Bloomberg Law® Privacy & Data Security

Workplace Privacy Requirements: ISRAEL

Haim Ravia and Dotan Hammer, of Pearl Cohen Zedek Latzer Baratz, Tel Aviv, provided expert review of the Israel Workplace Privacy Requirements. [Last updated September 2017. – Ed.]

100. WORKPLACE PRIVACY — INTRODUCTION

Israel has no specific workplace privacy law. The main law governing data protection is the Protection of Privacy Law, 5741-1981 (PPL).[1] Additionally, Basic Law: Human Dignity and Liberty § 7(a)[2] states that "all persons have the right to privacy and intimacy." Sections 7(b)–7(d) of that law restrict entry into the private premises of a person without consent; prohibit searches of private premises, individuals, or personal effects; and protect the confidentiality of a person's conversations, writings, and records. Exceptions are made for laws "befitting the values of the state of Israel, enacted for a proper purpose, and to an extent no greater than is required" (§ 8). Israel does not have a complete written constitution, but Basic Laws have been held by the Israeli Supreme Court to have constitutional status.[3] The Israeli Law, Information and Technology Authority[4] (ILITA) acts as Israel's data protection authority and is responsible for enforcing the PPL.

300. BACKGROUND CHECKS

300.10. Laws and Regulations Governing Background Checks

- Protection of Privacy Law, 5741-1981 (PPL);
- Basic Law: Human Dignity and Liberty.

[1] Protection of Privacy Law, 5741-1981, *available in Hebrew at* http://www.justice.gov.il/Units/ilita/LawInfo/legislation/Pages/privacyprotectionlaw.aspx, *and at* https://www.nevo.co.il/law_html/Law01/087_001.htm. An unofficial English translation is available from the Israeli Ministry of Justice at http://www.justice.gov.il/En/Units/ILITA/Documents/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf. The translation is based on the official 1981 English translation, but as there is no official English translation for later amendments, the current translation is unofficial. A more up-to-date translation is available via WIPO at http://www.wipo.int/wipolex/en/text.jsp?file_id=347462.

[2] Basic Law: Human Dignity and Liberty, *available in Hebrew at* http://main.knesset.gov.il/Activity/Legislation/Documents/yesod3.pdf, and *in English at* http://www.knesset.gov.il/laws/special/eng/basic3_eng.htm.

[3] Israeli Law, Information and Technology Authority, "A Guide to Data Protection in Israel," § 2, *available in English at* http://www.justice.gov.il/En/Units/ILITA/Documents/AguidetodataprotectioninIsrael1.pdf.

[4] The Israeli Law, Information and Technology Authority website is *available in Hebrew at* http://index.justice.gov.il/Units/ilita/Pages/default.aspx, and *in English at* http://index.justice.gov.il/En/Units/ILITA/Pages/default.aspx.

300.20. Information Collection

300.20.10. Information Collection — In General

Broadly, Basic Law: Human Dignity and Liberty § 7(a) states that "all persons have the right to privacy and intimacy." Sections 7(b)–7(d) restrict entry into the private premises of a person without consent; prohibit searches of private premises, individuals, or personal effects; and protect the confidentiality of a person's conversations, writings, and records. Exceptions are made for laws "befitting the values of the state of Israel, enacted for a proper purpose, and to an extent no greater than is required" (§ 8). PPL § 1 states that no individual shall infringe the privacy of another without consent. Chapter One of the PPL was not intended as a database protection law and instead deals more with general privacy protection (e.g., phone tapping, spying, photographing a person in private). However, in *Database Registrar v. Ventura*[5], the Supreme Court of Israel held that requirements of Chapter One, which restrict certain privacy-invading conduct, apply to the subsequent processing of data gleaned from such restricted conduct in databases regulated under Chapter Two (dealing with traditional data protection).[6]

PPL § 7 defines "information" as "data on personality, personal status, intimate affairs, state of health, financial status, vocational qualifications, opinions and beliefs of a person." Further, "sensitive information" is "data on the personality, intimate affairs, state of health, financial status, opinions and beliefs of a person," and/or any information that the Minister of Justice deems sensitive, with the approval of the Constitution, Law, and Justice Committee of the Knesset (the Israeli legislature). However, with respect to the identical types of information set forth in the definition of "information" in comparison to the definition of "sensitive information," the PPL does not distinguish between information and sensitive information in reference to data protection in relation to databases. PPL § 11 states that any request to a person for information that will be kept in or used in a database must be accompanied by a notice indicating: (a) whether there is a legal duty to provide the information or whether a response is voluntary and subject to that person's consent; (b) the purpose of the information request; and (c) to whom the information will be given and the purpose for transferring the data. "Consent" under PPL § 3 must be informed, but can be either express or implied. There are several laws that apply to employers (as set forth below); however, employers should comply with these general information-gathering provisions of the PPL, as further interpreted by case law in the context of employment relations.

