XVIIth Meeting of European Labour Court Judges

12 June 2009

Grand Hotel Union
Miklošičeva ulica, 3
Ljubljana, Slovenia

General and national reports

Privacy in the workplace

General reporter:
Judge Alan C. Neal,
Employment Tribunal, UK

Belgium

Judge Koen Mestdagh,
Member, Labour Chamber of the Court of Cassation,
in collaboration with Dr. Ingrid Boone,
Legal secretary, Court of Cassation

PART 1. THE REGULATORY CONTEXT

1. The Belgian legal system does not possess a general **definition of "privacy"**. The notion of "privacy" refers to the respect for private life and family life. The concept of "privacy" covers information privacy (relating to intimate or sensitive information, such as details regarding beliefs or trade union affiliation) as well as medical privacy, communication privacy and personal autonomy or self-determination.

2. The **Belgian Constitution** provides a limited catalogue of constitutional rights, drafted in very general terms. The right of respect for private life is laid down in article 22 of the Constitution. This article was inserted in the Constitution in 1994. The text reads as follows: "Everyone is entitled to respect of his private life and his family life, except in the cases and under the conditions determined by law. The law, the decree, or the ruling stipulated in article 134, guarantee the protection of that right."

The right to respect of private correspondence is particularly protected by article 29 of the Constitution, that states: "The secrecy of letters is unviable. The law shall determine which officers are responsible for the violation of the secrecy of the letters entrusted to the postal services".

3. Belgium adheres to several **international instruments** that contain provisions relating to privacy.

The right to privacy is protected by:

- Article 8 of the European Convention on Human Rights (ratified by Act of 13 May 1955);
- Article 17 of the International Convention on Civil and Political Rights (ratified by Act of 15 May 1981);
- Convention of the European Council of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal data (ratified by Act of 17 June 1991);
- Articles 7 and 8 of the Charter of Fundamental Rights of the European Union of 12 December 2007;

- EU-Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- EU-Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector;
- EU-Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);
- ILO-Code of Good Practice, Geneva, 1996.

4. Norms established at the international level are **transposed into protections or rights for citizens at the domestic** level in different manners, depending on the nature of the international instruments.

- With regard to article 8 of the European Convention on Human Rights (ECHR) the Belgian Court of Cassation has ruled that this article applies directly to the law and prohibits violation of the private life of individuals by government (Cass. 26 September 1978). More recently the Court of Cassation has also accepted that article 8 ECHR applies directly to conflicts between private parties (so called "horizontal effect") (Cass. 27 February 2001 and Cass. 2 March 2005).
- In order to be able to ratify the Convention of 28 January 1981, Belgium has adopted general data-protection legislation with specific rights and obligations regarding the processing of personal data (Act of 8 December 1992 on the protection of the privacy in relation with the processing of personal data (Data Protection Act), see question 7).
- In order to bring Belgian data protection legislation in line with Directives 95/46/EC and 97/66/EC, the Data Protection Act has been amended by the Act of 11 December 1998.
- Directive 2002/58/EC is implemented in Belgian law by the Act of 13 June 2005 on electronic communication.

5. Several legal rules dealing with issues of privacy come from specific collective bargaining agreements (CBA), concluded within the National Labour Council, which is a public body where the main trade unions and employers' associations are represented. The rules established in these CBA's (see below, question nr. 7) **only apply to the private sector**.

6. There are no **groups of workers**, other than public sector workers, that are treated differently from the "normal model" in relation to rules on privacy. However, there is a specific CBA with regard to recruitment and selection (CBA nr. 38 of 6 December 1983). Article 11 of CBA nr. 38 stipulates that the private sphere of the applicant will be respected during the selection procedure. This implies that questions with regard to the private life of the applicant may only be justified if such questions are relevant in light of the nature of the job and/or the conditions of performance of the function (the so-called "relevancy principle").

Although this CBA nr. 38 only covers recruitment and selection, its underlying principles may also be used for post-entry cases.

7. The Belgian framework of rules dealing with issues of privacy

Besides the international instruments and constitutional guarantees mentioned above, Belgian law contains several rules dealing with specific aspects of "privacy".

Mention should be made of the following rules:

Acts:

- Act of 8 December 1992 on the protection of the privacy in relation with the processing of personal data (Data Protection Act; see question 13): this Act contains a general data-protection legislation with specific rights and obligations regarding the processing of personal data. The Act is applicable to private and public entities that collect and use personal data and subjects the data processing to a detailed list of principles and obligations very similar to the provisions of Directive 95/45/EC. This

general Act is completed with provisions in other laws that provide for data protection in specific fields, such as consumer credit and the organization of the so-called Social Security Crossroad database.

- Act of 30 June 1994 for the protection of the private life against listening in, taking knowledge and opening of private communication and telecommunication: this Act penalizes wiretapping. It provides penalties for the crimes of interception of communication by a public official or civil servant (art. 259*bis* Criminal Code) and for breaches of the secrecy of private communications and telecommunications (art. 314*bis* Criminal Code) during the transfer of a private communication between other parties, in cases not foreseen by law.
- Act of 13 June 2005 on electronic communications: the Act implemented the European directives on the new electronic-communications regulatory framework. It protects the secrecy of the existence of a communication amongst third parties, including the identification of the persons involved, and prohibits the intentional revealing of information related to a communication taking place via electronic means, without the consent of the parties concerned. Several exceptions to this principle of secrecy of communication are provided (see question 15).
- Act of 21 March 2007 on the installation and the use of surveillance cameras: this Act applies the principles of the Data Protection Act to protect privacy in relation with the processing of personal data to the practice of camera surveillance, unless expressly stated otherwise in the Act. The Act also adds some specific requirements. It does not apply to the use of camera surveillance at the workplace (see hereafter, CBA nr. 68).

Collective Bargaining Agreements (CBAs)

- Art. 11 of the CBA nr. 38 of 6 December 1983 with regard to recruitment and selection: this agreement protects the privacy of applicants during the selection period (see question 6).
- The use of cameras in the workplace is subject to regulation in CBA nr. 68 of 16 June 1998 relating to the protection of the privacy of employees in relation with camera surveillance on the work floor (see question 15).
- CBA nr. 81 of 26 April 2002 on the protection of privacy of the employees in relation with control of electronic on-line communication: this agreement sets rules on the control of electronic on-line communication data at the workplace, in an attempt to clarify the constitutional and legal rights and principles relating to privacy on the one hand, and the secrecy on communications on the other (see question 15).
- CBA nr. 89 of 30 January 2007 on the prevention of theft by employees and exit-control: this agreement imposes specific rules to the employer relating to the control of employees when leaving the workplace.

The text of the above mentioned laws and CBA's can be found at: http://www.ejustice.just.fgov.be/wet

PART 2. THE STATE AND THE EMPLOYER

8. As far as the employer is entitled to retain "intimate" or "sensitive" personal information such as related in the question about a member of its workforce (see questions 13 and 14), the **State authorities are not entitled to obtain this information** from him.

This doesn't mean that the employer can't reveal such information when heard as a witness against a member of its workforce who is under criminal investigation.

The employer is only obliged to provide the National Social Security Service with the necessary information to establish the rights on social security benefits of the members of its workforce, which doesn't include "intimate" or "sensitive" information. If such information is needed, for instance the National Unemployment Office needs information on family/marital status to determine the due amount of unemployment benefits, the worker has an obligation to provide this information himself.

9. The implementation of **surveillance of a workplace** by the State authorities is entirely covered by the rules on "special investigation methods" determined by articles 47*ter* to 47*septies* and 56*bis* of the Code of Criminal Procedure (CCP).

A "systematic observation" of persons, goods or places, this is an observation during more than five consecutive days or during more than five non-consecutive days over a period of one month or with the use of technical devices or with an international character (art. 47*sexies*, § 1, CCP), can only be carried out by police officers assigned by the Minister of Justice, under control of the public prosecutor (art. 47*ter*, §1, CCP) or the investigating judge (art. 56*bis* CCP). The public prosecutor or the investigating judge can only authorise an observation if they esteem it necessary for the investigation as ordinary police methods are insufficient to reveal the truth (the so-called principle of "subsidiarity"). An observation with the use of technical devices can only be authorised if serious indications of serious criminal activities exist (art. 47*sexies*, § 2, CCP). The authorisation of an observation has to be given in writing prior to starting it up. Only in a case of urgency the authorisation can be given orally but then needs to be confirmed in writing as soon as possible (art. 46*sexies*, § 5, CCP). The authorisation of an observation has to be motivated, in particular with respect to the existence of serious indications of criminal activity and its necessity to be able to reveal the truth (art. 47*sexies*, §3, CCP).

PART 3. THE EMPLOYER AND THE WORKER

10. In Belgian labour law, there is no general norm recognizing the **right to privacy of workers**. Nevertheless, the fundamental right to privacy, protected by article 8 ECHR and article 22 of our Constitution as well as by specific legislation (see question 7), plays an important role in labour relations. The right to privacy of workers covers all forms of privacy: information privacy (relating to "intimate" or "sensitive" information, such as details regarding beliefs, off-duty conduct, trade union affiliation or health), but also medical privacy, communication privacy and personal autonomy or self-determination.

11. As for citizens in general, the **right to privacy of workers is not absolute** (see Cass. 27 February 2001). It is limited by the employer's right to direct and manage the workplace, confirmed in article 17 of the Employment Contracts Act of 3 July 1978.

12. Employer's right to obtain personal information about a member of its workforce

In view of the employers right to direct and manage the workplace (see question 11), the employer has a legitimate interest in personal information (e.g. about the health and medical condition) of job applicants or employees. The employer's right to obtain (personal) information about a job applicant or member of his workforce is not absolute. Neither is the applicant's/employee's right to privacy. Therefore, the rights and interests of both parties should be reconciled. In this regard, Belgian labour law uses the principle of *relevancy*. This principle implies that questions concerning the applicant's or worker's private life can only be justified if such questions are relevant to the nature of the job and/or the conditions of performance of the function. The principle of relevancy is an established principle in Belgian labour law, largely inspired by article 11 of CBA nr. 38, referred to above (question 6).

It is important to note that relevancy is linked with the issue of equal treatment and non-discrimination. The link is made in article 3 of CBA nr. 95 of 10 October 2008 on equal treatment during all phases of the labour relation. It stipulates that the employer can not make a distinction on the grounds of *age, sex or sexual orientation, civil status, medical history, race, colour, national or ethnical origin, political or ideological belief, handicap or membership of a trade union or another organisation*, if these are not related to the job or the nature of the company, except in cases where this would be legally required. The same principle of equal treatment applies to the recruiting employer (art. 2*bis* CBA nr. 38). It is clear that this principle limits the employer's right of investigation and information: the worker or applicant can not be obliged to disclose (personal) information whenever the employer's investigation has to be considered illegitimate. This is the case when the employer asks personal information in order to treat workers or applicants in violation of the principle of equal treatment (e.g. discrimination on the ground of ideological belief or sexual orientation). The connection between the employer's right to investigate and the prohibition

of discrimination has already come up before the Belgian Labour Courts/Tribunals in pregnancy discrimination cases.

Some examples to illustrate how the abovementioned principles are applied to specific matters:

- *Criminal history of an employee*: in principle, the criminal history of an employee is part of his or her private life. However, exceptions should be made whenever such criminal information can be considered as relevant for the job. The Belgian Labour Courts seem to be reluctant to take criminal information into account as relevant for the job. It has been judged e.g. that a vehicle repairman was not obliged to disclose to his employer any information regarding past convictions regarding theft.
- *Trade union affiliation*: the employer can only inquire with regard to such affiliation if he or she is able to show that this is relevant to the job. E.g. it is argued that in case of a job with a trade union or trade union related organisation, the employer can take the applicant's trade union membership into account, to verify whether the applicant has not committed himself or herself already to another trade union. In some cases however, the knowledge by the employer of an employee's trade union affiliation becomes inevitable, e.g. when the employee is acting on behalf of a trade union at the employer's premises or when employees are candidates for "social elections" (these elections are held every four years to elect the worker's representatives for the company's work council and health and safety committee).

13. The conditions under which an employer in Belgium is entitled to **retain** (whether in the form of personal files, or electronically) **personal information about a member of its workforce** are determined by the Act of 8 December 1992 on the protection of the privacy in relation with the processing of personal data (Data Protection Act or DPA). This Act also applies to labour relations. It is applicable to both automatic and manual processing of personal data.

- Art. 4 DPA enumerates the general conditions to the lawfulness of processing personal data: personal data must be processed fairly and lawfully; must be collected for specific, explicit and legitimate purposes (***finality*** *principle*); must be adequate, relevant and not excessive in relation to the purposes for which it is collected and processed (*principle of* ***proportionality***). Moreover, the person responsible for the processing of personal data must provide the data subject with specific information, such as the purposes of the processing, the persons to whom the data will be passed on (art. 9 DPA - *principle of* ***information or transparency***). These three principles (finality, proportionality and information/transparency) are considered to be crucial for the protection of the privacy.
- The DPA provides for specific rules for the processing of "sensitive data", being personal data revealing ***racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership*** as well as data concerning ***health or sex life***. It is stipulated that the processing of such personal data is, in principle, prohibited. Only in limited circumstances, provided by the law, is such processing lawful, e.g. if processing is necessary for the purpose of carrying out the specific obligations and rights of the employer in the field of employment law or if processing is necessary for the exercise or defence of legal claims (art. 6 DPA).

  The issue of ***health-related data*** is covered by article 7 DPA. As is the case with sensitive data, the processing of health-related personal data is, in principle, prohibited, except in a number of specific cases, such as if processing is necessary for the protection of public health or for the prevention of a specific danger.

  With respect to ***criminal record*** information, article 8 DPA stipulates that the processing of personal data relating to litigations that have been submitted to courts and tribunals as well as to administrative judicial bodies, relating to suspicions, persecutions or convictions in matters of criminal offences, administrative sanctions or security measures, is prohibited. There are a limited number of exceptions to this prohibition (e.g. the processing under the supervision of a public

authority or ministerial officer within the framework of the Code of Civil Procedure, if processing is necessary for the fulfilment of their duties).

- The employer must inform the employee that he collects personal information about that employee and must provide him with specific information, such as the identity of the person responsible for the data processing, the purpose of processing and the persons or authorities to whom the information is passed on (art. 9 DPA). The employee has the right to obtain communication of the data as well as to appropriate correction thereof (art. 10 and 12 DPA).
- The employer is required to register the fact that he processes personal data to a supervisory authority, the Privacy Commission (art. 17 DPA).
- The employer can employ specialist companies to hold and manage personal data. The employer and/or the specialist company processing personal data, must implement appropriate technical measures to protect the confidentiality and security of the data (art. 16 DPA).
- Personal data cannot be kept longer than necessary for the purposes for which they are collected and used (art. 4, § 1, 5° DPA). The employee has the right to obtain the removal of data kept after this period (art. 12 DPA).
- The disclosure of personal data to third parties is a form of "data-processing" according to article 1 DPA. Thus, it is subject to the principles and obligations of the DPA.

14. Medical data

- Article 20,2° of the Employment Contracts Act of 3 July 1978 stipulates that the employer must take care that the work is performed in decent circumstances of health and safety within the enterprise. The employer therefore has a duty of care and is the first person responsible for health and safety in the company. In this view, the employer has a legitimate interest in obtaining medical information.

  However, ***questions with regard to the applicant's or worker's health, disability or medical history*** can only be justified if such questions are relevant to the nature of the job and/or the conditions of performance of the function (principle of relevancy, see question 12) or in cases where this would be legally required. The latter is the case for staff belonging to specific categories indicated by law, often referred to as "functions with an increased risk" (e.g. workers who are exposed to occupational diseases or who are entrusted with security tasks).

  The worker or applicant cannot be obliged to disclose information about his or her medical history or disability whenever the employer asks this information in order to treat workers or applicants in violation of the principle of equal treatment (discrimination on the ground of medical history or handicap; see question 12).

- As already mentioned, article 7 DPA prohibits, in principle, the collection and use of health related data. This prohibition does not apply if the data subject has given his or her ***written consent*** to the processing of this data on the understanding that the consent may be withdrawn at any time.

  However, the Royal Decree of 13 February 2001 stipulates that if the processing of health-related data is only made lawful on the basis of the consent of the data subject (employee), this processing is still prohibited if the controller of the processing is the current or potential employer of the data subject, except if the data processing has the purpose of providing an advantage to the employee. This implies that at least another justification than consent for the collection of medical data is needed.

- The performance of ***medical examinations*** in the employment context is delegated to a medical practitioner, mostly the "company practitioner". This is a medical doctor hired or paid by the employer, who takes care of the health of the employees.

- In some cases, the law prescribes a medical examination. As already mentioned, this is the case for staff that is hired and comes under specific categories indicated by law, often referred to as "functions with an increased risk" (e.g. workers who are exposed to occupational diseases or who are entrusted with security tasks). During the employment relationship, there are also several medical examinations prescribed by law. There are periodical examinations for staff employed in "functions with an increased risk", as well as ad hoc examinations, e.g. in certain cases of modification of the job. The employees are obliged to undergo these legally prescribed medical examinations, if they want to keep their jobs.

  It must be stressed that the company practitioner is bound to observe his professional secrecy. No medical information, gathered during the prescribed examinations, can be communicated to the employer, except for the conclusion whether or not the employee is fit for the job.

- As a general rule, ***genetic testing*** in the employment context is considered to be prohibited, because of the right to privacy of applicants and employees. However, genetic testing with regard to certain diseases in the interest of the employee, could be defended, in so far as specific guarantees for the individual concerned are put in place.

  There are no specific rules in Belgian law dealing with ***psychological testing*** of employees or applicants. There is also a lack of case law in order to give guidance on the issue. Reference is made to the general right to privacy and the principles relating to this right (relevancy, non-discrimination…).

15. Surveillance of workers at the workplace

- The use of ***video surveillance*** on the workplace is regulated in CBA nr. 68 of 16 June 1998. This CBA applies the principles of the Data Protection Act (finality, proportionality and information/transparency, see question 13) to the issue of camera surveillance on the work floor.

  Finality: camera surveillance on the work floor can only be used for one of the specific purposes indicated in article 4 CBA nr. 68: 1° security and health; 2° protection of the company goods; 3° control of the production process (control of machines, in order to evaluate their technical functioning, and/or control of employees, in order to evaluate or improve the organisation of the work); 4° control of the work performed by the employee. Depending on the purpose, the camera surveillance could be permanent or temporary.

  Proportionality: the camera surveillance must be adequate, relevant and not excessive in relation to the purposes for which it is used. If the camera surveillance interferes with the private life of the employee, specific guarantees apply to make sure the interference is limited to a minimum (art. 7-8 CBA nr. 68).

  Information: he employer must provide the working council or the employees with specific information on all the aspects of the camera surveillance (art. 9 CBA nr. 68).

  It is important to note that a decision by the Court of Cassation of 2 March 2005, stated that video images (showing theft by a worker) could be used in a criminal case, although the images had been obtained by the employer without observing the rules of CBA nr. 68. It may be deduced from a recent decision by the Court of Cassation of 10 march 2008, that not only in criminal cases, but also in employment and dismissal cases, ***unlawfully obtained evidence*** could be allowed by the judge, under certain conditions (relating to the reliability of the evidence and the right to a fair trial).

- The ***control of electronic on-line communication data*** at the workplace is regulated in CBA nr. 81 of 26 April 2002. This CBA determines how the principles of finality, proportionality and transparency of the Data Protection Act need to be applied to the control of employee on-line communications. The agreement states that the employer shall only control on-line communications data of his employees for the prevention of illegal activities, activities contrary to morality, or activities that may harm the dignity of another person, for the protection of the confidential information and interests of the company, for ensuring safety and proper technical functioning of

the network, or for controlling the compliance with the company's ICT-use regulations (art. 5 CBA nr. 81). In the latter case, the employer is not entitled to immediately identify the employee who does not respect the ICT policy, but shall first launch an information campaign stating that breaches have been spotted and that upon repetition thereof, the employee(s) concerned will be identified and sanctioned. The employee, however, is entitled to a hearing by the employer before sanctions are taken (art. 16-17 CBA nr. 81). In any case, the employer installing a system to control on-line communications data has to inform the working council or the employees on all the aspects of the control (art. 7-8 CBA nr. 81).

Furthermore, the Act of 13 June 2005 on electronic communications protects the secrecy of the existence of a communication amongst third parties, including the identification of the persons involved, and prohibits the intentional revealing of information related to a communication taking place via electronic means, without the consent of the parties concerned (art. 124).

Article 125 provides for exceptions to this principle of secrecy of communication, for example, if the law allows or imposes taking knowledge of the existence of the communication, for the good functioning of the network and network service, for emergency services and for preventing SPAM.

Especially relevant to labour relations is article 128, that allows the recording of electronic communications and the related traffic data carried out in the course of lawful business practice or other professional communication, when all parties are informed in advance of the recording, the precise purposes thereof, and the time period for which the recording will be stored.

Article 129 prohibits using electronic communication networks for the storage of information for gaining access to information stored in the terminal equipment of the user or subscriber, such as cookies and spy-ware. Such use is only allowed when the subscriber or the user concerned are informed in a clear and comprehensive way in accordance with the Data Protection Act, and when he is offered the right to refuse such processing.

- As far as ***traditional communications*** (post, telephone calls, …) are concerned, reference should be made to article 29 of the Constitution, that protects the secrecy of letters, and to article 314*bis* Criminal Code, that penalizes breaches of the secrecy of private communications and telecommunications during the transfer of a private communication, without consent of all the persons taking part to this communication.

16. Body search

- There are no circumstances where an employer in Belgium is entitled to conduct a physical body search of a member of his workforce.

  A search of the intimate parts of the body can only be ordered by the investigating judge or the criminal court (art. 90*bis* Code of Criminal Procedure).

  Body surface searches can be carried out by the police, according to the rules set out by article 28 of the Police Act of 5 August 1992.

  CBA nr. 89 of January 1997 on the prevention of theft, imposes specific rules to the employer relating to the control of employees when leaving the workplace (applying the principles of finality, proportionality and transparency to this issue). It states clearly that only the employee's *goods* carried by him or kept in his vehicle, may be controlled. This implies that the employee's body cannot be subject to control by the employer.

- An employer who carries out a body search to an employee would be violating the right to respect of the employee's physical integrity. This might constitute a serious fault (or even a crime), giving the employee reason to end the employment contract immediately.

17. Duty of confidentiality

- The employee's right to confidentiality of personal information held by the employer is an aspect of the general right to privacy. The Belgian concept of privacy indeed contains what is understood as "information privacy". This relates to the confidentiality of information regarding an individual, certainly if it regards intimate or sensitive information, such as details regarding beliefs or health.
- The disclosure of personal data held by the employer to third parties is a form of "data-processing" according to article 1 Data Protection Act. Thus, it is subject to the principles and obligations of this Act (see question 13). One of the rules laid down in the DPA implies that the employer processing personal data of his employees, must implement appropriate technical measures to protect the confidentiality of the data (art. 16 DPA).

  Passing on sensitive information to third parties is only lawful in specific cases, e.g. if this is necessary for the purpose of carrying out the specific obligations and rights of the employer in the field of employment law (art. 6 DPA).

18. Justifications for interfering in the privacy of employees

Reference can be made to the relevancy principle and the various applications of the principle of finality (in the Data Protection Act and in CBA's), described above.

e.g.:

- CBA nr. 68 of 16 June 1998: *camera surveillance* on the work floor can only be used for one of the specific purposes indicated in article 4: 1° security and health; 2° protection of the company goods; 3° control of the production process (control of machines, in order to evaluate their technical functioning, and/or control of employees, in order to evaluate or improve the organisation of the work); 4° control of the work performed by the employee.
- CBA nr. 81 of 26 April 2002: the employer can only *control on-line communications data* of his employees, for one or more of the following purposes (art. 5): 1° the prevention of illegal activities, activities contrary to morality, or activities that may harm the dignity of another person; 2° the protection of the confidential information and interests of the company; 3° ensuring safety and proper technical functioning of the network; 4° controlling the compliance with the company's ICT-use regulations.

