STATE OF ISRAEL

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

June 2017

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. We are pleased to submit this initial review of the significant changes and developments in Israel in this field.

This document consists of the following parts: (A) A brief overview of the regime for the protection of the right to privacy and personal data in Israel, which provides the basis for the developments described below; (B) A review of significant developments in legislation concerning protection of privacy and personal data, including examples of the implementation of privacy aspects in other legislation; (C) Updates on important case law; (D) the activities of the Israel Law, Information and Technology Authority (hereinafter "ILITA") (E) An account of relevant Attorney General Guidelines; (F) A description of the main government resolutions and binding instructions by various government ministries that relate to the advancement of privacy protection in Israel; (G) A description of public activities in Israel in which the Ministry of Justice has been involved, as well as the activities carried out by the Privacy Protection Council; (H) A review of the issue of access to personal data for national security and law enforcement purposes.

As you will see, Israel fully understands the crucial importance of personal data protection, both for individuals in Israel and for individuals in the EU whose data is transferred to Israel; therefore we believe the EU should maintain the Adequacy Decision.

A. The Regime for the Protection of the Right to Privacy and Personal Data under Israeli Law

1. As detailed within the documents on which the 2011 Adequacy Decision was based[1], Israel is a parliamentary democracy with a legal system of similar characteristics as those of the Common Law systems. Based on the tradition of this legal method, the law in Israel is not a full and complete codex of the law, but rather Court decisions play a central role in the legal system, as they develop and compliment legislation by way of interpretation and setting binding legal precedents. In addition, the constitutional regime in Israel is not based on a single document which constitutes a formal and complete constitution, but rather on several Basic Laws, which are granted a superior normative status[2]and are viewed as chapters of a constitution to be completed in the future.

2. Among the Basic Laws mentioned above, the Basic Law: Human Dignity and Liberty of 1992 is the most relevant with respect to privacy protection. This law lists explicitly a number of fundamental rights, including the rights to dignity, liberty, privacy and property, as it also provides that "Each and every government authority is obliged to respect the rights in accordance with this Basic Law." (Article 11). Article 7 of the Basic Law, which addresses privacy and personal matters, is the most detailed provision, and 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 premises of a person, without his permission. (c) No search shall be held on the private premises 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."

3. This Article has been interpreted by the Supreme Court and other Courts as granting broad protection of the right to privacy and its various componants amongst which, the right to

[1] Attached as Annex 1
[2]CA 6821/93 Bank Hamizrahi Ha'Meuchad v. Migdal Kfar Shitufi 49(4) 221 (1995)

privacy of data – data protection[3]. At the same time, like the other rights listed under the law, the right to privacy is not absolute , and violation of such by any of the government authorities is subject to the "Violation of Rights" Article 8 of the law, which is commonly referred to as the "Limitation Clause". This Article provides that "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."

4. Beyond the constitutional protection of the right to privacy, it received even prior to the enactment of the Basic Law: Human Dignity and Liberty of 1992, explicit and substantial statutory protection under the Privacy Protection Law of 1981 (hereinafter "the Privacy Protection Law"). This law had been considered to be one of the first modern laws in the world to explicitly regulate protection of the right to privacy and its various componants. The Privacy Protection Law applies both to the public and private sectors. It extablishes a civil tort and under certain conditions even a criminal offense with a maximum term of imprisonment of five years with respect to a violation of privacy. Chapter A of the law 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 (hereinafter: "the Registrar") with supervision and enforcement powers in order to execute the provisions under the Privacy Protection Law with respect of this matter; Chapter C of the law addresses situations where the Court may rule that the defendant is granted a defense despite the violation of privacy, as well as the applicability of the Privacy Protection Law to security authorities; Chapter D of the law imposes limitations on the transference of personal data by public entities, and sets forth certain exceptions to those limitations; chapter E of the law sets forth a variety of provisions concerning mainly the manner of conducting proceedings due to violation of privacy.

   Following the legislation of the Privacy Protection Law, regulations and orders have been enacted for various issues, including data security, personal data transfer outside of Israel,

[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) P.D. 842 (2004), within which the practice of providing financial entities, and other bodies with personal data listed in the Population Registry had been deemed unlawful.

transfer of personal data between public entities, and transference of personal data by public entities to private entities.

5. Towards the conclusion of this brief and general overview of the protection of privacy regime under Israeli law, it should be noted that in addition to the provisions under the Basic Law: Human Dignity and Liberty of 1992 and the Privacy Protection Law, Israeli law includes other legislations, which regulate various government or economic activities, and include specific provisions regarding the protection of privacy and personal data within such. For example, in a nutshell, provisions of this type are included under the Equal Rights for People with Disabilities Law, 5758 - 1998, the Income Tax Ordinance [New Version], the Credit Data Law, 5776 - 2016 and others, as will be discussed in depth below. Concerning the order between specific arrangements and the provisions under the Privacy Protection Law, it should be noted that as a rule, the provisions under the Privacy Protection Law apply in addition to the provisions under such specific laws, unless an explicit provision in the specific law grants preference to the specific arrangement.

6. Before we expand on the developments in Israeli law since the 2011 Adequacy Decision, we would like to expand upon the various important "players" in the Israeli legal system.

7. First and foremost, within the field of protection of personal data, the enforcement of the laws concerning privacy protection of personal data is first carried out by the Registrar of Databases, acting according to the authority given to it in the Privacy Protection Law. Extensive details on the activities of the Registrar of Databases, within the organizational framework of ILITA, shall be brought hereafter [see Chapter D]. The Registrar is a fundamental and independent player in the protection of personal data. The decisions of the Registrar and his enforcement activities have much influence on the conduct of the business, private and public sectors.

8. Two additional “players” are worthy of special attention and are relevant not only to the field of protection of personal data but to the law system at large, and which must be taken into account in order to fully understand the Israeli legal system and the manner in which human rights, including the right to privacy, are protected.

9. The **Judicial Authority** in Israel, and in particular the **Supreme Court,** plays a significant role in protecting human rights in Israel, as well as in the development of the law. This is done primarily by performing judicial review of all of the government authorities' activities. The Supreme Court constitutes a most significant player within the Israeli legal system, and when acting in its role as the High Court of Justice, serves also as a constitutional court. Within this framework, it is authorized to disqualify laws that contradict the Basic Law: Human Dignity and Liberty. Further, the Supreme Court plays a unique role, acting as an administrative and constitutional court, hearing petitions against the State as a first instance court rather than an appellant court. Additionally we shall note that the Supreme Court serves also as the highest appellate court for civil and criminal law, acting in its role as the Court of Appeals.

   As mentioned before, we would like to emphasize that precedents and interpretation of case law play a central role in the Israeli legal system. The ruling of the Court serves as a binding legal source under Israeli law. The implication of this is that the rulings of the Courts develop the law and complete the law, thus serving a significant role in protecting human rights, including the constitutional right to privacy.

10. An additional unique institution is the **Attorney General.** The Attorney General holds the most senior legal position within the executive authority, and although he is appointed by the government, based on a recommendation of a public professional committee, the Attorney General is an independent civil servant, free of any political affiliation. In addition to his roles as the head of prosecution and as the official representative on behalf of the State of Israel in any judicial proceedings, the Attorney General provides guidance to the government and its entities in all legal issues concerning the actions of ministers, ministries and government employees. The Attorney General holds a unique position since his interpretation of the law binds the government.. The Attorney General directs the Legal Counsel and Legislative Affairs Department and is also the professional supervisor of all government ministries' legal advisors. The Legal Counsel and Legislative Affairs Department acts on his behalf in providing legal advice and guidance, as well as in providing interpretation of the existing law and its limitations concerning the ongoing operation of the government and its units, while at the same time shaping policies in accordance with the binding legal framework. In addition, the department assists the ministers on behalf of the Attorney General, in evaluation and formulation of legislation amendments initiated by ministers, in order to ensure compliance

with constitutional restrictions. In addition, the department advises the Minister of Justice, who is responsible for the Privacy Protection Law, in forming the policy in the field of privacy and promoting amendments to the Privacy Protection Law and regulations promulgated by the law.

It is interesting to note that beyond the cases in which the Attorney General acts as the official representative on behalf of the State of Israel in judicial proceedings, he is at times requested by the courts, mainly the Supreme Court, to present his position regarding complex legal issues of public importance, even in cases in which the State itself is not a party to the proceedings. Several examples for such cases will be described in chapter C.

In the fulfilment of the aforementioned functions of the Legal Counsel and Legislative Affairs Department, it has been significantly involved in implementation of principles of privacy and personal data protection in legislation, government decisions and positions of the Attorney General in legal proceedings, including all of those that will be mentioned hereinafter.

11. Based on the brief overview above, we shall now turn to reviewing the central updates of recent years in all concerning the protection of privacy and personal data regime in Israel, starting with a review of the central legislative updates.

B. Legislation Updates

12. Below we shall briefly review the central developments relating to primary legislation and secondary legislation - both legislation mainly concerning the protection of privacy and personal data as well as other legislation including implementation of privacy protection principles.

i. Legislation Regarding the Protection of Privacy and Personal Data

a) Privacy Protection Bill (Enforcement Powers)

13. As aforementioned, the Registrar of Databases is entrusted with the protection of privacy in databases, and complying with the relevant provisions under the law. The purpose of the bill

is to improve the supervision and enforcement capabilities and supervisory mechanisms of the Registrar, in order to enable him to cope in a more effective manner with the updated risks threatening the right to privacy and personal data. The bill proposes to extend 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 sanctions. The expansion of the "toolbox" available to the regulator by way of establishing an alternative mechanism of the criminal procedure – a mechanism of imposing an administrative monetary sanction for breach of some of the provisions under the law – will enable a quick, efficient and proportionate response to violations of the law. This sanction will be imposed in a gradual manner that is appropriate to the types of violations, their severity and the circumstances in which they were made.

The monetary sanctions are significant, the sum of which is based on a calculating formula set out in the bill as a function of the severity of the violation, the amount of data subjects and the sensitivity of the data, and in severe cases the sanction may amount to the sum of 3.2 million NIS.

14. It is additionally proposed within the proposed bill, to 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.

15. Regarding the routine supervision powers, it is proposed in the bill, *inter alia*, to add the authority to require identification as well as the authority to require a copy of computer matters that includes system data (Meta-data that does not include personal data) or personal data samples, which would be collected in the required scope solely for the purpose of exercising supervision, and would be deleted when it is no longer reasonably required for such purpose. It is further proposed, to give the Director the authority to conduct administrative inquiries in cases where there are reasonable grounds to assume that a violation of the provisions under the law have been committed, 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 the provisions listed within the proposed bill, while imposing an explicit duty of confidentiality with respect to data collected as part of exercising the aforementioned authority. Nevertheless, it

should be noted that even today the Registrar has the authority to conduct criminal investigations, as will be detailed in the chapter regarding ILITA.

16. In addition, it is proposed to set forth a unique arrangement with respect to the manner of applying the supervisory and inquiry powers to security entities. The need for formulating a special arrangement for these bodies derives from the fact that a significant part of their classified activities is regarding databases, and exposing these databases to external inspection can create a threat to national security. On the other hand, there is a special importance to the supervision and the enforcement of the law regarding these databases. Taking this into consideration and understand the unique challenges, an internal supervision model is proposed for security bodies. According to this model the supervision activities will be done by the 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 provisions of the law apply fully to security bodies and the chapter formulated will set forth the methods of supervision and enforcement under the guidance of the Director.

17. Finally, it is proposed to adapt the penal part under the law concerning databases to the arrangement detailed within the bill, and as part of such to set forth a few new offenses. Violations of the law of excessive severity will be defined as criminal offences and will be enforced appropriately.

18. Regarding the status of the promotion of the proposed bill, it should be noted that it had been submitted on behalf of the government to the 18th Knesset and had passed the first reading, and later the continuity law had been applied to it, and it had been submitted for the second time to the 19th Knesset. However, unfortunately, the preparation for the second and third reading was not promoted by the Constitution, Law and Justice Committee of the Knesset, during the short term of this Knesset. Currently the relevant parties at the Ministry of Justice are working in order to bring soon the bill once more to be approved by the Committee of Ministers for Legislation Matters, and subsequently significant efforts will be made for its promotion in an effective manner at the stage of preparation for the second and third readings at the Constitution Committee of the Knesset, and completing the legislative process.

b) Privacy Protection (Data Security) Regulations, 5777 – 2017

19. One of the most major developments in data protection in Israel in the past year has been the publication of the Privacy Protection (Data Security) Regulations, 5777- 2017 in May 2017. The regulations will come into effect in May 2018.

    The regulations apply to both private and public sectors and establish organizational mechanisms aimed at making data security part of the management routines of all organizations processing personal data.

20. 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 the stake holders that would be effected by the regulations.

    It is expected that the regulations will substantially improve the level of data security in Israel because at the same time they are both flexible, concrete and specific to a degree that offer organizations regulatory certainty and practical tools that are simple to implement. With the entry into force of the regulations in May 2018, we expect a new era in which the protection of privacy in Israel will be stronger than ever.

21. The regulations classify databases to 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 with accordance to 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.

    In specific circumstances, ILITA may instruct a database to implement additional obligations in order to strengthen the security level of its activities, or exempt a database from applying specific details of the obligations in the regulations. For example, ILITA may instruct low level risk databases to implement provisions that apply on medium risk databases, and when justified, ILITA may exempt medium risk databases from specific provisions.

22. Following is a list of mechanisms that are included in the regulations and are aimed to strengthen data security by creating awareness, accountability and working procedures.

Database Settings Document

23. The regulations require data controllers to produce a "Database Settings Document" that will include the details of the data collection, processing and usages and more specifically: types of data, trans-border data transfers, types of processing activities by data processors, main risks for data, means of mitigating the defined risks, contact details of the controller, processor and security officer.

    The data controller needs to review and update the document annually or even more frequently if needed (in cases where technological or data breaches incidents occur). The annual review is also meant to examine if the controller is not holding excessive data.

Security Officer

24. The Privacy Protection Law determines that a Security Officer (SO) must be assigned for public sector controllers, finance sector controllers, and other substantive processors. The regulations establish the position of the SOs in the organization, their duties and their resources, weather the SO has been assign due to legal obligation or voluntarily.

25. The SO reports to the controllers' manager or another senior manager. The SO produces a draft of the organizations' data protection policy, for the approval of the controller's authorized governing bodies. The SO produces an audit plan for the organizations compliance with the regulations; implements the plan and reports to the controller. The SO is not to fulfil additional roles if those may cause him to be in conflict of interests and therefore any additional roles of the SO will be clearly defined. The controller will allocate appropriate resources required for the fulfilment of the SO's duties.

"Data Protection Policies"

26. Controllers must keep documented data protection 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 way of handling mobile devices. For databases subject to medium and high security level also – 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.

27. The procedures will be reviewed annually and even more frequently if major changes have been made in the systems or in a case of new risks. The controller will determine who in the organization will have access to the procedure and to what part of the procedures, according to their roles in the organization.

28. The regulations require mapping the database's structure and systems with security significance. The controller will 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. The documentation will be accessible only to relevant authorized functions within the organization.

29. High levels of security require data controllers to conduct risk assessments and penetration tests every 18 months.

Physical Security

30. Systems will be kept in protected spaces in order to avoid unauthorized access. In the case of medium and high levels of security, controllers will keep records of every access to the location of the systems.