In *Database Registrar v. Ventura*, the Supreme Court of Israel held that a "person's private affairs" with respect to § 2(9) and § 2(10) include a person's address and telephone number, bank account number, and national ID number.

300.20.20. Information Collection Restrictions

300.20.20.10. Financial Information

If an employer wishes to collect financial information from an employee or applicant with the intention of storing and using such data in a database, the employer must provide a notice as required under PPL § 11. Since there is no law specifically requiring an applicant to disclose financial information, the employer must also receive consent before gathering any such information.

For more information on general information collection, see 300.20.10, above.

300.20.20.20. Criminal History

An employer should follow the general information collection rules when seeking information about an employee's or an applicant's criminal background, and in most cases, the employer is not allowed to request a criminal record of the employee or the potential employee.[7] There is an exception for jobs that involve working with children or persons with mental or developmental disabilities. Under the Law for the

---

5 *See Database Registrar v. Ventura, available in Hebrew at* http://src.bna.com/egz.

6 *See* Israeli Law, Information and Technology Authority, "A Guide to Data Protection in Israel," *available in English at* http://www.justice.gov.il/En/Units/ILITA/Documents/AguidetodataprotectioninIsrael1.pdf; *see also* Library of Congress, "Online Privacy Law: Israel," n.12, *available in English at* http://www.loc.gov/law/help/online-privacy-law/israel.php#_ftn12.

7 The Crime Register and Rehabilitation of Offenders Law, 5741-1981, *available in Hebrew at* http://fs.knesset.gov.il//17/law/17_lsr_300059.pdf.

Prevention of Employment of Sex Offenders in Certain Institutions, 5761-2001,[8] prior to hiring an adult, a covered institution must obtain a certificate of confirmation from the Israeli Police that the applicant is not a sex offender or otherwise barred from employment under the law.

For more information on general information collection, see 300.20.10, above.

300.20.20.30. Driving Records

The PPL does not specifically address driving records. Therefore, the general guidelines on information collection apply.

For more information on general information collection, see 300.20.10, above.

300.20.20.40. Work History and Educational Background

Work history and educational background may be referenced as vocational qualifications and thus may be considered as "information" under the PPL with regards to the duty to register a database under certain conditions. The general guidelines on information collection apply. Note, however, that under Employment (Equal Opportunities) Law, 5748-1988 art. 2A,[9] an employer is prohibited from asking for the applicant's military medical profile rating or using the rating in any decisions affecting acceptance of employment, terms, advancement, training, dismissal, or benefits except as set forth in Section 2A(c).

For more information on general information collection, see 300.20.10, above.

300.20.20.50. References

The PPL does not specifically address references. Therefore, the general guidelines on information collection apply.

For more information on general information collection, see 300.20.10, above.

300.30. Notice of Information Collection

PPL § 11 requires anyone requesting information from an individual to include a notice informing the individual: (a) whether there is a legal duty to provide the information or whether a response is voluntary and subject to that person's consent; (b) the purpose of the information request; and (c) to whom the information will be given and the purpose for transferring the data. "Consent" under the PPL must be informed, yet can be either express or implied. Additionally, anyone keeping a database: (a) containing information of more than 10,000 people; (b) containing sensitive information; (c) containing information about individuals that was not provided by them, that was not provided on behalf of them, or which they did not consent to; (d) that belongs to a "Public Entity" (as defined under the PPL); or (e) that is used for direct mailing services (as set forth under the PPL) must register the database with the Israeli Law, Information and Technology Authority (ILITA).

300.40. Access to, and Correction of, Information Collected

PPL § 13 grants every person the right to inspect, personally or through an authorized representative, information about him kept in any database. The database controller must enable access in Hebrew, English, or Arabic, at the request of the data subject. An exception exists for health information if the database controller thinks disclosing the data would be likely to severely harm or endanger the physical or mental health of the data subject. In that case, the database controller can instead provide the data to a physician or psychologist on behalf of the individual making the request. ILITA published on Jan. 31, 2017, guidelines regarding the right to inspect voice calls, video footage, and additional types of digital information stored by a database controller.[10] Such guidelines are not legally binding *per se*, but reflect ILITA's position and serve as guiding principles when ILITA exercises its supervisory and investigative

---

[8] Law for the Prevention of Employment of Sex Offenders in Certain Institutions, 5761-2001, *available in English at* http://index.justice.gov.il/En/Units/CommitteeExaminationPrevention/Pages/default.aspx.