19. Notification of intrusions into the privacy of employees

See above, the principle of information/transparency laid down in the DPA and various CBAs.

e.g.:

- CBA nr. 68 of 16 June 1998: the employer must provide the working council or the employees with specific information on all the aspects of the *camera surveillance* (art. 9 CBA nr. 68). If the camera surveillance interferes with the private life of the employee, specific guarantees apply to make sure it is limited to a minimum (art. 7-8 CBA nr. 68).
- CBA nr. 81 of 26 April 2002: the employer installing a system to *control on-line communications data*, has to inform the working council or the employees on all the aspects of the control. Furthermore, the employer is only entitled to identify an employee who does not respect the ICT policy, if he first launches an information campaign stating that breaches have been spotted and that upon repetition thereof, the employee(s) concerned will be identified and sanctioned.
- Article 128 Act of 13 June 2005 allows the *recording of electronic communications and the related traffic data* carried out in the course of lawful business practice or other professional communication, when all parties are informed in advance of the recording, the precise purposes thereof, and the time period for which the recording will be stored.

20. Contractual provisions

The right to privacy is a fundamental right, protected by numerous imperative law-rules. A contractual provision permitting the employer to breach the privacy of a member of its workforce, contrary to these imperative rules, would be invalid (null and void).

21. Personal files on the computer belonging to the employer

There are no special rules in Belgian law concerning personal files or documents created or saved by a worker on a computer belonging to the employer at the workplace.

It is argued that the general right to respect of privacy also applies to this issue. The Labour Court of Brussels e.g. has stated in a recent case that personal files saved by an employee on the company's computer fall under the privacy protection (Labour Court of Brussels decision of 3 May 2006). The Labour Court of Liège, however, stated otherwise (decision of 11 January 2007).

Part 4. Miscellaneous procedural and other matters

22. Mechanisms to deal with the regulation of "privacy" at the workplace

The same mechanisms used to deal with more traditional issues that may arise between employers and workers are being used or can be used to deal with the regulation of "privacy" as between employers and workers.

The obligation to provide the working council or the employees with information on all aspects of video surveillance or control of electronic on-line communication data (see question 19) is the key to the mechanisms to deal with a collective dispute. The provided information could at first lead to a discussion between the workers representatives and the employer in the working council or between the trade union delegates and the employer. It could eventually lead to a strike, involving mediation by a mediator from the Ministry of Employment.

This actually happened a few years ago in a case that even made it to an item in a TV news program. An employer had installed a video surveillance system, according to him just to monitor the production process with the purpose to improve it. The workers though felt that they were being watched constantly and demanded the removal of the system. When the employer refused one of the trade unions took him to court and asked the local Labour Tribunal in summary proceedings to deliver a court order forbidding the use of that video surveillance system. At the same time the bigger trade unions called for a strike. The workers indeed went on strike. With the assistance of a mediator from the Ministry of Employment an agreement was finally reached. As a result the court case started by the smallest trade union became irrelevant and the proceedings were aborted.

This particular case demonstrates that court action also can be used to deal with the regulation of "privacy" at the workplace but isn't very effective to solve problems that may arise pending employment.

It is also important to note that the CBA 's nr. 68 and nr. 81 (see question 15) are declared generally binding by Royal Decree. According to article 56 of the Collective Bargaining Agreements Act of 5 December 1968, the employer who disrespects the obligations laid down in a CBA which is declared generally binding by Royal Decree, commits a criminal offence. Thus Labour Inspection officers can examine, be it on their own initiative or after receiving a complaint, whether an employer is acting in compliance with the CBA 's nr. 68 and nr. 81. If the Labour Inspection officer finds this is not the case, he has the authority to order the employer to make the necessary amendments. If the employer fails to do so, the officer can charge him, which could lead to the employer being criminally prosecuted or being fined by the Ministry of Employment.

The Data Protection Act or DPA (see question 13) provides for a mechanism that isn't part of the usual mechanisms put in place by Labour Law but can also be used to deal with privacy at the work place. As the employer is required to inform the Privacy Commission that he is processing personal data (art. 17 DPA), this allows the Privacy Commission to examine the particular "data-processing" set up by the employer.

The Privacy Commission can make a recommendation on its own initiative (art. 30 DPA). The Privacy Commission can also examine complaints and mediate between the parties concerned. If this doesn't result in an agreement, the Privacy Commission gives its opinion and can at the same time make a recommendation (art. 31 DPA). Failing to inform or preventing the Privacy Commission to examine the case is also a criminal offence (art. 39 DPA).

23. The last decade **issues of "privacy" arise regularly before the Belgian Labour Courts/Tribunals**, nearly always in dismissal cases. In most of these cases the worker claims that the employer has unlawfully obtained the presented evidence for the invoked ground for his dismissal, such as abusive use of electronic communications and internet facilities at the workplace or other wrong conduct. The judge is then asked to disregard the evidence obtained by making use of camera surveillance or by inspection of the worker's web-browsing, electronic or traditional communications or "personal" files created on a computer belonging to the employer at the workplace.

One example to illustrate: a specialised job agency accused its employee of acting as a stock trader during working hours and using the company computer for that purpose. The employee was immediately dismissed without notice and without compensation. The letter of dismissal mentioned a list of websites the employee had consulted for his trade. The employer also found spreadsheets with details on the evolution of stock ratings. The employee was also accused of having browsed porn sites during 3 full days. The URL's of these sites, most of them had very explicit names, was also mentioned in the letter of dismissal. To prove all this, the employer presented a "view access log" of the employee's web-browsing.

The employee demanded to disregard the presented evidence claiming violation of article 314bis of the Criminal Code (breach of the secrecy of private communications and telecommunications during the transfer of a private communication between other parties) and violation of the old, since abolished Telecom Act (intrusion into electronic communication with fraudulent intention).

The employee's demand was rejected and it was ruled that the employer had due grounds for immediate dismissal. The court considered that article 314bis of the Criminal Code didn't apply to the case because the "view access log" wasn't made during the transfer of a private communication. The court also considered the employer had no fraudulent intention because he had serious indications that the employee was taking care of his personal affairs instead of working. To this was added that even if the employer hadn't respected the old Telecom Act, he was entitled to do so since the employer is entitled to control if the employee respects his obligations laid down in the Employment Contract Act of 3 July 1978 (Labour Court of Ghent decision of 9 May 2005).

It's important to notice that the fact took place before the CBA nr. 81 of 26 April 2002 on the protection of privacy of employees in relation with control of electronic on-line communication was drafted.

24. Trial proceedings are public (art. 149 of the Constitution, art. 757 Code of Civil Procedure). Unlike the Criminal Courts/Tribunals, the Labour Courts/Tribunals can not exclude the public from (part) of the hearing if it risks jeopardising public order or morality.

However, trial proceedings in the Labour Courts/Tribunals generally don't attract a lot of audience which makes it easy for the judge, if he wishes to do so, to make sure that except for the Court and the parties concerned, nobody else is present at the hearing. As long as it is not made impossible for the public to be present by closing the doors.

25. The freedom of press is guaranteed by article 25 of the Constitution that states that **no censorship can be established**. Consequently, there are no provisions which enable particular proceedings in the Labour Courts/Tribunals not to be disclosed in the press.

However, proceedings in the Labour Courts/Tribunals rarely get the attention of the media. If a particular proceeding is disclosed in the press, it is generally because one of the parties concerned seeks media attention. Therefore it is unlikely that the proceedings in a case involving evidence of an intimate or embarrassing nature would be disclosed in the press.

Although the judgement must always be pronounced in public (art. 149 of the Constitution), the judgment and the official records of judicial proceedings are not available to the general public. In principle only the

parties concerned have access to the official records of judicial proceedings and can get a copy of the judgment. If a judgment is given free for publication in a law journal or data base, it is made anonymous.

Finland

President Pekka Orasmaa
Jorma Saloheimo
Labour Court of Finland

Part 1. The regulatory context

1. Does your legal system possess any general definition of "privacy"?
   - If so, please indicate the content and source of that definition. If not, how have notions of "privacy" been approached in your country conceptually, in academic writings, or as matters of socio-legal policy?
   - ***There is no general definition of privacy in the Finnish legal system. The concept "private life" used in the Constitution is based on the provisions in the European Convention on Human Rights and it has nearly the same effect and interpretation.***
   - ***Personal data has been definied as any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household. (Personal Data Act)***

- Does your country have a Constitution, and does this make any provision in relation to "privacy" for citizens (whether at work or otherwise)?

  The Constitution of Finland includes the following provisions on the right to privacy (Section 10):

  The right to privacy

  Everyone´s private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act.

  The secrecy of correspondence, telephony and other confidential communications is inviolable.

  Measures encroaching on the sancity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act. In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sancity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act.

2. Does your country adhere to International Instruments which contain provisions relating to "privacy" (e.g. at the level of the Council of Europe, etc.)?
   - If so, please indicate which instruments and when your country signed up to, or ratified, each of those instruments.

   As a member state of ILO, the Council of Europe and European Union Finland has implemented or ratified all the international instruments concerned.

The Personal Data Act (1.6.1999) accommodates the EU Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the of personal data and on the free movement of such data).

There are special regulations concerning the processing of personal data in other laws and acts as well. The Act on the Openness of Government Activities controls the access to public registers. The protection of privacy is also controlled by the Act on the Protection of Privacy and Data Security in Telecommunications. This Act has implemented the Directive 2002/58 EC.

3. As a general matter, how are norms established at the international level transposed into protections or rights at the domestic level for citizens in your country?

   - Please illustrate this by reference to any International Instruments mentioned in relation to Q.3.

See above.

4. Are public sector workers/officials in your country subject to a different regime from private sector staff in relation to rules on "privacy"?

   - If so, please indicate what the differences are, and whether there can be said to be broad equivalence between the different regimes.

The Act on Data Protection in Working Life (759/2004), applies to civil service relationships and to comparable relationships under public law. The Act relates to state, municipal and church officials or to people in the service of independent public institutions. At the same time, civil servants are also covered by certain special provisions, including those of the Act on the Publicity of the Activity of the Authorities, the Register Act, the Act on State Officials, the Church Act etc.

5. Are any groups of workers (other than public sector workers/officials) treated differently from the "normal model" in relation to rules on "privacy"?

No.

6. Please describe briefly your national framework of rules dealing with issues of "privacy". Where these are contained in legislation or administrative regulations, please indicate the sources *[and, if possible, please attach a copy/version of the relevant provisions]*.

The Act on Data Protection in Working Life entered into force on 1st October 2004. The Act supplemented the former Act on Protection of Privacy in Working Life (477/2001). The purpose of the Act is to respond to questions concerning the protection of private life specifically in the area of working life. Thes scope of the Act is confined to the relationship between employee and employer.
The Act lays down provisions on the processing of personal data about employees, the performance of tests and examinations on employees and the related requirements, technical surveillance in the workplace, and retrieving and opening electronic mail messages addressed to the employer. Important provisions of the Act regulate requirements of processin personal data. The Personal Data Act (523/1999) and the Act on the Protection of Privacy in Electronic Communications (516/2004) include general provisions relating to data protection which are also applied in working life beside the special Act on Data Protection in Working Life.

Part 2: The State and the employer

7. Please outline the areas in which the State authorities in your country are entitled to obtain personal information from an employer about a member of its workforce.

   - In particular, please indicate whether the State authorities possess such powers in relation to nationality or national origins; residence status; work permit status; previous employment

records; criminal records; tax status; family/marital status; medical records, health and/or disability-related material; bank account information (e.g. for payment of wages); trade union membership.

Personal data may in general be processed, for instance, for purposes of historical or scientific research, statistics and for purposes of official planning and reporting. Personal data may be processed also for purposes of a public register, as follows: identifying data on the data subject, his/her spouse, children and parents, data on the connecting factor on the basis of which the public register has been compiled and related data, as well as the data subject's contact information.

Most of the data specifically referred to in the question are defined as sensitive information under Chapter 3 of the Personal Data Act. As a general rule, processing such information is forbidden. The Act lists certain exceptions to this prohibition, but none of these seems to mandate state authorities to obtain information from an employer.

8. Please indicate whether the State authorities in your country are entitled, under any circumstances, to implement surveillance of a workplace (electronic, video, visual observation, etc.) for the purpose of obtaining personal information about any member of the workforce?

   - In particular, please indicate whether the State authorities possess any special powers of this kind in the context of measures intended for "combating terrorism" or in relation to investigation of serious criminal activities (e.g. drug dealing, "money laundering", etc.).

There is detailed legislation on means and procedures available for the police when investigating serious crimes listed in the Act. These rules are in principle applicable also at a working place.

Part 3. The employer and the worker

9. Does a worker in your country enjoy any form of "right to privacy"?

   - If so, what form or forms does this right take? How is that right reflected in the legal system of your country?

10. To what extent (if at all) is any "right to privacy" for a worker more limited **when that person is at work** than any "general right to privacy" enjoyed by citizens in general?

11. Under what conditions (if at all) is an employer in your country entitled **to obtain** (e.g. by way of questions contained in job application forms) personal information about a member of its workforce?

    - In particular, please indicate the position in relation to the following specific areas (and please add information about any other matters which are of particular significance in your country):
      - information about the address, telephone contact numbers, etc. of the worker
      - information about the marital status of the worker
      - information about the health and medical condition of the worker (including, for example, details of the worker's personal doctor)
      - information about the sexual orientation of the worker
      - information about the religion of the worker
      - information about the political affiliation or activities of the worker
      - information about the tax (fiscal) affairs of the worker
      - credit information about the worker
      - court information (e.g. for enforcement of court orders by way of deductions from salary – "attachment of earnings")
      - information about any criminal convictions which the worker may have

An employer may process only personal data that are directly necessary as regards an employee's employment relationship, relating to the management of the rights and obligations of the parties to the employment relationship or the benefits provided to employees by the employer or which are due to the special nature of the work. No exception may be made to the data having to be necessary even with the employee's consent, and this requirement of necessity shall be implemented alongside the other more detailed provisions of the Act.

In connection with the planning of data collecting already, an employer must define the necessity for examining the data in such a way that it is evident for which kinds of tasks the personal data are to be collected. This kind of assessment must always be performed in each case separately.

For practical reasons, it is impossible to list all of the personal data which an employer is entitled to process. Situations in working life vary according to sector or task. An employer requires an employee's personal data for a variety of reasons such as for the authorities when dealing with taxation and social security payments, for the management of the personnel administration and development of the organisation, for customers etc. As regards personal data concerning the collecting of which some other act lays down separately, an employer no longer needs to consider the necessity of collecting the data.

Data that are necessary as regards managing an employer's and employee's rights and obligations include, for example, data relating to the performance of tasks, selection of an employee, working conditions and compliance with the regulations in collective agreements. Data relating to the benefits provided by an employer can relate, for example, to swimming pool tickets and discounts provided by an employer and to the use of these. Data based on the special nature of work can relate, inter alia, to the family circumstances of an employee who is to be transferred to assignments abroad whenever the employer is responsible for the education of the children.

In recruitment situations, an employer has to assess the necessity for data with regard to the job which the person has applied for. This mainly means data showing the applicants competence and suitability and also a statement on the job applicant concerning his or her suitability health-wise for the job.

12. Under what conditions (if at all) is an employer in your country entitled **to retain** (whether in the form of personal files, or electronically) personal information about a member of its workforce?

    - In particular, please indicate the position in relation to the specific areas mentioned in Q.12 (and please add information about any other matters which are of particular significance in your country).
    - Is an employer in your country obliged to tell the worker that it is holding personal information about that worker and/or to make any such information available to the worker for inspection (e.g. to ensure the accuracy of the information)?
    - Are there any provisions in your country which require the employer to handle such information in a particular way?
        - For example, is the employer required to register the fact that it holds such information with a public official (a “data protection commissioner” or the like)?
        - Does the employer personally/physically have to retain such information under its control at the workplace, or can it employ specialist companies to hold and manage any such data?
        - Is the employer required to destroy such information after a certain period of time?
    - Are there provisions in your country which regulate the freedom of the employer to disclose or pass such information to third parties (including to the public authorities)?

Outdated or unnecessary data must not be kept. The provisions of the Personal Data Act on this matter are also applied in working life. Such provisions include § 9(2), § 29, § 34 and § 35, and § 48(2).

The legislation contains special provisions on the retention periods for personal data which an employer must comply with. These provisions include, for example, the periods of limitation according to the Contracts of Employment Act, Working Hours Act and the Bookkeeping Act. In public administration there are also special regulations on the retention of personal data on employees and officials

Personal data refer to all kinds of records describing the characteristics or living conditions of an employee. Personal information can be information that is written or recorded mechanically, electronically, optically or magnetically but not solely oral information unless it is based on information recorded in a personal data file.

Processing of personal data refers to the collection, recording, organising, use, transfer, surrender, retention, alteration, combining, protection, deletion and destruction of personal data and to other measures affecting personal data.

Personal data register refers to a file that is kept manually or by means of automatic dataprocessing. The employer is the controller. The delegation of the management of employment relationships to an outside body does not remove the position of controller or obligations from an employer. Nevertheless, it has to be observed that an implementer of occupational health services has an independent position as a keeper of a personal data fie that does not depend on an employer. For this reason, a personal data file of an occupational health person and an employer 's personal data file must not form an entity.

An employer must primarily collect personal data from the employee personally because, in that way, the employee is best able to determine what data are being collected about him or her. If an employer collects data from elsewhere, he or she must obtain the employee's consent for this. Consent is not required whenever an authority passes on information to an employer for carrying out a duty that is laid down for the latter in law or whenever an employer obtains personal credit data or criminal record data in order to ascertain an employee's trustworthiness. In those cases, too, it is required that the personal data obtained are necessary as regards the employment relationship.

An employee's credit data can be necessary in jobs where the person will have direct financial responsibility for the employer's assets or whenever the employment relationship otherwise calls for particular trust. The Personal Data Act (§ 20 (4)) lays down rules concerning when personal credit data may be passed on and the fact that an employer must also notify a job applicant of the acquisition of credit data if their use will affect decision-making (§ 25(2)). On the other hand, the Criminal Record Act and Decree regulate the purposes for which criminal record data can be surrendered and to whom.

At some workplaces, particular information is required on the trustworthiness of personnel. These workplaces can include airports, nuclear power stations, telecommunications operator centres, certain ADP service companies, production plants and research institutions, and the authorities. For these jobs, the Act on Safety Clarifications is applied. The Act includes provisions on the grounds for these c1arifications.

If an employer obtains information in order to determine the trustworthiness of an employee, the employer should, prior to obtaining the information, tell the employee of its intention to obtain such information. This obligation to notify relates not only to personal credit data and criminal record data but also to other data obtained in order to ascertain trustworthiness which an employer collects on the basis of an employee's consent elsewhere than from the employee personally. An employer must notify an employee personally of

data that are collected elsewhere than from the employee personally, and of their content, before the data are used in decision-making affecting the employee. The employer is obliged to inform the employee on his own initiative.

13. In addition to the situations mentioned in Q.12 and Q.13, are there any circumstances under which an employer in your country is entitled to obtain (or to demand) medical details about a member of its workforce?

    - In particular, please indicate whether there are any situations in which an employer is obliged to obtain information about the health of the worker (e.g. before permitting that worker to perform tasks at heights, or where there may be exposure to dangerous substances or radiation during the course of performing the job).
    - Is there any procedure laid down for an employer in your country to obtain the formal consent of a worker to accessing such personal medical information?
    - Is an employer in your country entitled to ask specific questions about whether a member of its workforce is "disabled"? – If so, what are the consequences if the worker refuses/fails/chooses not to disclose such information?
    - Can an employer in your country require a worker to submit to a medical examination, and subsequently have access to the results of that medical examination (e.g. where the employer is considering dismissing the worker on grounds such as "capacity", or "fitness to do the job", or because of a high level of absences from work for medical reasons)?
    - Is an employer in your country entitled to make use of (and act on the basis of information obtained as a result of) techniques such as "psychological testing" or "genetic testing"?

      Health information is defined as sensitive information, and so an employer's right to process data on an employee's health has been particularly restricted in law.

      An employer may process an employee's health information solely if the employee personally supplies him or her with them or if the employee has given written consent for such information to be passed on to the employer. Whenever an employee personally passes on information relating to his or her health, this meets the characteristics of consent.

      An employer is entitled to process information on an employee's health which contain information on the diagnosis if it is necessary

      - ***for the payment of sick leave pay or comparable health-related benefits (e.g., a visit to a doctor, during which is agreed that salary will be paid, for the purposes of examinations or treatment without the employee being incapable of work) or***
      - ***in order to determine whether there is a justified reason for absence from work.***

      An employer can also process an employee's health information if the employee specifically wants his or her capacity for work to be investigated on the basis of information of this kind. This means, for example, information which is of significance as regards the employee's health and development of working conditions at the workplace or if an employee, who is unwilling to use occupational health services, wishes to investigate his or her impaired capacity for work without being completely incapable of work.

      As a general rule, an employer can not require an employee to submit to a medical examination. Civil servants are an exception to this rule. Also, if an examination is necessary due to a special occupational health risk, an employee may not refuse it without a valid ground. An employer's interest in clarifying the reasons for the employee's absence from work would not as such warrant him to order the employee to undergo a health check. It is another matter that an employee who does not provide such clarification runs the risk of loosing his or her right to sickness pay.

An employer is also entitled to process an employee's health information in those situations and to the extent to which it is laid down separately elsewhere in legislation, such as legislation on safety at work and occupational health. An employer can process, inter alia, statements provided by health care professionals concerning an employee's capacity for his or her job that are based on a health examination if the assessment does not contain detailed information on the diagnosis.

The aforesaid also applies to a job applicant. Job application forms must not include questions about detailed health-related information but, rather, the questions ought to be restricted in such a way that they relate to the nature of the work, bearing in mind solely the information that is of significance as regards managing the tasks.

Health information on an employee may be processed solely by those individuals who prepare decisions on the basis of the said information or enforce them. For this reason, an employer must designate the individuals who have to process health information or define the duties which involve processing of data concerning health. In order to safeguard the confidentiality of information on health, the individuals who process health information on employees are also under an obligation to maintain secrecy and may not divulge information to outsiders. The obligation to maintain secrecy also continues after the end of the employment relationship. The Act does, however, include a provision according to which the employer may submit the medical certificate given to him by the employee to the occupational health care for the implementation of occupational health care, unless the employee has prohibited any submitting.

An employee's health information must be kept separately from other personal data collected by an employer. Sensitive data must be removed from the personal data file as soon as there is no ground for examination and the need for retaining information has to be assessed by the employer in any case at least every five years (Personal Data Act, § 12(2)).

An employer must not require a job applicant or an employee to take part in genetic testing. As regards others tests, such as personality and aptitude assesment, a job applicant or employee can be tested only if he or she gives his or her consent for this. Tests can be conducted if their purpose is to determine prerequisites for carrying out tasks or the need for training or other professional development. In accordance with the aforesaid, the results obtained by means of tests should be directly necessary as regards the employment relationship of each employee. This requirement in fact restricts both the content of tests and their scope, since there are differences in requirements between different professions and tasks.

14. Is an employer in your country entitled to implement any forms of surveillance of workers at the workplace?

- In particular, please indicate whether there are any situations in which an employer is entitled to make use of the following:
  - CCTV (video surveillance)
  - Monitoring and inspection of web-browsing by the worker
  - “Keystroke monitoring” of workers performing computerised tasks
  - Monitoring and inspection of a worker’s electronic communications (eMail, social networking websites, etc.)
  - Monitoring and inspection of a worker’s traditional communications (post, telephone calls, etc.)