Human Resources

31. Access to data will be granted to employees only after they were found suitable to receive access and only after receiving proper training with regards to data protection and security. In cases of medium and high levels of security, employees will receive training periodically, and a least once every two years.

Access Authorizations

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

33. In cases of medium and high levels of security, access will be granted subject to physical means that are in the sole control of the employee, and the authentication means and their strength will 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 will be valid for no more than 6 months), automatic disconnection following inactivity, etc.

Access Control

34. 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.

    Control system will make notifications about attempts to make alterations or deactivations of its functions.

Security Incidents and Data Breach Notification

35. The regulations define severe data incident in high levels of security as unauthorized data usage or data infringement, and in medium risk processing as unauthorized data usage or data infringement in major fraction of the database.

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

36. Controllers are required to keep record of **every** security incidents, through an automatic mechanism if possible. Organizational Security procedures should include instructions with regards to addressing security incidents with accordance to the severity of the incident and

the sensitivity of the data. Such provisions will include, *inter alia* termination of access rights, notifying the controller and more.

37. In cases of medium risk processing the controller's management must conduct an annual discussion regarding the security incidents that occurred in the organization and will update the security procedures if necessary. In cases of high levels of security, the management discussions will take place every 3 months.

Additional Provisions

38. The regulations include provisions with regards to the caution 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 connecting those systems to the internet or taking appropriate means when connecting the systems to the Internet, encrypting data, relevant authorization and authentication means for remote access.

Outsourcing

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

Periodical Reviews

40. Medium and high levels of security require conducting periodical audits (every 2 years), both internal or external, in order to ensure compliance with the regulations. The audit will indicate if the security means comply with the regulations, identify inadequacies and will suggest measures to amend them.

c) Amendment of the Privacy Protection Regulations (Terms of Holding Data and its Maintenance and Procedures for Transfer of Data between Public Entities), 5746 - 1986

41. Chapter D of the Privacy Protection Law addresses, as aforementioned, the limitations on the transference of personal data by public entities. The main provision under the Chapter (Article 23b) prohibits public entities to transfer personal data, unless the data is released to the public in a manner that is duly authorized or in cases where the data subject had given his consent to it being provided in such a way. Notwithstanding this instruction, provision of personal data is allowed between public entities only according to the terms listed later in the chapter, including in cases where the provision of data had not been prohibited under legislation or professional ethics principles, as well as, generally, that the provision of the data is required for a cause within the framework of the authorizations or roles of the one providing the data or the one receiving it, or in the event where the public entity receiving the data is entitled to require such data under law of any other source.

42. Thus the provisions under the law set forth essential terms for the transference of personal data between public entities. In order to supplement the law, the regulations set forth a procedure for examining whether the terms are met. In short, this arrangement is based on the establishment of a committee for the transfer of data by the general manager of any public entity, the members of which shall include the legal advisor of the public entity or a representative on his behalf, as well as employees engaging in data management and its security. In accordance with the arrangement set forth under the regulations, the committee is required, *inter alia*, to discuss and pass a resolution regarding requests for providing personal data by such public entity, as well as approve requests on its behalf to be provided with personal data by another public entity. The regulations further include in their current version, *inter alia*, provisions concerning data security in the course of its transfer between public entities, the manner of treating excess data, and forms to be filled out by the entity requiring the data and the entity providing the data.

43. The method of examining requests for transfer of data by the committees at government ministries is regulated by binding guidelines given by the Deputy Attorney General. In the guidelines the Deputy Attorney General refers to the Basic Law: Human Dignity and

Liberty, and instructs that the committees should examine the requests also in light of the of proportionality and reasonableness tests, while giving special weight to the possibility of violation of privacy. So for instance the committee should consider the following questions: whether the request is suitable for implementation of the goal for which the data is required, and there is a logical connection between the request and the goal; whether the transfer of data as requested is the lesser means among the variety of possible means for implementing the goal; and is there a reasonable proportion between the goal and the violation of privacy in order to achieve such. All these should be considered, while assessing the measure of violation of privacy entailed in the transfer of data, taking into consideration the sensitivity of the data.

44. During 2016, the issue of transfer of data between government entities was examined by an inter-ministerial team based, *inter alia*, on a comparative review of the laws on this issue in other countries. Within the report of the team in July 2016, various components had been reviewed concerning the difficulties in sharing data between governmental entities, amongst which had been listed difficulties in the existing work process for sharing data. Further noted in the report were a number of principles which the team believes to be appropriate for inter-ministerial transfer of data, amongst which is the continued maintenance of the data in a compartmentalized manner and upon request, subject to access permissions. On this basis, the team had recommended, *inter alia*, that the supervision over the transfer of data between the entities should remain with the committees, and such shall act pursuant to the clear guidelines regarding the frequency of meetings of the committee and a clear timeline (Service Level Agreement) which would be established within relevant regulations, along with additional amendments designed to clarify the requirements for securing the data during its transfer between the entities. The team's recommendations had been embodied in Government Resolution 1933 dated 30.8.2016. It should be noted that this Government Resolution addresses additional issues, and includes balancing mechanisms and additional significant aspects concerning the protection of privacy and personal data, as shall be elaborated below in this document.

45. Based on the report of the team, a draft has been formulated for amending the regulations, including substantial standards that will guide the committees in exercising their consideration upon reviewing the requests, including explicitly referring to the proportionality tests. This, in order to clarify the law on this point, and embody within the

regulations a regulated and clear process of monitoring transfer of personal data between public entities, in a manner that will ensure to the extent possible prevention of transfers of data violating privacy that exceed that necessary, but will still enable transfer of data and effective activities by the public entities in the appropriate cases meeting the provisions under law.

Our assessment is that the regulations will be brought to be approved by the Knesset during the coming year.

d) Annulment of the Privacy Protection Regulations (Fees)

46. Finally, we shall note below an additional normative modification currently planned, which is of great significance for the public maintaining databases in Israel, as well as for the reinforcement of the monitoring and enforcement of the Registrar of Databases' activities - a move for canceling the fees currently imposed by the regulations for registration of a database.

    As part of a conceptual and organization change at ILITA, within which the Registrar of Databases is acting - a modification of which shall be detailed later in this document - it had been decided, *inter alia*, on revoking the duty of paying the fee currently imposed for registering databases. This change is planned in order to enable ILITA to shift human resources and budgets currently serving for handling fees' issues to supervision and enforcement activities. This was suggested after it was learnt that revoking the fees will not adversely affect ILITA's budget or its monitoring capabilities.

ii. Implementation of the Principles of Protection of Privacy and Personal Data under Other Legislation

47. As aforementioned, in addition to the provisions set forth under the Privacy Protection Law, which apply in general, Israeli Law also includes individual provisions concerning protection of privacy and personal data, embedded in various other legislation - usually in legislation that regulates governmental or economic activities that entail collection and processing of personal data. Such provisions are intended to minimize to the extent possible the privacy risks involved in the regulated activity, as well as concerning various aspects in

the stages in collecting and processing the data, including planning and designing the technological system that will serve the database, the allowed use of the collected data, access to the data, its maintenance, and finally the security and deletion of the data. We believe that such provisions implement the principle of Privacy by Design, both in its technological aspects regarding the design of data systems and securing the data, as well as in its essential aspects regarding minimizing the scope of the data, access to such and use of such to the imperative scope for achieving the essence of the arrangement. As mentioned before, the Attorney General guides the government so that bills are formulated in a way that is in accordance with the constitutional framework, including the protection of human rights. Therefore, the Legal Counsel and Legislative Affairs Department, that works directly under the Attorney General, works with the various government ministries to design new legislation, initiated by them, according to the Privacy by Design principle. Meaning, in early stages of the legislation process, the Legal Counsel and Legislative Affairs Department assists in shaping the bill taking into account protection of privacy and personal data protection considerations, and implementing them in legislation. . This forward thinking design ensures that at future stages of implementation of the law, privacy risks will be minimized, whether it refers to government, private or corporate activities regulated under law.

Below we shall briefly review a few examples of such individual arrangements over recent years.

a) Financial Legislation

48. **The Credit Data Law, 5776 - 2016** - a law that had been legislated lately and sets in law a comprehensive reform within the field of credit data in Israel, intended to go into affect towards late 2018. The arrangement under this law is based on the recommendations of a government committee instated for the examination of the issue of sharing credit data, which is needed for various public and economic purposes. The law sets forth a new system that will be established for the collection and sharing credit data, while protecting the privacy of the data subjects in accordance with the restrictions set forth under law, and limiting the purposes for which it is collected and used.

After reviewing the existing arrangement, the conclusions of the committee had indicated a link between this arrangement and the lack of competition within the centralized retail credit

market in Israel, and was of the view that collection of more complete credit data that indicates the probability of a person complying with repayment of his debts (combining positive and negative data) is expected to bring about, *inter alia*, increase of competition in the credit market, for expanding access to credit and minimizing the discrimination in this field. Regarding the identity of the entity that will collect the data, the team has recommended a mixed model: the data will be collected and maintained once in a governmental database established by the Bank of Israel, rather than its current collection by various private entities, whilst providing licensed private credit bureaus access to the government database and so creating a kind of "vessel" for transferring the data from the database to credit providers.

49. The new legal arrangement based on the conclusions of the committee thus involves expansion of the scope of data collected by default regarding a customer, however at the same time, it includes a most extensive protection of principles of protection of privacy and personal data, while delicately balancing its public goals and violation of the right to privacy, and thus minimizing any violation to the minimal imperative scope. First, the arrangement gives the data subject the possibility of objecting to the collection of his positive data, and should one object, the law sets forth that the data regarding that person that will be collected will be only the substantial negative data, which is less than the negative data that is normally collected by according to the existing law. Regarding the quality of the data collected by default, it should be noted that such is data focused on credit extended to a customer, or which a customer is entitled to borrow, and its repayment, rather than other economic data. As to the technological system that will serve the database, the law expressly states that such shall be designed and updated in order to minimize to the extent possible the risk of violating the customers' privacy. Further included under the law is a section unprecedented in its scope, which sets forth that a supervisor will be appointed at the Bank of Israel for the protection of privacy, as setting forth his roles in detail. The arrangement also includes detailed provisions in order to ensure the quality of data, the scope of access to it and the allowed purposes for use of the data, which are less extensive than the purposes for use of credit data allowed pursuant to the existing law; as well as provisions concerning data security, the period of keeping it and its deletion. In addition, the arrangement explicitly distinguishes between identified data and unidentified data, whilst allowing provision of access to identified data only given the consent of the data subject, and includes an explicit normative prohibition on any attempt to identify the customers

based on unidentified data. Finally, the arrangement includes an encompassing framework of supervising, administrative inquiry and enforcement powers, which may be exercised also with respect to external entities that obtained data originated at the database, in order to minimize to the extent possible the concern of violation of the provisions according to law, further distribution of the data and violation of the privacy of the data subjects.

50. **The Supervision of Financial Services Law (Regulated Financial Services), 5776 - 2016** - this new law includes a chapter concerning services of financial costs comparison. The provisions under this chapter require a financial entity to enable the customer or a service provider on his behalf to view on-line financial data regarding the customer held by the financial entity. Along with this duty, which constitutes a concrete expression of the right to review data which is already preserved in the Privacy Protection Law at present, the arrangement under this law includes a system of balances and restrictions intended to cope with the risks for the customer's privacy, arising from the sensitivity of the data, on-line access to it, and its disclosure to a third party - the service provider. Within this framework, the law sets forth terms regarding the access to the data and its security, a general restriction on the manner of engaging with the financial data received pursuant to the provisions under the law, and a closed list of the individual purposes for which the services provider is allowed to make use of such data. In addition, the law also includes a section granting wide authorization for introducing regulations by the Minister of Finance, after receiving the consent of the Minister of Justice, and consulting with additional government entities, intended to ensure the rights of customers in a variety of aspects, emphasizing protection of the customer's privacy and securing the data.

    Currently government work is carried out for the formulation of the regulations, and after the regulations are instituted will the arrangement under law take effect.

b) Tax Legislation

51. **The Income Tax Ordinance [New Version]** - under the 2013 amendment of the Income Tax Ordinance, a temporary order has been installed, imposing on money changers a duty of reporting to the Tax Authorities any financial actions they had carried out in the sum of NIS 50,000 and over, including identification details of the one benefiting from the action. This order has been installed due to the widespread phenomenon of money laundering and tax

offences related to money changers, as an interim order until a new regulator is established under the Financial Service Providers Law (Regulated Financial Services).

52. Along with this temporary order, a list of detailed restrictions has been set forth, including the duty of maintaining the data in a database separated from any other information for a period of three years, after which the data is to be deleted; a duty to design the database and the layout of collecting and intake of the reports in a manner that will minimize the risk of violating the privacy of the data subjects and consulting with the Registrar of Databases; authorizing people allowed access to the database; and setting forth detailed provisions concerning the entities entitled to obtain data from the database, the terms for providing such and the purposes of their provision. The arrangement also includes an individual confidentiality duty, as well as a section regarding authorization for enacting regulations in respect of the details of the arrangement, including defining the data held by the Tax Authority, which may be cross-referenced with data collected in the database.

c) Equality Legislation

53. The **Equal Rights for People with Disabilities Law, 5758 - 1998** - the 2015 amendment of the law had forth a concrete goal for proper representation of employees with significant disabilities among the employees of a large public employer, standing at 5% of the employees. In order to test compliance with the representation goal, an arrangement was set forth under the law, according to which several public entities will be required to annually provide the National Insurance Institute with data regarding people with disabilities that meet the provisions under the law and the details of employees, in order to cross-reference the data and examine the measure of compliance of large public employers with the representation goal. Regarding the data collected according to this provision, the law dictates that it should be saved in a designated database separated from any other information, and that the Minister in charge shall enact regulations regarding its delivery, processing, maintenance, securing and deletion, all for the purpose of protection of privacy.

d) Traffic Legislation - Photographing within Public Domain

54. **The Traffic Regulations (Operating Cameras by a Local Authority for Documenting Illegal Use of a Public Transportation Lane), 5777 - 2016** - a 2015 amendment to the Traffic Ordinance [New Version] has authorized local authorities to enforce traffic offenses of illegally driving in a public transportation lane by photographing the public transportation lane and giving fines to people documented while committing an offense. The arrangement under the Ordinance has included restrictions concerning protection of the privacy of the passengers and passers-by, including the duty of maintaining the photographs in a manner that would not enable the identification of passers-by, maintaining the data while reducing data security risks, and minimizing the connection of the database keeping the photographs to any other database beyond what is required for implementing the arrangement. In addition, the Minister of Justice shall enact detailed regulations for implementing the arrangement.