[9] Employment (Equal Opportunities) Law, 5748-1988, *available in Hebrew at* https://www.nevo.co.il/law_html/law01/p214m1_001.htm, and *in English at* http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_127881.pdf.

[10] Registrar of Databases, Directive No. 1/2017, *available in Hebrew at* http://www.justice.gov.il/Units/ilita/subjects/HaganatHapratiyut/MeidaMerasham/Hanchayot/12017.pdf.

powers. It is also an example of ILITA's involvement with respect to privacy issues to adjust the PPL to changes in technology that were made since the PPL was originally legislated in 1981.

If the database controller keeps the data offsite (e.g., with a processor), PPL § 13A requires the database controller to provide the data subject seeking access with the location of the data processor along with an order, in writing, for the processor to provide access to the data subject.

PPL § 14 states that if a person inspecting personal information finds it incomplete, incorrect, out of date, or unclear, the person may request the controller of the database (or, if such controller is a non-resident, the processor of the database) to amend or delete the information. If the database controller denies the request, the denial must be made and explained in writing to the person who made the request.

If access to personal information or a request for correction or deletion is denied, the data subject can appeal to a Magistrate's Court under PPL § 15. The Magistrate will determine whether access should be granted or a correction or deletion of data allowed.

300.50. Employment Verification Requests

The PPL does not specifically address employment verification requests. PPL § 16 prohibits disclosure of any information in a database unless it is part of carrying out one's work, required by the PPL, or required by a court order in relation to a legal proceeding. Violation of § 16 is punishable by imprisonment of five years. Therefore, an employer should only provide verification information to a requesting party at the request of, or with the consent of, the data subject, unless otherwise required by law or ordered by a court.

500. HEALTH INFORMATION, MEDICAL EXAMINATIONS, AND DRUG AND ALCOHOL TESTING

500.10. Health Information — In General

Information on an individual's "state of health" is considered sensitive information by Protection of Privacy Law, 5741-1981 (PPL) § 7. In addition, under the Israeli Patients' Rights Law 1996, each person has a right that all medical records pertaining to him shall be kept in confidence and may not be disclosed unless the patient gives his consent or unless required under law or for treatment (there are other requirements pertaining to the use and disclosure of medical records that are beyond the scope of this document). Accordingly, anyone who collects health data must register[11] the database with the Israeli Law, Information and Technology Authority (ILITA) under PPL § 8(c)(2). Other than the registration requirement, the Protection of Privacy Regulations, 5746-1986 (Conditions for Possessing and Protecting Data and Procedures for Transferring Data between Public Bodies)[12] sets forth certain high-level data security requirements applicable to all databases, which requirements will be superseded in May 2018 when the new information security regulations take effect. PPL § 11 states that any request to a person for information that will be kept in or used in a database must inform the individual: (a) whether there is a legal duty to provide the information or whether a response is voluntary and is subject to that person's consent; (b) the purpose of the information request; and (c) to whom the information will be given and the purpose for transferring the data. "Consent" must be informed, yet can be either express or implied under PPL § 3.

Note also that under Employment (Equal Opportunities) Law, 5748-1988 art. 2[13] an employer is prohibited from discriminating against an employee or an applicant due to pregnancy or fertility treatments, and

---

[11] Israeli Law, Information and Technology Authority, "Focus on Registration and Fees," *available in Hebrew at* http://index.justice.gov.il/Units/ilita/Pages/MokedRishum.aspx.

[12] Protection of Privacy Regulations, 5746-1986 (Conditions for Possessing and Protecting Data and Procedures for Transferring Data between Public Bodies), *available in Hebrew at* https://www.nevo.co.il/law_html/Law01/087_004.htm.

[13] Employment (Equal Opportunities) Law, 5748-1988, *available in Hebrew at* https://www.nevo.co.il/law_html/law01/p214m1_001.htm, and *in English at* http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_127881.pdf.

requesting such information from employees or applicants may, in certain circumstances, be suggestive of discrimination.

500.20. Pre-Employment Health Questions

The PPL does not contain any provisions relating to pre-employment health questions. Therefore, the general guidelines on information collection apply.

For more information on health information in general, see 500.10, above.