The law provides for the right to implement camera surveillance in premises where employees are working, although the purpose of the observation may not be the

surveillance of the employees. The employer may conduct camera surveillance, if the purpose of the observation is to ensure the personal safety of the employees and other persons working in the premises, to protect property or supervise the adequate operations of productional processes, or to prevent or clarify situations endangering safety, property or productional processes.

As a rule, camera surveillance must not be used for observing a certain employee or certain employees at the working place. There must not be any camera surveillance in the toilets, locker rooms or social premises of the employees. It is also prohibited in working rooms which have been assigned for the personal use of the employees.

If camera surveillance is necessary, it can, however, be focused on a certain place of work, where there are employees working, if

- its purpose is to prevent apparent threat of violence related to the work of the employee, or apparent disadvantage or danger to his safety or health, or

- observation is necessary for preventing and c1arifying crimes against property, if an essential part of the employee's tasks consists of handling property that is significant as to its value or quality, such as money, bonds or valuables, or

- the interests and rights of the employee should be secured, if the camera surveillance is based on the request of the employee.

The surveillance of electronic comminications is regulated in the Act on the Protection of Privacy in Electronic Communications (2004). Under the Act, an employer does not have access to the contents of personal messages of an employee. The Act is, however, not quite so absolute when it comes to access to identification data, meaning data which can be associated with an individual subscriber or user and which is handled in communications networks for the purposes of transmitting, distributing or providing messages (e.g. IP address or receiver of message). Any corporate subscriber, such as an employer company, may under certain conditions that are regulated in detail handle identification data if this is necessary to detect, prevent or investigate unauthorized use of internet services or suspected disclosure of business secrets. A set of amendments to this regulation, nicknamed "Lex Nokia", was adopted after a heated debate in 2009. It was said that that major companies and other business life organizations exercised pressure under the preparations of the law amendment in order to achieve relaxations to these rules. The Government Bill also raised doubts as to the compatibility of the new provisions with the constitutional right to privacy, and the Constitutional Committee of the Parliament indeed made a number of further changes in the proposed provisions before the Bill was accepted.

15. Are there any circumstances where an employer in your country may be entitled to conduct (e.g. by security staff belonging to the enterprise) a physical (possibly including intimate) body search of a member of its workforce?

    - What would be the consequences if the worker refused to submit to such a search?
    - What would be the consequences if an employer carried out such a search without the consent of the worker?

    An employer is not entitled to conduct a physical body search of an employee. Carrying out such a search would amount to a punishable offence.

16. Is an employer in your country subject to any recognised "duty of confidentiality" in relation to members of its workforce and/or others?

    - If so, what is the extent of any such duty, what form or forms does this duty take, and how is that duty reflected in the legal system of your country?

17. Under what circumstances can an employer in your country justify breaching the "privacy" of a member of its workforce or any "duty of confidentiality" owed to a worker in its employment?

- In particular, please indicate how this might be the case in relation to:
  - the employer's business interests (e.g. protection of trade secrets)
  - supervision of security at the workplace
  - prevention of criminal activity (drugs abuse, etc.)
  - when required to act under instructions from the public authorities (e.g. as part of a police investigation)

It is obvious that the parties to an employment contract have an "duty of confidentiality" towards each other. The duty is not expressly provided for, but it can be derived from the general duties laid down int the Employment Contracts Act (2001). Only a very important ground, such as perhaps the prevention of serious crime, migh warrant the breach of the duty.

18. Is it possible for an employer in your country to justify intrusions into the privacy of members of its workforce by giving clear notice that particular measures are in use (e.g. signs stating that the workplace is subject to CCTV surveillance)? - ***No.***

19. Is it possible for an employer in your country to include contractual provisions in the terms of the employment relationship which effectively permit the employer to breach the privacy of a member of its workforce? - ***No.***

20. Are there any special rules in your country concerning "personal" files created by a worker on a computer belonging to the employer at the workplace?

- Is there any guidance in relation to who "owns" any rights in relation to such "personal" files?

The assessment of whether a message belongs to the employer may in practice only happen on the basis of the information concerning the sender's identification data or the title space in the e-mail address. This information does not belong to the core substance of a confidential message. Although in most cases, it is possible to conclude from this information whether the message is private or not, this is not always possible. For this reason, the precondition for retrieving e-mail messages is additional criteria which all must be fulfilled before the e-mail is brought out:

- ***the employee attends to his tasks independently, which as a rule means that others do not attend to the matter at the same time***
- ***because of the tasks or pending matters of the employee it is obvious that the abovementione d messages have been sent to him***
- ***the employee is absent from his work***
- ***before beginning to open the e-mail, the employer offers the employee an opportunity to give his consent to the opening***
- ***clarifying the matter of the message does not endure delay.***

The law also includes a special provision for situations where the employee has died, or he is permanently hindered from performing his work tasks, in which case his consent to disclosing the messages cannot be had.

The employer can only use his right by means of a person using the authority of the main user of the data system. A written c1arification has to be made to the employee on the retrieving of the message, unless it leads to the opening of the message. Neither must the

persons involved in the retrieving of the message reveal the content of the message during the employment relationship, nor after its termination.

After disclosing the message, the message may be opened, if on the basis of the above-mentioned c1arification it is obvious that it clearly belongs to the employer and fulfils the criteria described above. A precondition is also that attempts have, without results, been made to contact the sender or recipient of the message in order to find out the content of the message or to send it to another email address assigned by the employer.

A written notification of the opening of the message has to be given to the employee. The same requirements concerning the persons involved in the opening and the same secrecy provisions as in the disclosure of the message also apply to the opening. The Act on the Protection of Privacy in Electronic Communications also generally includes provisions on the prohibition of taking advantage of messages not intended for the recipient.

Part 4. Miscellaneous procedural and other matters

21. Please provide a brief overview of the mechanisms in place in your country to deal with the regulation of "privacy" as between employers and workers.

The legislation on worker participation includes provisions, according to which the purpose of camera surveillance, passage control and other surveillance done by technical methods, introduction and the methods use for it as well as the use of e-mail and data networks are matters to be handled through the cooperation procedure. The cooperation procedure must be implemented before decisionmaking on the matter. Fundamental changes to the monitoring method also fall within the scope of the cooperation procedure. With regard to e-mail and the other data network, the cooperation procedure mainly applies to operational rules.

In those companies and public corporations such as municipalities which the cooperation acts do not apply to, the employer should provide employees or their representatives with an opportunity to be heard before decision-making on corresponding matters.

Following the cooperation or hearing procedure, the employer must define both the purpose for which monitoring is to be used and the monitoring methods to be employed and the principles relating to the use of electronic mail and a data network. After this, the employer must make sure that employees are notified of the content of the decision.

Sanctions for violating cooperation legislation have been laid down, inter alia, in the Act on Cooperation within Undertakings. On the other hand, if an employer violates its aforesaid obligations to define and notify, he or she can be ordered to pay a fine for violating the Act on Data Protection in Working Life.

Compliance with the Act is supervised by the occupational safety and health authorities together with the Data Protection Ombudsman. Where necessary, they can also provide advice on the application of the Act.

22. Do issues of "privacy" arise before the Labour Courts/Tribunals in your country, and, if so, what form do these tend to take?

The issues of "privacy" do not normally arise before the Finnish Labour Court.

23. Do the procedures of the Labour Courts/Tribunals in your country make provision for private/secret hearings in particular circumstances:

- In particular, please indicate whether this might be the case in relation to:
  - national security
  - cases involving disability or medical evidence of an intimate or embarrassing nature
  - cases where allegations are made that criminal acts been committed by a party or witness

- cases where allegations are made of sexual or other abuse, and/or where the evidence may involve disclosure of intimate sexual or other acts by a party or witness

According to the Act on Publicity of Court Proceedings (370/2007), publicity of proceedings and court records is the main rule and the exceptions are specifically provided for. The Act is applicable to general courts and, among certain other courts, the Labour Court.

Under the Act, the court may, at the request of a party or even otherwise, if the court finds it warranted, order that the hearing is conducted wholly or partly secretely in particular circumstances. Obvious threat to national security is one of these circumstances, and the same goes for sensitive data concerning a person's private life, state of health or disability being treated in the trial. The two other items referred to in the question are not expressly mentioned in the Act, but they may fall under the heading of sensitive information about private life.

24. Are there any provisions in your country which enable particular proceedings in the Labour Courts/Tribunals not to be disclosed in the press and/or not to be available to the general public as part of official records of judicial proceedings?

- If so, please indicate under what circumstances this might arise, and whether there is any special form of appellate or supervisory jurisdiction in relation to exercise of any such powers.

Official records of judicial proceedings must be kept secret in certain cirtumstances, which are partly the same as those explained above, for instance in relation to national security and sensitive information about a person's private life. If the disclosure of information on a victime of crime could violate the victim's rights, such information must also be kept secret. Furthermore, a secrecy order may be issued if the document in question is defined as secret elsewhere in legislation, as may be the case regarding e.g. business secrets.

The court's decisions concerning secrecy may be appealed the same way as other decisions. The Labour Court, however, is the last instance and therefore its decisions are normally not subject to appeal.

Germany

Annelie Marquardt,
Richterin am BAG

Part 1. The regulatory context

25. Does your legal system possess any general definition of "privacy"?

- If so, please indicate the content and source of that definition. If not, how have notions of "privacy" been approached in your country conceptually, in academic writings, or as matters of socio-legal policy?

- **German law does not have a legal definition of privacy. However, the Constitutional Court has developped a theory of "spheres" in the course of its jurisdiction concerning the general rights of personality (constitutional right, Art. 1 and 2 GG), i.e. an "intimate sphere" which is completely off limits for any public institution, a "private sphere" which can only be intruded for the cause of strong reasons which must appropriately,relate to the degree of intrusion and a "social sphere" which can be touched for simpler reasons, The definitions stay a little vague, though. Protection of privacy on one hand means matters which are considered typically private due to their**

contents of information and on the other hand a local area in which the person has the right to be alone and undisturbed.

26. Does your country have a Constitution, and does this make any provision in relation to "privacy" for citizens (whether at work or otherwise)?

Germany has the Grundgesetz (fundamental law) which is a constitution. The general right of personality (Art. 1 para 1 and Art 2 para 1) protects among others the private sphere and the right of informational self-determination. The latter entitles everybody to determine himself which data shall be collected, revealed and to whom; no matter of their original sphere. The Grundgesetz does not distinguish between workplace and other areas. It protects also the fundamental right of the unviolability of the private home (Art 13) and the secret of mail-. post- and tele-communication (Art 10) These rights are immediate rights of the individual against the state, but there is a so-called third-party effect for civil law.

27. Does your country adhere to International Instruments which contain provisions relating to "privacy" (e.g. at the level of the Council of Europe, etc.)?

- If so, please indicate which instruments and when your country signed up to, or ratified, each of those instruments.
- **Germany is subject to international law concerning the protection of privacy, especially the EU-rules, e.g.**

  - EU charta of fundamental rights

  - data-protection-directive 95/46/EU of 1995-10-24

  - data-protection-directive for electronic communication 2002/58/EU of 2002-07-12

  - Regulation 45/2001/EU of 200-12-18 for the protection of natural persons at the processing of personal data by the executive bodies and institutions of the Community

  European Council: European Convention of Human Rights

  Convention for the protection of Humans at the processing of personal data, ratified by law of 1985-03-13

28. As a general matter, how are norms established at the international level transposed into protections or rights at the domestic level for citizens in your country?

- Please illustrate this by reference to any International Instruments mentioned in relation to Q.3.
- **it depends on the nature of the norm. EU-regulations are immediately valid without any transformation-act. Directives have to be transformed into law. The data-protection directive 95/46/EU has been transformed by the Federal Data Protection Act in the year of 1995 and has been adapted several times since then. There has been a preliminary act of 1977.**

29. Are public sector workers/officials in your country subject to a different regime from private sector staff in relation to rules on "privacy"?

- If so, please indicate what the differences are, and whether there can be said to be broad equivalence between the different regimes.
- **Yes, partly. E.g. civil servants have stricter duties concerning their behaviour out of work in their private time There are differences also in the field of data protection. The Federal data protection Act distinguishes between data processing by and transfer to public bodies and private bodies. § 12 para 4 has the purpose of creating a universal**

data protection for all federal civil sevants which often refers to the rules concerning private sector staff. But inspite of some differences there is - generally speaking - a large equivalence.

30. Are any groups of workers (other than public sector workers/officials) treated differently from the "normal model" in relation to rules on "privacy"?

Employees of the churches usually have stricter duties concerning their private lives. They are not subject to the Federal data protection Act. There are specific church-laws and regulations. There are also differences concerning so-called tendency-enterprises, i.e. serving immediately or predominantly ideological, political, coalition (union and employers organisations)-referrred, confessional, charitabe, educational, scientific or artistic purposes or purposes of media or expression of opinions. Employees who are immediately responsible for executing those purposes may have lesser rights concerning their private life. Bearers of professional secrets (like employed psychologists) have the right to refuse collection of confidetial data and data concerning those secrets.

31. Please describe briefly your national framework of rules dealing with issues of "privacy". Where these are contained in legislation or administrative regulations, please indicate the sources *[and, if possible, please attach a copy/version of the relevant provisions]*.

Firstly, the above mentioned constitutional rights protecting privacy. There are numerous federal and Länder- acts concerning those rights. E,g. :

in penal law: § 203 StGB (penal act) punishing the violation of private secrets and § 123 StGB punishing trespassing on private grounds. Since 2004 § 201 a StGB protects the individual who is in a private home or a place which is protected against visibility against the making and transfer of unconsented photographs or film/videos. § 206 StGB punishes the owner or employee of a telecommunication-enterprise who transfers data underlying the secrets of post and telecommunication which have come to his knowledge by his work. Generally the penal protection of the right of informational self-determination is rather weak.

in penal procedure: rules on violation of privacy, e.g. surveillance of telecommunication (§ 100 a StPO = penal procedure act). §160 para 3 StPO limits a deliberate and systematic investigation by the prosecuting officials to the cases which have a high probability of leading to a conviction. So there has to be strong §evidence for suspicion.

in civil law: the general right of personality is recognized as an especially protected legal interest. § 823 para 1 BGB (Civil code) gives a right for compensation of damages if this gerneral right of personality is violated.

The works council has the right and the duty to protect and promote the free development of the workers personality (§ 75 para 1 BetrVG = Works Ccouncil Constitution Act). This includes protecting their privacy. Certain measures of control can only be executed by the employer if the works council has agreed. The individual worker has a right to complain when he feels he has been treated unjustly or was otherwise impaired (§ 84 BetrVG).

Of special importance are the federal and the Länder data protection acts. At the moment there is much discussion about the necessity for a special workers- or employee-data protection act as numerous scandals have been discovered in German and international enterprises. E.G.

The Lidl-companies had a wide-spread system of video and acoustic surveillance (even in the toilets) and surveillance by detectives aimed at the collection of causes of diseases, reasons for sick-leaves, possible irregularities, how often and how long the cashiers go to the toilet, what are they talking about, do they have plans to have children by normal or artificial fertilization etc. Neither the works councils (as far as they exist because Lidl is

rather successful in preventing their foundation) were informed - of course they did not codetermine either - nor had Lidl appointed a data protection official which would have been their duty according to the BDSG. The Landes-dataprotection officials intervened and at the end Lidl was fined to 1.5 Mio Euros altogether which they accepted.

From 1997 till 2006 the Deutsche Bahn AG (German railway) had given (oral) orders to extern firms to collect data on bank accounts of ca. 170.000 employees in order to find out if there was any corruption - so they claim. They compared tha data with the names and addresses of spouses and relatives to find out if there were coincidences with contractors, It is suspected that they collected data not only on the numbers of bank-accounts but also on movements in these accounts on a large scale, some cases are proved. The extern company got 800.000 Euros for their services without any written contract which shows the clandestine character of the order. The data protection official of the Deutsche Bahn was not informed, neither were the concerned employees which is also a duty the company violated according to § 33 BDSG. The result of the surveillance are 150 investigations against Bahn employees by the state prosecution officials. It is not clear yet if anyone will be accused, let alone sentenced.

In the spring of 2008 it was reported that the German Telekom company had surveilled about 60 managerial employees in 2005 and 2006. Their telephone records were compared with the numbers of unpopular journalists in order to find leaks of information. Obviously Telekom was able to get and use not only their own data but also those of all mobile and not mobile telephone companies active in Germany. As they did not intend to transfer the investigated data to others these controls would not be punishible by § 206 StGB.

Part 2: The State and the employer

32. Please outline the areas in which the State authorities in your country are entitled to obtain personal information from an employer about a member of its workforce.

    - In particular, please indicate whether the State authorities possess such powers in relation to nationality or national origins; residence status; work permit status; previous employment records; criminal records; tax status; family/marital status; medical records, health and/or disability-related material; bank account information (e.g. for payment of wages); trade union membership.

    - **the employer is forced to submit numerous data to state authorities like tax offices, unemployment agencies, offices of social security, chambers of industry or commerce or craftsmen. The legitimacy of such data collecting is measured by the individual right of informational selfdetermination.In some cases there are legal provisions for the transfer of even very delicate data, e.g for workers in atomic plants according to the Control-of safety-Act.**

    - **Almost all the above mentioned informations may be obtained by state authorities according to their tasks but only as far as they are necessary to fulfill these tasks. They may not ask or store information of union membership The unemployment agencies may under narrow conditions even ask for that, but only the former employee himself, not a third party.**

33. Please indicate whether the State authorities in your country are entitled, under any circumstances, to implement surveillance of a workplace (electronic, video, visual observation, etc.) for the purpose of obtaining personal information about any member of the workforce?

    - In particular, please indicate whether the State authorities possess any special powers of this kind in the context of measures intended for "combating terrorism" or in relation to investigation of serious criminal activities (e.g. drug dealng, "money laundering", etc.).

- **Yes, there may be e.g. surveillance of telecommunication also at the work place legitimated by the Länder police acts, the penal procedure act or other acts aiming at the prevention of and the fight against danger. There is no law concerning exactly the work place (yet). If state authorities order the transfer of certain data there is no right of codetermination of the works council unless there is a range of possible measures.**
- **After 9/11 the state authorities exercised a large and unaimed investigation (Rasterfahndung) on the entire area of the Federal Republic of Germany in order to search for terrorist "sleepers" or supporters. In its course private and public employers had to transfer data on employees to the police according to a fixed scheme of criteria.**

Part 3. The employer and the worker

34. Does a worker in your country enjoy any form of "right to privacy"?
    - If so, what form or forms does this right take? How is that right reflected in the legal system of your country?
    - **see questions 2, 5 and 6. The worker enjoys the same rights to privacy as any other citizen. Any restriction of his right to free development of his personality has to be justified by a legitimate aim and can be achieved only by appropriate and necessary means.**
    - **In the present discussion many voices claim that the existing system of protection is not sufficient any more. the basic judgement of the Constitutional court, which established the right to informational self determination, is from 1983, so to speak the dawn of data collecting and processing. Nobody at those times could foresee the possibilities there are today.**
35. To what extent (if at all) is any "right to privacy" for a worker more limited **when that person is at work** than any "general right to privacy" enjoyed by citizens in general?

    Depending on the kind of work and the company rules - e.g. concerning uniforms, clothes, controls of behaviour, defence of smoking etc. if the principle of proportionality is respected and the works council has codeterminated

36. Under what conditions (if at all) is an employer in your country entitled **to obtain** (e.g. by way of questions contained in job application forms) personal information about a member of its workforce?

    Generally the collection , storage, modification, processing transfer and use of data for the employers' own purposes is determined by § 28 BDSG. It is only admissable in accordance with the purposes of a contract (or a quasi-contractual fiduciary relationship) with the data subject, in so far as this is necessary to safeguard justified interests of the controller of the filing system (= the responsible agency) and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use, or if the data is generall accessible or the controller of the filing system would be entitled to publish them, unless the data subject's legitimate interest in his data being excluded from processing or use clearly outweighs the justified interest of the controller of the filing system. In connection with the collection of personal data, the purposes for which the data are to be processed or used are to be stipulated in concrete terms. Transfer and use for other purposes are admissable for justified interests of a third party or to avert threats to the state security and public safety and to prosecute criminal offences or for purposes of advertising, market and opinion research if the data, compiled in lists or otherwise combined, concern members of a group of persons and are restricted to the data subjest's membership of this group of persons, occupation or type of business, name, title,academic degrees, address and year of birth. Further restrictions follow.

There is a large jurisdiction of the Federal court of labour law concerning the right of the employer to ask questions and the duty of the employee to reveal information or have the right to lie. Always it is decisive to weigh the interest of information of the employer and the interest of the employee of his freedom of personality, respecting the principle of proportionality.

§ 94 BetrVG (works council constitution act) establishes a codetermination for staff questionnaires.

- In particular, please indicate the position in relation to the following specific areas (and please add information about any other matters which are of particular significance in your country):
  - information about the address, telephone contact numbers, etc. of the worker
  - information about the marital status of the worker
  - **both admissible for the sake of salary statements**
  - information about the health and medical condition of the worker (including, for example, details of the worker's personal doctor)
  - **generally not allowed, except when the disease or disability limits the aptitude for the intended work, e.g. addiction to alcohol or drugs for a pharmacist. § 1 AGG (general antidiscrimination act) limits the right to ask for disabilities even more.**
  - information about the sexual orientation of the worker
  - **inadmissible**
  - information about the religion of the worker
  - **inadmissable before the working contract is agreed to (except churches as employers), afterwards it is possible for the sake of church-tax deduction. There are different opinions on the question for scientology membership**
  - information about the political affiliation or activities of the worker
  - **generally inadmissible (except for tendency-enterprises) before hiring. The public employer may ask for membership in anticonstitutional organisations or the Ministery of State-Security or the Socialist-Union-Party of the former GDR**
  - information about the tax (fiscal) affairs of the worker
  - **admissable for the sake of tax-deduction**
  - credit information about the worker
  - **only admissible when special trust is required in his future position, e.g. when he has to handle money or will have a key position.**
  - court information (e.g. for enforcement of court orders by way of deductions from salary – "attachment of earnings")
  - **Controversially discussed: pro inadmissibility: every court order has to be served formally to each new employer anyway; contra: the employer has a lot of work with these orders and runs own risks in case of error or incorrect fulfillment (which can easily happen)**
  - information about any criminal convictions which the worker may have
  - **admissible when and as far as the future work requires special trust worthiness or if the mobility is limited (truck driver who is serving time in an open prison) and generally if the aptitude for the prospected work is concerned. (in narrow limits)**
  -

Under what conditions (if at all) is an employer in your country entitled **to retain** (whether in the form of personal files, or electronically) personal information about a member of its workforce?