    Indeed, the regulations have been enacted, including detailed terms in respect of positioning cameras and their operation, notifying the public of photographing, maintaining the photographs in the camera and in the central database at the local authority, as well as provisions regarding data security. The regulations further include the definition of the people in senior positions within the local authorities, who will be responsible for the implementation of the provisions under the regulations and examine compliance with their provisions, as well as a routine process of an annual periodic approval of the compliance of operating the cameras at the local authority with the provisions under the regulations.

e) Political Parties Legislation

55. **The Political Parties Regulations (Update and Verification of Identifying data of Political Parties' Members out of the Population Registry in Primaries), 5775 - 2014** - as part of the 2012 amendment of the Political Parties Law, 5752-1992, an arrangement had been set forth for updating and verifying identifying data regarding party members prior to conducting primaries, in order to allow for contacting party members and conducting the primaries. Pursuant to the provisions under the law, a party making contact with a request for updating and verifying data concerning its members is required to confirm that no other use of the data it shall obtain will be made and it shall not pass on such data to another, other than for the purposes listed above. The Minister of the Interior, after receiving the consent of the Minister of Justice, shall enact regulations as to the manner of updating and verification

procedure, provided that it is ensured that no data on the identity of the party members will be disclosed to any entity that is not the party.

In 2014 the regulations in question were enacted, setting forth a detailed arrangement for conducting cross-reference between the party members' data file and the Population Registry file. In order to ensure that no data regarding the identity of party members will be disclosed, and that no data would leak out of the Population Registry, the regulations set forth that the cross-reference will be conducted in a computerized manner, on a designated computer at the Population Registry that is not connected to the Population Registry's database and does not enable keeping data. The regulations also set forth additional provisions concerning the terms for conducting cross-reference, and deletion of all of the data from the designated computer upon its conclusion.

f) The Inclusion of Biometric Methods of Identification and Biometric Identification Data in Identification Documents and Databases (Amendment and Transitional Provisions) Law, 5777-2017:

56. 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 unprecedented 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 outstanding considerations of State security and public security together with the protection of privacy. Therefore the Law was enacted after holding a prolonged and substantial professional process in the Government and the *Knesset.* Moreover the law was constructed in such a way that it was applied gradually, setting forth a trial period ("pilot") 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 the other alternatives to the database. Likewise, a multi-disciplinary **advisory committee** was formed whose function was to supervise the conduct during the trial period and examine its results

After the examination process detailed above had been completed in all matters pertaining to the question of the necessity of the database and the scale of the data to be kept there, 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, so that

the arrangement would be proportionate and ensure the maximum protection for the right to privacy, arrangements were prescribed in the law in order to ensure the protection of the residents' privacy and data security. Thus, for example, it was prescribed that the biometric database would contain only photographs of facial features and that the inclusion of two fingerprints in the database was conditional upon the resident's expressed written consent**.** It should also be noted that the voluntary arrangement relating to two fingerprints of the residents who had agreed thereto was prescribed as a **transitional provision**, namely as a temporary arrangement only, valid for 5 years, with the possibility of reducing this period of time. During the course of this period a periodical examination would be conducted that would examine whether technological means exist that might provide an appropriate solution for the purposes of the law, instead of including fingerprints in the database.

Likewise it should be noted that pursuant to the provisions prescribed in the law and the regulations enacted thereunder, extremely stringent data security arrangements were prescribed, including encrypting the data kept in the database, determining control and monitoring mechanism, restricting access 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 is to prevent any leak of data and ensure the protection of the right to privacy.

g) Preventing Sexual Harassment - Publishing Sexual Content

57. As part of this brief overview of the development of privacy protection laws in Israel in recent years, we would like to note a legislation amendment that deviates in essence from the arrangements noted above, and does not concern regulation of governmental activities, but rather protection of privacy within the private sector, in light of the spreading social phenomenon of distributing videos and photos of a sexual nature on social networks, as detailed below.

58. **The Prevention of Sexual Harassment Law 5758-1998** - as part of a 2014 amendment (which is commonly referred to as “the Video Law”), the definition of sexual harassment under section 3 of the law was changed in order to include the behavior 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, and his consent had not been given

for its release". Along with this definition, the law also added protection for such a publication in the context of a criminal or civil law proceeding, similar to the protection fixed in the Privacy Protection Law, which due to the extensive applicability of the law, intended to balance between protecting the victim and other interests and rights, particularly the right to freedom of speech.

It should be noted that the behavior defined as part of the amendment to the Prevention of Sexual Harassment Law, was already at the time of legislating the amendment to the law (and still to this day), as a violation of privacy pursuant to the Privacy Protection Law (Section 2(4) of the law concerning "releasing to the public a photo of a person under circumstances where such release may degrade or humiliate him"). Even so, defining distribution of photos - as such is focused on the sexuality of a person - as sexual harassment under this law, had been mainly intended to characterize such behavior as being prohibited because of being "sexual harassment", including its public implications, as well as in order to grant those hurt by such an additional channel of suitable remedies. Therefore, the amendment to the law grants additional protection to the right to privacy in the important context of sexual harassment.

C. Case Law Updates

i. Judicial Review of Legislative and Administrative Powers

59. As we shall demonstrate below, in a series of judgments from recent years, we can see the supervision on the part of the courts over the various government authorities, in all matters pertaining to personal data. These judgments embody the judicial authority being a significant and effective regulatory authority in the Israeli legal system, in a manner that ensures the protection of basic rights, including the right to privacy. As mentioned before, the Court is also competent to disqualify *Knesset* laws that affect the right to privacy in cases where they don't adhere to the "violation of rights" article in the Basic Law: Hunan Dignity and Liberty.

60. Thus, for example, in the case of **The Association for Civil Rights in Israel**[4] the High Court of Justice examined the legality of the arrangements made within the framework of the Criminal Procedure Law (Powers of Enforcement-Communications Data) that allows the investigative authorities in Israel to take possession of communications data from the communications companies. It should be noted that the receipt of this data does not include receiving the content of the messages sent. In the judgment, the Court focused upon the need for a balance between the constitutional right to privacy and the fear of excess government interference in the life of the individual, and the provision of tools that will provide the investigative authorities with effective tools for the assurance of security and the public order. Within the framework of its judgment the Court emphasized that in view of the potential for significant damage to the residents' right to privacy, complex arrangements should be determined that give appropriate weight to the range of interests on the agenda. 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 interpretation of the arrangements prescribed in the 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 prescribed that paying attention to the necessity to protect the right to privacy, this arrangement should be interpreted as allowing the authorities to apply to the court with a request to receive an order, solely for the purpose of exposing concrete offenses or offenders, and the arrangement should not be interpreted as allowing the receipt of an order for the purposes of general intelligence activity in relation to offenses or offenders. This is despite the language of the law that *prima facie* allows this 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 and over-precision 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 hold ongoing scrutiny over the matter of the scale of the use made by the authorities by virtue of the law. Finally, the Court approved the law, but emphasized that the powers given in the law should be given narrow interpretation and only to the extent necessary.

[4] *Bagatz* 3809/08 **The Association for Civil Rights in Israel v. the Israel Police** (published in *Nevo*, 28.5.2012)

61. Another judgment that illustrates the scrutiny exercised by the Court over the government authorities in all matters pertaining to personal data is the judgment of the **Regional Labor Tribunal** that deals with the activity of an apprentice investigator at the National Insurance Institute, who conducted an undercover investigation in the plaintiff's home. During the course of the undercover investigation the plaintiff was filmed without her knowledge, while giving the plaintiff a misrepresentation of the situation and the investigator hid his identity[5]. The filming was made for the purpose of investigating the Plaintiff's eligibility for an allowance from the National Insurance Institute.

    In the judgment the Tribunal held that the use of deception for the purpose of an investigation constitutes an invasion of privacy, and this invasion is reinforced when the investigation is conducted in the insured's own home. In this context the Tribunal emphasized the importance of the right to privacy as allowing a person's control over the course of his life and the data about him. The Tribunal further held that under the circumstances of the case, the investigation made did not meet any of the constitutional tests. The Tribunal held that it would have been possible to conduct the investigation outside the plaintiff's home, without the necessity of such a severe invasion of her privacy and held that the invasion was not proportional under the circumstances of the case and therefore inadmissible. An important determination in this context is that the investigator's entering into the plaintiff's home, while making a misrepresentation, constitutes a severe infringement of the right to privacy.

    In this context 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.[6]

    In view of the severity of the infringement of privacy that the Tribunal saw in such instance of an act of a governmental authority using impersonation, the Tribunal disallowed the admissibility of the photographs obtained by the National Insurance Institute.[7]

62. Another judgment that compelled the public authority to act in accordance with the basic principles in the field of the protection of privacy concerned several legal proceedings that were conducted in the District Court, in which a national cellular car parking arrangement

[5] N.I. (Tel Aviv Regional) 59213-01-12 ***Plonit* v. the National Insurance Institute** (published in *Nevo*, 4.3.2014).
[6] Paragraphs 13-16.
[7] Paragraphs 17-18.

operated on behalf of the Coalition of Local Authorities was discussed.[8] The operation of the car parking arrangement was made via outsourcing.

In the opinion submitted to the Court by the Attorney General, the Attorney General emphasized several central principles enshrined in the Privacy Protection Law that should be applied to the circumstances of the case – the principle of consent, informing, and the principle of "purpose limitation" (namely, restricting the use of the data solely for the purpose for which it was delivered). The Attorney General explained that pursuant to the provisions of Section 11 of the Privacy Protection Law, the collection of data about a person for a database is conditional upon the person being informed in advance whether he is under a duty to deliver the data or where the delivery is dependent upon his own will and consent; what is the purpose for which the data is requested; and to which parties the data will be delivered.

The entirety of these principles, that are expressed in the Privacy Protection Law, is consistent with the concept whereby a person's control over the data about him – his control over the very fact of the delivery of the data, the parties who will hold the data and the purposes of the use thereof – constitute one of the main foundations of the right to privacy in Israeli law.

Furthermore, the Attorney General explained in his opinion that wherever outsourcing involves the processing of personal data, it should be ascertained that the personal data is collected with the consent of the data subject to the entirety of the aspects required, while informing the data subject in advance, as required pursuant to the statutory provisions. Similarly, the Attorney General emphasized that paying attention to the significance and importance of the principle of the consent of the data subject, clear mechanisms for receiving informed consent should be determined, and the assurance of informing the individual that it is a matter of a database owned by a body that is authorized to fulfill a public function by law, when the collection of the data is carried out by the concessionaire within the framework of outsourcing on behalf of the aforesaid body.

Finally, in his position the Attorney General related to the aspects concerning the responsibility of the database owner and the holder of the database. In this context the Attorney General noted that as transpiring from the provisions of the Privacy Protection Law, even during use of outsourcing services, the obligations and liabilities imposed by law upon a database owner continue to apply to it, as if it was performing the activity by itself.

[8] Originating Motion 60239-03-15 **The Local Government Economic Services Co. Ltd. v. Milgam Cellular Car Parking Ltd. et al** (published in *Nevo*, 27.10.15).

Furthermore, various obligations pursuant to the Privacy Protection Law apply to the holder of the database, in the same way as they apply to the owner, including with regard to data security, determining rules of day to day operation etc. These aspects are also emphasized in the directive of the Database Registrar regarding the use of outsourcing for the processing of personal data that expresses its interpretation of the statutory provisions in this matter.

The Court adopted the principles in the opinion of the Attorney General in its judgment.

ii. **Protection of Privacy Balanced against Freedom of Information**

63. **The Freedom of Information Law, 5758-1998** (hereinafter – the Freedom of Information Law) enshrines the right of every Israeli citizen or resident to receive information from a public authority. Nevertheless, the Law makes this right subject to reservations and outlines the balance between it and various rights and interests. In the context of the right to privacy, the Freedom of Information Law in Section 9(a)(3) forbids a public authority to deliver "information of which disclosure constitutes an infringement of privacy, within the meaning thereof in the Privacy Protection Law, unless the disclosure is permitted by law". It should also be noted that the Freedom of Information Law prescribes provisions designed to protect a third party that is liable to be hurt as a result of the delivery of the information. *Inter alia*, the Law regulates the right of a third party to express its objection to the delivery of the information (Section 13), and its right to have its arguments in this context heard before the Court (Section 17(c)).

    As shall be demonstrated below, a study of court decisions given during recent years by the Supreme Court that deal with the balance between the right to privacy against the right to freedom of information and the right of the public to know, shows that between these two rights, the right to privacy has the upper hand.

64. Thus, for example, in the **Shenrom** case[9] there was a request to receive details about the owner of properties by a private company. The Supreme Court held that the "innocent" information *prima facie* of which the receipt was requested (the size and classification of the properties, plus data regarding the names and addresses of the people occupying the properties) would allow conclusions to be drawn concerning the type of use of the property

[9] ADMINISTRATIVE PETITION APPEAL 1386/07 **the Municipality of Hadera v. Shenrom** (published in *Nevo*, 19.6.12).

and thus deriving conclusions about the owners. In the words of the Court, this possibility of obtaining this data unlawfully penetrates the cloak of privacy of the occupier of the property, and it should be prevented.[10] Therefore, despite the claim that the information requested would reinforce the supervision of the Municipality's activity, the Court held that the delivery of the information would only be with regard to the owners of the properties who on their own initiative had expressed their explicit consent thereto.

The importance of the judgment is in the emphasis of the extreme importance in the protection of the constitutional right to privacy within the framework of the handling of the freedom of information requests. The judgment explains that the public authority must act with caution and precision when it considers delivering information of which disclosure is liable to infringe a person's privacy. This and more, according to the judgment, where an authority is considering delivering information in the matter of a third party that will infringe upon the right to privacy, it shall be assumed that the data subject objects to the delivery of the information, unless he has expressed his explicit consent thereto. This consent shall be assumed following a request in the opt-in mechanism ordered by the Court. The Court notes that when taking into consideration the constitutional protection awarded to the right to privacy, one should deviate from the "opt-out" mechanism that is the routine mechanism operated in the request of the public authority pursuant to the Freedom of Information Law (see Section 13 of the Freedom of Information Law). Within this framework, a unique mechanism has been determined for the purpose of protection of the right to privacy, so that in order to object to the delivery of the information, the owners of the properties are not required to do anything, and their silence shall be deemed to be objection to the delivery of the information.

65. In a later judgment of the Supreme Court, in the **Rozenberg** case[11], the Court repeated the rule in the **Shenrom** case while holding that when it is a matter of the delivery of "private" information, active consent on the part of the data subject is required for this purpose[12]. Likewise, in its judgment the Court emphasized the importance of the right to privacy as a constitutional right, and noted that in the balance between the right to privacy and the right to freedom of information – the legislator elected to give priority to the right to privacy.

[10] *ibid.*, Paragraph 11.
[11] ADMINISTRATIVE PETITION APPEAL **Rozenberg v. the Enforcement and Collection Authority** (published in ARS), 11.6.14)
[12] *ibid.*, Paragraph 20.

66. Finally, it should be noted that even in cases where within the framework of the conflict between freedom of information and the right to privacy, when the Court was of the opinion that considerable public importance is attached to the delivery of the information, it was held that for the purpose of the protection of the constitutional right to privacy, the delivery of the information would only be in the future, and after it had been explained to the persons concerned that the relevant information in their matter was liable to be exposed[13].

iii. The Registrar's Powers

67. The powers of the Registrar of Databases were defined in the Privacy Protection Law and they comprise of, *inter alia*, the power of supervision over the fulfillment of the provisions of the law, as shall be detailed in chapter D.

    The court provided broad interpretation of the Registrar's power of supervision, so that it is not limited only to the express sanctions prescribed in the law. This interpretation reinforces the protection of the right to privacy.