500.30. Medical Examinations

The PPL does not contain any provisions relating to employee medical examinations. Therefore, any medical examinations an employer requires of employees must comply with the general rules in PPL § 11 for collecting and processing personal information, and the disclosure of the medical records is also limited. Note, however, that under Youth Labour Law, 5713-1953 § 11,[14] no one under the age of 18 can be employed until they have undergone a medical examination and been issued a medical certificate for employment. The pre-employment medical examination is free under Youth Labour Law § 9. Section 11 also allows for the Minister of Labour and Social Affairs to deem that certain jobs require "suitability examinations." Anyone under 18 wishing to work such a job must be examined by an authorized physician, free of charge, under § 9, to determine whether he is suited to such work. Anyone under 18 in work requiring "suitability examinations" must be re-examined at least every 12 months pursuant to Youth Labour Law § 12(a). If an exam determines that the individual is not medically fit for the work in which he is engaged, § 13 requires the medical institution to send a report to the Regional Inspector of Labour, to the individual's parents, and to the individual's employer. Finally, under § 16, if employment presents a particular danger to health, the above health examination requirements under the Youth Labour Law also apply to anyone under 21 years of age.

In addition, employees exercising their rights to social benefits due to sick leave, pursuant to the Illness Compensation Law, 5736-1976, must submit to their employer an illness certificate issued by a physician, though the certificate need not disclose the nature of the illness, the diagnosis, or other specific medical information.

Pursuant to Civil Service Law (Appointments), 5729-1959 § 29, candidates for positions in the Israeli civil service (government departments or agencies) must undergo medical examinations to determine whether they are suited for the position.

500.40. Drug and Alcohol Testing

The PPL does not contain any provisions relating to drug and alcohol testing in the workplace. Therefore, if an employer wishes to institute drug and alcohol testing, the general information collection provisions of PPL § 11 apply, together with the general approach in Israeli employment law that disfavors subjecting employees to sensitive procedures unless they are objectively justifiable for the proper performance of the job. While not specifically allowing an employer to test for drugs or alcohol, it should be noted that under Work Safety Ordinance (New Version), 5730-1970 § 202,[15] "no employed person shall intentionally and without reasonable cause do anything likely to endanger himself or another," which might include coming to work under the influence of drugs or alcohol. Under Work Safety Ordinance § 223, an employer is not liable for a violation of § 202 by an employee unless the employer failed to take reasonable steps to prevent the violation.

500.50. Genetic Data

The PPL does not contain any provisions relating to genetic data. However, under Genetic Information Law, 5761-2000 § 11,[16] no DNA sample can be taken nor can any genetic testing be conducted without

---

[14] Youth Labour Law, 5713-1953, *available in Hebrew at* https://www.nevo.co.il/law_html/law01/p175_001.htm, and *in English at* http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/36150/97928/F2017460185/ISR36150.pdf.

[15] Work Safety Ordinance (New Version), 5730-1970, *available in English at* http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/36158/97939/F1486776006/ISR36158.pdf.

[16] Genetic Information Law, 5761-2000, *available in Hebrew at* http://www.health.gov.il/LegislationLibrary/Poriut_09.pdf, and *in English at*

the subject's informed, written consent. As part of the informed consent process, the subject must be given an explanation of the significance of genetic testing to himself as well as to his relatives.

Genetic Information Law § 17 requires anyone who keeps genetic information identifiable by name or national ID number in a database to register the database pursuant to PPL §§ 8–9. In addition, the provisions of the PPL shall apply in the event that no other provision set forth in the Genetic Information Law applies with respect to a certain matter. Further, any person who within the scope of his work receives genetic information about an individual must keep it in confidence and can only use it with consent from the subject, and only in ways consistent with any consent received (Genetic Information Law § 18(a)). Genetic data can be transferred by genetic practitioners and researchers in accordance with Patients' Rights Law 1996 § 20.[17] Section 20 lists the conditions necessary to transfer a patient's medical information to a third party. Among others are: (a) with the patient's consent; (b) where required by law; or (c) the transfer is related to the treatment of the patient by another clinician or physician. Section 21 of the Genetic Information Law requires any communication of genetic data to avoid identifying the subject to the greatest extent possible.

Genetic Information Law § 29 relates to preventing discrimination in employment. Specifically, § 29(a) states that an employer shall not require an employee or applicant to provide genetic information or undergo genetic testing. Section 29(b) states that if an employer requires genetic information in violation of § 29(a) and the employee or applicant refuses, the employer cannot take negative action (e.g., refusal to hire or promote, decisions regarding employment terms, and termination of employment) based on the refusal. Section 29(c) bars the use of any genetic information in employment, including in relation to decisions to hire, fire, or promote. Finally, § 29(d) allows the Minister of Health, in consultation with the Minister of Labour and Welfare and with the consent of the Science Committee of the Knesset, to determine places of employment where genetic testing and information may be necessary for certain categories of work. In such cases, an employer can require genetic testing in relation to employment decisions.