- In particular, please indicate the position in relation to the specific areas mentioned in Q.12 (and please add information about any other matters which are of particular significance in your country).
- **see question 12 § 28 BDSG (Federal Data Protection Act)**
- Is an employer in your country obliged to tell the worker that it is holding personal information about that worker and/or to make any such information available to the worker for inspection (e.g. to ensure the accuracy of the information)?
- **Yes, § 33 BDSG states the duty to inform the data subject completely about the data collected and stored. The worker has a right to look into his personal file, whether in paper or electronic form (§ 83 para 1 BetrVG (works council constitution act)), furthermore there is a right to information according to § 34 BDSG (Fed.data protection act) and a right to ensure correction acc. to § 35 para 1 BDSG**
- Are there any provisions in your country which require the employer to handle such information in a particular way?
  - For example, is the employer required to register the fact that it holds such information with a public official (a "data protection commissioner" or the like)?
  - **Yes, § 4 f BDSG provides a data protection official who is to be assigned in every public or private institution or organisation (with exceptions for enterprises with less than 10 data-collecting or -processing persons) So principally control is assigned to the inner-enterprise mechanisms, also the works council. Otherwise the Länder and Federal data protection officials have to be informed.**
  - Does the employer personally/physically have to retain such information under its control at the workplace, or can it employ specialist companies to hold and manage any such data?
  - **The employer may employ extern companies for data collection, use and processing (§ 11 BDSG) He stays responsible for the compliance with the requirements of the data protection act himself.**
  - Is the employer required to destroy such information after a certain period of time?
  - **Yes, § 35 para 2 BDSG : Personal data must be erased if their storage is unadmissible, if they concern information on racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life, criminal offences or administrative offences and the controller is unable to prove their correctness. They must also be erased if they are processed in the course of business for the purpose of transfer and an examination at the end of the forth year after first storage shows that further storage is not necessary. Under certain circumstances data must be blocked.**
- Are there provisions in your country which regulate the freedom of the employer to disclose or pass such information to third parties (including to the public authorities)?
- **Yes, acc. to § 28 BSDG or prevalent other legal provisions. This counts also for a group of enterprises (Konzern), as other enterprises within this group are "third party". Exception; Employing extern data processing companies**
- 14. In addtion to the situations mentioned in Q.12 and Q.13, are there any circumstances under which an employer in your country is entitled to obtain (or to demand) medical details about a member of its workforce?
- **Yes, contagious diseases which may endanger other workers or clients**. **Aids: actual outbreak of the disease; yes, mere infection: no**

- In particular, please indicate whether there are any situations in which an employer is obliged to obtain information about the health of the worker (e.g. before permitting that worker to perform tasks at heights, or where there may be exposure to dangerous substances or radiation during the course of performing the job).
- **Yes, in certain fields of labour according to special laws. For example §§ 60 ff Radiation Protection Ordinance, 37 ff Röntgen Ordinance or § 81 Seaman's Law for the staff of ships. For state officials: before they get assigned they are examined by a public health officer who tests the general aptitude.**
- Is there any procedure laid down for an employer in your country to obtain the formal consent of a worker to accessing such personal medical information?
- **No formal procedure, just the requirements of the BDSG. § 4a deals with the necessary provisions for an effective consent of the data subject.**
- Is an employer in your country entitled to ask specific questions about whether a member of its workforce is "disabled"? – If so, what are the consequences if the worker refuses/fails/chooses not to disclose such information?
- **see qu. 12 If a question is not allowed, the worker may lie without any consequences. If the question was admissible and the worker has lied the employer might rescind the contract. Whenever a worker claims the protection of laws protecting the disabled he must reveal within certain time limits that he is disabled.**
- Can an employer in your country require a worker to submit to a medical examination, and subsequently have access to the results of that medical examination (e.g. where the employer is considering dismissing the worker on grounds such as "capacity", or "fitness to do the job", or because of a high level of absences from work for medical reasons)?
- **Only in the case of legal provisions (s.above) or when it is necessary for the protection of others. The physician has the duty to professional confidentiality and may not reveal medical results to the employer or other persons (except the paying insurance company). He must only tell if the worker is apt for the job or not. If the employer wants to dismiss the worker he cannot ask him to submit to a medical examination. When the worker contests the dismissal he must free the physician from his duty of confidentiality in order to give the employer the possibility of proof.**
- Is an employer in your country entitled to make use of (and act on the basis of information obtained as a result of) techniques such as "psychological testing" or "genetic testing"?
- **Genetic testing is not allowed**. **There is a draft of a Genetic Diagnosis Act (just today(2009-04-23)agreed to by the government) which will formally forbid it. Psychological tests are only admissible - even if the worker agrees - if necessary for the specific position. The psychologist may only give the result (apt or not) to the employer without stating single points of his examiniation. The same goes for assessment centers. IQ-tests are not allowed, neither are general personality tests. However, in selection interviews many hidden testing may take place without the applicant ever noticing it.**

15 Is an employer in your country entitled to implement any forms of surveillance of workers at the workplace?

Yes, even if there is no specific legal provision the employer may implement surveillance of workers In case there is a works council it has to agree. The Federal Court of Labour Law has decided on several cases of video-surveillance (the last one 2008-08-26 1 ABR 16/07). Surveillance is admissible according to the principle of proportionality. The limitation of the personality right must be in an appropriate relation to the the necessity of control

In particular, please indicate whether there are any situations in which an employer is entitled to make use of the following:

- CCTV (video surveillance)
- **A general control of the workers is not allowed. There must be a necessity to watch and control certain workplaces for the sake of security or concrete suspicion of a criminal act. The intensity of the encroachment in the right of personality depends on the degree of necessity. The employer cannot survey 50 workers when he is only suspecting one to cheat. He cannot survey for months when the suspected offence is light and concerns few workers. He always has to choose the lightest possible intrusion. The workers have to be informed about the surveillance in due time. Only if there is a situation of emergency or self-defence the employer may have the right to a secret action. That means that the Lidl-surveillance was far beyond any rightfulness.**
- Monitoring and inspection of web-browsing by the worker
- **Nothing is clear there and just about every question is controversially disputed. If the employer has allowed a private use of the computer and internet at work the rules of the telecomunication act are applicable. They protect the secrecy of telecommunication and forbid control without the approval of the worker. If only professional use is allowed the employer may control the exterior data, like numbers and addresses. If and how far contents of the usage can be controlled is disputed.**
- "Keystroke monitoring" of workers performing computerised tasks
- **unadmissable because it is unappropriate.**
- Monitoring and inspection of a worker's electronic communications (eMail, social networking websites, etc.)
- **see above**
- Monitoring and inspection of a worker's traditional communications (post, telephone calls, etc.)
- **similar to video-surveillance. The worker must be informed and agree unless there is a specific suspicion of criminal action. The collection of telephone data (number, hour) is admissible for official calls, not for private calls. Traditional post is protected by the secrecy of mail. If a letter is directed to an employee under the address of the employer he has to get it closed. Official post can be opened.**

16. Are there any circumstances where an employer in your country may be entitled to conduct (e.g. by security staff belonging to the enterprise) a physical (possibly including intimate) body search of a member of its workforce?

- What would be the consequences if the worker refused to submit to such a search?
- What would be the consequences if an employer carried out such a search without the consent of the worker?
- **The employer has no police-like rights. However every citizen has certain rights in case of emergency or self-defence, also the employer. So he may catch a thief and hold him until the police comes. This does not give him the right to systematic body searches of workers. There may be cases in which the works council has agreed to body searches under certain circumstances. Also those can be contested as unlawful by the searched worker if the means are unappropriate. I think that body searches by the employer are always unlawful under all circumstances. unless the worker agrees. But there is not a general opinion on that question. Control of bags and purses or luggage at the exits of an enterprise may be appropriate means, if the works council has codeterminated.**

- **Presumed the worker has to tolerate a search he may be admonished in case of refusal. Refusal might add to other indications of suspicion for unlawful behaviour which might lead to a dismissal at the end.**
- **The worker has the right to claim damages in case of unlawful searches, also immaterial damages caused by the violation of his personality rights. Possible proof found in an unlawful search cannot be used at court.**

17. Is an employer in your country subject to any recognised "duty of confidentiality" in relation to members of its workforce and/or others?

- If so, what is the extent of any such duty, what form or forms does this duty take, and how is that duty reflected in the legal system of your country?
- **see question 10**

18. Under what circumstances can an employer in your country justify breaching the "privacy" of a member of its workforce or any "duty of confidentiality" owed to a worker in its employment?

- In particular, please indicate how this might be the case in relation to:
  - the employer's business interests (e.g. protection of trade secrets)
  - supervision of security at the workplace
  - prevention of criminal activity (drugs abuse, etc.)
  - when required to act under instructions from the public authorities (e.g. as part of a police investigation)
  - **see above; the most important rule is the principle of proportionality.**

19. Is it possible for an employer in your country to justify intrusions into the privacy of members of its workforce by giving clear notice that particular measures are in use (e.g. signs stating that the workplace is subject to CCTV surveillance)?

No, notification alone never justifies the intrusion. On the contrary: secrecy contibutes to the unadmissibility of the intrusion even if there might have been indications for a due reason in the first place.

20. Is it possible for an employer in your country to include contractual provisions in the terms of the employment relationship which effectively permit the employer to breach the privacy of a member of its workforce?

No, a contract may not object to higher-ranking law. The right of personality and the dignity of a person are stronger than any contractual provision.

21. Are there any special rules in your country concerning "personal" files created by a worker on a computer belonging to the employer at the workplace?

- Is there any guidance in relation to who "owns" any rights in relation to such "personal" files?
- **No, there are the same disputes over this questions as over the issue of internet use. If the employer has agreed to private use of his equipment the worker may possibly "own" the file and have the right to use it for himself.**
- **Part 4. Miscellaneous procedural and other matters**

22. Please provide a brief overview of the mechanisms in place in your country to deal with the regulation of "privacy" as between employers and workers.

In certain limits individual contracts. More important are works agreements between employer and works council concerning the introduction and use of technical devices which are

determined (and apt) to survey the behaviour and the performance of the worker (§ 87 Para 1 Nr. 6 BetrVG = works Constitution Act) or staff-questionnaires (§ 94 para 1 BetrVG)

23. Do issues of "privacy" arise before the Labour Courts/Tribunals in your country, and, if so, what form do these tend to take?

Yes **especially between employer and works council when technical control is concerned. The works council usually claims that a surveillance is not admissible because it was not codeterminated and the employer has to stop the measure. If works council and employer cannot reach an agreement the conciliation committee has to be called and decides the matter. This ruling can be contested in front of the labour courts again.**

23. Do the procedures of the Labour Courts/Tribunals in your country make provision for private/secret hearings in particular circumstances:

There are general rules for all courts in the Judicature Act. § 171 b allows a concerned person to apply for the exclusion of the public for the sake of the protection of the personal life. The court has the right to exclude the public in certain cases without the application of a party.

- In particular, please indicate whether this might be the case in relation to:
  - national security
  - **Yes, § 172 Nr. 1 Judicature Act**
  - cases involving disability or medical evidence of an intimate or embarrassing nature
  - **Yes, § 171 b**
  - cases where allegations are made that criminal acts been committed by a party or witness
  - **no special exclusion provision unless the other constellations are given.**
  - cases where allegations are made of sexual or other abuse, and/or where the evidence may involve disclosure of intimate sexual or other acts by a party or witness
  - **Yes, § 171 b**

25. Are there any provisions in your country which enable particular proceedings in the Labour Courts/Tribunals not to be disclosed in the press and/or not to be available to the general public as part of official records of judicial proceedings?

- If so, please indicate under what circumstances this might arise, and whether there is any special form of appellate or supervisory jurisdiction in relation to exercise of any such powers.
- **Aside from the above mentioned provisions for excluding the public (including the press and other media) there are no such provisions. There is no public right to look into court files. Only the immediate parties heve a right to do this. A third party must prove a legitimate interest which is normally not assumed,**

Hungary

Judge Maria Kulisity
Labour Court of Budapest

Part 1. The regulatory context

Does your legal system possess any general definition of "privacy"?

If so, please indicate the content and source of that definition. If not, how have notions of "privacy" been approached in your country conceptually, in academic writings, or as matters of socio-legal policy?

We don't have any general definition of privacy. Some of the decisions of the Constitutional Court deals with the concept of privacy. For example the Constitutional Court stated that the information regarding someone's property or estate are part of his privacy and these are personal data (21/1993. (VI.2.) decision, decisions 1993/172-173.).

Does your country have a Constitution, and does this make any provision in relation to "privacy" for citizens (whether at work or otherwise)?

The Act XX of 1949 on the Constitution of the Republic of Hungary (hereinafter the Constitution) states in Article 59 paragraph (1) that in the Republic of Hungary everyone has the right to the good standing of his reputation, **the privacy of his home and the protection of secrecy in private affairs and personal data.**

It also recognizes that in the Republic of Hungary everyone has the right to freedom of thought, freedom of conscience and freedom of religion. This rights shall include the free choice or acceptance of a religion or belief, and the freedom to publicly **or privately express or decline to express,** exercise and teach such religions and beliefs by way of religious actions, rites or in any other way, either individually or in a group (section 60).

Does your country adhere to International Instruments which contain provisions relating to "privacy" (e.g. at the level of the Council of Europe, etc.)?

Yes, for example the Convention for the Protection of Human Rights and Fundamental Freedoms

- *If so, please indicate which instruments and when your country signed up to, or ratified, each of those instruments.*

The Convention for the Protection of Human Rights and Fundamental Freedoms is ratified on 5th of November, 1992.

As a general matter, how are norms established at the international level transposed into protections or rights at the domestic level for citizens in your country?

Mainly the Hungarian law has a dualistic approach: the Act L of 2005 on the procedure of international treaties regulates the issue in details. **It states that the transformation, incorporation of international treaties ratified by Hungary is necessary by an independent Act.** This Act should contain the authentic text of the international treaty with the exceptions, objections and the date of effect. Retroactive effect is not possible.

So the general rule is that the norms established at the international level can not apply directly. Even if the government signed the act, it needs to be transformed

However the Constitution of the Republic of Hungary also states that the legal system of the Republic of Hungary accepts the generally recognized principles of international law, and shall harmonize the country's domestic law with the obligations assumed under international law (Subsection (1) of Section 7.). The Constitutional_Court interpreted this rule in its 53/1993. (X.13.) decision: the Court stated that the above mentioned provision means that the generally recognized principles of international law are directly part of the Hungarian law without transformation. In these cases the transformation is executed by the Constitution itself. This provision is not excluded that international treaties contain one or more of the generally recognized principles of international law and in this regard separate transformation can happen. In some other decisions the Constitutional Court is expressed the direct applicability of international treaties (decision 36/1996. (IX.4)).

The national treaties also have a great part in the interpretation of the Hungarian law.

- *Please illustrate this by reference to any International Instruments mentioned in relation to Q.3.*

The Convention for the Protection of Human Rights and Fundamental Freedoms is incorporated in the Act XXXI. of 1993.

Are public sector workers/officials in your country subject to a different regime from private sector staff in relation to rules on "privacy"?

Yes, there are differences.

- *If so, please indicate what the differences are, and whether there can be said to be broad equivalence between the different regimes.*

There are strict rules regarding public officials to prevent them from any kind of (political, economic or any other) influence, the act gives incompatibility rules. The Act generally prohibit that public officials conduct activities being unworthy of the office of the public official or threatening the impartial and unbiased activities of the public official; They are the representative of the state therefore their behaviour – even in their private life – should be appropriate to their position.

Public officials

- Public officials may not be a representative of a local government at the self-government operating in the jurisdiction of the public administration agency employing the particular public official.
- Public officials may only establish other and further legal relationships - with the exception of scientific, educational, artistic, literary advisor.', editorial activities and intellectual activities subject to legal protection - with the consent of the entity exercising employer's authority.
- Public officials with senior official assignment may not establish other and further legal relationships associated with performance of work - with the exception of scientific, educational, artistic, literary advisory, editorial activities and intellectual activities subject to legal protection.
- Public officials may not conduct activities being unworthy of the office of the public official or threatening the impartial and unbiased activities of the public official;
- may not hold a post in any part, may not appear in public on behalf or in the interest of any party - with the exception of participation in the parliamentary or self-governmental elections as candidates (section 21).

There are even stricter rules for judges:

Judges

- judges must disclose data about our property
- judges can't be member of any political party and can't exercise any political activity, can't be a representative of Parliament or local government, member of the government, can't be mayor of local government, or state leader.
- Except the judicial job judges can practise only scientific, artistical, literaly, tutorial, engineering creative work as an earning work, but just in case if it is not endangering the independence and the impartiality of the judge or it doesn't show the appearance of endangering it and it mustn't obstruct his/her judicial activity.
- It is prohibit to be a member of an arbitration board, board of supervision, to be an executive or a member with total responsibility, or personal activity in a business association.
- Outside of the labour relationship the judge mustn't disclose any opinion regarding any case that is due or finished, particularly the case decided by his/her. The judge obliged to behave worthy to his/her position and his/her conduct must be unobjectionable. He must to abstain from a behaviour that damages the trust of the judicial procedure or the authority of the court.

Are any groups of workers (other than public sector workers/officials) treated differently from the "normal model" in relation to rules on "privacy"?

There are strict limitations regarding <u>executive workers</u>:

- Executive employees shall not establish additional employment relationships or other employment-related legal relationships. Unless prescribed in the contract of employment to the contrary, this provision shall not apply to legal relationships established for the purpose of scientific or educational activities or activities under copyright protection.
- Executive employees shall not acquire shares, with the exception of the acquisition of stocks in a public limited company, in a business association which is engaged in the same or similar activities or is in regular business contact with their employer,
- shall not conclude any transactions falling within the scope of the employer's activities on their own behalf, and
- shall report if a close relative has become a member of a business association which is engaged in the same or similar activities or is in regular business contact with the employer, or has established an employment relationship or other employment-related legal relationship with an employer engaged in such activities.

The employer shall be entitled to terminate the employment relationship of an executive employee if a close relative [Subsection (2) of Section 139] of such officer has become a member of a business association which is engaged in the same or similar activities or is in regular business contact with the employer, or has established an employment relationship or other employment-related legal relationship with an employer engaged in such activities.

Generally there are bigger expectations towards the executive workers. Judicial decisions also states that their behaviour in their private life needs to be worthy to their position.

There are also other workers in the private sector who has special status for example the bank officials, the church officials. etc. There privacy are also limited according to their needs of service.

Please describe briefly your national framework of rules dealing with issues of "privacy". Where these are contained in legislation or administrative regulations, please indicate the sources [and, if possible, please attach a copy/version of the relevant provisions].

- Act XX of 1949 on the Constitution of the Republic of Hungary,
- Act XXII of 1992 on the Labour Code,
- Act IV of 1959 on the Civil Code,
- Act of 1978 in the Criminal Code
- Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest
- Act XLVII of 1997 on the Handling of Medical and Other Related Data
- Act LXVI of 1992 on the Name and Address Records of Citizens ("the Records Act")
- Act LXV of 1995 on State Secret and Service Secret
- Act LXVI of 1995 on Public Records, Public Archives, and the Protection of Private Archives
- Act XC of 2005 on the Freedom of Information by Electronic Means
- Act XIX of 1998 on the Criminal Procedure
- Act IV of 1978 on Criminal Code
- decisions of the Constitutional Court courts.
- The recommendations and other acts of the Data Protection Officer

In Hungary **the Data Protection Commissioner takes care of the protection of data and for this he has powerful instruments.** The Data Protection Commissioner shall monitor the conditions of the protection of personal data and of the realisation of public access to data of public interest and data public on grounds of public interest. He shall make proposals for the adoption or amendment of legislation on data processing or on public access to data of public interest and data public on grounds of public interest, and give an opinion on such draft legislation. Upon observing any unlawful processing of data, the Data Protection Commissioner shall call on the data controller to discontinue the data processing. The data controller shall take the necessary measures without delay and inform in writing the Data Protection Commissioner thereof within 30 days. The Data Protection Commissioner may inform the public of the launching of his investigation, of the fact of the unlawful processing (technical processing) of data, of the person of the data controller (technical data processor) and of the range of processed data, as well as of the measures initiated and decisions made by him. If the data controller or technical data processor fails to discontinue the unlawful processing (technical processing) of personal data, the Data Protection Commissioner may order in a decision the blocking, deletion or destruction of unlawfully processed data, prohibit the unlawful processing or technical processing of data, and suspend the transfer of data to foreign countries.

Part 2: The State and the employer

Please outline the areas in which the State authorities in your country are entitled to obtain personal information from an employer about a member of its workforce.

- *In particular, please indicate whether the State authorities possess such powers in relation to nationality or national origins; residence status; work permit status; previous employment records; criminal records; tax status; family/marital status; medical records, health and/or disability-related material; bank account information (e.g. for payment of wages); trade union membership.*

General rules from the Data Protection Act:

‘personal data’ shall mean any data relating to a specific (identified or identifiable) natural person (hereinafter referred to as ‘data subject’) as well as any conclusion with respect to the data subject which can be inferred from such data. In the course of data processing such data shall be considered to remain personal as long as their relation to the data subject can be restored. An identifiable person is in particular one who can be identified, directly or indirectly, by reference to his name, identification code or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

‘special data’ shall mean any personal data relating to

a) racial, or national or ethnic minority origin, political opinion or party affiliation, religious or ideological belief , or membership in any interest representing organisation;

b) state of health, pathological addictions, sexual life or criminal personal data;

‘criminal personal data’ shall mean any personal data which originated – during criminal proceedings or prior to such proceedings in connection with the criminal offence or the criminal proceedings – by the organs authorised to conduct criminal proceedings or to investigate criminal offences or by the penal authorities and which can be related to the data subject, as well as personal data relating to previous criminal convictions;

Personal data shall not be processed unless

a) the data subject has given his consent; or

b) ordered by an Act, or – based on authorisation conferred by an Act, and within the range of data specified therein – ordered by a local government decree.

Special data shall not be processed unless

a) the data subject has given his **written consent**; or

b) regarding data set out in point a), an international agreement prescribes it or it is ordered by an Act, either in order to enforce a fundamental right provided for in the Constitution or in the interest of national security, crime prevention or criminal investigation; or

c) ordered by an Act in other cases.

Personal data shall be processed **only for a specified purpose,** in order to exercise a right or perform an obligation. This purpose shall be complied with in all phases of the data processing. No personal data shall be processed **unless indispensable and suitable** for the achievement of the purpose of the data processing, and **only to the extent and for the duration** necessary to achieve that purpose.

General rules from the Labour Code: Employers may only disclose facts, data and opinions concerning an employee to third persons (like state also) in the cases specified by law or with the employee's consent. Information and data pertaining to employees may be used for statistical purposes and may be disclosed for statistical use in a manner that precludes identification of the employees to whom they pertain (Section 3).

Employers may not demand employees to reveal their trade union affiliation (Section 26.). Employees must not be compelled to take a pregnancy test or to produce a certificate thereof, unless it is prescribed by legal regulation so as to determine the employee's proficiency for the position in question (section 77). Therefore these data are not registered, so state authorities can not be knowledge of these.

Most of the above mentioned data are personal data or special data therefore these can not be registered by the employer and disclose these to the state authorities unless the employee hives his/her consent. There is an exception: Information and data pertaining to employees may be used for statistical purposes and may be disclosed for statistical use

in a manner that precludes identification of the employees to whom they pertain. Also there are cases when the court orders the employer to disclose data about the employee but in these cases the law regulates this possibility.

Please indicate whether the State authorities in your country are entitled, under any circumstances, to implement surveillance of a workplace (electronic, video, visual observation, etc.) for the purpose of obtaining personal information about any member of the workforce?

- *In particular, please indicate whether the State authorities possess any special powers of this kind in the context of measures intended for "combating terrorism" or in relation to investigation of serious criminal activities (e.g. drug dealng, "money laundering", etc.).*

The main rule is that for such surveillance, the consent of the worker giving in writing is necessary. There are exceptional rules if there is a danger of an indeed serious crime (these are precisely defined in the Act) and the state authorities can not obtain the evidences in any other way. In such cases a judge (ore before the investigation the Minister of Justice also has the right) decides in a formal decision that the "secret" surveillance is permitted or not. The conditions are strictly regulated in the Act on Criminal Procedure.

There are some workplaces, where the surveillance is necessary and regulated by the laws. For example the court houses, the building of the ministries are such workplaces.

Part 3. The employer and the worker

Does a worker in your country enjoy any form of "right to privacy"?

Yes. The main rules are:

Employers may only disclose facts, data and opinions concerning an employee to third persons in the cases specified by law or with the employee's consent. Information and data pertaining to employees may be used for statistical purposes and may be disclosed for statistical use in a manner that precludes identification of the employees to whom they pertain (Section 3).

An employee shall only be requested to make a statement, fill out a data sheet, or take an aptitude test if it does not violate his personal rights and which essentially provides information considered substantive for the purposes of entering into an employment relationship. Employees must not be compelled to take a pregnancy test or to produce a certificate thereof, unless it is prescribed by legal regulation so as to determine the employee's proficiency for the position in question (section 77).