68. Thus for example, in the **I.D.I.** case, a petition was heard against the Registrar's decision determining that the use of the **I.D.I.** insurance company of the particulars of an attachment order, that was designed to seize the debtor's funds in its possession, for another purpose – appraising the possibility of insuring the person against whom the attachment order was issued- infringes upon the provisions of the Privacy Protection Law and the Registrar's directives, and accordingly is unlawful. The Court held that the power of the Registrar of Databases was broad and not limited only to the sanctions set forth explicitly in the law.[14] The Registrar is entitled to exercise his discretion in an individual case or according to a general policy determined in accordance with the professional interpretation of the Privacy

[13] Thus, for example, it was held in the matter of the exposure of the names of assessees who had signed ransom arrangements with the Taxes Authority, and also in the matter of the exposure of the particulars of candidates for the position of director in government companies, who had been disqualified by the appointments Committee [see, respectively, ADMINISTRATIVE PETITION APPEAL 398/07 **the Movement for Freedom of Information v. the State of Israel – the Taxes Authority**, *Piskei Din* 63(1) 284; ADMINISTRATIVE PETITION APPEAL 9341/05 **the Movement for Freedom of Information v. the Government Companies Authority**, [published in *Nevo*] (19.5.2009).

[14] Administrative Petition (Tel Aviv District) 24867-02-11 **I.D.I. Insurance Company Ltd. v. Ministry of Justice the Israeli Law, Information and Technology Authority – the Registrar of Databases**, in Section 3 of the judgment of Judge Agmon-Gonen (published in *Nevo*, 20.7.2012).

Protection Law. Thus, tit is within the authority of the Registrar to give working directives to the owners, holders or managers of the databases.[15]

The importance of the judgment is that it emphasizes the importance in the protection of the Registrar's discretion, within the framework of his interpretation of the law. The judgment explains that whenever the data is stored in databases, there exists an additional hurdle of the protection of the private data of the data subjects, by means of a broad interpretation of the powers of the Registrar of Databases. It should be noted that an appeal that was filed against this judgment was struck down, when the Supreme Court adopted the decision of the District Court and the reasoning on which the judgment was based.[16]

iv. Protection of the Right to Privacy in the Virtual Space

69. As will be presented below, the courts in Israel are well aware of the need to safeguard the right of privacy in the virtual sphere, taking into account the significant challenges that threaten this right especially given technological advances and more specifically the use of the personal computer.

70. In the **Ezra** case, the Court discussed a petition for leave for criminal appeal filed by the State after the acquittal of the accused of the offenses of penetration into computer material. In an *obiter,* the Court referred to the significant challenges facing it in view of the technological changing times in general, and that contained in the use of the computer in particular, that endanger the privacy of the data subjects and that necessitate a renewed examination of the existing legal protection.[17] Based on this, the court used the principal of the consent – a basic principle in the laws of privacy – in its interpretation of the "unlawful" circumstance[18] that constitutes part of the definition of the offense "penetration into computer material".[19] Thus, the Court clarified that penetration into a computer constitutes,

[15] *ibid*., in Paragraph 3 of the judgment of Judge Agmon-Gonen.
[16] ADMINISTRATIVE PETITION APPEAL 7043/12 **I.D.I. Insurance Company Ltd. v. Ministry of Justice the Israeli Law, Information and Technology Authority – the Registrar of Databases** (published in *Nevo,* 15.01.14).
[17] Leave for Criminal Appeal 8464/14 **the State of Israel v. Nir Ezra**, in Paragraph I of the judgment of Justice Rubinstein (published in *Nevo*, 15.12.2015).

[18] *ibid*., in Paragraph R of the judgment of Justice Rubinstein; 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).
[19] Section 4 of the Computers Law, 5755-1995.

inherently, an infringement of the privacy of the owner of the computer. This and more, the judgment illustrates that the necessity of the protection of the right to privacy in the virtual sphere is not different from that required in the physical sphere, and that penetration into computer material, without obtaining consent, and bypassing technological obstacles (such as a password) – is a particularly serious offense.[20]

71. The Court's position in the **Dvir** case appears similar to the ruling in the **Ezra** case. In this matter, the Court heard an appeal against the decision of the District Court to convict the accused on the charge of stealing mobile telephones, and the severity of his punishment. In its judgment the Court related to the power of the infringement of privacy that is inherent in the theft of a mobile telephone, and emphasized that the very fact of the theft of a mobile telephone constitutes penetration into the person's most private area, and hence is "a damage multiplier" and an aggravating circumstance in the offense.[21] This is because the mobile telephone constitutes an entrance portal into the entire range of the persons' digital assets and the penetration thereto constitutes an infringement at the heart of the right to privacy.[22]

72. The protection of the right to privacy in the virtual sphere is expressed further in a debate on the legal status of the e-mail accounts. Thus, for example, in the **Reihani** case, the petition of the petitioner, who acted as the special manager of the respondent's assets in bankruptcy proceedings, to receive a copy or access to the debtor's email account was dismissed, despite his suspicions that the email account was being used for running businesses and receiving concealed income in an illegal manner.

    It should be noted that statutory provisions exist, in the laws pertaining to bankruptcy, which regulate the possibility of the Court ordering, under specified conditions and according to conditions and restrictions prescribed by law, that items of mail addressed to the debtor shall be sent to the Receiver. Nevertheless, in its judgment, the Court emphasized the unique characteristics of the email account and the significant differences regarding the infringement of privacy between reviewing actual mail and reviewing the content of an email account. In the opinion of the Court, allowing access to the debtor's email account constitutes a greater infringement of the right to privacy.[23] In the judgment, the Court gave

[20] The Ezra case, above footnote 10, in Paragraph V of the words of Justice Rubinstein.
[21] Criminal Appeal 8627/14 **Dvir v. the State of Israel**, Paragraph 7 of the judgment of Justice Amit (2015).
[22] *ibid*.
[23] *ibid*., in Paragraph 24 of the judgment of Justice Solberg.

priority to the right to privacy over the purposes of the laws of bankruptcy, when in its opinion the email account constitutes a personal space into which no person other than its owner has permission to penetrate. 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 the implementation thereof to the letter of the law might to lead to an infringement of privacy. The judgment clarifies that in view of the changing times and technical advancement, the Court must adapt the various terms so that they will conform to the functional purposes of the law, and this interpretation must be in accordance with and to the extent of the effect on the privacy.[24]

73. The status of the email account in the context of the constitutional right of the data subject to privacy was also debated in the **Zinger** case.[25] In this case, the Court held that copying the contents of private-personal email correspondence, which had been left on a person's computer screen by another person, constitutes an infringement of privacy, pursuant to Section 2(5) of the Privacy Protection Law. This ruling testifies as to the Court's position concerning the importance of the right to privacy in the virtual space, in noting that the virtual sphere contains unprecedented sensitive data, that leaving the email addresses open on another person's computer screen does not mean that there is permission to view them but rather the possibility the person forgot to close his email account.[26] This ruling emphasizes the importance that the Court attaches to the necessity of ensuring that the consent to the infringement is "informed" consent.

74. The status of the right to privacy in the virtual sphere was also debated in the **Savir** case[27], when Google was required to remove an harmful publication, after a third party that published it refused to cooperate and remove it. As part of the Court's ruling it was held that whenever the search results are absolutely erroneous, the right to privacy prevails over the rights embodied in the publication appearing on the Internet, so that the search engine must

[24] 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". *Ibid.*, in Paragraphs 11-14 of the judgment of Justice Solberg.
[25] Civil Leave to Appeal 2552/16 **Yehuda Zinger v. Yahav Hamias Technologies Company (1990) Ltd.** (published in *Nevo*, 10.05.2016).
[26] *ibid*., in Paragraph 43.
[27] Civil Appeal (Tel Aviv District) 44711-11-14 **Ami Savir Adv. v. Shaul Bar No**, in Paragraph 7 of the judgment of Judge Cohen (published in *Nevo*, 22.06.2015).

remove the harmful publication, even if the third party refuses to remove the publication it published.[28]

75. An additional issue that was brought before the Supreme Court and raises complex questions in the interplay between law and technology is the judgment in the matter of **Hashavim**[29]. In this matter the Court was requested to address the question of whether it should be allowed to prohibit a commercial company from indexing 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.

    Within the judgment, 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 before the right to privacy, a path is to be found that would enable enjoying the fruits of technology, whilst minimizing violation of the individual's rights[30]. 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 in a manner that would provide a suitable and proper solution for this issue and that, for the time being, it may not be allowed to obligate the publishing companies to prevent the indexing of judgments. The judgment also mentioned the work of the public committee headed by the Honorable Former Justice Englerad. This committee had been established in order to examine all of the questions related to stating identifying 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, we shall note that recently, in August 2015, the Minister of Justice established a public committee headed by former Supreme Court Justice Arbel, intended for formulating measures of protection against hurtful activities and publications within the cybernetic sphere.

v. <u>Protection of the Right to Privacy in Private Law</u>

[28] 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 information upon the existence of a judicial order.
[29] HCJ 5870/14 **Hashavim H.P.S Financial Information Ltd. v. the Judicial Authority** (published in ARASH. 12.11.15) (hereinafter the "**Judgment**" or the "**Matter of Hashavim**").
[30] There, Clause 31 of Justice Rubinstein's judgment

76. The protection of the right to privacy applies not only within the confines of public law. In our view, the roots of the right to privacy are planted in public constitutional law, but the branches of the right extend over the private sphere, in creating a comprehensive protection of this right within the confines of private law, *mutatis mutandis*.

    Below we shall survey several judgments that were given during recent years, which shall illustrate the scale of the protection enjoyed by the right to privacy in the context of private law.

77. Thus, for example, in the **Gottesman** case, a client refused to give his consent to publications and photographs of his home by the architect who had planned the house. The judgment extends the scale of the protection of the right to privacy, *inter alia*, by means of the determination that in order to prove that there had been an infringement of a person's private life there was no requirement for setting a high threshold of intimacy, and that the publication of a imaging of a person's home constitutes an infringement of the person's private life.[31] The Court emphasized in its judgment that "a person's home is his castle", and therefore a high level of protection of the right to privacy must be provided in this context. Likewise, the judgment contains determinations concerning the question of the identification of the data subject, and it held that this should be interpreted broadly with a substantive examination, instead of a technical examination. Accordingly, the Court held that it was not necessary to publish a person's name in order to enable his identification, but the data would be deemed to be identifiable as long as any party had the ability to perform reverse engineering and attribute the data to a particular person.[32] Beyond this, the judgment relates to the relation between the right to privacy and the right to freedom of expression, and holds that the client's right to privacy prevails over the architect's creative freedom of expression, so that there it was not legal to publish the images of the client's home in mass circulation.[33]

78. The status of the right to privacy in the private sphere is also expressed in the **I.D.I** case surveyed above.[34] As may be recalled, in this case, the court held that the Registrar had been correct in his decision when he prevented the **I.D.I.** Company from using the particulars of an attachment order that it had received by virtue of its being the holder of the debtor's assets, for the purpose of appraising the possibility of the insurance of the person against whom the attachment order had been issued in his matter. Thus, the Court in its

[31] Civil Appeal 1697/11
[32] *ibid.*, in Paragraphs 21-22 of the judgment of Justice Fogelman.
[33] *ibid.*, in Paragraph 29 of the judgment of Justice Fogelman.
[34] See the part "the Registrar's Powers" in this document.

judgment gave expression to the basic principle in the laws of privacy in Israel – "the purpose limitation", in the private sphere.[35] According to this principle, data collected for one purpose may not be used for another purpose.[36]The judgment emphasizes in this context the importance of the principle that a person has control over data relating to him, and that right extends to the transference of the data to others.

79. The status of the right to privacy in the private sphere, and the question of the balanced between this right and freedom of expression, were debated at length in the ***Ploni*** case. The Supreme Court gave a ruling on the question of the publication of an autobiographical book written by the Appellant and that describes the intimate relationship between the Respondent and the Appellant.

    In the judgment, the Supreme Court again noted 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 that every person is entitled to as a person, as a value in of itself".[37]

    This judgment is significant for the understanding of the importance of the right to privacy and balance between privacy and the freedom of expression. In the judgment the Court related to the intensity of the significant infringement of the right to privacy under the circumstances of the case, and the importance attached to the protection of this right within the framework of an intimate relationship. Under the circumstances of the case, the Court held 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 and greatly affect the heart of the Respondent's right to privacy.

    Beyond this, this judgment has importance with regard to the consent of the data subject to an infringement of his privacy and the question whether it is possible to withdraw this consent. The court held in this context that a person's consent to the infringement of his right for privacy is not final. In the Court's opinion, the constitutional status of the right to privacy, and the strength of the infringement thereof under certain circumstances, may

[35] The **I.D.I.** case, above footnote 6, in Paragraph 8 of the judgment of Judge Agmon-Gonen.
[36] This principle is also entrenched in the Protection of Privacy Law, in Section 2(9).
[37] Civil Appeal 8954/11 ***Ploni* v. *Plonit***, in Paragraph 67 (published in *Nevo*, 24.04.2014).

justify in some instances the failure to grant the relief of enforcement in cases of where the consent is withdrawn.[38]

After an examination of all the relevant considerations in the circumstances of the case, the Court held that the right to privacy had the upper hand, and that the publication of the book describing the relationship between the Respondent and the Appellant should be forbidden.

This comprehensive and fundamental judgment drafts the limit of the right to privacy in private law when balanced against freedom of expression, in the context of a trusted relationship between partners. These limits, as demonstrated above in several judgments, are on a broad scale, as befitting the normative status of the right to privacy. Accordingly, the courts in Israel award this right broad protection within the framework of an exam of the conflict between it and other rights.

vi. Protection of the Right to Privacy in Cases of Power Disparities

80. In general, in cases in which there is an ingrained imbalance in power between two parties, the law will often gives extra protection to the weaker party. In the context of the right to privacy, this will often mean that the Court will be more stringent in following the letter of law and will interpret the law in a way that protects the weaker party.

a) Labor Law

81. It is well known that the employment relationship is characterized by an intrinsic imbalance of powers between an employer and employee. In view of these intrinsic imbalances of powers, the Israeli legislator decided to create various balances that form a basic layer in the protection of the employee's rights. In view of the increased obligations imposed upon the parties to the employment relationship, in the world of labor laws the protection of the employee's privacy has been given extensive importance[39] In accordance with the aforesaid, and as shall be demonstrated below, the case law has held, in several judgments, that one should be precise and be strict in all matters pertaining to the particular requirements in the field of protection of privacy, such as the requirement of consent.

[38] *ibid*., in Paragraph 160 of the judgment of Justice Solberg.
[39] The Iskov case, Paragraph 12.

82. The main judgment given in recent years and that dealt with the questions concerning the use made by an employee at his place of employment of the email account, and the employer's ability to penetrate these email accounts, is the judgment in the **Iskov** case.

In this judgment, the Tribunal related to the personal dimension of the computer, holding that the private virtual sphere of the use is tantamount to the private physical space, and accordingly, penetration into this space is equivalent to prying into a person's intimate belongings, in a manner constituting an infringement of the constitutional right to privacy.[40]

In the judgment the Tribunal determined several principles the purpose of which is to restrict the employer's ability to supervise its employees' activity, and to ensure the protection of the employee's privacy. Accordingly, it was held that the employer must act in accordance with the principles of good faith, proportionality, transparency, legitimacy, and the principal of purpose limitation. 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 purpose that has been predefined. Likewise the employer must act in accordance with the principle of transparency, and 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. Beyond this, the judgment emphasizes the necessity, as a prerequisite for monitoring, of obtaining the employee's free and informed consent to the infringement of privacy. In this context it was held that a high threshold of consent should be set so as to ensure that the employee's consent is explicit, of his own free will and informed, and after the employee has been given the data he requires concerning the employer's intention. The Tribunal emphasized that beyond the employee's general consent in advance for the tracking activity policy of the employer, the employer must also receive the employee's consent to any specific tracking activity or specific penetration into the personal correspondence.