700. EMPLOYEE MONITORING AND SURVEILLANCE

700.10. Employee Monitoring and Surveillance — In General

Basic Law: Human Dignity and Liberty § 7(a) states that "all persons have the right to privacy and intimacy." Sections 7(b)–7(d) restrict entry into the private premises of a person without consent; searches of private premises, individuals, or personal effects; and violation of conversational confidentiality or a person's writings or records. Protection of Privacy Law, 5741-1981 (PPL) § 1 states that "no person shall infringe the privacy of another without his consent." Infringement of privacy is defined in § 2 to include spying on a person in a manner likely to harass, any "listening-in" prohibited by law, and photographing a person in the private domain. In *Database Registrar v. Ventura*, the Supreme Court of Israel held that requirements of PPL Chapter One (containing §§ 1 and 2), which restrict certain privacy-invading conduct, apply to the subsequent processing of data gleaned from such restricted conduct in databases regulated under Chapter Two (dealing with traditional data protection).[18] In general, an employer cannot institute monitoring that could be construed as "spying," or "listening-in," without employee consent, and other terms as determined by Israel's National Labour Court in February 2011 in

https://www.jewishvirtuallibrary.org/jsource/Health/GeneticInformationLaw.pdf (English translation provided by jewishvirtuallibrary.org, a project of the American-Israeli Cooperative Enterprise).

[17] Patients' Rights Law 1996, *available in Hebrew at* http://www.health.gov.il/LegislationLibrary/Zchuyot_01.pdf, and *in English at* http://src.bna.com/mfw (English translation provided by the University of Haifa).

[18] *See* Israeli Law, Information and Technology Authority, "A Guide to Data Protection in Israel," *available in English at* http://www.justice.gov.il/En/Units/ILITA/Documents/AguidetodataprotectioninIsrael1.pdf; *see also* Library of Congress, "Online Privacy Law: Israel," n.12, *available in English at* http://www.loc.gov/law/help/online-privacy-law/israel.php#_ftn12.

the landmark case of *Tali Isakov Inbar v. the State of Israel – The Commissioner for Women's Labour Law*.[19]

700.20. Electronic Communications

PPL § 2(5) prohibits "copying or using, without permission from the addressee or writer, the contents of a letter or any other writing not intended for publication." There is an exception if the writing has historical value and is more than 15 years old. *Tali Isakov Inbar v. the State of Israel – The Commissioner for Women's Labour Law* (*Isakov Inbar*) is a 2011 landmark ruling from Israel's National Labour Court that directly addressed an employer's right to monitor employee e-mail.

In *Isakov Inbar*, the National Labour Court set forth the conditions under which employers can monitor employee e-mail. Based on the ruling, the following principles must be fulfilled by the employer in order for the monitoring to be legal:

1. *Legitimacy*: There must be concrete circumstances and situations in which the employer has a good reason to believe that the employee illegally uses the computer or uses it in a way that exposes the employer to third-party claims or that would damage its business.

2. *Proportionality*: The employer must avoid impairing the basic fundamental privacy right of the employee, and if such violation occurs, it must be proportionate and reasonable. The employer must examine alternatives for monitoring that are less intrusive. In addition, the employer should analyze the balancing of interests between the benefits of achieving the purpose of the monitoring and the damage to the privacy, dignity, and autonomy of the employee.

3. *Limited purpose*: The use of the information received from the monitoring will be limited to the initial goal of the monitoring, even if, as part of such investigation, the employer finds reason to believe that he should conduct further surveillance on other issues.

4. *Transparency*: First, the employer must set a clear policy regarding the allocation of virtual space for computer use and distinguish between the virtual space and technologies designated to the work and the virtual space and technologies available to the employee for his personal needs, considering the character of the workplace and its special needs. Second, the employer must inform the employee with maximum clarity about all existing information technologies in the workplace, including the boundaries of the permissible use of them, professionally and personally. In addition, the employer must specify the circumstances justifying general monitoring and specific monitoring, as well as the monitoring technologies and their nature. Furthermore, the employment contract has to include the employer's policy regarding the use of information technology, and the employer is encouraged to publish such policy in the employment handbook. Pursuant to the *Isakov Inbar* decision, the policy should preferably be drafted in cooperation with the labor union at the workplace (where relevant) or with representatives from among the employees.

5. *Consent*: Informed, explicit, freely-given, and written (to the extent possible) consent of the employee is a basic condition for monitoring and accessing employee's privacy. The employer has to obtain the employee's consent before monitoring is carried out. The consent has to be based on complete disclosure and transparency by the employer, after providing all required information to the attention of the employee. The National Labour Court also determined that it is appropriate that the requirement of informed and prior consent be included in the employment agreement and the workplace's procedures. The employee's waiver of his privacy rights must be explicit and in writing, shall be narrowly interpreted, and shall be valid upon exceptional circumstances only. The employee may request to be present at the time of access to the correspondence in his computer. Moreover, the employee's prior, informed, and voluntary consent is duly required to the workplace policy regarding monitoring activities and to any specific act of monitoring.