The employers must also keep the above mentioned general rules of special and personal data and the procession of these.

- *If so, what form or forms does this right take? How is that right reflected in the legal system of your country?*

See above d.

To what extent (if at all) is any "right to privacy" for a worker more limited when that person is at work than any "general right to privacy" enjoyed by citizens in general?

There are limitations. For example there are unwritten law for the dressing in the workplace. The employee's right for expression of his/her opinion is also limited.

Under what conditions (if at all) is an employer in your country entitled to obtain (e.g. by way of questions contained in job application forms) personal information about a member of its workforce?

- *In particular, please indicate the position in relation to the following specific areas (and please add information about any other matters which are of particular significance in your country):*

- *information about the address, telephone contact numbers, etc. of the worker*

  Yes

  - *information about the marital status of the worker* **No, but there are exceptions for example when the new wife/husband changes her name, or it is necessary to disclose his/her property (in case of public servants).**
  - *information about the health and medical condition of the worker (including, for example, details of the worker's personal doctor)* **just if it is necessary to accomplish the work.**
  - *information about the sexual orientation of the worker* **No**
  - *information about the religion of the worker* **No, with the exception of church workers or workers who employed by an institute funded by the church**
  - *information about the political affiliation or activities of the worker* **No**
  - *information about the tax (fiscal) affairs of the worker* **No**
  - *credit information about the worker* **No**
  - *court information (e.g. for enforcement of court orders by way of deductions from salary – "attachment of earnings")* **just in case if the court orders the employer to withhold some percentage of the worker's salary because the worker didn't pay the debt ordered in a court decision. It is typical in maintenance of children cases.**
- information about *any* criminal convictions which the worker may have

  No with the exception where an employee has to have a clean criminal record to work in a position. That is the case with the judges and the public officials.

Under what conditions (if at all) is an employer in your country entitled to retain (whether in the form of personal files, or electronically) personal information about a member of its workforce?

- *In particular, please indicate the position in relation to the specific areas mentioned in Q.12 (and please add information about any other matters which are of particular significance in your country).*

  Personal data undergoing processing shall be:

  a) obtained and processed fairly and lawfully,

  b) accurate, complete and, where necessary, kept up to date,

  c) stored in a way that allows identification of data subjects for no longer than it is required for the purpose for which these data are stored.

- *Is an employer in your country obliged to tell the worker that it is holding personal information about that worker and/or to make any such information available to the worker for inspection (e.g. to ensure the accuracy of the information)?*

  The employer is not obliged to tell the worker that it is holding personal information but the data subject may request

  a) information on the processing of his personal data ; as well as

  b) the rectification, or – except for data processing ordered by a rule of law – deletion of his personal data.

- *Are there any provisions in your country which require the employer to handle such information in a particular way?*

For example, is the employer required to register the fact that it holds such information with a public official (a "data protection commissioner" or the like)?

Registration in the data protection register shall not be required where data processing operations involve the data of persons having an employment relationship with the data controller.

Does the employer personally/physically have to retain such information under its control at the workplace, or can it employ specialist companies to hold and manage any such data?

The employer has a possibility to employ specialist companies to hold and manage such data, but in that case the employees' consent is necessary for processing their data.

Is the employer required to destroy such information after a certain period of time?

Personal data shall be deleted if the purpose of processing has ceased to exist, or the time limit for the storage of data, as specified in an Act,.

- *Are there provisions in your country which regulate the freedom of the employer to disclose or pass such information to third parties (including to the public authorities)?*

  Yes, see aboved mention rules.

  Personal data shall not be transferred and data processing operations shall not be combined unless **consented to by the data subject or provided for by an Act,** and unless the conditions for data processing are met with regard to each personal datum. This rule shall apply to the combination of data processing operations by the same data controller, or by state or local government organs.

In addition to the situations mentioned in Q.12 and Q.13, are there any circumstances under which an employer in your country is entitled to obtain (or to demand) medical details about a member of its workforce?

- *In particular, please indicate whether there are any situations in which an employer is obliged to obtain information about the health of the worker (e.g. before permitting that worker to perform tasks at heights, or where there may be exposure to dangerous substances or radiation during the course of performing the job).*

  Yes, there are certain works that require good physical ability for example works where need to conduct in the in the high. In these cases the worker usually every year must go to a medical examination. There are other jobs where this period is even shorter. The employer doesn't have direct access for the medical data, he just gets the certificate that the worker can do the work or not.

  There are rules for pregnant workers for example that a woman, from the time her pregnancy is diagnosed until her child reaches one year of age, shall be temporarily reassigned to a position suitable for her condition from a medical standpoint, or the working conditions in her existing position shall be modified as appropriate, on the basis of a medical report pertaining to employment. The new position shall be designated upon the employee's approval. Therefore the employer naturally gets to know also that one of his employee become pregnant.

- *Is there any procedure laid down for an employer in your country to obtain the formal consent of a worker to accessing such personal medical information?*

  No.

- *Is an employer in your country entitled to ask specific questions about whether a member of its workforce is "disabled"? – If so, what are the consequences if the worker refuses/fails/chooses not to disclose such information?*

No. However the Labour Code says that the employee shall notify his/her employer if his/her receives invalidity (accident-related disability) benefits.

- *Can an employer in your country require a worker to submit to a medical examination, and subsequently have access to the results of that medical examination (e.g. where the employer is considering dismissing the worker on grounds such as "capacity", or "fitness to do the job", or because of a high level of absences from work for medical reasons)?*

  Yes, there are certain works that require good physical ability for example works where need to conduct in the in the high. In these cases the worker usually every year must go to a medical examination. There are other jobs where this period is even shorter. The employer doesn't have direct access for the medical data, he just gets the certificate that the worker can do the work or not.

- *Is an employer in your country entitled to make use of (and act on the basis of information obtained as a result of) techniques such as "psychological testing" or "genetic testing"?*

  Genetic testing is prohibited. Psychological test is allowed if it is fulfil the requirements:

  an employee shall only be requested to take an aptitude test if it does not violate his personal rights and which essentially provides information considered substantive for the purposes of entering into an employment relationship.

Is an employer in your country entitled to implement any forms of surveillance of workers at the *workplace*?

- *In particular, please indicate whether there are any situations in which an employer is entitled to make use of the following:*

  CCTV (video surveillance) **Just with the workers' consent if there are security questions.**

  Monitoring and inspection of web-browsing by the worker: **Just with the workers' consent**

  "Keystroke monitoring" of workers performing computerised tasks: **Just with the workers' consent**

  Monitoring and inspection of a worker's electronic communications (eMail, social networking websites, etc.) **Just with the workers's consent.** There is a difference **if the employer gives an e-mail address to the employee exclusively for working** (the worker couldn't use it for private messages). In that case the employer has a right to claim for a concrete letter in printed form the worker. The worker can refuse this claim with only one reason: that is the third person's protection of secrecy. The employer couldn't see that what web sites were visited because he has another legal possibility: generally with the use of a program he can control the internet access so there is no need monitoring the worker's personal data.

  Monitoring and inspection of a worker's traditional communications (post, telephone calls, etc.) **Just with the worker's consent with the exception if it is unambiguous from the envelope, that it is an official letter.**

Are there any circumstances where an employer in your country may be entitled to conduct (e.g. by security staff belonging to the enterprise) a physical (possibly including intimate) body search of a member of its workforce?

There are big supermarkets where the security staff conduct physical body search after the work time. In general it couldn't be used just in case of a supposed danger of a concrete crime. It is necessary that the employer has <u>the employee's previous and voluntary consent</u> for this. It mustn't be humiliating and must take care that just women can examine women workers.

- *What would be the consequences if the worker refused to submit to such a search?*

It is not regulated. The law says in general that in the course of exercising rights and fulfilling obligations, **employees shall act in the manner consistent with the principle of good faith and fairness, and they shall be required to cooperate with one another.**

- *What would be the consequences if an employer carried out such a search without the consent of the worker?*

Employers shall be subject to full liability for damages caused to employees in connection with their employment, regardless of accountability. In this situation the damage can be damage of the personal integrity. Besides this it also qualified as crime according to the Criminal Code.

Is an employer in your country subject to any recognised "duty of confidentiality" in relation to members of its workforce and/or others?

- *If so, what is the extent of any such duty, what form or forms does this duty take, and how is that duty reflected in the legal system of your country?*

Employers may only disclose facts, data and opinions concerning an employee to third persons in the cases specified by law or with the employee's consent. Information and data pertaining to employees may be used for statistical purposes and may be disclosed for statistical use in a manner that precludes identification of the employees to whom they pertain (Section 3).

For example at the employee's request (and just in case), upon cessation (termination) of his/her employment, or within a year thereof, the employer shall provide a work certificate. The work certificate shall contain:

a) the job profile filled by the employee at the employer;

b) an evaluation of the employee's work.

Otherwise than that the employer can not disclose „an opinion" of the employee's work to third party.

Under what circumstances can an employer in your country justify breaching the "privacy" of a member of its workforce or any "duty of confidentiality" owed to a worker in its employment?

- *In particular, please indicate how this might be the case in relation to:*

the employer's business interests (e.g. protection of trade secrets) **No, just if it constitutes crime**.

supervision of security at the workplace **Yes, but with strict rules and conditions. Just if there is a real, concrete and direct danger, not in case of a "general" danger.**

prevention of criminal activity (drugs abuse, etc.) **No, this is the task of the state authorities.**

when required to act under instructions from the public authorities (e.g. as part of a police investigation) **Yes**

Is it possible for an employer in your country to justify intrusions into the privacy of members of its workforce by giving clear notice that particular measures are in use (e.g. signs stating that the workplace is subject to CCTV surveillance)?

No, this is not enough, the data processing need to meet with the legal requirements.

Is it possible for an employer in your country to include contractual provisions in the terms of the employment relationship which effectively permit the employer to breach the privacy of a member of its workforce?

Yes, if the employee gives his consent for the data process in the contract. However it couldn't be a general authorization, because there is an obligatory rule: personal data shall

be processed **only for a specified purpose,** in order to exercise a right or perform an obligation. This purpose shall be complied with in all phases of the data processing. No personal data shall be processed **unless indispensable and suitable** for the achievement of the purpose of the data processing, and **only to the extent and for the duration** necessary to achieve that purpose.

Are there any special rules in your country concerning "personal" files created by a worker on a computer belonging to the employer at the workplace?

- *Is there any guidance in relation to who "owns" any rights in relation to such "personal" files?*

There is no any legal rules for personal files. There is only two recommendations from the Data Protection Commissioner regarding the programs/personal files and e-mail address. The Data Protection Commissioner states that the employer has the right to control the personal files and programs on the employee's computer, if the employer gave the computer to the employee exclusively just for work, and he expressly prohibit to make personal files or program on this. Otherwise these are personal data, and the employer couldn't control or see it.

The Data Protection Commissioner also states that if the employee got an e-mail address from the employer and he can uses it for both private messages and business e-mails, the employer should cancel the e-mail address after the termination of the employment-relationship and he couldn't use it or see the messages. He also recommends that the messages arrived in the cancelled e-mail address should dend back with the notice that the e-mail address was cancelled.

Part 4. Miscellaneous procedural and other matters

Please provide a brief overview of the mechanisms in place in your country to deal with the regulation of "privacy" as between employers and workers.

See question 7 and 8.

Personal data shall not be processed unless **the data subject has given his consent.** Personal data shall be processed **only for a specified purpose,** in order to exercise a right or perform an obligation. This purpose shall be complied with in all phases of the data processing. No personal data shall be processed **unless indispensable and suitable** for the achievement of the purpose of the data processing, and **only to the extent and for the duration** necessary to achieve that purpose.

Do issues of "privacy" arise before the Labour Courts/Tribunals in your country, and, if so, what form do these tend to take?

Definitely. **We have lots of cases when the party provide evidence (recording of sound or picture) that he got by breaching the provisions of law.** For example when a party secretly, without the consent of the other person makes record of sound. In these cases the question is can it be used as an evidence in the court proceeding. There are different opinions about these. In Hungary only the Criminal Act prohibits exactly the use of these evidence. Therefore in most civil cases – without concrete prohibition – these can be used. However there are judges who don't permit to use this illegal proof.

Do the procedures of the Labour Courts/Tribunals in your country make provision for private/secret hearings in particular circumstances:

- *In particular, please indicate whether this might be the case in relation to:*

national security - **Yes**

cases involving disability or medical evidence of an intimate or embarrassing nature **Yes**

cases where allegations are made that criminal acts been committed by a party or witness **No**

cases where allegations are made of sexual or other abuse, and/or where the evidence may involve disclosure of intimate sexual or other acts by a party or witness **Yes, just if it arises by the side a party.**

Are there any provisions in your country which enable particular proceedings in the Labour Courts/Tribunals not to be disclosed in the press and/or not to be available to the general *public as part of official records of judicial proceedings?*

- *If so, please indicate under what circumstances this might arise, and whether there is any special form of appellate or supervisory jurisdiction in relation to exercise of any such powers.*

In Hungary every court decisions are open to the public, and anybody can ask a copy of the decision but just in an anonymous form. We have to take care that names or any other data what makes the parties recognizable must be deleted.

Ireland

Judge Kevin Duffy,
Chairman, The Labour Court
Dublin

Part 1. The regulatory context

37. Does your legal system possess any general definition of "privacy"?

- If so, please indicate the content and source of that definition. If not, how have notions of "privacy" been approached in your country conceptually, in academic writings, or as matters of socio-legal policy?

There is no statutory definition of the term "privacy" although its ambit has been judicially considered. It was held that it is a "right to be let alone". It has been held that the nature of the right to privacy must be such as to ensure the dignity and freedom of an individual in a democratic society.

In practice the right to privacy was held to exist in cases involving, inter alia,: -

- ***Unauthorised telephone tapping***
- ***Where a solicitors office was searched by the Police on foot of an unlawfully issued warrant but the details of the search were leaked by the Police to a newspaper***
- ***Intrusive covert surveillance of an individual by the police***

A Bill to provide for a statutory right to privacy was introduced in Parliament by the Government in 2006 but fell with the dissolution that year. It is now being reintroduced.

Section 3 of the Bill provides as follows: -

"3.—(1) For the purposes of this section, the privacy to which an individual is entitled is that which is reasonable in all the circumstances having regard to the rights of others and to the requirements of public order, public morality and the common good.
(2) Without prejudice to the generality of subsection (1) and subject to sections 5 and 6, it shall be a violation of the privacy of an
Individual for a person—

(a) to subject an individual to surveillance,

(b) to disclose information, documentation or material obtained by surveillance whether or not such surveillance was carried out by or on behalf of the person disclosing such information,

(c) to use the name, likeness or voice of the individual, without the consent of that individual, for the purpose of—
(i) advertising or promoting the sale of, or trade in, any property or service, or
(ii) financial gain to the said person, if, in the course of such use, the individual concerned is identified or, as a result of such use, is capable of being identified, and the said person knew that that individual had not given such consent,
(d) to disclose letters, diaries, medical records or other documents concerning the individual or information obtained therefrom, or
(e) to commit an act described in section 10 of the Non-Fatal Offences Against the Person Act 1997 **[stalking]**

The scope for asserting a right to privacy in domestic law has been further enhanced following the enactment of legislation incorporating the provisions of the European Charter of Human Rights. There are, however, no decided cases as yet in this jurisdiction on the scope to be ascribed to Article 8 of the convention.

The question of privacy is further dealt with by the Data Protection Act 1988, as amended, which is referred to in response to many of the questions below.

38. Does your country have a Constitution, and does this make any provision in relation to "privacy" for citizens (whether at work or otherwise)?

Ireland has a written Constitution. Article 40 of the Constitution provides what in effect is a Bill of Rights. No express provision is made for a right to privacy. However it is now well settled in the jurisprudence of the Supreme Court that Art. 40 of the Constitution contains a number of implied or unenumerated rights which inhere in the individual. The right to privacy has been held to be one such unenumerated right. However the precise character and scope of this jurisprudential right remains uncertain.

39. Does your country adhere to International Instruments which contain provisions relating to "privacy" (e.g. at the level of the Council of Europe, etc.)?

- If so, please indicate which instruments and when your country signed up to, or ratified, each of those instruments.

  The State is party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe 28/01/1981). This is the only such instrument to which the State is party.

40. As a general matter, how are norms established at the international level transposed into protections or rights at the domestic level for citizens in your country?

- Please illustrate this by reference to any International Instruments mentioned in relation to Q.3.

  International conventions and agreements are implemented by primary legislation. In the case of the Convention referred to at Q. 3 provision for implementation was made in the Data Protection Act 1988 (as amended to transpose Directive 95/46/EC)

41. Are public sector workers/officials in your country subject to a different regime from private sector staff in relation to rules on "privacy"?

- If so, please indicate what the differences are, and whether there can be said to be broad equivalence between the different regimes.

There is no difference between private sector and public sector workers. However workers involved in childcare (including teachers), or the care of mentally impaired people are subject to police vetting as are workers employed in certain areas involving state security.

42. Are any groups of workers (other than public sector workers/officials) treated differently from the "normal model" in relation to rules on "privacy"?

No

43. Please describe briefly your national framework of rules dealing with issues of "privacy". Where these are contained in legislation or administrative regulations, please indicate the sources *[and, if possible, please attach a copy/version of the relevant provisions]*.

While specific legislation in this filed is in contemplation, the only legislation currently in place relating to the right to privacy is the Data Protection Act 1988, as amended. The right to privacy, in so far as it is derived from the Constitution, can be vindicated in proceedings before the High Court. An action for breach of a Constitutional right is equivalent to an action in tort (but can only be initiated in the High Court) and the reliefs available include all of the reliefs normally available in such an action. There is also the possibility of an action grounded in the tort of breach of confidence.

The Data Protection Act 1988, as amended, established the Office of Data Protection Commissioner who has responsibility for enforcing the provisions of the Act.
The Data Protection Amendment Act, 2003, updated the legislation implementing the provisions of EU Directive 95/46.The Acts set out the general principle that individuals should be in a position to control how computer data relating to them is used. "Data controllers" - people or organisations holding information about individuals on computer or in structured manual files - must comply with certain standards in handling personal data, and individuals have certain rights.
The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Acts, and enforcing the obligations upon data controllers. The Commissioner is appointed by Government and is independent in the exercise of his or her functions. The Commissioner makes an annual report to the Oireachtas, (the Irish Parliament). Individuals who feel their rights are being infringed can complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve it.
Section 8(b) of the Act does allow for the disclosure of an individual's data for the purpose of "detecting or investigating an offence" Hence the disclosure of such information to the police would be legitimate if the employer has reasonable grounds to believe that an offence has been or is about to be committed.

Part 2: The State and the employer

44. Please outline the areas in which the State authorities in your country are entitled to obtain personal information from an employer about a member of its workforce.

- In particular, please indicate whether the State authorities possess such powers in relation to nationality or national origins; residence status; work permit status; previous employment records; criminal records; tax status; family/marital status; medical records, health and/or disability-related material; bank account information (e.g. for payment of wages); trade union membership.

An employer is required to maintain records in relation to workers from outside the EU showing their national origin and other identifying details, including their permit status. These records can be inspected by authorized officials for the purpose of verifying the workers entitlement to work and remain within the country. This power is derived from the general provision in the Data Protection Acts which allows for the disclosure of protected data where this is necessary in order to investigate the commission of an offence. There is no provision for the maintenance of records in relation to the workers health, marital status, bank account etc.

45. Please indicate whether the State authorities in your country are entitled, under any circumstances, to implement surveillance of a workplace (electronic, video, visual observation, etc.) for the purpose of obtaining personal information about any member of the workforce?

    - In particular, please indicate whether the State authorities possess any special powers of this kind in the context of measures intended for "combating terrorism" or in relation to investigation of serious criminal activities (e.g. drug dealing, "money laundering", etc.).

      The police have wide powers to prevent and investigate terrorism and serious organized crime. It has been held that these powers extend to placing suspects under surveillance. Where the surveillance involves phone tapping or interception of correspondence a warrant is required. The use of all forms of visual surveillance in permitted but where it involves entering private property without the consent of the owner or occupier a warrant is required.

Part 3. The employer and the worker

46. Does a worker in your country enjoy any form of "right to privacy"?

    - If so, what form or forms does this right take? How is that right reflected in the legal system of your country?

      There is no particular right to privacy conferred on workers per se. All citizens have the same right to privacy under the constitution and now under the European Convention on Human Rights.

47. To what extent (if at all) is any "right to privacy" for a worker more limited **when that person is at work** than any "general right to privacy" enjoyed by citizens in general?

    There is no difference in the right to privacy while at work than in other situations. However, the right to privacy may be limited by express provision in an individual contract of employment. For example an employee may be required by his or her contract of employment to submit to being searched when entering or leaving his or her place of employment.

48. Under what conditions (if at all) is an employer in your country entitled **to obtain** (e.g. by way of questions contained in job application forms) personal information about a member of its workforce?

    - In particular, please indicate the position in relation to the following specific areas (and please add information about any other matters which are of particular significance in your country):
      - information about the address, telephone contact numbers, etc. of the worker
      - information about the marital status of the worker
      - information about the health and medical condition of the worker (including, for example, details of the worker's personal doctor)
      - information about the sexual orientation of the worker
      - information about the religion of the worker

- information about the political affiliation or activities of the worker
- information about the tax (fiscal) affairs of the worker
- credit information about the worker
- court information (e.g. for enforcement of court orders by way of deductions from salary – "attachment of earnings")
- information about any criminal convictions which the worker may have

In general a prospective employee can be asked to provide any information which the employer considers relevant. However, in practice, this entitlement is circumscribed by employment equality legislation. Thus questions regarding a person's marital status, age, sexual orientation, race, religion etc are regarded as irrelevant and if asked can give rise to liability in equality law.

When information of this nature is provided it is protected by the Data Protection Acts. At present, Irish data protection law makes special provision for the handling of "sensitive" categories of personal data, namely data relating to:

- ***racial origin***
- ***political opinions or religious or other beliefs***
- ***physical or mental health***
- ***sexual life, or***
- ***criminal convictions.***

Persons keeping such categories of personal data are required to register annually with the Data Protection Commissioner. The Commissioner may not accept an application for registration from such a person unless the Commissioner is satisfied that appropriate safeguards are in place to protect the privacy of the individuals concerned.

49. Under what conditions (if at all) is an employer in your country entitled **to retain** (whether in the form of personal files, or electronically) personal information about a member of its workforce?

- In particular, please indicate the position in relation to the specific areas mentioned in Q.12 (and please add information about any other matters which are of particular significance in your country).
- Is an employer in your country obliged to tell the worker that it is holding personal information about that worker and/or to make any such information available to the worker for inspection (e.g. to ensure the accuracy of the information)?
- Are there any provisions in your country which require the employer to handle such information in a particular way?
  - For example, is the employer required to register the fact that it holds such information with a public official (a "data protection commissioner" or the like)?
  - Does the employer personally/physically have to retain such information under its control at the workplace, or can it employ specialist companies to hold and manage any such data?
  - Is the employer required to destroy such information after a certain period of time?
- Are there provisions in your country which regulate the freedom of the employer to disclose or pass such information to third parties (including to the public authorities)?

See answers to questions 7 and 12.

50. In addition to the situations mentioned in Q.12 and Q.13, are there any circumstances under which an employer in your country is entitled to obtain (or to demand) medical details about a member of its workforce?

- In particular, please indicate whether there are any situations in which an employer is obliged to obtain information about the health of the worker (e.g. before permitting that worker to perform tasks at heights, or where there may be exposure to dangerous substances or radiation during the course of performing the job).

  In general there is no such obligation on an employer except in the case of a pregnant worker.