After noting the general principles applicable to the employer's monitoring and penetration into the employee's email accounts, the Tribunal made a distinction between the different email accounts ("professional account" intended solely for work purposes; "mixed account" and "external-private account"). Thus, for example, in all matters pertaining to the employee's external-private account (as in the example of the gmail account), the tribunal held that this account was owned exclusively by the employee. Accordingly, it was

[40] The Iskov case, Paragraph 6.

forbidden for the employer to track or penetrate this account, unless a Court order had been given, that would be given under highly exceptional circumstances and when accumulative conditions had been fulfilled (conditions which were set out in detail in the judgment).[41] The Court emphasized that even if the employee's consent had been given to the penetration into the external email account, then in view of the inherent imbalances of power between the parties, the presumption was that this consent had not been given of his own free will, and so penetration based upon such consent should not be allowed.[42]

This significant judgment enshrined the principles of the protection of privacy in the field of labor law, placing special emphasis on the importance of ensuring the protection of the employee's privacy in the employee-employer relationship, and the stringent requirements that the employer must comply with in this context.

83. The principles of the judgment in the **Iskov** case and the importance of ensuring the protection of the right to privacy within the framework of the employment relationship were reiterated in a judgment recently handed down by the tribunal in the **Kalansawa Municipality** case.[43] In this proceeding, the question arose whether an employer was entitled to install a biometric timekeeping clock in the work place that would be signed by fingerprinting, without the employee's consent.

According to his authority by law, the Attorney General appeared in this proceeding, and expressed his position concerning this question before the Tribunal.

In essence, the Attorney General claimed that forcing an employee to give a biometric sample involved an infringement of two basic rights - the right to privacy and the right to autonomy. Given that this coercion was made for the sole purpose of registration of attendance at the work place, 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 the very fact of the existence of human society; the necessity of

[41] *ibid.*, Paragraph 50.
[42] *ibid.*, Paragraphs 45-50.
[43] Collective Dispute Appeal 7541-04-14 The New Workers' General Federation v. the Kalansawa Municipality (published in *Nevo*, 15.5.17).

interpreting this right from a broad view and the ever-increasing necessity of protecting this right and setting stable limits for it.[44]

Likewise, concerning the relevant data under the circumstances of our case, it was held that a fingerprint is a person's "personal-private" data, and that its delivery to another, infringes, already by the very fact of its delivery, upon the person's right to privacy and autonomy. Another separate infringement is caused as a result of the significant risk of abuse of the fingerprint.[45] In light of this, the Tribunal held, in accordance with the Attorney General's position, that an employer is not entitled to compel the delivery of fingerprints for the purpose of use in a biometric attendance system.

Similarly to the **Iskov** case descried above, the tribunal noted the importance of the protection of the right to privacy within the framework of the employment relationship and the importance of being much more precise in the requirement to obtain the employee's consent to the infringement.

Accordingly, it was held that one should examine whether consent was given in an informed manner and of his own free will, in accordance with certain criteria that are set out in detail in the judgment.[46]

b) Standard Contracts

84. Another field which demonstrates the implementation of the privacy principles in cases in which there is a form of imbalance of powers is in the case of standard contracts.

85. Within the proceedings heard before the Standard Contracts Tribunal, the Attorney General submitted a motion for the annulment of discriminatory terms included in the agreement of an Israeli cellular company with its customers. After the representatives on behalf of the Attorney General held deliberations with the cellular company, the representatives on behalf of the company had agreed to modify the terms of the engagement agreement, so that the privacy protection chapter included in the agreement would be modified in a manner that will increase the protection of the privacy of the cellular company's customers. For example, the agreement includes provisions that restrict the use of the data and its transfer onto third parties. The agreement also includes provisions regarding the right of review of

[44] Paragraphs 101-107.
[45] Paragraph 113.
[46] Paragraphs 130-133.

the data subject, and concerning the consent of the data subject to the use made with data regarding him. The Tribunal granted parties' agreements the validity of a judgment[47].

D. ILITA

i. About ILITA

a) Overview

86. The Privacy Protection Law empowers the Database Registrar, to enforce its provisions with regards to data protection, and provides the Registrar a variety of enforcement tools. The Registrar conducts criminal investigations, administrative investigations and audits. The Registrar imposes administrative fines and possesses the power to terminate or suspend activities of databases by suspending or erasing their registration. As mentioned above, the Registrar and his workers, provided with these authorities, work within the organizational framework of Israeli Law Information and Technology Authority (ILITA). Hereinafter we will refer to the Registrar as ILITA.

ILITA regulates and enforces data protection across all sectors, private and public, according to the provisions of the Privacy Protection Law, bearing in mind that according to the Basic Law: Human Dignity and Freedom, the right for privacy is a constitutional right.

As an independent authority specializing in data protection, ILITA's main mission is to outline the Israeli data protection policy, and to build trust in the digital economy. ILITA focuses on strengthening data protection and empowering individuals by promoting individual's control on personal identifiable data, and by promoting processes of privacy by design across the economy. ILITA's aim is to reduce the risks for data, taking into consideration the frequent advancements in the digital environment.

As a civil rights gatekeeper in the field of data protection, ILITA is dedicated to ensure compliance with the Privacy Acts' provisions on data protection in every Israeli company, business, NGO and public body that manage personal data.

ILITA enforces and promotes compliance to the Privacy Act's provisions regarding data protection with enforcement activities, educational activities and by issuing guidelines

[47] SC 42799-03-10 **the Attorney General v. Cellcom Israel Ltd.** (25.1.17)

reflecting the way ILITA interprets the Privacy Protection Law when exercising its enforcement powers. In addition, ILITA advises the Israeli Knesset on privacy and data security in legislation processes and advises the government in the creation of major databases and digital projects.

According to Article 10 of the Privacy Act, ILITA prepares an annual report about its activities for the review and oversight of the Israeli Knesset.

b) ILITA is Adapting to Future Changes

87. In order to advance and improve ILITA's capabilities in coping with future challenges to data protection, and in order to strengthen ILITA 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 ILITA went through a significant strategic change that includes re-organization of its structure and modifying and re prioritizing its aims.

The strategic change is still underway, and its main pillars are the following:

c) Two New Departments in ILITA

88. ILITA established 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 to privacy protection and its significant role in the digital economy, by educational, informative and training programs and activities. In addition, the department aims to raise awareness to the rights of the public and relevant actors protected in the Privacy Protection Law, and to the various roles and responsibilities under the law. 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 economy.

The main tasks of the Innovation and Policy Development Department are identifying innovative trends in the field of technology, business and social privacy, conducting research and initiating innovative regulatory solutions to data protection in the sophisticated and dynamic digital economy. In addition, the department will consult the Head of ILITA in the process of determining ILITA's policy and strategic planning.

Merger of the Criminal and the Administrative Enforcement Departments

89. Until recently the Criminal Investigations Department and the Administrative Department, operated each on their own.

    Following the re-organizational change the two departments merged into one. The goal of the merge is to establish an effective, focused and broad-based enforcement policy that will promote compliance across all relevant organizations in the Israeli economy.

    Enforcement and guidance activities will expand and focus on cases that involve particularly sensitive data or big amounts of data, and on cases in which individual or disadvantaged sections in society lacking sufficient tools and skills, face large and powerful organizations processing their personal data. ILITA intends to investigate and supervise more sectors and companies, by increasing its enforcement department and staff and by deploying a new audit mechanism.

d) More Guidelines and Standardization as an Alternative for "Case by Case" Advice and Guidance

90. In the dynamic reality of the digital economy in which digital developments are frequent and dramatic, guidelines are a significant tool for the promotion and enforcement of data protection. Guidelines are one of the most effective and guiding methods that assist in effectively responding to the new growing challenges to data and privacy protection. During the year 2016 ILITA promoted data protection by publishing for public consultation 3 draft guidelines, reflecting the way it interprets the Privacy Protection Law when exercising its enforcement powers, on the following issues: "Surveillance in Workplaces", "Right of Individuals to Access Records of Communications with Service Providers" and guidelines with regards to "Direct Mailing" (data traders).

e) ILITA's Cooperation with Other Enforcement and Investigations Authorities

91. ILITA's activities include cooperation with security bodies, parallel enforcement bodies, investigative authorities, and digital authorities (eg, the Israeli Police, the National Authority for Cyber Defense, the National Cyber Headquarters, the General Director of Biometrics, Digital Headquarters, etc.) One of the main goals of mutual activities is that all of these enforcement bodies, investigative authorities and security bodies will act in harmony and synergy, with a high degree of

awareness to privacy rights, in order to create adequate balances when protecting the cyberspace while at the same time protecting human rights, as required in light of the constitutional framework mentioned above and the principles of democracy. ILITA plays a critical role in protecting citizens' privacy and in shaping the ability of the relevant bodies to use data in a lawful manner.

ILITA provides these authorities with training activities in order to promote compliance with and awareness to the Privacy Protection Law and its regulations. ILITA also receives information from these authorities with regards to data leakages and violations of the Privacy Act.

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

f) A Dramatic Increase in ILITA's Budget

92. Until 2016, ILITA's budget was approximately 10 million NIS and had not gone through significant changes over the years. Following the strategic change ILITA is currently going through its budget has dramatically increased. ILITA's budget went through a 50% increase, reaching 15 million NIS. In 2018 ILITA's budget is expected to increase in an addition of 10% and will reach 16.5 NIS (total increase of 65%).

In terms of manpower, in the end of 2017 ILITA's staff will include 51 employees. ILITA's staff consists of lawyers, technologists, administrative staff, interns, national service volunteers and students. Between 2016 and 2018, ILITA was granted the addition of 10 professional positions of "full – time" public service employees and 10 additional part time none permanent employees. This represents a significant increase of 25% in the number of permanent public service employees in the Authority.

ii. ILITA'S Guidelines and Draft Guidelines

93. As mentioned above, ILITA considers guidelines as a significant regulatory tool. ILITA uses guidelines in order to clarify the way in which it interprets the provisions of the Privacy Protection Law when exercising its enforcement powers on specific sectors or activities, in an environment which is exposed to frequent technological developments, before ILITA exercises its powers by investigations acts or audits.

The guidelines promote compliance and awareness; remove uncertainty and direct organizations in the manner in which they manage their data.

ILITA publishes its guidelines after a proper process of public consultation with all relevant stakeholders in the economy. Following is a short description of recent guidelines and draft guidelines issued by ILITA.

a) ILITA's New Guidelines on the Right to Access

94. The Privacy Protection Law grants data subjects the right to access their personal data. In its new guidelines, ILITA expressed its opinion that the right to access includes data in any format or file type, including video, text messaging and voice recordings, and this right applies to customers who want to access data collected/stored by their service provider. According to ILITAs 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 must authenticate the identity of the data subject and ensure that the applicant will not receive data about other data subjects.

b) Surveillance Cameras

95. In 2012, ILITA published guidelines with regards to surveillance cameras. The aim of the guidelines is to ensure proportionality and transparency with regards to surveillance. The guidelines include provisions with regards to data retention, transparency, right to access, and accountability principles that are linked to the decision to use surveillance cameras.

    ILITA intends to update its guidelines due to new developments such as drones, wearable cameras, improvements in automatic face recognition technologies, and increase of surveillance cameras usages in households, apartment buildings and workplaces.

c) Draft Guidelines on Workplace Surveillance

96. Workplace surveillance is becoming a common practice, and it raises difficult questions with regards to privacy and employees' rights. Employees are not of equal status to their employers, and

therefore even if they agree to the implementation of such practices in their workspace, it is hard to determine that under the circumstances the obligation of the employer to receive free and informed consent has been met.

The draft guidelines emphasize the main principles that employers who install surveillance means in work places are required, under the law, to act according to, including the duty to act in reasonable, fair and proportional manner, and in good faith.

The installment of surveillance means is allowed only for legitimate purposes, which are essential to the employers' interests, and are in accordance with the employers' business agenda or in circumstances in which their installment is required to fulfill a legal obligation.

Prior to the installment of surveillance means, the employer will establish a clear and detailed policy with regards to the manner and the extent of the usage, and its purposes. The policy will be presented to the employees and will be updated from time to time.

The draft guidelines include also parameters regarding specific justifications required regarding installment of surveillance means in certain sensitive areas.

The draft of this guideline is currently going through a process of governmental and public consultations.

d) Guidelines on the Use of Outsourcing Services for Personal Data Processing

97. The guidelines provide organizations with guidance on the proper way to process data via outsourcing services. Accordingly, the guidelines elaborate on data controllers' and subcontractors' obligations when designing a data processing service to be outsourced and its subsequent performance, with special regard to the required organizational controls.

The principles set forth in the guidelines apply to private sector organizations as well as public ones, and their purpose is to ensure that obtaining data processing services from a third party will not diminish an individuals' right to privacy.

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

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

- 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;
- Definition of data security and confidentiality provisions to prevent data leakage;
- Provisions and procedures with regards to the fulfillment of the data subjects' reviewing and rectification rights;
- Criteria for choosing an outsourcing contractor, e.g. previous experience in processing personal data and avoiding risk for conflict of interests;
- Integration and instruction mechanisms to ensure that personal data protection principles are incorporated by the contractor's employees;
- Defining means to perform follow-ups and supervisions of the contractor's fulfillment of legal obligations (provisions of the law and contract);
- Duration of retention period of the data by the contractor and deletion of data upon conclusion of the contractual engagement.

The guidelines include a checklist appendix, designed for easy and quick examination of outsourcing contracts compliance with the guidelines.

It should be noted that the guidelines provide that organizations using outsourcing services must verify that trans-border outsourced data flows comply with the Privacy Protection Regulations (Transference of Data to Databases Located Outside the State of Israel), 2001, that regulate trans-border data flows.

Failing to comply with the guidelines may lead to a determination by ILITA that an organization had violated the relevant provisions in the Privacy Act, and to the imposition of administrative sanctions by ILITA. In some cases, failing to act in certain ways may constitute a criminal offence as well.

It should be noted that the Privacy Protection (Data Security) Regulations, from May 2017 referred to in chapter B, reflect some of the provisions of these guidelines, as well.

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

98. The guidelines were published following an audit ILITA initiated amongst recruitment agencies conducting "Employee Compatibility Tests" which aim is to screen potential employees searching for employment.

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

According to the Privacy Act, the controller needs to receive the informed consent of the data subject, prior to the data collection. In addition, the Privacy Protection Law prohibits the use of the data from a database for a purpose other than the one the database has been created for, and generally defines usage of data for purposes other than the one it was been collected for as an infringement of privacy (the principal of "purpose limitation"). ILITA's guidelines make it clear that the recruitment agencies are the processors, while the controllers of the data are the potential employers. Therefore the recruitment agencies are not permitted to use and process the data for different purposes other than the ones of the potential employer,. In addition, the employer must draw up a list of employees who are authorized to access the results of the tests and the accumulated data, based on their role in the organization and only if necessary to fulfill their tasks.