The ruling has distinguished between the categories of e-mail accounts available to employees in the workplace:

Professional e-mail: Professional e-mail is an e-mail account owned by the employer that is designated only for professional activities and professional correspondence of the workplace. Employees are

[19] *Tali Isakov Inbar v. the State of Israel – The Commissioner for Women's Labour Law,* Labor Appeal no. 90/08 (Feb. 8, 2011), *available in Hebrew at* http://www.law.co.il/media/computer-law/isakov_inbar_appeal.pdf.

forbidden to use it for private needs, including personal correspondence. The employer may monitor this mailbox and backup its data communications and data content, provided that he has fulfilled the principles set above. However, even if the employee uses the account for personal correspondence in contravention of employer policies prohibiting such use, the employer should not access the contents of the personal correspondence (yet monitoring and accessing the metadata of such correspondence is permissible). Such access is conditioned on the employer's serious concern or a reasonable basis to believe that the employee is involved in criminal activity or wrongdoing. Only then, and after the above principles are fulfilled, may the employer seek the consent of the employee to access the personal correspondence in the professional e-mail account.

Personal or mixed e-mail: The employer may choose to allocate the employee a "personal virtual space" in which personal correspondence is allowed. This account is also fully owned by the employer. Given the proper balance required between the employee's right to privacy in his personal correspondence in this account and the employer's right to protect his enterprise, the employer may not use technological means to monitor personal correspondence in accounts allocated for personal use. Accessing personal correspondence (whether in metadata or content) in this mailbox is not allowed except under exceptional circumstances, such as a serious concern of criminal activity or other wrongdoings of the employee. Only then, and after the above principles are fulfilled, may the employer seek the consent of the employee to access the personal correspondence in the personal e-mail account (provided, however, that they are not exterior-private e-mails—see below).

Exterior-private e-mail: Exterior-private e-mail is a personal e-mail account privately held by the employee that may be accessed through the employer-provided Internet connection. The ruling states that such an account is in the virtual "premises" of the employee, and the employee's protected privacy rights cover this account regardless of the employee's physical location when accessing the e-mail account. Employers may not rely on the employee's notice and consent of a workplace policy for accessing the exterior-private e-mail account of the employee.

Generally, access to such an account is only permissible pursuant to a judicial order. Even if the employee grants specific, informed consent, it is presumed that the employee would not agree to allow his employer access to a private e-mail account and would not consent voluntarily, but only out of professional obligation. Thus, employee consent is presumed invalid with regard to a private e-mail account—if the employer argues otherwise, the burden of proof to rebut these presumptions is on him.

Therefore, if the employer wants access to an employee's private e-mail, or if the employee does not provide his consent, the employer must turn to the Labour Court in order to obtain such right (we note that such court order will be given only upon very rare and exceptional circumstances).

700.30. Internet

The PPL does not directly address Internet use. While there is no case in Israeli jurisprudence similar to *Isakov Inbar* dealing with Internet monitoring, it is most likely that, because the privacy principles underlying *Isakov Inbar* are similar to those inherent in Internet surveillance, many of the same principles would likely apply if an Internet monitoring policy were challenged in the Labour Court. Therefore, an employer should promulgate a workplace Internet use policy specifying the allowable uses of company Internet resources in the workplace. This policy should be part of the employment contract and available in the employee handbook. Any monitoring should take place only in extreme circumstances where significant harm would be caused to the employer without surveillance. Extrapolating from the *Isakov Inbar* decision, monitoring should first be performed by automated means, and in extreme circumstances, flagged as requiring further review due to the potentially significant harm caused to the employer, follow-up review may be conducted by personnel. In addition, monitoring Internet communication of content or metadata of e-mail messages in an employee's personal webmail accounts is prohibited absent an appropriate court order, and a similar prohibition may hold true for monitoring the content or metadata of an employee's other HTTP/S communications of a private or personal nature, such as an employee accessing a personal bank account via the web, a personal online account of his health service provider, etc.

For more information, see 700.20, above.