- Is there any procedure laid down for an employer in your country to obtain the formal consent of a worker to accessing such personal medical information?

  There is no fixed or formal procedure

- Is an employer in your country entitled to ask specific questions about whether a member of its workforce is "disabled"? – If so, what are the consequences if the worker refuses/fails/chooses not to disclose such information?

  Asking such questions may give rise to liability under employment equality legislation. Where, however, such questions are directed at identifying special needs or facilities which a worker may require so as to adequately perform the duties of their employment, they would be permissible.

- Can an employer in your country require a worker to submit to a medical examination, and subsequently have access to the results of that medical examination (e.g. where the employer is considering dismissing the worker on grounds such as "capacity", or "fitness to do the job", or because of a high level of absences from work for medical reasons)?

  Yes, provided that an entitlement to do so is provided for in the individual contract of employment or in a collective agreement.

- Is an employer in your country entitled to make use of (and act on the basis of information obtained as a result of) techniques such as "psychological testing" or "genetic testing"?

  There is no prohibition on the use of such techniques.

51. Is an employer in your country entitled to implement any forms of surveillance of workers at the workplace?

- In particular, please indicate whether there are any situations in which an employer is entitled to make use of the following:
  - CCTV (video surveillance)
  - Monitoring and inspection of web-browsing by the worker
  - "Keystroke monitoring" of workers performing computerised tasks
  - Monitoring and inspection of a worker's electronic communications (eMail, social networking websites, etc.)
  - Monitoring and inspection of a worker's traditional communications (post, telephone calls, etc.)

  In practice such measures are permissible where they are provided for by a contract of employment or a collective agreement.

52. Are there any circumstances where an employer in your country may be entitled to conduct (e.g. by security staff belonging to the enterprise) a physical (possibly including intimate) body search of a member of its workforce?

- What would be the consequences if the worker refused to submit to such a search?
- What would be the consequences if an employer carried out such a search without the consent of the worker?

There is no simple or definitive answer to this question. In general it can be said that where a contract of employment, or a collective agreement the terms of which are incorporated in the individual contract of employment, authorizes searches it could be held that a refusal to submit to such a search constitutes misconduct so as to expose a worker to disciplinary action up to and including dismissal.

However all citizens have a constitutional right to bodily integrity and intrusive bodily searches would amount to a violation of that right. Consequently it is difficult to conceive of a situation in which a refusal to submit to such a search, even where an individual contract of employment purported to authorize it, would be accepted as giving grounds for disciplinary action.

53. Is an employer in your country subject to any recognised "duty of confidentiality" in relation to members of its workforce and/or others?

- If so, what is the extent of any such duty, what form or forms does this duty take, and how is that duty reflected in the legal system of your country?

The common law tort of breach of confidence is recognized in Irish law.

54. Under what circumstances can an employer in your country justify breaching the "privacy" of a member of its workforce or any "duty of confidentiality" owed to a worker in its employment?

- In particular, please indicate how this might be the case in relation to:
  - the employer's business interests (e.g. protection of trade secrets)

    An employer is entitled to protect its trade secrets and that would include the right to adequately investigate any suspected improper disclosure of those secrets. This could involve surveillance of individuals provided that the constitutional rights of the employee is not infringed. Hence, an employer could not intercept an employee's private mail or telephone conversations.

    supervision of security at the workplace

    An employer is entitled to put security arrangements in place and to supervise those arrangements.
  - prevention of criminal activity (drugs abuse, etc.)

    Yes. The Data Protection Act 1988 does allow for the disclosure of an individual's data for the purpose of "detecting or investigating an offence" Hence the disclosure of such information to the police would be legitimate if the employer has reasonable grounds to believe that an offence has been or is about to be committed.
  - when required to act under instructions from the public authorities (e.g. as part of a police investigation)

    An employer is not obliged to cooperate with the public authorities in detecting crime provided that the degree of non-cooperation does not amount to obstruction. Depending on the seriousness of the offence under investigation the police may be entitled to enter a premises and conduct surveillance if authorized by warrant or to demand and retain records, including records of a personal nature.

55. Is it possible for an employer in your country to justify intrusions into the privacy of members of its workforce by giving clear notice that particular measures are in use (e.g. signs stating that the workplace is subject to CCTV surveillance)?

Yes.

56. Is it possible for an employer in your country to include contractual provisions in the terms of the employment relationship which effectively permit the employer to breach the privacy of a member of its workforce?

Yes

57. Are there any special rules in your country concerning "personal" files created by a worker on a computer belonging to the employer at the workplace?

- Is there any guidance in relation to who "owns" any rights in relation to such "personal" files?

There are no formal or statutory rules in this area. In general such matters are regulated by the individual contract of employment or collective agreements. Normally employers tend to restrict the use of work computers to work related activity and to provide that all material entered on the computer can be accessed by the employer. It that it clearly provided for in a contract of employment or in a policy which is incorporated in the contract, an employer could access the "personal" files of an employee.

While there is no decided case on the point it would seem that if the employer owns the computer it also owns the property in the files contained in the computer.

Part 4. Miscellaneous procedural and other matters

58. Please provide a brief overview of the mechanisms in place in your country to deal with the regulation of "privacy" as between employers and workers.

There are no formal statutory mechanisms other than those provided by the Data Protection Acts already referred to. In practice such matters may are frequently dealt with in collective agreements or in an employee handbook which sets out the rights and duties of the employer and the employee. Moreover, an employer is required by a non-binding code of practice to have a grievance procedure in place and issues relation to any alleged breach of privacy could be processed through that procedure.

There is a further mechanism available under the Industrial Relations Acts 1946 – 2004 whereby an employee may pursue an individual grievance before a Rights Commissioner who can make a recommendation. That recommendation is appealable to the Labour Court, the decision of which is then binding. This process could be used to address issues relating to privacy.

59. Do issues of "privacy" arise before the Labour Courts/Tribunals in your country, and, if so, what form do these tend to take?

As indicated above these matters can come before the Court as individual grievances by way of an appeal from a Rights Commissioner. Such issues have also come before the Court as forming the subject matter of a collective industrial relations dispute. Case have been before the Court concerning the proposed introduction of security systems including surveillance systems. In such cases the Court issues non-binding recommendations on how the dispute should be resolved

60. Do the procedures of the Labour Courts/Tribunals in your country make provision for private/secret hearings in particular circumstances:

- In particular, please indicate whether this might be the case in relation to:
  - national security
  - cases involving disability or medical evidence of an intimate or embarrassing nature
  - cases where allegations are made that criminal acts been committed by a party or witness

- cases where allegations are made of sexual or other abuse, and/or where the evidence may involve disclosure of intimate sexual or other acts by a party or witness

In general the proceedings of the Labour Court are in private unless a party requests that a hearing be conducted in public. Even where there is a public hearing the Court, on its own motion, or at the request of a party, can hold part of the hearing in private. The Court would hold a private hearing in all of the situations referred to above. In the case of the Equality Tribunal all hearings are in private. In the case of the EAT, hearings are in public unless, in exceptional cases the Tribunal determines to hold a hearing in camera.

61. Are there any provisions in your country which enable particular proceedings in the Labour Courts/Tribunals not to be disclosed in the press and/or not to be available to the general public as part of official records of judicial proceedings?

- If so, please indicate under what circumstances this might arise, and whether there is any special form of appellate or supervisory jurisdiction in relation to exercise of any such powers.

- ***Please see above. The Court can, and frequently does, refer to parties and witnesses pseudonymously. While the Labour Court is always subject to the appellate jurisdiction of the High Court and to judicial review, this practice has never been challenged.***

Israel

Elisheva (Elika) Barak,
Deputy President (ret.),
National Labour Court of Israel

Laws that could be obtained in English are attached.
Articles that could be obtained in English are attached.
General collective Agreement, 2008, which established principles and rules of conduct regarding employee's usage of his employer's computer is attached.

Part 1. The regulatory context

Part 1 Question **1**

The Israeli legal system has several laws that deal with "privacy", though there is no one definition of "privacy". Chronologically the first law concerning privacy is **The Secret Monitoring Law, 5739-1979**. This law imposes criminal sunctions on secret unlawful monitoring. Its deifintion of unlawful secret monitoring is "monitoting without the consent of any of the participants in the conversation".

The Protection of Privacy Law 5741-1981 (attached) is the most conclusive law protecting the right for privacy. The law aplies to its purpose:

1. Prohibition of infringement of privacy

No person shall infringe the privacy of another without his consent.

The law lists a not exclusive list of cases that are considered infringement of privacy. Article 2 states that:

2. What is infringement of privacy

Any of the following constitutes an infringement of privacy:

(1) Spying on or trailing a person in a manner likely to harass him, or any other harassment;

(2) listening is prohibited under any Law;

(3) photographing a person while he is in a private domain;

(4) publishing a person's photograph under circumstances, in which the publication is likely to humiliate him or to bring him into contempt;

(5) copying or using, without permission from the addressee or the writer, the contents of a letter or of any other writing not intended for publication, unless the writing is of historical value or fifteen years have passed since the time when it was written;

(6) using a person's name, appellation, picture or voice for profit;

(7) infringing an obligation of secrecy laid down by law in respect of a person's private affairs;

(8) infringing an obligation of secrecy laid down by explicit or implicit agreement in respect of a person's private affairs;

(9) using, or passing on to another, information on a person's private affairs, otherwise than for the purpose for which it was given;

(10) publishing or passing on anything that was obtained by way of an infringement of privacy under paragraphs (1) to (7) or (9);

(11) publishing any matter that relates to a person's intimate life, state of health or conduct in the private domain.

Article 3 defines various terms. One of them is:

"consent" - explicit or implied consent

It was amended in this way. There is a discission now in order to amend the law again so that "consent" will be only cxplicit consent (when discussing a consent of an employee we have to consider the weigh one has to give to a consent of a worker vis-à-vis the employer, especialy when the worker wishes to be exepted to work.

Article 2(5) was amended to include digital forms of writing as well.

Infringement of privacy under this law is both a criminal offence and a civil tort.

Part 1. Question **2**

The constitutional right to privacy

Israel has a partial constitution consisting of a set of basic laws (similar to the German Grundgesez).Two of these basic laws define human rights: **Basic Law: Human Dignity and Liberty**; and **Basic Law: Freedom of Occupation (profission**). Both were enacted in 1992 (Basic Law: Freedom of Occupation was reenacted in 1994). The Supreme Court has declared Israeli Basic Laws to be Israel's partial constitution (to be completed by future Basic Laws).

Basic Law: Human Dignity And Liberty, protects the right to privacy.

Article 7 states:

Privacy

7. (a) All persons have the right to privacy and to intimacy.

(b) There shall be no entry into the private premises of a person who has not consented thereto.

(c) No search shall be conducted on the private premises or body of a person, nor in the body or personal effects.

(d) There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.

The basic law has a **limitaion clause:**

Violation of rights

8. There shall be no violation of rights under this Basic Law except by a Law befitting the values of the State of Israel, enacted for a proper purpose, and to an extent no greater than is required, or by regulation enacted by authorization in such Law.

The limitation clause demands that laws enacted in the future will adhere with values of the State of Israel, and will be for a proper purpose.

Article 11 states that:

Application

11. All governmental authorities are bound to respect the rights under this Basic Law.

The questions whether the rights stated in the Basic Laws apply also in private relations (in private law) was discussed in several cases.The Israeli Supreme Court has adopted the German Constitutional Court's approach of indirect application of constitutional rights in private relations. Basic rights such as the right to privacy are applied in private law through flexible terms such as good faith and reasonableness. The Israeli Supreme court has broadened the indirect application approach so that if there is no enacted remedy for violation of constitutional rights through private law, such a remedy will be filled by constitutional norms.

To summarize, the right for privacy is a constitutional right, included in Basic Law: Human Dignity and Liberty. It is applied both on public-private relations and on the private sphere.

Part 1. Question **3**

To the extent that privacy is part of international customary law the Israeli system regards it as part of its common law. To the extent that privacy is part of an international treaty, Israel would interpret its own laws with the presumption that they are aimed to fit the international law. If the treaty is ratified by Israel, Israel has an obligation to follow it.

Israel is not part of the Europran Community, yet the directives of the community have an interpretive force in our legal system. Israel has ratified the International Covenant on Civil and Political Rights and the International Covenants on Social and Economic Rights. Israel applies the ILO directions through government action and court interpertation. The ILO's minimal standards of employers' rights were adopted by the legislator.

Part 1. Question **4**

International laws are directly applied in Israel only if they are enacted as laws. To the extent that privacy is part of an international treaty that was ratified by Israel, laws are interpreted under the presumption that they are aimed to fit international law.

The Israeli National Labour Court, as well as the Supreme Court uses comparative law extensivally. The labour court often refers to The European Community Instruments. Thus for example president Menachem Goldberg refered to the The European Communities' Charter of

Fundamental Social Rights of Workers, when the court discussed the right of association in trade unions.

The labour court also relied on the European charter of Human Rights when it delt with the right to work.

As mentioned, the labour court refers a lot to ILO decisions. For example president Steve Adler refered to the Freedom of Association Committee of the Governing Body of the ILO when he delt with the question of the freedom of the employer to leave the employers' organisation in which he was a member.

Part 1. Question **5**

(1) In general there is no difference between private and public sector workers.

(2) Public sector emplyees are subject to Israeli Administrative law thet is mostly judge ruled (common law).

(3) The public sector may consider prior convictions when deciding on hiring.

(4) In 2008, a General collective Agreement, establishing principles and rules of conduct regarding employee's usage of his employer's computer has been signed in Israel. The parties to this Agreement are The New General Labour Federation (the New Histadrut) which is the most representative Labour Union in Israel, and the Federation of the Israeli Economic Organization, a federation comprising of the majority of employers and economic organizations of Israel - who also signed it on behalf of many and major employers associations specified at the end of the Agreement. This agreement doesn't yet apply to Public sector employees since there is no extention order yet. As there is an appeal pending in the National Labour Court, the government awaits the result before issuing an extention order. A detailed explanation of this agreement is in answer to question 7.

Part 1. Question number **6**

Israeli soldiers may be viewed as a special sector. According to the caselaw soldiers are not considered to be in working relations with the state. In one case the majority of the National Labour Court (president Steve Adler and judge Nili Arad) ruled that serving army soldiers are not considered to be in working relations with the state. Judge Shmuel Zur in a minority opinion decided that they are employees of the state. The Israeli Supreme Court (Justice Dorith Beinish) ruled that there are no employment relations between serving army soldiers and the State. The main reason was that this was the Common Law and the court thought it was not suitable to deviate from the previous case law.

The question of intruding privacy in the army might arise concerning censorship of soldiers' letters and phone calls. These issues are regulated by orders only.

There is no difference between different sectors of employees in relation to the right to privacy at work. President Steve Adler ruled that a director might also be considered an employee. This is the law now.

Part 1. Question **7**

(1) As already mentioned the most important rules concerning the right to privacy are article 7 in the Basic Law: Human Dignity and Liberty and the Protection of Privacy Law 5741-1981 (attached) (see answer to question 1).

(2) The Protection of Privacy Law includes (in Part II) an arrangement regarding databases which determines that databases, as defined by the Act, must register with the Registrar of Databases. The law imposes a number of obligations on whom ever seeks to

collect information for holding in a database or whomever operates such a database. A breach of these provisions is both a criminal offence and a civil wrong.

Part 2: The State and the employer

Part 2. Question number **8 and 9**

Israel has a law dealing with free flow of information - Freedom of Information Act, 5758-1998. The law provides freedom of information to every Israeli citizen. The State is obliged to give information to every citizen and resident

The law for example **Prohibition of Money Laundering Law, 2000 - התש"ס** . The law indicates when information should be given. The law indicates in what circumstances information should be provided (the law is attached).

Criminal Procedure [text of an integrated], 1982 Indicates when one is obliged to provide information.

The law of criminal record and rehabilitaion 1981 authorises the police to manage criminal records and prohibits the transfer of its content to any person unless he is authorised to recieve it acording to this statuue. Acording to this statute there is an authorisation to a named oficial of the state to receive the criminal record of state employees. This applies to their apointment and work in the government.

Part 3. The employer and the worker

Part 3. Question number **10**

In general the worker's right to privacy is derived from the general rules regarding the right to privacy. As mentioned above, a fairly new General collective Agreement between The New General Labour Federation (the Histadrut) and the Federation of the Israeli Economic Organization from 2008 deals with privacy regarding computer usag. This is a special arrangement regarding the worker's privecy. **Judge Sheely Wallach** described this agreement in her presentation in the **IXth European Congress of Labour and Social Security Law** as follows:

> "I. The opening statements and declarations at the very beginning makes it very clear that it aims to strike a fair balance between the employer's Rights of property (as the computer he puts at the employee's disposal is his property) on the one hand, and the employee's Right to Privacy when doing so. Both rights, as stated there, are enshrined in Basic Law: Human Dignity and Liberty (Basic Laws in Israel are like the German "Grund Gesetze").
>
> II. Article 2: Agreed Principles, in which both parties acknowledge the employer's right of property and managerial prerogative and that the employee's use of the computer shall be made: "for work related purposes, fairly reasonably and in good faith according to the Law and this Agreement", but also stresses in subsection D that: "an Individual's Private life is no one else's affair and his dignity and privacy in the workplace shall be preserved and respected".
>
> III Article three deals with Rules of Conduct, of which the most important are subsection B, C & D. Sub Section B makes it clear that although the use of the computer is for work related purposes, the employee may "to a proportional degree and for a reasonable length of time" make use of it also for personal and private purposed that are not work related.
>
> While subsection C makes it clear that the activities made by the employer in subsection A. (which deals with uses, maintenance and soft wares), shall be done in "Good faith, reasonably, observing transparency and for a legitimate purpose" and

shall make “no use of personal Data of his employee in a harmful way that effects his dignity and private life.”

But perhaps the most important subsection is D: “in circumstances in which a reasonable employer would have a cause to assume in good faith that an employee is making an illegal use of the computer or such use that could expose the employer to a legal suit by a third party or such that can harm the enterprise, the employer shall be entitled to take actions to check the employee's computer, internet and/or e-mail, but it shall be done in a reasonable and proportional way, for a reasonable length of time and for the above mentioned purposes.

Any entry into a personal mail box bearing only the employee's mail address and his personal files requires an explicit consent by the employee, and shall be done in his presence if he so wishes.”

- that deals with situation in which the employer shall be entitled to check the employee's computer, internet and or E-mail, the key words being in the beginning of this section: “In circumstances in which a reasonable employer would have a cause to assume in good faith…”, that means that this right of the employer to actively monitor or check the employee's computer: internet and or E-mail - should not be used on a whim, arbitrarily or out of pure unfounded suspicion but has to be well grounded on reasonable causes and in good faith.

It is important to stress in this context that this subsection deals with two situation: the first one in which the mail box is allocated by the employer and bearing the mail address at work (i.e.: shelleywallach@court.gov.il), and the second, in which case the mail address has been chosen as a private address by the employee but while using the employers server and on the computer made available to him by his employer (i.e.: shelleywallach@gmail.com).

In the later case, any entry or checking of this mail box can be done only subject to the employee's consent and also in his presence if he so wishes.

Again it is worth to point out, that this subsection, as indeed the Agreement itself, does not touch on a situation whereby the computer itself and the mail box is on a computer owned by the employee himself but only the one owned by the employer.” (the collecteve agreement and the lecture of Shelley Wallach are attached).

Such a collcteve agreement, to my best knowledge, is the second one in the world after Belgium).

The issue of employer’s right to check his emplyee’s e-mail was discussed with regard to the acceptability of employee’s email as evidence in court. (this was a case where the collective agreement did not apply). In that case, an employee claimed that she was unlawfully fired while being pregnant (it is illegal to fire a pregnant woman in Israel). The employer claimed that she was seeking another job and brought as evidence an e-mail she sent to a friend with her CV. It was ruled that the employee’s right to privacy must be balanced with the employer’s property rights. The court decided that there should be a distinction between private emails and work-related emails. It should be checked whether the employee knew her e-mail was being scrutinized. In this case the emplyee has consented to a virus check of her e-mails. It was ruled that this was a consent to brief reading of her mail. The court distinguished between data derived from e-mails (including for exmaple the subject line in the emails) to their content. The evidence was accepted. This case (and another similar case in which the evidence was not axepted) are waiting for a decision of the appealate court (The National Labour Court)

Another law that specifically reffers to employees is defamaiotn Law - 1961 The law prohibits publications that could harm a person’s job, proffession or work.

Part 3. Questions number **12 &13**

(1) The employer may need facts in order to establish the salary of the employee. Thus he has to know the adress, the marital status, tax related information etc. If there is a judgement according to which the employer is obliged to deduct from the employees salary a debt that the employee has, the employer must know of it and act according to the judgment.

(2) There are several cases regarding the employer's right to find out information about a prospective employee prior to hiring him.

- It was ruled that suitability tests are acceptable only as far as they are specific for the job, are made with the prospective employee's consent and their infringement of privacy must be minimal.

- In another case the legality of a graphological test was examined. The majority opinion was that a graphological test is a non-proportianate infringement of privacy.

- As for lie-detector exams, in this case the courts have applied a proportionality test, ruling that lie detectors can only be used for a proper purpose and only if there is no other mean that can be used which is less intrusive.

(3) Governement offices and most public employers demand medical check ups before hiring a person. This issue is disputed. In my view the medical check up has to be proportional, namely, relevant to the specific job. If for example a worker has to work on hights, it is essential that he will not have epilepsy. Such a medical exam is relevant in this case. On the other hand if he has to work in an office, this question should not be relevant. The law, as well as the common law, does not allow to discriminate against workers becouse of irrelevant reasons. Thus if the medical condition is not relevant to the performance of the specific work, an employer should not be able to ask about it. Israel has a law - **Law of Equal Rights for people with disability**. Not excepting disable people to work because of irelevant health problems violates this law. It discriminates against people with a disability.

(4) The Equal Opportunities at Work Act, 5748-1988 states in article 2 that

(a) An employer shall not discriminate among his employees or among persons seeking employment on account of their sex, sexual tendencies, personal atatus or because of their age, race, religiona, nationality, country of origin, views, party or duration of reserve service, within the meaning thereof under the Defence Service Law,

This law specificallly prohibits employers from asking applicants for employment or employees for their military profile (information involving their medical and phsycological condition during their compulsary military service) exept if needed for security jobs.

The list in my view gives just examples. Any irrelevant discrimination is forbiden.

(5) Criminal convictions: An amnedment to **The law of criminal record and rehabilitaion 1981** (from 2008) prohibits employers from obtaining information about prior convictions of their employees (or prospective employees). Exceptions to this law include rules applying to candidates for admission to the Bar and the Israeli Bar Association is allowed to obtain information of prior convictions.

Laws that deal with specific professions allow questioning on relevant issues to those professions. Thus a law about psychologists allow checking of their mental condition, mental

illnesses etc. Other laws that demand special licencing, like social workers, allow questioning about relevant issues.

* I am attaching part of an article I wrote on good faith in labour law (The Principle of Good Faith in Labour Law). A book written in honor of Ruth Ben Israel). This part deals with good faith in accepting people to work. Good faith in the Israeli legal system is considered an objective criterion. It is an objecteve legal measure of behaviour.

V. Good Faith in Hiring Candidates – the

Pre-Contractual Stage

During the negotiations that precede the hiring of an employee (negotiations between a potential employer and a potential employee, or negotiations by means of tender) civil rights may be at loggerheads with each other. The principle of good faith applies to the pre-contractual stage. The balancing of rights and conflicting interests must be inspired by good faith. The employer's interest is to manage his enterprise well and in order to do this it is essential that he hire only the most successful and suitable workers. It is his interests to receive maximum information from the potential employee. The employer may have several reasons for wanting to receive the maximum amount of information from the candidate:

1. The employer wants to hire the most suitable employees in order to manage his enterprise under optimal conditions.

2. There are positions which require a professional license, such as law or medicine. The employer cannot employ workers of this kind who do not have such a license.