According to the guidelines, the consent of a candidate to additional uses of the data (that were not required for the purposes of completing the selection procedures for joining the ranks of the employer who referred him) 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 as aforesaid is only likely to be valid and based on real freedom of choice if it was given after receiving a notification with regards to his acceptance or rejection for the position he was originally tested for.

The guidelines also emphasize the significance of the right to access the results of the compatibility tests (excluding analysis of the compatibility to the characteristics of the specific position), especially because the results serve as the basis for decisions which may impact the candidate's future.

f) Draft Guidelines on Direct Mailing

Legislative Background

99. In the Privacy Protection Law (Amendment No. 4) (databases), 1996, the Israeli legislator revised Part Two of the law, titled "Protection of Privacy in Databases" and added, *inter alia*, a specific chapter addressing direct marketing, which is defined in Article 17C of the law (the term used is "direct mailing", but it applies to all kinds of communications) as follows: *"...contacting a person* ***personally, based on their belonging to a group of the population that is determined by one or more characteristics*** *of the people whose names are included in the database."*

    Sec. 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."* Note that this definition excludes bulk, impersonal direct marketing via unsolicited mail and other forms of communications (otherwise known as "spam mail"), which is primarily regulated under the Communications Law of 1982, as amended in Amendment No. 40 of 2008.

    According to the Privacy Act, the operation and holding of a database for the purpose of direct mailing triggers stricter regulation than a "regular" database. In addition, databases established for the purpose of direct mailing **services** are subject to even stricter rules. Thus, in addition to the duties imposed on "regular" databases, a database created for direct mailing **services** must withstand the following criteria:

    1) They must be registered with ILITA, no matter how many data subjects are listed, or whether or not the data is sensitive.

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

    3). Data subjects may require that the data will 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 subjected to duties towards the data subject regarding notice, access, rectification and deletion.

ILITA's Guidelines

100. In recent years, technological developments and the multiplicity of media platforms resulted in 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, in August 2016 ILITA published draft guidelines on the interpretation and implementation of the Privacy Protection Law provisions with regard to the relationship between a company or a business and their current or potential customer, where that customer is being contacted by the former in ways the law defines as "direct mailing" or as "direct mailing services". Following a period of public consultation, ILITA has completed its revision of the Draft's text, and will publish the final version thereof during June 2017.

The draft guidelines shed light on the way ILITA interprets the Privacy Protection Law when exercising its enforcement powers. The draft details 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 services. It also outlines the conditions and 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 (in standrad contracts, in general "opt-in") or direct mailing.

Furthermore, the draft 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).

ILITA also published a list of "Dos and Don'ts" , in order to give guidance to organizations considering purchasing direct mailing lists, in order to ensure that the data sources they acquire are ones that were lawfully obtained. Unlawful uses of personal data expose both data traders and buyers to enforcement actions and, where appropriate, to the imposition of sanctions by ILITA. They can also be ground for a civil claim in a court of law.

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

101. ILITA published the guidelines after imposing an administrative fine on IDI Insurance Company Ltd, due to the fact that the company abused data it received regarding

registered liens. The company receives automatic applications to register liens on insurance policies it holds from enforcement authorities. Sometimes the applications refer to data subjects that are not customers of the company. The company used data about a debtor that wanted to use its services, in order to deny his application for insurance. ILITA determined that the data regarding registered liens is sensitive data about the private affairs of the debtor, and the company's use of such data for that purposes is forbidden under the law.

Following this case, ILITA published guidelines prohibiting the use of data regarding the imposition of foreclosures. The guidelines clarify that data regarding the imposition of 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 company filed a petition with the district court against the guidelines, and it was denied. The company appealed to the Supreme Court, which confirmed the district court's decision and ruled that the guidelines reflect a reasonable and proper policy. The Supreme Court clarified that ILITA has the authority to publish guidelines regarding the interpretation of the provisions of the Israeli Privacy Law.

The main principles in the guidelines are as follows:

- The data included in the foreclosure order has been 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.
- The Israeli Execution law (1967) states that a person who received data regarding a debtor, in means that the law permits, is not allowed to use it for any purpose other than the one stated by the law, thus, using data included in the foreclosure order in a way that deviates from the purpose of the foreclosure order, harms the debtor's right to privacy.
- Using data included in the foreclosure order in a way that deviates from the purpose of the foreclosure order is also forbidden by the Privacy Act, which prohibits the use of data for any other purpose than the purpose for which the database established.
- 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 who receive registered liens on assets of a policyholder, are not allowed to process the personal data in order to decide whether to give them services.

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

iii. Prominent Enforcement Actions

a) Criminal Investigations and Proceedings

102. ILITA has powers to conduct criminal investigations which can result in indictments. Following is a short description of ILITA's most prominent criminal investigations in the past year:

Investigation against Communications Services Provider

103. ILITA investigated suspicions regarding offenses under the Privacy Act, carried out by employees and managers of "Rami Levy Information Marketing – Communications", which is 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 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 Jerusalem District Attorney's Office to for review and consideration for indictment.

Investigation against Health Service Providers and Data Traders

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

ILITA's findings 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 the patient, 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 Insurer), so there is "a competition" between the nursing services providers to be the first to reach the patient, and seal a very 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 elder patients, to "middle men". These "middle men" 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.

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 have been conducting their actions for 3 years before they were discovered by ILITA's enforcement team.

<u>18 Months of Imprisonment for Massive Personal Data Theft and Dissemination in a Verdict Given by the Israeli Magistrate Court in Tel Aviv after ILITA's Investigation</u>

105. The Israeli Magistrate Court in Tel Aviv sentenced Mr. Lever to 18 months Imprisonment, 100,000 NIS fine (approximately 25,000$) and 6 months' probation for invasion of privacy and obstruction of justice offences, following his role in a personal data theft and dissemination case.

The investigation of this case was conducted by the Criminal Investigations Unit in ILITA. The investigation reflects the strong investigation skills and robust forensic capabilities of ILITAs investigation unit.

This verdict concludes a case that began with an outsourced worker who stole the Population Registry Database from a government ministry. The database contained dozens of fields of personal data about all residents ((including minors and deceased).

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.

Mr. Lever, the recently sentenced defendant, made the data accessible to the entire public by uploading links, and a 30 page manual, encouraging the public to use the application. Lever

disguised his identity using proxies and inaccessible servers. After realizing the strong digital evidence against him, Mr. Lever confessed in court about his role in the case.

Mr. Lever is one of 6 defendants that were charged with invasion of privacy and other crimes in this case. The other 4 defendants have already been sentenced to community service and imprisonment, according to their role in the case, and another defendant was sentenced to 6 months imprisonment. The case received high attention from the Israeli media.

b) Prominent Administrative Enforcement Actions

ILITA's Actions against Data Traders and Their Clients

106. This case presents how ILITA handled different parts of the "data chain" that were all using illegally obtained data. ILITA accommodated its enforcement tools accordingly to the parts of the chain as follows:

As mentioned above, a few years ago data from the Israeli population registry was stolen. ILITA conducted a complex criminal investigation, and due to its findings 6 people were convicted, two of which were sentenced to jail. Jailing the involved data abusers did not prevent using the data by other parties that got hold of it and integrated the data with other sources of data, some of which were illegally obtained as well. In a complex forensic investigation, which took place in 2016, ILITA found a company that obtained the illegal data and sold it to third parties. ILITA conducted a search and seizure of computer materials in simultaneous on-site inspections at 4 sites and seized documents of the orders and payments.

ILITA 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 base of the offenders included over 1,000 companies from various market sectors including banks, insurance companies, HMO's, newspaper publishers, charity organizations, legal firms, research and more.

Following the investigation, ILITA determined that the activity of the company was illegal, and terminated its activities by deleting the database from the database registrar. ILITA

"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. ILITA investigated some of the clients and found that one of them did not delete the data. This client was fined as well.

This case represents how ILITA acts against all the data chain components, and it's actions include administrative supervision, inquiries, instructions, reviews (on some of the customers), shutting down illegal activities and even criminal treatment. This case is an excellent example of a policy that involves the integration of various regulatory tools and the power that exists in the synergy of ILITA's activities, to tackle severe privacy violations.

An Investigation against the Political Party "Yesh Atid"

107. In Israel there is a variety of non-profit organizations that give 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" (The Organization). The Chairwoman of the Organization was asked by a representative of the 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 explicit consent of the survivors, while violating their privacy and the Privacy Act.

Later on, the party used the data for propaganda purposes and for direct mailing to survivors prior to the elections for the 20th Knesset.

In a hearing held by ILITA, representatives of the party and the Organization were invited to respond to ILITA's allegations against them. After the completion of this procedure, it was decided that all the parties acted in violation of the law, and therefore administrative fines were imposed on the party, the Organization and the Organizations' chairwoman.

Leumi Card's Data Breach

108. Leumi Card is the largest credit card company in Israel. ILITA investigated the level of data security in the company's systems and it's compatibility with the Privacy Act's obligations to secure personal data, after a former employee stole extensive and sensitive data and tried to extort the company.

ILITA found that 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, and therefore the company is in a breach according to the Privacy Act.

ILITA determined 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, and therefore the company was aware of the data theft only after the former employee began to extort the company.

In addition, ILITA assisted the Israeli Bank Supervisor, who investigated this case as well.

c) Data Breaches and Leakages

109. ILITA came to the conclusion that organizations are not aware of their obligation to secure data and therefore data leakages have become too common. In order to strengthen awareness to the duty to secure data, ILITA's enforcement team initiates security checks by locating data leakages online.

ILITA has publicized its actions in the media in order to create more awareness and thus enhance deterrence, in order to assist in tackling this problem.

Following is a description of a few cases in which ILITA's team identified data breaches and instructed organizations to secure their data.

<u>"TAF's" Data breach</u>

110. 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.

ILITA issued an immediate demand to amend the flaw, but due to slow and unsatisfactory response from the NGO, ILITA's inspectors 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 findings of the inspection, due to the fact that the Adoption Law imposes obligations on confidentiality.

Due to the severity of the findings, ILITA 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 is prohibited from making any use of the registered database files and its derivatives or copies without obtaining once again the Registrar's approval.

Data Leakage exposing Data of Labor Party's Members

111. ILITA 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.

ILITA instructed the 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 Movement will have to report to ILITA about the implementation of its instructions.

Miscellaneous

112. ILITA has also found data security deficiencies in a company that performs deductive assessments to minors (very sensitive data including data about families in distress, learning disabilities and psychological problems); the servers of the Prisoner Rehabilitation Authority; law firms, Employees Fund (exposing sensitive data about employees), and more.

iv. **ILITA is Involved in Legislative Processes with Privacy and Security Implications and in the Initiation and Development of Broad and Sensitive Governmental Digital Projects**

113. ILITA is involved in complicated legislative processes with privacy and data security implications. In addition, ILITA ensures that certain legislation involving sensitive digital projects empowers ILITA to act as an advisory agency or as a certification authority.

ILITA is also involved in the initiation and development of broad and sensitive digital national governmental projects that effect national digital infrastructure and the national economy.

Following is a list of examples of legislation processes and government activities ILITA is involved in:

The new Credit Data Law– ILITA 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, ILITA pushed for heavy data security mechanisms. Thanks to ILITAs advice, the law mandates the appointment of a data protection officer for the project, as mentioned above.

The Committee for Increasing Competition in the Banking Services Market – the committee aimed to enforce financial institutions to open API's of online accounts after customers consent, to enable "comparison services providers" to offer the public the best deal for financial services. ILITA presented the committee with the privacy implications.

The Supervision of Financial Services Law (Regulated Financial Services), 5776 – 2016, mentioned above, was formulated based on the committee's report. ILITA, continues to support strong mechanisms of privacy by design and enhanced data security during the governmental work over formulating the required regulations.

Biometric Applications Law- ILITA has advocated for privacy in the Biometric Database projects pre-legislation, during legislation, during the entire pilot period and during the final decision process. Many privacy by design principals where implemented in the project, and ILITA has achieved better privacy protection. These include conducting a Privacy & Security Risk Assessment, limited purposes enacted by law, transparency mechanisms for the public, data collection limitation, end to end security embedded in the architecture, accountability in the form of a Data Protection Officer, Dedicated Supervisory Authority, reporting obligations, supervision by the Knesset and supervision by ILITA.

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. ILITA advised and issued specific guidelines for the public transportation operators, in order to make sure that citizens' privacy risks are mitigated in the systems. ILITA also conducted security audits on all operators and gave instructions to improve security. ILITA continues to advise during the legislation process.

Income Tax Regulations – ILITA advised the Minister of Finance on the manner in which data should be collected, managed and stored with regards to reports that monitory service providers are required to issue with regards to money laundering (these regulations were issued under the 26. The Income Tax Ordinance [New Version], mentioned above).

Draft Regulations on Equality for People with Disabilities – ILITA advised on necessary privacy controls with regards to new regulations enacted to maintain equal rights for people with disabilities. As aforementioned regarding The Equal Rights for People with Disabilities Law, 5758 - 1998, The draft regulations, issued under the law, aim to ensure people with disabilities receive proper representation as public servants in public work places. ILITA 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.

ILITAs opinion before the "National Academy of Science"- the academy has initiated a national project for the establishment of a big database in the education sector which aim is to use big data analysis in order to promote better education based on statistical conclusions. ILITA was asked to present on the privacy implications and legal requirements with regards to personal data in this project.

Government Cloud Computing Committee - ILITA collaborated with the Israeli Governments' Computer 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, ILITA is a member of the committee that examines each request of a government body to use cloud services.

Re-use of public service Data (Open Data) – ILITA was a member in the advising committee on the "Re-Use of Public Service Data". ILITA gave its opinion with regards to principles of privacy, privacy by design, anonimization as a privacy by design mechanism and more. Some of these principles were embedded in Government resolution No. 1933 aforementioned**.**

The Committee for Data Transfers Within the Government – ILITA, alongside the Department of Legislation and Legal Council, was a member of the "Data Transfers Within the Government" that aimed to review access mechanisms of public sector organizations to data. Government resolution No. 1933 aforementioned, was formulated on the base of the work of this committee as well.

Stirring Committee for the Improvement of the Government Real Estate Database – ILITA is a member of the stirring committee.

International Agreements – ILITA advises on international trade agreements that involve data transfers.

ILITA advises the Knesset Committee on Science and Technology – ILITA advised on a variety of subjects including drones, smart cities, databases to combat car accidents, Facebook, managing government data and more.

ILITA is an observer in a research group founded by the **Israeli Institution for Democracy.**

v. Public Awareness Activities And Cooperation Within The Government

114. The Strategic Alliances Department at ILITA was established in order to create and promote a meaningful public debate on privacy, and engage the public, in order to establish privacy protection awareness and actions.