700.40. Video Monitoring

PPL § 2 prohibits "spying on . . . a person in a manner likely to harass him . . ." as well as "photographing a person while he is in the private domain" without the individual's consent. PPL § 3 defines "photography" to include filming. By 2012, at least two Israeli Regional Labour Courts indicated the requirement of informing employees about the use of cameras.[20] A later decision by the Regional Labour Court in Haifa held that an employee has no privacy expectation in the public area of a workplace, where cameras may be installed.[21]

The courts distinguish between installing hidden cameras and visible cameras. In the event that the employer has installed visible cameras (that are not hidden cameras) in order to prevent crimes by customers or disciplinary offenses made by employees, such act shall be considered as a legitimate management tool, provided that the volume and duration of filming are related to the conduct of the business, and provided further that the employee knows that he is being filmed. It was also determined that there may be situations where placing a "hidden camera" would constitute an invasion of the employee's privacy, and that neither a hidden camera nor a visible camera may be installed in the employee's office or private workspace.[22]

On Aug. 29, 2016, ILITA published draft guidelines (in Hebrew) on using surveillance cameras in the workplace. The draft guidelines state that surveillance cameras may not be used in some public work areas such as bathrooms, changing rooms, and break rooms, and may be used to protect the employer's property, security, and cybersecurity systems in place to manage sensitive personal information, provided that they are not hidden. Also, managers may use cameras to monitor employees to ensure quality of customer service, all subject to fulfillment of additional principles such as legitimacy, transparency, and proportionality. The draft is based on the Israeli National Labour Court's judgment in *Tali Isakov Inbar v. the State of Israel – The Commissioner for Women's Labour Law* in February 2011. The draft guidelines further advise that employers who wish to install surveillance cameras to monitor the workplace may only do so after formulating a clear policy regarding how the footage will be used, the reasons for the surveillance, and the extent of the surveillance; this policy must be formulated in consultation with the employees or their representatives. Once the cameras are in place, employers may only use recorded footage as established in the policy. ILITA accepted public comments on the draft guidelines until Nov. 6, 2016. See "Israel Limits Workplace Use of Surveillance Cameras," *Privacy Law Watch* (Sept. 12, 2016).

700.50. Location Monitoring

PPL § 2 prohibits "spying on or trailing a person in a manner likely to harass him . . ." without the consent of the individual. Israeli case law has recognized the employer's legitimate interest in monitoring the location of its employees who work in "field" positions (such as sale agents, couriers, etc.), yet only during work hours, and subject to the principles of transparency, proportionality, and prior informed consent.

700.60. Telephone Use

PPL § 2 prohibits "spying on . . . a person in a manner likely to harass him . . ." without the consent of the individual. Presumably, this would apply to telephone use. It should be noted that, according to Israeli Eavesdropping Law – 1979, eavesdropping is considered a criminal offense punishable by imprisonment for a term of five years (§ 2(a) to Israeli Eavesdropping Law – 1979).

700.70. Searches and Inspections

Basic Law: Human Dignity and Liberty § 7(c) prohibits searches of the body or personal effects. Basic Law § 8 allows an exception only if provided by law "befitting the values of the State of Israel, enacted for a proper purpose, and to an extent no greater than is required." Therefore, presumably, an employer cannot search the person or the personal property of an employee without consent. The PPL provides

---

[20] *Eisner v. Richmond Knitting Factory* (Tel Aviv Reg. Ct., July 20, 2001), *confirmed in Salman v. Aleimi* (Nazareth Reg. Lab. Ct., Jun 20, 2012, appeal to the Nat'l Lab. Ct. withdrawn upon the appellant's request).

[21] *Malul v. Roni Amar Accountancy Servs. Ltd.* (Haifa Reg. Lab. Ct., Feb. 3, 2013, appeal to the Nat'l Lab. Ct. withdrawn upon the appellant's request).

[22] *Irena Belkireski v. Optica Halperin Ltd.*, 41111-02-12, *available in Hebrew at* http://src.bna.com/lW1.

that spying on or trailing a person in a manner likely to harass him, or any other harassment, is considered an infringement of privacy.

700.80. Biometrics

The PPL does not address biometrics. In 2009, the Knesset enacted the Inclusion of Biometric Means of Identification in Identity Documents and in an Information Database Law, 5770-2009.[23] The law and regulations promulgated thereunder had set out a trial phase spanning a number of years, during which enrollment in the database was voluntary. The trial phase ended in early 2017, when the Knesset legislated the permanent phase of the biometrics database project. Citizens desiring to issue or renew their national ID cards or passports must submit high-quality photos for facial recognition to the nationwide database. Fingerprint data may be voluntarily submitted and is only collected from individuals 16 years of age or older. A petition seeking to invalidate the biometrics database law on constitutional grounds of allegedly disproportional invasion of privacy was filed with the Israeli Supreme Court.

In a landmark decision delivered on March 15, 2017, the Israeli National Labour Court ruled that employers may not compel workers to use biometric time clocks at the workplace. The court noted that the mere sampling of fingerprints infringes a person's privacy and autonomy, as well as the additional violation of those rights arising from the risks of misuse or unauthorized use for purposes beyond those originally intended. The court concluded that absent a statute expressly permitting employers to compel employees to use biometric time clocks, employers may not require employees to give fingerprints, or any other biometric information, without their freely given consent.