3. In order to prevent lawsuits against the employer arising from negligence in hiring employees. Suits of this type have been on a rise around the world.

4. In order to insure safety in the workplace by hiring employees, who can be trusted completely.

Many employers and labour relations consultants such as psychologists claim that it is essential that the employer acquire not only information directly relevant to the specific employment, but also information about the physical and mental health of the potential employee.

The employee has an interest in being hired to work in a workplace where his human dignity can remain intact despite the inequality between him and the employer during negotiations. The employee desires that his privacy will not

be unreasonably intruded upon and also that he receive maximum information on the employer and place of work.

What is the employee's duty of disclosure during negotiations? How can a balance be struck between the duty of disclosure and the protection of privacy? What is the correct balance between the obligation of equal treatment and the right to autonomy of personal will? I will examine all of these questions as they pertain to individuals in the relationship of employee with an employer which is a private enterprise providing a public service, and employee with a government employer.

1. Obligation of Disclosure

The hiring of an employee is done by the simultaneous acts of the employer offering a job position and the candidate offering his services. Negotiations take place and eventually the employer chooses a person whom he believes to be the most suitable candidate for the job. The Law of Contracts applies to the negotiations between the

parties, including the obligation in article 15 of the Law. The Law also applies to non-contractual relationships (art. 6l(b) of the Law of Contracts). Article 15 requires that:

> **15. Whoever enters a contract because of a mistake that is the result of the deception of the other party to the contract or someone on his behalf, may cancel the contact; For these purposes 'deception'- including the lack of disclosure of information which according to law, custom or circumstances should have been disclosed to the other party**.

The question is what is the obligation of disclosure according to custom or circumstances which applies to the party to negotiations. The obligation of disclosure in article 15 is subject to the obligation of article 12 of the same law to negotiate in good faith. The custom and circumstances are subject to the obligation of good faith. Under the obligation of disclosure, the interests of the other party with whom he plans to cooperate for a long period must be considered. This activity will constitute a significant part of the lives of both parties. The parties must depend on one another. Each party must have relevant information n respect of the other party. The obligation of good faith requires complete disclosure of all aspects concerning the employment. For example, if a person wishes to hire a caretaker for his children, he must completely disclose all of the particular characteristics of his children and any special difficulties the caretaker may encounter. The caretaker has a similar obligation. He must disclose all of the details of his experience in caring for children, facts relating to unsuccessful care, relevant character traits and so on. This obligation results from the obligation of disclosure end an increased obligation of good faith. This is all the more true when the hiring is done by means of a tender, which is a special way of conducting negotiations 24. he laws of tenders, by definition, require a greater obligation of disclosure. The stages of a tender for hiring workers require a greater obligation of disclosure by law (the law of tenders and the increased requirement of good faith). As such, a tender for hiring workers is different from a tender for other services.

2. Intrusion of Privacy

The duty of disclosure is increased in an employer-employee relationship. It is not absolute, neither during negotiations before hiring nor in negotiations by means of a tender. The duty of disclosure is an intrusion on the privacy of the potential employee (the candidate) and the employer. Two opposing interests are contra posed one against the other. It is in the interests of the potential worker and employer not to answer questions which infringe on their privacy and are irrelevant to the specific work; opposed is the interest of the parties in creating an optimal workplace and work in optimal conditions as far as efficiency and workplace environment are concerned. The need to discover relevant information and protection of the privacy of the employee and employer must be balanced. The correct balance may be struck if we allow relevant questions concerning the relationship which is about to be created. The criterion for examining the balance between the duty of disclosure and the right to privacy must be objective. I will examine the different ways that information may be obtained from the candidate.

a. ***Questionnaire***

A candidate being interviewed for a job may be asked to fill in a questionnaire (either a written or an oral one). The same applies to a person submitting a tender, and may be a condition of the tender being accepted for consideration. It is important that these questions be answered truthfully.

Despite this, the obligation of good faith requires that the questions be relevant to the potential work, such that there is no useless and unreasonable invasion of privacy of the interviewee, but insuring the possibility of choosing the best candidate. The relevancy of

the questions should be examined using an objective criterion. There should be some sort of supervision of the type of questions asked. For example, the requirement of a specific talent is relevant, whereas questions regarding disappointments in romantic relationships may be an unlawful invasion of privacy. In Germany, the work council is authorized to check the questions asked of candidates and asked in tender questionnaires. In workplaces of less than 1,000 workers, the work council is authorized to make suggestions for changes to the questions and in workplaces with more than 1,000 workers the work council can veto questions which appear irrelevant.

b. ***Psychological Tests***

Many employers send workers to tests and meetings with psychologists. The psychologists ask questions relevant to the specific position such as whether the candidate was successful in previously held positions of a similar nature,

how he or she performs under pressure, and so on. Some psychologists ask invasive questions which are not related to the position to be filled, such as questions about the private lives of the employees, their sex lives, failures in their private lives and their religious beliefs. Employers may claim that this is the only way to determine the candidate's character and emotional health.

According to this claim, the employer must maintain a healthy environment in the workplace, including the integrity and honesty of the employees. As the examiners cannot ask direct questions relating to the integrity and honesty of candidates or their emotional health, the only way to find out about them is by asking generally invasive questions about their personal lives and the personal tendencies of the candidates. In the United States, candidates for the position of security guards in a large chain store were asked hundreds of invasive questions of the type mentioned. The psychologist examiners claimed that a security guard is a position with responsibility, that many security guards are caught stealing goods from the chain's stores, and that this is the only way to discover the character of the candidates. In order to protect the privacy of the candidate, the psychologists claimed that the candidate's details would not be disclosed by means of the chain's computer, because the details were filed according to numbers and would be anonymous. A few Californian Courts in which the claim of intrusion of privacy was first heard, concluded that candidates are eligible to less protection than employees. Others believed that there is no room to differentiate between the two. According to the first approach, the

employer may interrogate the candidate and invade his privacy much more than the privacy of an employee, for the employee is not free to apply to another employer. The employer can also directly supervise the performance of the employees and therefore an invasion of his privacy is less necessary. I do not agree with this approach. In the first place, the essence of labour law is the idea that not only the employee but also the candidate has a weaker bargaining position. The candidate wants to be hired and then frequently has no option but to answer the questions asked of him. This was the case in a Californian claim, *Sibi Soroka et al. v. Dayton Hudson Corp*. The candidate for a store security position continued to answer the questionnaire in the psychological test despite his increasing resentment at the questions, which became more and more invasive, because of his need to find work. In the second place, and more importantly, whether the questions are legitimate and should be allowed should be determined according to striking a balance between the duty of disclosure and the right to privacy. In order to strike a balance between the two rights, all the circumstances must be considered, including the uniqueness of labour law, the need for increased disclosure in continuing relationships such as an employment relationship, and along with all these the need to protect privacy.

The test is proportional. The criteria established by the German legal system, the source of the proportionality

test, are:

1. The criterion must be appropriate for achieving the goal.
2. The criteria must be essential, and no other means which infringe less on the rights of others are enough to achieve the goal.
3. The means must be proportional to the goal (proportionality in the narrow sense).

The Israeli Supreme Court referred to these three foundations in examining the principle of proportionality - In most legal systems, which accept the principle of proportionality, it has been determined that it is made up of three elements or subcriteria.

The first element of the proportionality principle is that a connection of suitability must be established between the goal and the means. The means which the administration has utilised needs to be derived from the goal, which the administration desires to achieve.

The second element of proportionality is that the means that the administration chooses must be the least harmful to the individual. The administrative tailor must sew an administrative suit in a way that is derived from the goal which guides him, while choosing the least prejudicing means.

The third element of proportionality is that the means that the administration chooses is not appropriate if its harm to the individual has no proportion when compared to the benefit it brings in achieving the goal. The is the test of the proportional means (or proportionality 'in the narrow sense')...The combination of these three elements – which sometimes overlap – compose the proportionality test, essential criteria in the operation of administrative discretion. More precisely, these elements are of principal importance. Their utilisation in each specific case may change according to the characteristics of the goal, and the type of injury to the individual.

The necessity of questions which invade privacy, will be examined according to this test and compared to the interest of creating optimal conditions in the workplace. Among the considerations taken into account is the right of the employer to discover all he can about the potential employee. This right will be juxtaposed against the rights of the employee and their proportionality assessed. There is no need to reach conclusive standards on the issue, if, in cases of invasion of privacy, a larger invasion is allowed of a candidate's privacy than an employee's.

c. ***Graphology***

Many workplaces regularly transfer a sample of the potential employees handwriting to a graphologist. This is a severe intrusion of an individual's privacy. Many countries do not allow graphologist evaluations of potential employees. In Germany, any such transfer of a potential handwriting sample is illegal. The supervision is carried out by the work council, which permits a graphological evaluation only as an exception. This exception has several conditions. First, the explicit consent of the candidate must be given that his handwriting be sent to a graphologist; a request that the candidate submit his handwritten resume is not sufficient. Secondly, even if the candidate's consent is given, the potential employer may only ask the graphologist questions relevant to the work that will be performed. The employer may not ask for a general evaluation. Thirdly, before sending the handwriting to the graphologist, the work council examines the questions which will be asked of the graphologist in order to assure their relevancy to the type of work to be

performed. In my opinion, graphology should be used as little as possible in screening job applicants, and should only be used in exceptional cases.

d. ***Assessment of a Job Applicant's Lifestyle***

Another invasion of privacy is interference with the private life of the candidate. I referred to this regarding the specific case of questions in psychological evaluations. The criteria should be similar to those used in questions asked by the employer, and not those asked by a psychologist. In one case where an employer hired an employee and than discovered that the female employee was married to her lesbian partner, the employer cancelled her employment. The US llth Circuit ruled that in general, employers should adhere to strict criteria. The employer must prove with a great deal of certainty that this aspect of the employee's private life will negatively affect her work in the workplace. Off-duty behavior may sometimes influence workplace behavior, but good faith requires a great deal of scrutiny before it is decided that a specific lifestyle may influence the decision to hire a new worker.

e. ***Medical Examinations***

The general requirement that an employee submit to a medical examination is not in good faith if that examination is not relevant to the job to be performed. Any such general requirement constitutes a severe invasion of privacy. In the first place, the examination itself is invasive and is not acceptable for every individual. Secondly, not hiring an individual for health reasons that are not related to the performance of the job may amount to unjustified discrimination between an employee who is unwell and his healthy colleague. Therefore, the prerogative of employer to require that employees take medical examinations should be referred to examinations that are relevant to the work to be performed. Not hiring an epileptic for secretarial duties is, in my opinion, discriminatory and based on irrelevant considerations. Not hiring an epileptic as a construction worker who is required to work on scaffoldings is based on relevant considerations. The consideration that the employer may have to pay an early pension because of early retirement for health reasons is a faulty consideration. In my opinion, a consideration irrelevant to the work potential of the candidate is, therefore, a consideration which is not in good faith. The same is true regarding genetic testing of the candidate.

f. ***Conclusion***

My goal was to describe a few of the means by which employers attempt to evaluate the character, nature and history of the job applicant. Many of these means are put to use by potential employers in Israel. As such, the public's awareness of the subsequent invasion of privacy is very important. The legislator has referred to the need to limit the invasion of privacy in one instance. Article 2A of the Employment (Equal Opportunities) Law, 1988, determines that:

> **1. 2A**
>
> **(a) Employers shall not ask applicants for employment or employees for their military profile and shall not make use of his military profile, where it has been obtained by the employer, for any of the purposes enumerated in Section 2(a)(1) to (6).**
>
> **(b) Where an employer asks for a military profile, contrary to the provisions of subsection (a), he shall not prejudice such an employee or applicant for work in any matter enumerated in Article 2(a)(1-6) by reason of a refusal to give his military profile.**

One exception to this provision is when the army medical profile is relevant, such as would be the case with a national security position. Evaluation of the good faith of the

employer when hiring employees must be examined from an objective perspective. His behaviour must not unreasonably invade the privacy of the candidate.

We compare how we would expect a reasonable employer to behave with the behavior of the employer in the specific case at hand. Justice Steve Adler commented on this in the ruling regarding apptitude tests for candidates of internal tenders at Tel-Aviv University:

The University's right to send candidates of internal tenders [to tests] is subject to the University's notification of the Tender Committee regarding:

(l) the validity and reliability of the candidate's test

(2) that the test that the candidate has taken is relevant to the position and its requirements.

(3) that the Committee must chose the winning candidate by considering the sum total of all the information on the candidate and that the results of the suitability test are only one factor of this information.

In addition to this, the University must take all reasonable steps to maintain the privacy of the test takers so that the invasion of privacy will be reasonable, and not disproportional and the results of the tests must only be used for the purpose of hiring and promoting of employees.

Part 3. Question number **15**

There is no specific law regulating cameras in the workplace. The courts have discussed this issue and it was decided that installing such cameras is part of the employer's managerial prorogative, but that the cameras must be for a concrete and legitimate purpose. Such purposes may include safety, protection against theft and even a suspicion of a criminal action by an employee. The employer must notify the emplyee of the cameras. The court have applied the reasonableness, good faith and proportionality tests. For example, it was ruled that even when a camera is installed in a bank's vault, it should as much as possible, be targeted at the room's door and not at the empolyee. It was also ruled that the existance of employment relationship are not considered an implied consent to cameras.

In another case an emplyee discovered her workplace was scrutinized by cameras. She has violently pulled the cameras from the wall, and was thus fired. The court decided that the installation of cameras are a change in the working conditions. Since the conditions were worsened the employee was entitled to severance payment although her behavior was destructive.

In another case an evidence produced by an employer who compared his employees' reports with mechanical location reports (from a machine installed in their cars) was ruled legal. It was ruled that when the nature of the job is to travel, checking the employees' specific location is part of the employer's right to manage his employees.

Part 3. Question number **17**

There are no special statutory provision concerning "duty of confidentiality" in relation to members of its workforce and/or others. However a general duty of confidentiality is imposed on every employer towards his employees and vice versa. The source of this duty is either contractual good faith or a general common law duty of confidentiality between rmployer and employee

Part 3. Question number **18**

There are no specific statutory provisions concerning these questions. The answer to them is within the general duty of confidentiality of the employer under the employment contract, and the proper balance between those principles and other relevent values

Part 3. Question number **19**

Please view my answer to question number **15**

Part 3. Question number **20**

On principle of informed consent to a violation of privacy is legal, subject to the general rules of contract of employment (e.g. duress, mistake, the weaknes in bargaining ability of the cmployee vis-à-vis the employer). On top of it the consent has to be specific. The question arises for example when the consent of the worker is to cheque the computer for viruses. The question is if this is satisfactiory. The principle has to bend to the concept of public policy

Part 3. Question number **21**

The constitutional right to privacy in the **Basic Law: Human Dignity and Liberty** provides that

> **(b)There shall be no entry into the private premises of a person who has not consented thereto.**
>
> **(c) No search shall be conducted on the private premises or body of a person, nor in the body or personal effects.**
>
> **(d) There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.**

As mentioned the constitution aplies indirectly also to private relations. As such the interest of the employer has to be balanced with the right to privacy. There is no special law yet. Good faith and public policy have to conduct the behaviour of the employer.

Part 4. Question number **22**

Israel has a separate system of labour courts. There are five regional trial courts and one court of appeal- the National Labour Court. In rare cases there may be a petition to the Supreme Court sitting as a High Court of Justice. The Supreme Court rarely interferes. It only interferes when questions of general law arise or a consititional question is involved or there is an extreme mistake.

The labour courts deal with individual disputes and collecteve disputes. Thus the court may deal with any intrusion into privacy of either a candidate to be employed, or an employee or an employer.

The jurisdiction of the Labour Cort in individual disputes is:

A Regional Cour shall have exclusive power to hear:

> **(1) actions between an employee or his successot and an employer of his succesor, which arise out of employee-employer relationship, including the questionof the existence of an employee-employer relationship**
>
> **(1a) An action involving negotiations for a contract to create an employee-employer relationship, or after after the termination of the aforesaid relationship or an action involving acceptance or non-acceptance for employment.**

Thus every dispute about infringement of privacy may occur in all stages of the relationship – the stage of negotioations including beeds (tenders) to be accepted to work. Questions in tenders that infringe privacy have to be chequed for their relevance as well as proofing that they are propotional to the harm they cause.

The union might file a case in the collecteve relations when the union considers questions in a tender not legitimate.

The above cases considering apptitude tests to be excepted to work in the tel aviv university are such cases.

Part 4. Question number **23**

The court may deal with questionairs regarding acceptance to work. During the negotiations that precede the hiring of an employee (negotiations between a potential employer and a potential employee, or negotiations by means of tender) there is always an intrusion to privacy. The court is balancing between the relevance and importence of the questions and the intrusion into privacy.

The court dealt with the question if medcal examintions. The question arises if sending the handwriting to a Grapologists is legitimate or if demanding a polygraph test is not an unproportional mean (see the judgment attached of **Sharon Plotkin and The Israel Women's Network v. Eisenberg Bros. Inc.** attached.

The labour court deals also with cases of discrimination. This is the case when intruding privacy with irelevant questions. This might cause discrimination of a worker or a candidate. This is the case for example when the cmployer or potencial employer asks about health information, religion, age, intention of a woman to become pre gnant etc. if the information asked is irrelevant to the kind of work. The result might be discrimination against people witourth disability, which is forbiden by the law - **Equal Rights of Person with Disability,** or any other irelevant feature.

Part 4. Question number **24**

There is a constitutional right to aproach the court. Therefor the principle is the the proceedings have to be in open court. Proceedings in closed doors is an exception.

The law thas dictates the way courts should act is **The Courts Law 1984**, which indicates that as a rule all proceedings should be open to the public unless any law allows exceptions. The court may consider hearing a case in closed doors when:

(1) to protect state security

(2) to prevent a harm in foreign affairs of the state

(3) to protect morality

(4) to protect a minor, a helpless person as defind by law as well as a porson woth a mental or psychological disability as defind by law

(5) in order to protect a complainant or accused in sexual offence or an offence acording to the **Law to avoid sexual harasment- 1998**

(6) the public hearing might deter a witness from giving evidence freely or from giving evidence at all

(7) to protect a comercial secret

(8) to protect a witness on secret knowledge

The **Law to prevent Sexual Harassment 1998** gives authority to the labour court to deal with all cases of sexual harassment at work. The same principle of hearing the case in closed doors applies here too. Exept this specific law the principles of the **law of courts** applies to the labour courts as well.

The court that hears a case in closed doors has to write an accurate protecol. The rule is that the court should be open. Closed doors is an exception. The decision to hear a case in closed doors is an interemediate decision on which the appeal is be leave.

There is the theoretical posibility to approach the Supreme Court in its capacity as a High Court of Justice. But in fact the Supreme Court does not interfere in such discretionary questions/

Part 4. Question number **25**

Israel has a constitutional right to freedom of speech, derived from the reight to human dignity. Israel also has a constitutional right to privacy. The constitutional rights are not absolute. The rights have to be balanced vis-à-vis other rights, values and interests. The law **Protection of Pivacy Law** protectes privacy –

No person shall infringe the privacy of another without his consent.

Thus privacy has to be balanced vis-à-vis the right to free speech and press and the right of the public to have a free market of ideas.

The Israely Supreme Court tends to give priority to free speech in an ante case, and allow suing post for defamation according to the **Defamation Law, 1966**. There is no special law for tne labour courts in this area. The general rules apply.

Attached laws, the Collective Agreement and articles

(some laws and articles I will send seperately by e-mail as there is no possibility to copy them from the internet

BASIC LAW: HUMAN DIGNITY AND LIBERTY,

5752-1992

Basic principles

1. Fundamental human rights in Israel are founded upon recognition of the value of the human being, the sanctity of human life, and the principle that all persons are free; these rights shall be upheld in the spirit of the principles set forth in the Declaration of the Establishment of the State of Israel.

Purpose

1A. The purpose of this Basic Law is to protect human dignity and liberty, in order to establish in a Basic Law the values of the State of Israel as a Jewish and democratic state.

Preservation of life, body and dignity

2. There shall be no violation of the life, body or dignity of any person as such.

Protection of property

3. There shall be no violation of the property of a person.

Protection of life, body and dignity

4. All persons are entitled to protection of their life, body and dignity.

Personal liberty

5. There shall be no deprivation or restriction of the liberty of a person by imprisonment, arrest, extradition or otherwise.

Leaving and entering Israel

6. (a) All persons are free to leave Israel.

(b) Every Israel national has the right of entry into Israel from abroad.

Privacy

7. (a) All persons have the right to privacy and to intimacy.

(b) There shall be no entry into the private premises of a person who has not consented thereto.

(c) No search shall be conducted on the private premises or body of a person, nor in the body or personal effects.

(d) There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.

Violation of rights

8. There shall be no violation of rights under this Basic Law except by a Law befitting the values of the State of Israel, enacted for a proper purpose, and to an extent no greater than is required, or by regulation enacted by virtue of express authorization in such Law.

Reservation regarding security forces

9. There shall be no restriction of rights under this Basic Law held by persons serving in the Israel Defense Forces, the Israel Police, the Prisons Service and other security organizations of the State, nor shall such

rights be subject to conditions, except by virtue of a Law, or by regulation enacted by virtue of a Law, and to an extent no greater than is required by the nature and character of the service.

Validity of laws

10. This Basic Law shall not affect the validity of any law in force prior to the commencement of the Basic Law.

Application

11. All governmental authorities are bound to respect the rights under this Basic Law.

Stability

12. This Basic Law cannot be varied, suspended or made subject to conditions by emergency regulations; notwithstanding, when a state of emergency regulations; notwithstanding, when a state of emergency exists, by virtue of a declaration under section 9 of the Law and Administration Ordinance, 5708-1948, emergency regulations may be enacted by virtue of said section to deny or restrict rights under this Basic Law, provided the denial or restriction shall be for a proper purpose and for a period and extent no greater than is required.

PROTECTION OF PRIVACY LAW 5741-1981

CHAPTER ONE: INFRINGEMENT OF PRIVACY

1. Prohibition of infringement of privacy

No person shall infringe the privacy of another without his consent.

2. What is infringement of privacy

Any of the following constitutes an infringement of privacy:

(1) Spying on or trailing a person in a manner likely to harass him, or any other harassment;

(2) listening in prohibited under any Law;

(3) photographing a person while he is in a private domain;

(4) publishing a person's photograph under circumstances, in which the publication is likely to humiliate him or to bring him into contempt;

(5) copying or using, without permission from the addressee or the writer, the contents of a letter or of any other writing not intended for publication, unless the writing is of historical value or fifteen years have passed since the time when it was written;

(6) using a person's name, appellation, picture or voice for profit;

(7) infringing an obligation of secrecy laid down by law in respect of a person's private affairs;

(8) infringing an obligation of secrecy laid down by explicit or implicit agreement in respect of a person's private affairs;

(9) using, or passing on to another, information on a person's private affairs, otherwise than for the purpose for which it was given;

(10) publishing or passing on anything that was obtained by way of an infringement of privacy under paragraphs (1) to (7) or (9);

(11) publishing any matter that relates to a person's intimate life, state of health or conduct in the private domain.

3. Definition of terms

In this Law

"person" does not - for purposes of sections 2,7,13,14 and 25 - include a body corporate;

"consent" - explicit or implied consent;

"holder, in connection with database" - a person, who has a database in his permanent possession and who is entitled to use it;

"publication" has the meaning it has in the Defamation (Prohibition) Law, 5725-1965

"photography" includes filming;

"use" includes disclosure, transfer and delivery.

4. Infringement of privacy - a civil wrong

An infringement of privacy is a civil wrong, and the provisions of the Civil Wrongs Ordinance (New Version) shall apply to it, subject to the provisions of this Ordinance.