The department's responsibilities include:

- Communications, PR, new-media;
- Policy Delivery;
- Government and Parliament relations;
- Training and Education;
- Conferences organization & participation;
- Handling public complaints and inquiries;
- Database Registration

In the last 10 months, since it's initiation the department has accomplished the following:

- Creating a dominant presence in the media with numerous written, radio and television appearances;
- Creating a social media presence with an active Facebook account;
- Establishing a forum for privacy awareness & training in the Israeli public sector which currently includes 140 members, from both legal and tech background and positions, meeting 4 times a year and receiving monthly updates. The establishment of this forum is another step towards introducing the requirement to appoint privacy champions in public bodies;
- Participating as lecturers and instructors in over 30 events;
- Sending a monthly newsletter including updates of activities in both enforcement, guidelines and events to a list of approximately 3,000 followers from the professional community (lawyers, accountants, academia, researchers, governance, IT, security etc.);
- Writing Q&As for ILITA's guidelines and working on a guide to the new Israeli Security Regulations in order to make the regulatory regime more accessible to the public;
- Re-building ILITA's website with an approachable concept and updated content; It is estimated that a new, advanced and updated website will be launched in August. An English version of the new website will be launched in the near future as well.
- Re-branding ILITA with a new name and logo dedicated to privacy protection;
- Conducting a public survey of people's views on privacy in various sectors, answered by 1,300 people;
- Producing a special meeting of the Science & Technology Parliament Committee on Privacy day, dedicated to the current issues in the world of privacy;
- Initial talks with the Ministry of Education on a joint project on Privacy Education.

vi. ILITA's Activities In The International Arena

115. 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. ILITA acknowledges that it needs to participate in international activities and to be a member of international organizations.

ILITA is a member of the following organizations:

1. The International Conference for Data Protection and Privacy Commissioners (Israel hosted the conference in the year 2010);
2. The Global Privacy Enforcement Network - ILITA is a member of the GPEN committee together with ICO (UK), FTC (USA), OPC (Canada) and PCPD (Hong Kong).
3. OECD's Working Party on Security and Privacy in the Digital Economy- the working party operates under the Committee for Digital Economy Policy;
4. The International Working Group on Data protection in Telecommunications ("The Berlin Group");
5. The Digital Clearing House Network – the network brings together authorities who are responsible for regulation of the digital sector. ILITA joined the network and participated in its first meeting in May 29th.
6. International conferences on Data Protection and Privacy.

E. The Attorney General Guidelines

The Attorney General Guideline no. 3.1103 - **"**Obtaining a Voice Sample from Prison Inmates and Maintaining It in a Database**"**

116. As noted above, the Attorney General is authorized to set forth legal guidelines that bind the government in its activities.

An additional 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 Guideline in respect of obtaining a voice sample from prison inmates and maintaining such in a database. This Guideline addresses the obtaining of a voice sample from prison inmates, as part of a new telephony system adapted to the needs of the Correctional Services. A petition objecting to the implementation of this system had been filed with the High Court of Justice, in which the petitioner argued that implementing the system constitutes a prohibited

violation of the prison inmates' right to privacy.[48] 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, and so as an interim stage until the matter will be legislated[49]. A bill to this affect passed the first reading in the Knesset.

The Attorney General Guideline conditions operating the telephone system on the implementation of basic principles of privacy law: First, it is clarified that the legal basis for obtaining the voice sample shall be the inmate's informed and free consent, which will be exercised both by the existence of a true alternative for use of telephony services with no need for obtaining a voice sample and notification regarding this alternative, as well as by providing the inmate with an explanation as to the purposes for obtaining the voice sample and maintaining such in a database, the implications entailed in so and his option to withdraw his consent at any given time[50]. Second, the Guideline requires the implementation of additional basic principles concerning, *inter alia*, the data that will be stored in the database and the use to be made of it, access to it, the duration of storing the data, etc. For example, the establishment of the database will be carried out in accordance with the Privacy by Design approach, so that identification data in it will be maintained in a manner that will ensure protection against illegal disclosure, use or copy, or contrary to the Attorney General Guideline.[51] Further, pursuant to the "Control of Data "principle, data stored in the database shall be deleted per the inmate's request or upon termination of his prison term, including granting the inmate the right to refer to the Correctional Services and inquire whether the identifying data regarding him had been duly deleted. Additionally, the Attorney General Guideline emphasizes the "Purpose Limitation" principle, and defines the restricted use that may be made with the database.

[48] 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 Correctional Services** (published in Nevo, 24.12.2013).

[49] "Obtaining a voice sample from prison inmates and obtaining such is a database "**Attorney General Directives** 3.1103 (2015)

[50] There, on pp. 2.

[51] There, on pp. 3.

F. Government Decisions and Central General Director Circular Embodying Privacy Protection Aspects

117. The need for protection of the right to privacy and setting forth specific mechanisms designed to protect this right, is expressed also within government resolutions and procedures set forth in government ministries.

The government acts, pursuant to the legal advice it is given by the representatives on behalf of the Attorney General, in a way it addresses the concept of protecting the privacy of personal data from the early stages of formulating any policy. The two examples below will illustrate this.

Government Decision No. 1933 dated 30.8.16, Concerning Improving the Transfer of Government data and Granting the Public Access to Government DataBases

118. The first part of this decision engages in the transfer of information between government offices, in order to improve government services provided to the public. The focus of this decision is placed on improving services, however in order to protect the constitutional right to privacy, within the government decision provisions had been added that were designed to ensure that the transfer of data will be carried out in a proportionate manner. According to the government decision, with regards to data about a person, only data that had been approved by the Inter-Ministerial Committee for Transfer of Data (which as stated above in Chapter B, examines the requests for transferring data) has reviewed and found that such transfer is allowed under privacy protection laws may be transferred. The committee 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 decision further states that sharing data will be carried out while examining, *inter alia*, the sensitivity of the transferred personal data, the scope of the data, and the benefits embodied in the data to the public. In addition, the government decision sets forth that transfer of data between government ministries shall be carried out subject to all laws, including privacy laws, and subject to proper arrangements for the protection of the data, and limiting its disclosure solely to the entities authorized for such.

The second part of the government decision concerns providing access to databases. Within the government decision it had been set forth that the government ministries are to provide

access to the databases they are responsible for, provided that their release does not constitute "identified data", and considering the issue of protection of personal data and data security. It should be noted that the definition of "identified data" per the government decision is wide and addresses "data as its definition under the Privacy Protection Law, including data concerning a person's private matters, and including data that as aforementioned is not identified data, should it be identifiable, in itself or together with additional data. The decision of whether data that is not identified 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'.

Government Decision no. 2733 Concerning the Promotion of the National Project "Digital Israel" was Passed on 11.6.17.

119. This government decision, which was passed very recently, is intended, mainly, to encourage innovation within the public sector and for implementing innovative technologies though digital tools. This decision too referred to the principles of the protection of the right to privacy. For example, it is set forth that as part of implementing the government decision, concerning the promotion of programs entailing collection of identified or identifiable data, the relevant bodies shall consider the privacy protection aspects for the use of the data, transfer or provision of access to databases 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. All this, as provided under law, and pursuant to the principles and balances detailed within government resolution no. 1933 noted above.

The Ministry of Education Director General Circular Regarding Operation of Cameras in Educational Institutions

120. 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.

In May 2015, a Director General Circular issued by the Ministry of Education was published, concerning "Cameras in education institutions - regulating their introduction and the manner of their installation". This Director General Circular was designed to set forth the balance between the students' right to privacy and maintaining security and protection in schools.

The Circular emphasizes that in light of the possible violation of students' privacy, "continuous use of the cameras is considered to be a last resort, as along with its benefit, it entails violation of privacy, and thus the mere use of such must be carefully considered, and should use be made of it, it should be carried out in a measure that does not exceed that required".

According to the Circular, the decision on placing cameras in schools will be passed in writing, by the director of the education institute, after he takes into account the considerations specified in the Circular, which are intended for ensuring maximal protection of the right to privacy.

Further, the Circular sets forth various instructions designed to reduce violation of privacy, to the extent it was decided that there is a need for placing cameras and there is no other mean, less offensive, capable of obtaining the goal. So for example, it had been set forth that cameras may not be placed in kindergartens. Regarding schools it had been set forth that the camera would be placed so that it would photograph only the "public area", which serves all of those visiting the school (such as the school yard, sports fields, etc.), and that "no camera shall be placed and shall not be operated in a manner that enables photographing personal space or a place within the public area where private and pseudo-private activities take place (such as bathrooms, counselor's room and infirmary). It had also been set forth that cameras would not be placed in classrooms. Further, instructions were set forth, *inter alia*, regarding notification and posting signs on the placement of cameras, data security that must be used, those authorized to access the photos and the permissions they are granted, restricting uses of the photos, maintaining confidentiality, characteristics of the camera and photography, elimination of the material recorded, etc. All so, in order to reduce violation of privacy that might be caused as a result of placing and operating the cameras.

G. Public Activity

i. The Privacy Protection Council

121. The Privacy Protection Council is a statutory body by virtue of the Privacy Protection Law[52], whose function is to advise the Minister of Justice in matters connected to the protection of privacy. Within the framework of its function, the Council expresses its

[52] See Section 10A of the Protection of Privacy Law

opinion before the Minister of Justice and before the *Knesset* in matters connected to privacy. This is with the aim of influencing the shaping of the policy and determining arrangements designed to protect privacy in Israel. Thus, for example, the public Council expressed its position in debates held in the *Knesset* concerning the Credit Services Providers Law, 5776-2016, that was mentioned above. In addition, arrangement regarding the supervisor appointed at the Bank of Israel for the protection of privacy in the context of the Credit Data Law was initiated by a suggestion of the Council.

It should be noted that the Council was formed in 1986, and its members comprise representatives from academia, the private sector and the public sector, all having the relevant expertise in the field of privacy protection.

ii. Public Activity in the Matter Of Privacy: The '*Publicly Private*' Program

122. Following the amendment to the Prevention of Sexual Harassment (Amendment No. 10) Law, 5774-2014, that prohibited the circulation of photographs of a sexual nature on the social networks (mentioned above in Chapter B), it was decided to conduct a joint project of Ministry of Justice and the Ministry of Education, with the aim of raising awareness to the amendment and promoting safe use of the Internet. The purpose of this project was to raise awareness of teenagers to the issue of privacy in general and in the context of the Internet and social media in particular. As part of this program, lawyers gave approximately 1,000 presentations in schools all over the country, and this was accompanied with an advertising campaign on TV, radio and newspapers.

H. Access to Personal Data for National Security Purposes and Law Enforcement

123. We were asked to refer, *inter alia*, to limitations and safeguards applicable in the State of Israel as regards access to personal data by public authorities, in particular for national security and law enforcement purposes.

124. For information about the general restrictions on the access of public authorities to personal data, please refer to the brief review in the first part of this document, regarding the protections of the right to privacy in Israeli law. It is an established principle that public authorities are allowed to act solely within their statutory powers. This limitation is especially relevant in relation to activities that touch upon basic rights, including the right to privacy. Therefore, any authority whose statutory mandate involves the collection and processing of personal data is subject to the general provisions set forth in the Privacy Protection Law, and in addition, in many cases it is subject to a specific law or specific regulations, which include restrictions regarding the activity of that authority.

For the purpose of providing a full account it should be noted that, as stated above, chapter D of the Privacy Protection Law deals with the communication of personal data between public bodies for different public purposes, including for national security and law enforcement purposes. According to this chapter, in general a public body is prohibited to disclose personal data. An exception exists, where such disclosure is to another public body, subject to conditions and restrictions set forth in the law which in general permits disclosure of the data between public bodies, to the extent it is required for the purpose of fulfilling the mandate of the provider or recipient of data. As aforementioned in Chapter B(i)(c), regulations[53] that set out a procedural mechanism for the purpose of supervising the sharing of the data were promulgated by virtue of these provisions, so as to ensure that only data that complies with the statutory requirements will be transferred in this framework, including the requirement that the transference of the data will not infringe privacy to an excessive degree.

125. Regarding access to personal data by public authorities for national security and law enforcement purposes, below is a brief overview of the principal provisions of the legal framework and the primary supervision and control mechanisms in connection therewith, with respect to the Israel Police, the Israel Defense Forces (IDF) and the Israeli Security Agency (ISA). We conclude by providing a brief summary of the provisions of the Privacy Protection Law pertaining to the security agencies, as defined by this law, and to the general, across-the-board supervision and control mechanisms that apply to these agencies.

[53] Privacy Protection Regulations (Terms of Holding Data and its Maintenance and Procedures for Transfer of Data between Public Entities), 5746 - 1986

i. Access to Personal Data for Law Enforcement Purposes

126. The Israel Police is the main law enforcement authority in Israel. Nevertheless, there are other authorities in Israel that are entrusted with powers to conduct inquiries to supervise and enforce certain provisions of the law. Among these powers, the power to conduct criminal investigations is naturally entrusted with the Israel Police. In addition, such power is entrusted with a number of regulatory authorities with unique and complex specialties such as the Israel Securities Authority, the Israel Antitrust Authority and the Israel Tax Authority. We will focus in our response will focus on the Israel Police.

127. The Israel Police manages different databases that include personal data for operational, investigative or administrative purposes. In general, it obtains personal data for the purpose of fulfilling its functions, by virtue of the Police Ordinance [New Version], 5731-1971. In addition, all procedures in connection with the collection and storage of certain types of sensitive data are regulated in specific legislation: management of the Crime Register Database is governed by the Crime Register and Rehabilitation of Offenders Law 5741-1981; 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) 5756-1996; communications data database is regulated by the Criminal Procedure (Enforcement Authorities–Telecommunication Data) Law, 5768-2007; and wiretapping is regulated under the Wiretapping Law 5739-1979.

128. The regulation in each of the aforementioned laws is detailed and includes 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 onward transmission of the data; and in some cases – specific provisions regarding data security, deletion of data and right to access the data.

In addition, each of the above laws includes internal and external supervision and control mechanisms and reporting duties to outside entities in accordance with regulatory requirements.

129. For example, the Wiretapping Law, 5739 - 1979 (hereinafter - the Wiretapping Law) imposes a criminal prohibition on illegal wiretapping and illegal use of wiretapping. The law

sets forth 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 President of a District Court or a Deputy President of the District Court; the order can be issued only if they are "convinced, after considering the measure of violation of privacy, that such is required for identification, investigation or prevention of crime offenses". The order must state the identity of the person subject of the wiretapping, or the line on which wiretapping had been allowed, if they are known in advance, and must detail the manners of wiretapping that was permitted. The validity of the permit is limited to three months, though the order is renewable. In urgent cases, the Israeli Police Chief 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. In addition, the law includes provisions regarding deletion and elimination of wiretapping data.

Finally, the law sets forth reporting mechanisms - both a monthly inter-government reporting 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 to which wiretapping had been allowed.

130. All police databases are subject to the provisions of chapters B and D of the Privacy Protection Law and the regulations enacted thereunder. This is also the case with respect to the other databases that were specified above although these databases may be subject to specific alterative provisions, set forth in the specific laws aforementioned. In addition, specific instructions apply to some of the databases and the types of data, 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 ordinances of the Israel Police such as ordinances that regulate the supervision of police emails or travel routes of police vehicles.

131. In addition to the normative provisions that were specified above, the activities of the police in the field of access to data and use thereof is subject to internal and external control and oversight mechanisms, intended to assure that the use of the police of personal data and

its access to such data will be made solely within the statutory powers that are vested in the police and subject to concrete permission. . We shall now refer briefly to the main control and oversight mechanisms for the purpose of this matter:

1. Internal Supervision and Control:

    1. **The Data Security Unit** – This unit is a police unit whose function is to supervise the classification of the organizational information and its proper use. Among other things, the unit is responsible for issuing instructions regarding the protection of data and databases. With respect to the activities of the police personnel, the unit conducts different investigations and inquiries so as 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 as part of 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. It should be noted that all police data is managed, supervised and monitored in the police computer center and there are 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 ensures that the data is accessible only to people that have the correct 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 audits unit of the police and the legal department that accompanies the activities 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.

