individual's rights.[184] At the same time, the Court noted that in light of the violation of additional basic rights (especially the petitioning company's freedom of occupation), the State is required to formulate a legislative solution that provides an appropriate solution, and is not allowed to prevent the publishing companies from indexing of judgments, without legislation. The judgment also mentioned the work of a public committee headed by the Former Supreme Court Justice Englerad, which had been established in order to examine all of the questions related to stating personal

[182] Nevertheless, it should be noted that the judgment held that insofar as there is doubt in the correctness of the publication, the search engine may decide that it will only erase the data upon the existence of a judicial order.
[183] HCJ 5870/14 Hashavim H.P.S Financial Information Ltd. v. the Judicial Authority (Nov. 12, 2015), Nevo Legal Database (by subscription, in Hebrew).
[184] *Id*, para. 31 of the judgement of Justice Rubinstein.

data within judgments, considering the release of such documents in legal databases and web sites. This committee has not yet submitted its recommendations. In the context of the issue the judgment raises, in August 2015, the Minister of Justice established a public committee headed by Former Supreme Court Justice Arbel, tasked with formulating measures of protection against hurtful activities and publications on the Internet.

Protection of the right to privacy in civil law

The protection of the right to privacy applies not only within the confines of public law. The roots of the right to privacy are planted in public constitutional law, but the branches of the right extend over to the civil law, in creating a comprehensive protection of this right throughout the legal system. In addition to the other relevant judgements mentioned in the report and in the next part regarding Labor Law, what follows is a more elaborated overview of a significant case law addressing this topic, that was mentioned briefly in part 3.1.2 of the report.

In the **Jane Doe** case,[185] the Supreme Court considered at length the status of the right to privacy in the civil law and the question of the balance between this right and the right to freedom of expression. The concrete question the Court faced concerned the publication of a book written by an individual, the appellant, that describes the intimate relationship between him and the respondent. In the judgment, the Supreme Court reiterated that the right to privacy is "one of the freedoms shaping the character of the regime in Israel as a democratic regime and it is one of the supreme rights establishing dignity and freedom".[186] Regarding the circumstances of the case, the Court related to the intensity of the significant infringement of the right to privacy, and the importance given to the protection of this right within the framework of an intimate relationship. The Court found that the fiction in the book is scant and that the book contains highly intimate details (such as thoughts, feelings and secrets) concerning the respondent's inner life circle, and therefore publication of the book would seriously affect the core of the respondent's right to privacy. In light of the grave infringement of the respondents' privacy, the Court held that her right to privacy should prevail over the

[185] CA 8954/11 John Doe v. Jane Doe, (Apr. 24, 2014), Nevo Legal Database (by subscription, in Hebrew).
[186] *Id.*, para. 67 of the judgement.

appellant's freedom of expression, such that the publication of the book in this particular case should be forbidden.

Protection of the right to privacy in standard contracts

The field of standard contracts is one of the legal fields aiming to address situations of an intrinsic imbalance in power between two parties.[187] Here follows a case which demonstrates the implementation of the privacy principles in this context.

In the **Cellcom** case,[188] heard before the Standard Contracts Tribunal[189] the Attorney General submitted a motion for the annulment of depriving terms included in the agreement of an Israeli cellular company (Cellcom) with its customers. After the representatives on behalf of the Attorney General held deliberations with the company, the company agreed to modify the terms of the engagement agreement so that the privacy protection chapter included in the agreement would be modified to increase the protection of privacy of its customers. For example, the updated agreement includes provisions that restrict the use of the data and its transfer to third parties. The agreement also includes provisions regarding the data subject's right to access and the obligation to receive his consent to the use of such data. The Tribunal approved the agreement of the parties.

[187] Another similar field deleing with intrinsic power disparities is the field of Labor Law. Relevant Labor case law were mentioned in parts 2.3.2 and 3.2 of the report (the Isakov case and the Kalanswa case).
[188] SC 42799-03-10 the Attorney General v. Cellcom Israel Ltd.(Jan, 25, 2017), Nevo Legal Database (by subscription, in Hebrew).
[189] The Standard Contracts Tribunal is a special tribunal empowered by the Standard Contracts Law, 5743-1982 to judge in cases of standard contracts. According to article 1 of the Law, the purpose of the law is to protect consumers from depriving terms in standard contracts. Accordingly, the Tribunal is empowered to annul or alter terms in a standard contract which the Tribunal considers as depriving terms.

Appendix 5 – Access to personal data by public authorities for national security and law enforcement purposes

Part 5.3.2.1 – Powers of the Registrar of Databases

Below are few additional examples of investigations by the PPA with regards to personal data processed by security and law enforcement authorities:

Data regarding the Israel police and prison service personnel

During the criminal investigation by the PPA of a theft of data from the Israeli Population Registrar database, the PPA uncovered, on the computer of one defendant, a database that included personal data on about 14,000 people working for the Israeli Police and the Israeli Prison Service. The PPA revealed that the defendant carried out a big project for the Police and for the Israeli Prison Service, and had kept the data regarding the personnel on his personal computer, at his home, for a few years. The defendant was found guilty in court for violating the PPL.

Data transferred between the National Insurance Institute, the Tax Authority, the Ministry of Defense and the Rehabilitation Department for the Disabled

The PPA inspected data transfers between these public bodies in accordance to chapter D of the PPL. During its inspection, the PPA found that the Tax Authority and the National Insurance Institute continued to transfer data to the Ministry of Defense and the Rehabilitation Department for the Disabled despite the fact that the authorization to transfer data by the relevant committee had been expired for about 18 months. The PPA ordered the parties to identify the data that is necessary to transfer between the public bodies to fulfill their tasks and missions, and ordered the parties to submit a new request for a valid permit to transfer the data.