On Dec. 18, 2012, ILITA published a manifest regarding the use of biometric attendance control in the workplace. According to such manifest, due to the bargaining power differences in employment relationships, such use shall be subject to the general principles of Israeli constitutional law, the central of which is the proportionality requirement. The employer is required to consider less offensive alternatives. In addition, the maintenance of the biometric data in a database significantly raises the information security risks. Therefore, it is recommended to keep the biometric information in smart cards rather than in databases. Collection of biometric data in the workplace may be disproportionate, unless there is a significant justification to such collection of data, such as a clear security interest.

For more information on general information collection, see 300.20.10, above.

900. PERSONNEL RECORDS

900.10. Personnel Records — In General

Since personnel records will inherently contain information on an individual's vocational qualifications, and may contain information on his personal status or economic position, such records qualify as "information" under PPL § 7 and may even be considered as "sensitive information." Therefore, these records are subject to the general information collection provisions of PPL § 11 and the database registration provisions of § 8.

Wage Protection Law (Amendment No. 24), 2008—Payslips and Unlawful Deduction of Wages[24] requires an employer to maintain records and include comprehensive information on employee payslips. Under art. 24(b), this includes, among others, the employee's name, ID number, workplace address, date of commencement of employment, seniority, number of hours worked, the calendar year period, number of working days and hours in the pay period, how many hours the employee worked, the number of vacation and sick days taken, and the remaining balance of each. The payslip must also indicate total wages paid;

[23] Inclusion of Biometric Means of Identification in Identity Documents and in an Information Database Law, 5770-2009, *available in Hebrew at* http://src.bna.com/sYd; *see also* Israeli Population and Immigration Authority, SmartID, "Questions and Answers," *available in Hebrew at* https://www.gov.il/he/Departments/Guides/questions_and_answers_smartid.

[24] Wage Protection Law (Amendment No. 24), 2008—Payslips and Unlawful Deduction of Wages, *available in Hebrew at* https://www.nevo.co.il/Law_word/law14/law-2162.pdf.

a breakdown of wages by regular time, overtime, vacation pay, sick pay, etc.; as well as any deductions taken, such as for income tax or health insurance payments.

For more information, see 300.20.10, above.

900.20. Access to, and Correction of, Personnel Records

PPL § 13 grants every person the right to inspect, personally or through an authorized representative, any information about him kept in any database. The database controller must enable access in Hebrew, English, or Arabic, at the request of the data subject. An exception exists for health information if the database controller thinks disclosing the data would be likely to severely harm or endanger the physical or mental health of the data subject. In that case, the database controller can instead provide the data to a physician or psychologist on behalf of the individual making the request.

If the database controller keeps the data offsite (e.g., with a processor), PPL § 13A requires the database controller to provide the data subject seeking access with the location of the data processor along with an order, in writing, for the processor to enable the data subject's inspection of his records.

PPL § 14 states that if a person inspecting personal information finds it incomplete, incorrect, out of date, or unclear, he may request the controller of the database (or, if the controller is a non-resident, the processor thereof) to amend or delete the information. If the database controller denies the request, the denial must be made and explained in writing to the person who made the request.

If access to personal information or a request for correction or deletion is denied, the data subject can appeal to a Magistrate's Court under PPL § 15. The Magistrate will determine whether access should be granted or a correction or deletion of data allowed.

900.30. Fees for Access to Personnel Records

Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal from a Denial of a Request to Inspect), 1981[25] sets the fee for access to personal information stored in a database pursuant to PPL § 13 at a minimal fee that was originally determined in 1981, has depreciated since then to nearly zero, and was not updated or linked to any price index.

900.40. Retention of Personnel Records

Any personnel records can be retained as the employer sees fit, but pursuant to ILITA's position (rather than any statutory provision or case law precisely on point), they are subject to the purpose limitation principle specified in § 2(9) of the PPL, under which a person may not use or disclose personal information for purposes other than for which the data subject's consent was given.

900.50. Disclosure of Personnel Data to Third Parties

PPL § 16 prohibits a person from disclosing any information in a database unless it is part of carrying out his work, required by PPL, or required under a court order in relation to a legal proceeding. Violation of § 16 is punishable by imprisonment of five years. Therefore, an employer should only disclose personnel data to a third party at the request of, or with the consent of, the data subject, unless otherwise required by law or ordered by a court. Also, § 2(9) of the PPL provides that a person may not use or disclose personal information for purposes other than those for which the data subject's consent was given.

[25] Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal from a Denial of a Request to Inspect), 1981, *available in Hebrew at* https://www.nevo.co.il/law_html/Law01/087_002.htm.