2. External supervision and control

As mentioned above, 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 by virtue of the Wiretapping Law. An additional reporting mechanism is included under the Inclusion of Biometric Identification Means and Biometric Identification Data in Identification Documents and Databases Law, 5770 – 2009. This law requires the police to report semi-annually to the Attorney General regarding applications filed with the Court for obtaining data from the biometric database and on orders issued by the Court for providing such data, where it had been convinced, for reasons recorded, that such data is required for any of the purposes listed in the arrangement and that such transfer would not excessively violate a person's privacy.

Finally, it should be noted that alongside the parliamentary supervision conducted with regard to built-in reporting requirement as described, such supervision is also conducted in routine meetings as part of the ongoing monitoring activities of the Knesset. In addition, the police is subjected to all of the external and general monitoring mechanisms that will be detailed below under Section 159.

ii. Access to personal data for national security purposes

a) Israel Defense Forces

132. Regarding the access to personal data for the purpose of protecting national security, we shall first refer to the activities of the Israel Defense Forces (hereinafter "IDF"). As we shall see, as part of its functions, the IDF obtains different types of data, and it manages a database that includes personal data about citizens and residents of Israel that are either intended to serve in the army, are currently in the course of their compulsory army service or serve as part of the reserve army units. This includes data that was collected for criminal and disciplinary enforcement purposes as part of internal military mechanisms, as will be described below.

133. The IDF is a unique body among all the other bodies in the State of Israel when it comes to criminal and disciplinary enforcement since it maintains independent enforcement mechanisms, both in the realm of disciplinary enforcement and in the realm of criminal enforcement, in accordance with the provisions set forth in the Military Justice Law 5715-1955. The Criminal Investigations Department in the IDF Military Police is the entity that is in charge, *inter alia*, of the criminal enforcement in the military. For the purpose of enforcing the powers of Criminal Investigations Department it is required, *inter alia*, to collect personal data for the purpose of solving crimes. All the data collection activities of the Criminal Investigations Department are performed in accordance with the provisions set forth in the general Israeli law, the provisions set forth in the Military Justice Law 5715-1955 and the supplementary military instructions.

134. In that manner, for example, when the Criminal Investigations Department performs wiretapping for the purpose of solving crimes, then these activities are performed in general in accordance with the provisions set forth in the Wiretapping Law 5739-1979 and the rules set forth in that law for the purpose of striking a balance between the rights of the individual and the requirements of the investigation. This is also the case with respect to searches, seizure of different materials and more, that are all done on the legal basis of the relevant laws and the balances they include.

135. Moreover, the Criminal Investigations Department receives full-time legal counseling by legal counsels that accompany the investigators of the Criminal Investigations Department and its commanders regularly and that help to assure to the balances that were set out by the legislator would be maintained as part of the enforcement of the law by this unit. This also helps in striking an ongoing balance between the needs of the investigation and individual rights.

136. Beyond these requirements, the IDF also takes action for the purpose of gathering intelligence for national security purposes. This activity also sustains the requirements set forth in Israeli law and international law regarding this issue; nevertheless, naturally, we cannot elaborate on the methods and actions that are performed for the purpose of collecting this type of data.

137. Finally, as stated above, the IDF manages a database of the soldiers that serve in the IDF in compulsory army and in reserve duty and prospective IDF soldiers. This database is necessary for the proper management of the army and it is protected carefully and managed in a manner that limits access to it to the minimal number of persons that require using it for the purpose of filling their position.

Supervision and control mechanisms

138. For the purpose of stressing the commitment of the IDF to the protection of individual rights with emphasis on the right to privacy, a directive that was published by the General Staff Instructions No. 02.0102 titled: "General Staff – Manpower Directorate" emphasizes specifically the right to privacy and the obligation to protect privacy. The directive states, *inter alia*, that the function of the Manpower Directorate in the IDF is, *inter alia*, the management of the main manpower databases and the enforcement of the Privacy Protection Law 5741-1981 in the IDF.

139. Accordingly, the IDF keeps personal data in a designated infrastructure (Mainframe) and from this mainframe the personal data is transmitted to a number of separate networks that operate in the IDF and to decentralized personal data systems that are operated in military entities. In this regard it should be noted that there are physical and computer protections in the IDF computer systems whose purpose is to prevent the leakage of data contained in them. Among other things, the information systems and the work stations in the IDF are connected by an internal network that is not connected directly to the global World Wide Web and so the risk that personal data that is stored on this network will leak is considerably lower.

140. The IDF database that includes data regarding the soldiers in the IDF and the prospective soldiers of the IDF is managed by the Head of the Planning and Organization Department (hereinafter: "Head of P&A") in the Manpower Directorate in the IDF (hereinafter: "Manpower Directorate") who is an officer in the rank of Colonel who was appointed for this position in accordance with military commands. The head of the information systems branch works under him and is an officer in the rank of Lieutenant Colonel, who is appointed as head of the security of the database.

141. Except for the responsibility of the Head of P&A to protect the privacy of the soldiers in the army and the prospective soldiers in the army in the IDF databases, military commands state that a commander whose unit keeps information systems is responsible to apply the measures that are necessary for the purpose of protecting their data. The measures that are applied are in accordance with the instructions set forth in the Teleprocessing Division and the Data Security Department as defined by the Head of P&A.

142. Administrative and disciplinary enforcement – in general data security instructions and instructions regarding the use of data in the IDF are set forth in binding instructions. Consequently, commanders in the IDF are authorized to conduct a disciplinary trial to soldiers who breached these provisions in accordance with the provisions set forth in the Military Justice Law 5715-1955. The powers of judicial officers, as part of the disciplinary enforcement mechanism in the IDF, is unique in terms of the scope of their application and even allow to instruct the actual imprisonment for considerable periods of time of those that violated these provisions in such manner that allows effective deterrence and considerable enforcement of privacy protection in the IDF databases.

143. Except for these powers for disciplinary enforcement, the military commands granted unique and significant powers to Planning Directorate entities that engage in the enforcement of the Privacy Protection Law and the relevant military commands with relation to the database of prospective IDF soldiers and the soldiers that already serve in it. And so, the following entities were granted the following powers, *inter alia*:

1. Monitoring the current activities of work terminals and stations that are connected to the IDF information database.
2. In circumstances in which arises a suspicion of breach of instructions related to the use of data or data security instructions, Planning Directorate entities are entitled to take unilateral actions such as disconnection of computer systems, cancellation of access permissions and more for the purpose of terminating the breach of these instructions and preventing additional breaches.
3. Filing a complaint against any soldier that breached instructions pertaining to the use of data and data security – even if his rank is higher than the rank of the complainant.

4. Giving an instruction to prosecute on the grounds of disciplinary violations (including a trial by the Head of P&A himself or a judicial officer he appoints for that purpose), the appointment of an investigations officer or even instituting an investigation in the Criminal Investigations Department, in circumstances in which violation of the instructions regarding use of data or data security instructions was detected.

5. Disqualification of soldiers who breached the instructions regarding the use of data or data security from serving in different positions in the manpower and adjutancy corps.

144. As a result of the powers that are granted as stated above, there is a full "circle" of administrative monitoring and enforcement on the use of the said database by the different Planning Directorate entities. As aforesaid, these entities engage regularly in the monitoring of access to personal data in the IDF computers; when irregular requests for data are detected, an inquiry is conducted in the relevant units, under the supervision of the Planning Directorate entities; concurrent with this inquiry, permissions for use by the user or the system that allegedly exceeded from the permissions that were granted are denied; in general, the unit is required to institute military or administrative proceedings according to the circumstances of the case.

145. In addition, military commands state that the Center of Encryption and Information in the Teleprocessing Division and the Data Security Unit in the Intelligence Division have corresponding powers in the field of data security, including monitoring, supervision and control with relation to all types of data and databases that were specified above. In addition, there are a number of IDF entities that operate for the purpose of creating a number of data security layers in the IDF and that include protection of personal data and, to a great extent, also enforce the requirements for protection of such data in terms of protection of privacy.

146. We shall further add that even the Medical Corps, which is responsible for the medical care provided to the IDF soldiers, applies a separate mechanism of monitoring unauthorized access to medical records in the IDF medical information system. This mechanism also monitors cases of irregular and unauthorized access to medical data. Entities in charge of the management of the data system demand from the different units to

conduct an inquiry and prosecute the persons responsible for disciplinary violations when necessary.

147. Criminal enforcement – as stated above, beyond the disciplinary enforcement mechanisms, the IDF also applies criminal enforcement mechanisms. These mechanisms are applied sparingly for the purpose of investigating serious cases in which the instructions of use of the data or the data security instructions were violated and for the purpose of prosecuting the persons involved in these events in a military court, if necessary, and according to evidence.

148. Therefore, enforcement in the IDF includes all enforcement components, starting from the stage of inquiry or investigation, through prosecution – whether disciplinary or criminal – and ending with punishment, including imprisonment.

149. In light of the foregoing we can see that the IDF maintains an internal multi-layer system that is intensive and effective and that provides protection of privacy and personal data protection to the data that is stored in the IDF databases. This system includes monitoring, supervision and control mechanisms, and disciplinary and criminal enforcement for the purpose of restricting the leakage of personal data and preventing any unauthorized access to IDF databases.

150. Regarding across-the-board supervision and control mechanisms, which also apply to the IDF operations, see in section 159 hereunder.

b) The Israeli Security Agency

151. The activities of the Israeli Security Agency (hereinafter: "ISA") and its powers are regulated in the Israel Security Agency Law 5762-2002. In addition, certain specific powers to obtain data by the ISA are regulated in other laws, for example in the Wiretapping Law 5739-1979.

152. Due to the unique nature of the powers that are granted to the ISA, and in order to ensure that the balance between the right to privacy and national security that the ISA is tasked with protection is maintained, the applicable legislation sets out several internal and external mechanisms of checks and balances, and especially with relation to personal data.

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

1. Section 11 of the Israel Security Service Law that deals with communication data, as well as the Wiretapping Regulations 5746-1986, stipulate the use of relevant data, on issuance of a permit or getting authorization by the Head of the ISA, in such manner that only the relevant agents, and only them, will be privy to the relevant data. Regarding communications data, the law states that the type of data that will be transferred to the ISA will be as needed for the fulfillment of the functions of the ISA and will be approved in rules issued by the Prime Minister. Regarding the permit granted by the Head of the ISA as mentioned above, such permit can be granted "after he has been convinced that it is required by the Service to fulfill its functions under this Law". The Law also requires that "the permit shall 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 Service is entitled to extend it in accordance with the provisions set forth in that section.

   Regarding wiretapping, the Wiretapping Law provides that wiretapping for the purpose of protecting national security may be approved by the Prime Minister or the Minister of Defense, should he be requested to give approval by the Security Agency Director, but only after giving consideration to the measure of violation of privacy. The law further provides that a wiretapping authorization must be concrete and must describe the identity of the person or the line to which the wiretapping had been approved, if their identity is known in advance, as well as the permitted manners of wiretapping. The authorization is valid for a maximum period of three months.

2. The Service is particularly cautious with respect to the protection of the data in its possession, *inter alia*, by ensuring compartmentalization with respect to access to data, setting out strict and specific data security arrangements, providing specific

training to the Service personnel regarding the use of data, regulating the manner of its storage and security and constant supervision of the use of sensitive data.

3. In light of the sensitivity of data, even in the Service itself the 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 to do so according to the instructions in the ISA.

154. In addition to the above, the internal control mechanisms also include administrative and legal supervision and control mechanisms, and oversight by the internal comptroller of the organization (the Service Comptroller). These entities conduct audits from time to time that also pertain, *inter alia,* to the conduct of the Service with relation to the data it possesses for security purposes.

155. The external supervision and control mechanisms include:

A. Periodic reports to the Attorney General, for the purpose of ensuring that the data obtained by the Service is used in accordance with the law:

1. Reporting pursuant to section 11 of the General Security Service 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 every three months.

2. Reporting pursuant to section 4(d) of the Wiretapping Law –the Service provides to the Attorney General data regarding licenses for secret monitoring that were issued under chapter B of the Law for national security purposes.

   Based on this report, the Attorney General conducts an inquiry with the Service on issues that in his opinion require such inquiry, 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, and while applying the instructions of the Attorney General in circumstances in which this is needed.

B. Parliamentary supervision – the General Security Service Law and the Secret Monitoring 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.

156. In addition to the above, see further information regarding across-the-board supervision and control mechanisms, which apply also to the ISA and its activity, in section 159 hereunder.

c) <u>General Provisions and Supervision Mechanisms that Apply to all the Security Agencies that were Specified Above</u>

157. It should be noted that section 19(b) of the Privacy Protection Law refers to the application of the law to "security agencies", defined for the purpose of this matter to include five agencies – Israel Police; the Intelligence Division in the IDF General Staff, and the Military Police of the IDF; Israeli Security Agency; Mossad; and the Witness Protection Authority.

Regarding the security agencies that were specified above, the law states that "A security agency or a person employed by it or acting on its behalf shall bear no responsibility under this Law for an infringement reasonably committed within the scope of their functions and for the purpose of carrying them out."

This section focuses on the personal liability of employees of the security agencies with regard to potential legal procedures under the Privacy Protection Law. The Legal protection provided by this section is limited to actions taken by these employees, which infringe the right to privacy, on the condition that the infringement is "reasonably committed within the scope of their functions and for the purpose of carrying them out" as aforesaid.

158. The security agencies are also mentioned in other contexts in the Privacy Protection Law: section 13 sets out a comprehensive right of a data subject to access data regarding him kept in a database, and the databases of the security agencies are specified as part of several exclusions of this right (despite this, we should note that there are other norms in Israeli law regarding transparency principles and the right to information, which require security agencies to provide some information under certain conditions); section 23b(b) states that security agencies may receive or transfer data for the fulfilment of their duties, unless prohibited by law or regulations.

159. Finally, we shall mention briefly the general institutional supervision mechanisms that are applied in the State of Israel with relation to all government bodies, including with respect to the security agencies specified above. The Supreme Court sitting as High Court of Justice is the principal body in this regard, and it adjudicated both as first and final instance in petitions against government authorities, both in specific matters and in matters of principle. In addition, different Knesset committees exercise important oversight functions, both as part of their regular activities and in their review of periodic reports (by virtue of specific laws) received by security agencies regarding their activities as stated above. In addition, the State Comptroller conducts periodic inspections of the different State authorities including the security agencies, and he is empowered to examines in-depth a variety of issues including data security and protection of privacy issues. The Database Registrar, working within ILITA, whose supervisory powers over the protection of privacy in databases also apply to the security agencies and their databases. 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 routine 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.

160. As a final note we reiterate that this document constitutes a general, survey that does not include the full details regarding the conditions and the restrictions that are set out in the different laws that were specified above. We note that there is a more elaborate survey of the provisions set out in a significant part of these laws as part of the experts' report on which the decision of the Commission from 2011 was based, *inter alia*.

We remain at your disposal for any questions and clarifications.