5. Infringement of privacy - an offense

If a person willfully infringes the privacy of another in any of the ways stated in section 2 (1), (3) to (7) and (9) to (11), then he is liable to five years imprisonment.

6. Trifling act

No right to bring a civil or criminal action under this Law shall accrue through an infringement that has no real significance.

CHAPTER TWO: PROTECTION OF PRIVACY IN DATA BASE

7. Definition

In this Chapter and in Chapter Four -

"data security" - protection of the integrity of data, or protection of the data against exposure, use or copying, all when done without due permission;

"data base" - a collection of data, kept by magnetic or optical means and intended for computer processing, exclusive of -

(1) a collection for personal use other than for business purposes; or

(2) a collection that includes only names, addresses and ways of communicating, which by itself does not create any characterization that infringes on the privacy of the people whose names are included in it, or condition that neither the owner of the collection, nor a body corporate under his control owns an additional collection,

"information" - data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person,

"sensitive information" -

(1) data on a person's personality, private family relations, state of health, economic condition, opinions and faith,

(2) information which the Minister of Justice - by order with approval by the Knesset Constitution, Law and Justice Committee - designated as sensitive information.

"data base manager" - the active manager of the body, which owns or holds a data base, or a person authorized for this person by the aforesaid manager;

"Registrar" - a person qualified to be appointed Magistrates Court judge, whom the Government appointed by, notice in Reshumot, to keep the "Register of Data Bases" (hereafter: Register) as said in section 12;

"integrity of information" - the identity of data in the data base to the source from which they were derived, without having been changed, delivered or destroyed with due permission.

Article One: Data Bases

8. Registration and use of data base

(a) No person shall manage or possess a data base that the must be registered under this section, unless one of the following holds true:

(1) the data base was registered in the Register;

(2) an application for registration of the data base was submitted and the provisions of section 10 (b1) are complied with,

(3) the data base must be registered under subsection (e) and the Registrar's instructions included permission to operate and keep the data until it is registered.

(b) No person shall use information in a data that must be registered under this section, except for the purposes for which the data base was set up.

(c) The obligation of registration in the Register falls on the owner of the data base, and the owner of the data base must register it if one of the following applies,

(1) the data base includes information about more than 10,000 persons;

(2) the data base includes sensitive information;

(3) the data base includes information about persons and the information was not provided to the data base by them, on their behalf or with their consent;

(4) the data base belongs to a public body, within its definition in section 23;

(5) the data base is used for direct mail, as said in section 17c.

(d) The provision of subsection (c) shall not apply to a data base which only includes information made public by lawful authority, or which was opened to public inspection by lawful authority.

(e) The Registrar may, for special reasons which shall be recorded, order hat the obligation to register be in effect for data bases that are exempt of the obligation to register under subsection (c) and (d); a said order shall be served on the owner of the data base, and in it the registrar shall spell out directions for the operation and maintenance of the data base until its registration; the owner of the data base may appeal against a decision of the Registrar under this subsection before the District Court within 30 days after he was served notice of the Registrar's decision.

9. Application for registration

(a) An application for registration of a data base shall be submitted to the Registrar.

(b) An application for registration of a base shall specify -

(1) the identities of the owner of the data base, of the person who holds possession of the data base, and their addresses in Israel;

(2) the purposes of setting up the data and the purposes for which the information is intended;

(3) the types of information to be included in the data base;

(4) particulars on the transfer abroad of information;

(5) particulars on the constant receipt of information from a public body, as defined in section 23, the name of the public body that provides the information provided, exclusive of particulars delivered by consent of the persons who are subjects of the information.

(c) The Minster may-by regulations - prescribe further particulars to be stated in the application for registration.

(d) The owner or possessor of a data base shall notify the Registrar of every change in any of the particulars specified in subsection (b) or prescribed under subsection (c), and of the discontinuation of the operation of the data base.

10. Power of Registrar

(a) When an application for registration of a data base has been submitted -

(1) the Registrar shall register it in the Register within 90 days after the application was submitted to him, unless he has reasonable grounds to assume that the data base is used or is liable to be used for illegal activities or as a cover for them, or that the information included in it was obtained, accrued or was collected in violation of this Law or in violation of the provisions of any enactment.

(2) The Registrar may register a purpose different from that specified in the application, register a number of purposes for a data base, of order that several applications be submitted instead of the application that was submitted, all if he concludes that doing so is appropriate to the actual activity of the data base,

(3) The Registrar shall refuse to register a data base under paragraph (1) or use his powers under paragraph (2) only after he gave the applicant an opportunity to state his case.

(b) The owner of a data base may appeal before the District Court against a decision by the Registrar under subsection (a), within 30 days after he was served notice of the decision.

(b1) If the Registrar did not register the data base within 90 days after the day on which the application was submitted and if he did not inform the applicant of his refusal to register, or of a delay in the registration for special reasons which shall be specified in his notice - then the applicant may operate or keep the data base, even if it is not registered.

(b2) If the Registrar informed the applicant of his refusal to register the data base, or of a delay as said in subsection (b1), then the applicant must not operate or keep the data base, except when the Court has decided otherwise.

(b3) The Registrar shall strike the registration of a data base from the Register, if the owner of the data base informed him that the information in that data base has been deleted and if he supported his notice by affidavit; if the data base was kept by a person different from the owner of the data base, then the notice shall also be supported by an affidavit of the person who kept it.

(c) The Registrar shall supervise compliance with the provisions of this Law and of the regulations thereunder.

(d) The Minister of Justice shall, by order with approval by the Knesset Constitution, Law and Justice Committee, set up a unit for the supervision of data base, for their registration and for the security of the information in them: the size of the unit shall be according to the needs of supervision.

(e) The Registrar shall head the supervision unit and he shall appoint inspectors to carry out the supervision under this Law, only persons with suitable professional training in computers, information security and the use of authorities under this Law shall be appointed inspectors, if the Israel Police expressed no objection to their appointment for reasons of public security.

(f) In order to perform his duties, an inspector may -

(1) require any concerned person to deliver to him information and documents related to a data base,

(2) to enter any place in respect of which it is reasonable to assume that a data base is operated there, to conduct a search there and to seize any object, if he satisfied that it is necessary to do, so in order to assure implementation of this Law and to prevent violation of its provisions: the provisions of the Criminal Procedure Ordinance (Arrest and Searches) (New Version) 5792-1969 shall apply to any object seized under this section: arrangements for entry into a military installation or into an military installation or into an installation of a security authority, within its meaning in section 19(c), shall be prescribed by the Minister of Justice, in consultation with the Minister in charge of the security authority, as the case may be; in this paragraph: “object” includes computer material and output, within their definitions in the Computers Law 5755-1995:

(3) notwithstanding the provisions of paragraph (2), he shall enter a said place that is used only for residential purposes only under an order from a Magistrates Court judge.

Note: The designation of both the preceding and the following subsections as “(f)” is the result of an apparent eitor in the Hebrew original of Amendment No. 4 - Tr.

(f) If the possessor or the owner of a data base infringes any provision of this Law or of regulations thereunder, or if he fails to comply with a request made to him by the Registrar, then the Registrar may apply to the District Court fir an order that cancels the registration of the data in the Register or suspends it for a period prescribed by the Court.

(g) The Registrar and any person who acts on his behalf shall be treated as State employees.

10A. Privacy protection report

The Privacy Protection Council shall submit to the Knesset Constitution, Law and Justice Committee, not later than April 1 of each year, a report prepared by the Registrar about enforcement and supervision activities during the year that preceded the submission of the report, together with the Council's comments.

11. Notice to accompany request for information

Any request to a person for information, with the intention to keep and use it in a data base, shall be accompanied by a notice that indicates -

(1) whether that person is under a legal obligation to deliver that information, or whether its delivery depends on his volition and consent;

(2) the purpose for which the information is requested;

(3) to whom the information is to be delivered and for what purpose.

12. Register of data bases

(a) The Registrar shall keep a Register of data bases, which shall be open for inspection by the public.

(b) The Register shall include the registration particulars stated in section 9.

(c) Notwithstanding the provisions of subsections (a) and (b), the particulars said in section 9 (b) (3), (4) and (5) shall not be open to inspection by the public for data bases of security authorities.

13. Right to inspect information

(a) Every person is entitled to inspect - in person, through a representative authorized by him in writing, or through his guardian - any information about him which is kept in a data base.

(b) The owner of a data base shall, at the request of a person said in subsection (a) (hereafter: applicant), make it possible to inspect the information in the Hebrew, Arabic or English language.

(c) The owner of a data base may refrain from delivering to the applicant information that relates to his state of physical or mental health, if he believes that the information may cause severe harm to the applicant's physical or mental health or endanger his life; in such a case the owner of the data base shall deliver the information to a physician or psychologist on the applicant behalf.

(c1) The provisions of this section shall not obligate the owner of a data base to deliver information in violation of its privileged status, as prescribed under any enactment, unless the applicant's is the person for whose benefit the privilege is intended.

(d) The manner and conditions in which the right to inspect information can be exercised, and payment therefor shall be prescribed by regulations.

(e) The provisions of this section and of section 13A shall not apply -

(1) to the data of a security authority, within its meaning in section 19 (c);

(1a) to the data base of the Prisons Service;

(2) to the data base of a tax authority, within its meaning in the Tax Law Amendment (Exchange of Information Between Tax Authorities) Law 5727 - 1967;

(3) when the security or the foreign relations of the State or the provisions of any enactment require that information about any person not be disclosed to him;

(4) to the data base of any body, in resect of which the Minister of Justice determined in consultation with the Minister of Defense or the Minister of Foreign Affairs, as the case may be, and with approval by the Knesset Defense and Foreign Affairs Committee - that it includes information which the State's defense or foreign affairs require that it not be disclosed (hereafter'

secret information), however, any person who requests to examine the information about himself stored in that data base shall be entitled to examine the information that is not secret information;

(5) to a data base about investigation and law enforcement by an authority lawfully authorized to investigate an offense, so determined by the Minister of Justice by order with approval of the Knesset Constitution, Law and Justice Committee.

13A. Inspection of material not of the owner of a data base

Without derogating from the provisions of section 13-

(1) if the owner of a data base keeps it with another (in this section- possessor) - then he shall refer the applicant to the possessor, stating his address, and he shall instruct the possessor in writing that ha make the inspection possible;

(2) if the applicant first applied to the possessor, then the possessor shall inform him whether he holds information about him, and also of the name and address of the owner of the data base.

14 .Amendment of information

(a) If, on inspecting information about himself, a person finds that it is not correct, not complete, not clear or not up to date, he may request the owner of the base or - if that owner is foreign resident - its possessor to amend or delete the information.

(b) If the owner of a data base agrees to a request under subsection (a), he shall make the necessary changes in the information and he shall communicate it to every person who received the information from him within a period prescribed by regulations.

(c) If the owner of a data base refuses to comply with a request under subsection (a), he shall give notice to that effect - in the form and manner prescribed by regulations - to the person who made the request.

(d) The possessor must correct information, if the owner of the data base agreed to the requested correction, or if a Court ordered the correction to be made.

15. Appeal to Court

A person who requested information may - in the form and manner prescribed by regulations - appeal to a Magistrates' Court against a refusal by the owner of a data base to enable him to make inspection under section 13 or section 13A, and against a notice of refusal under section 14(c).

16. Secrecy

No person shall disclose any information obtained by him by virtue of his functions as an employee, manager or possessor of a data base, save for the purpose of performing his work or of implementing this Law or under a Court order in connection with a legal proceeding; if a request has been made before a proceeding was instituted, it shall be heard in a Magistrates' Court; if a person violates the provisions of this section, he shall be liable to five years imprisonment.

17. Penalty

The owner of a data base, the possessor of a data base and the manager of a data base are each individually responsible for the protection of the information in the data base.

17A. Possessor of data bases of different owners

(a) A possessor of data bases of different owners shall make sure that only persons explicitly authorized therefor in a written agreement between him and the owner of that data base be allowed access to each data base.

(b) A possessors of at least five data bases that require registration under section 8, shall annually deliver to the Registrar a list of data bases in his possession, standing the names of the owners of the data bases, an

affidavit that the persons authorized to have access to each data base have been designated in agreements between him and the owners, and the name of the person in charge of security said in section 17B.

17B. Security officer

(a) The bodies specified below must appoint suitable trained persons to be in charge of information security (hereafter: security officer):

(1) a person who holds five data bases that require registration under section 8;

(2) a public body, as defined in section 23;

(3) banks, insurance companies and companies engaged in ranking or evaluating credit ratings.

(b) Without derogating from the provisions of section 17, the security officer shall be responsible for the security of information in data bases kept by the bodies said in subsection (a).

(c) A person found guilty of an heinous offense or of an offense against the provisions of this Law shall not be appointed security officer.

Article Two: Direct Mail

17C Definitions

In this Article -

"direct mail" - an individual approach to persons, based on their belonging to a population group determined by one or more characteristics of persons whose names are included in a data base;

"approach" - includes in writing, in print, by telephone, by facsimile, by computerized means and by some other means;

"direct mail services" - the provision of direct mail services to others by way of transferring lists, adhesive labels or data by any means whatsoever.

17D. Direct mail

No person shall operate or hold a data base used for direct mail services, unless he is registered in the Register, and unless one of his registered purposes is direct mail services.

17E. Stating source of information

No person shall operate or hold a data base used for direct mail services, unless he has a record stating the source from which he obtained every collection of data used for purposes of the data base and the date of its receipt, as well as the purpose to whom he gave any said collection of data.

17F. Deletion of information from data base used for direct mail

(a) Every direct mail approach shall include, clearly and prominently -

(1) a statement that it is a direct mail approach, also stating the registration number in the data base Register of the data base used for the direct mail services;

(2) notice that the recipient of the approach has the right to be deleted from the data base as said in subsection (b), and also whom to address for that purpose;

(3) the identity and address of the data base that includes the information according to which the approach was made, and the sources from which the owner of the data base received that information.

(b) Every person is entitled to demand - in writing - from the owner of a data base used for direct mail that information related to him be deleted from the data base.

(c) Every person is entitled to demand - in writing - from the owner of a data base used for direct mail or from the owner of a data base which includes information on the basis of which the approach was made,

that information related to him not be given to any person, to a category of persons or to certain persons, either for a limited period of time o permanently.

(d) When a person has informed an owner of a data base of his demand said in subsections (b) or (c), then the owner of the data base shall act in accordance with the demand and shall inform that person, in writing, that he has done so.

(e) If the owner of a data did not give notice as said in subsection (d) within 30 days after he received the demand, then the person to whom the information relates may apply to a Magistrates Court in the manner set by regulations that it order the owner of the data base to act as aforesaid.

(f) The rights under this section of a deceased person included in a data base shall also be held by his spouse, his child and his parent.

17G. Applicability to items of knowledge

The provisions of this Article shall apply to items of knowledge that relates to a person's private affairs, even if they do not constitute information, to the same extent that they apply to information.

17H. Not applicable to public body

This Article shall not apply a public body, within its meaning in section 23(1), when it performs its tasks under an enactment.

17I. Saving of enactments

The provisions of this Article are intended to add to the provisions of any enactment.

CHAPTER THREE: DEFENSES

18. Defenses

In any criminal or civil proceeding for infringement of privacy, it shall be a good defense if one of the following is the case: (1) the infringement was committed by way of a publication protected under section 13 of the Defamation (Protection) Law 5725-1965 ;

(2) the defendant or accused committed the infringement in good faith in any of the following circumstances;

(a) he did not know and need not have known that an infringement of privacy might occur;

(b) the infringement was committed under circumstances, under which the infringer was under a legal, moral, social or professional obligation to commit it;

(c) the infringement was committed in defense of a legitimate personal interest of the infringer;

(d) the infringement was committed in the lawful pursuit of the infringer's occupation and in the ordinary course of his work, as long as it was not committed by way of publication;

(e) the infringement was committed by way of taking a photograph in the public domain, or of publishing a photograph taken there, and the injured party appears in it coincidentally;

(f) the infringement was committed by way of a publication protected under paragraphs (4) to (11) of section 15 of the Defamation (Prohibition) Law 5725 - 1965;

(3) the infringement involved a public interest that justified it under the circumstances of the case, on condition that - if the infringement was committed by way of publication - the publication was not untruthful.

19. Exemption

(a) No person shall bear responsibility under this Law for an act which he is empowered to do by Law.

(b) A security authority 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 their performance.

(c) For purpose of this section, “security authority” - any of the following:

(1) the Israel Police;

(2) the Intelligence Branch of the General Staff of the Israel Defense Forces, and the Military Police;

(3) the General Security Services;

(4) the Institute for Intelligence and Special Assignments.

20. Onus of proof

(a) If an accused or defendant proves that he committed an infringement of privacy under any of the circumstances said in section 18(2) and that it did not exceed the limits reasonable under those circumstances, he shall be presumed to have committed it in good faith.

(b) The accused or defendant shall be presumed not to have committed the infringement of privacy in good faith, if - in committing it - he knowingly exceeded what was reasonably necessary for purposes of the matters protected by section 18(12).

(c) If an accused person or defendant pleads a defense under section 18(2)(d), he shall be presumed not to have infringed privacy in good faith if he infringed it in violation of the rules or principles of professional ethics that apply to him by Law or which are accepted by the members of the profession to which he belongs.

21. Rebuttal of defense pleas

If an accused or defendant produces evidence or testifies in person to prove one of the defense pleas provided by this Law, the prosecutor or plaintiff may produce rebutting evidence; this provision shall not derogate from the Court's power under any Law to permit the production of evidence by the parties.

22. Mitigating circumstances

In passing sentence or awarding compensation, the Court may also take the following into account in favor of the accused or defendant;

(1) that the infringement of privacy was merely a repetition of something said before and that he mentioned the source on which he relied;

(2) that he did not intend to commit an infringement;

(3) if the infringement was committed by way of publication - that ha has apologized and has taken steps to discontinue the sale or distribution of copies of the publication that contains the infringement, provided the apology was published in the same place and in the same dimensions and manner in which the infringing matter had been published, and that it was unqualified.

CHAPTER FOUR: DELIVERY OF INFORMATION BY PUBLIC BODIES

23. Definitions

In this Chapter -

“public body” -

(1) a Government department and other State institution, a local authority and any other body that performs lawful public functions;

(2) a body designated by the Minister of Justice, by order with approval by the Knesset Constitution, Law and Judiciary Committee, provided the order specifies the categories of information and of items which the body is entitled to deliver and to receive.

(3) Repealed

23A. Applicability to information

The provisions of this Chapter shall apply even to those items about a person's private affairs which do not constitute information, just as they apply to information.

23B. Must not deliver information

(a) A public body must not deliver information, unless it is information that has been published under lawful authority, or unless it has been made available for public inspection under lawful authority, or unless the person to whom the information refers agreed to its delivery.

(b) The provisions of this section shall not prevent a security authority, as defined in section 19, from accepting or delivering information in the performance of its function, as long as the acceptance or delivery was not forbidden by legislation.

23C. Limitation on prohibition

Notwithstanding the provisions of section 23B, delivery of information shall be permitted - if it is not prohibited by legislation or by professional ethics -

(1) between public bodies, when one of the following holds true:

(a) delivery of the information is part of the authority or of the functions of whoever delivers the information and it is required in order to implement legislation or for a purpose within the authority or the function of whoever delivers or receives the information;

(b) the information is delivered to a public body which is entitled to demand the information lawfully from any other source;

(2) from a public body to a Government department or to another State institution, or between aforesaid departments or institutions, if delivery of the information is required for the implementation of any legislation or for a purpose within the authority or within the scope of activity of whoever delivers or receives the information;

however, information provided on condition that it not be delivered to others shall not be delivered as

aforesaid.

23D. Obligations of public body

(a) If a public body regularly delivers information in accordance with section 23C, then it shall specify that fact on all its lawful requests for information.

(b) If a public body delivers information in accordance with section 23C, then it shall keep a record of the information delivered.

(c) If a public body regularly receives information in accordance with section 23C and stores that information in a data base, then it shall so inform the Registrar, and that information shall be included in the list of data bases under section 12.

(d) If a public body received information in accordance with section 23C, then it shall use it only within the framework of its authority and functions.

(e) In connection with the obligation, under any Law, to maintain confidentiality, information delivered to a public body under this Law shall be treated like any information obtained by that body from any other source, and all the rules applicable to the body that delivered the information shall also apply to the body that receives it.

23E. Surplus information

(a) If information which may be delivered under sections 23B or 23C is located in a single file, together with other information (hereafter: surplus information), then the body that delivers the information may deliver the requested information to the recipient body together with the surplus information.

(b) The delivery of surplus information under subsection (a) shall be conditional upon the establishment of procedures that will prevent any use at all being made of the surplus information received; the said procedures shall be prescribed by regulations and - as long as they have not been prescribed by regulations - the body that requests the aforesaid information shall specify procedures in writing and it shall deliver a copy of them to the body that delivers information, on its request.

23F. Permitted delivery does not infringe privacy

A delivery of information, which is permitted under this Law, shall not constitute an infringement of privacy, and the provisions of sections 2 and 8 shall not apply to it.

23G. Regulations on delivery of information

The Minister of Justice may, with approval by the Knesset Constitution, Law and Justice Committee, make regulations on ways of the delivery of information by public bodies.

23H. Repealed

CHAPTER FIVE: MISCELLANEOUS

24. The State

This Law shall apply to the State.

25. Death of injured party

(a) If a person, whose privacy was infringed, dies within six months after the infringement without having filed an action or complaint in respect thereof, then his spouse, child or parent, or - if he left no spouse, child or parent - his brother or sister may file an action or complaint in respect of that infringement within six months after his death.

(b) If a person, who filed an action or complaint in respect of an infringement of privacy, dies before the proceeding is concluded, then his spouse, child or parent or - if he left no spouse, child or parent - his brother or sister may, within six months after his death, notify the Court that they wish to proceed with the action or complaint, and upon that notification they shall take the place of the plaintiff or complainant.

26. Prescription

The period of prescription of civil actions under this Law is two years.

27. Applicability of certain provisions of the Defamation (Prohibition) Law

The provisions of sections 21,23 and 24 of the Defamation (Prohibition) Law 5725 - 1965, shall apply, mutatis mutandis, to legal proceeding for infringement of privacy.

28. Evidence of a person's bad reputation, character or past

In a criminal or civil proceeding for infringement of privacy, no evidence shall be produced, and no witness shall be examined on the bad reputation or on the character, past, activities or options of the injured party.

29. Additional orders

(a) In a criminal or civil proceeding for infringement of privacy, the Court may order, in addition to any penalty and other relief -

(1) that distribution of copies of the infringing matter be prohibited or that they be confiscated; a confiscation order under this paragraph is effective against any person who has such material in his

possession for sale, distribution or storage, also if he is not a party to the proceeding; if the Court ordered confiscation, then it shall direct how to dispose of the confiscated copies;

(2) that all or part of the judgment be published; publication shall be at the expense of the accused or defendant, in a place, of a size and at the manner prescribed by the Court;

(3) that the infringing matter be surrendered to the injured party;

(4) that the unlawfully received information be deleted, or that use of the said information - or of the surplus information, as defined in section 23E - is prohibited, or it may make any other in respect of the information.

(b) The provisions of this section shall not prevent keeping a copy of a publication in public libraries. archives and the like - unless the Court imposes a restriction also on that by a confiscation order under subsection (a) (1) - and they shall not prevent an individual keeping a copy of a publication.

30. Responsibility for publication in newspaper

(a) If an infringement of privacy is published in a newspaper, within its meaning in the Press Ordinance (hereafter: newspaper), then the criminal and civil responsibility for the infringement shall be borne by the person who brought the material to the newspaper and thereby caused its publication, by the editor of the newspaper and by the person who actually decided on the publication of the infringement in the newspaper, and civil responsibility shall also be borne by the publisher of the newspaper.

(b) In a criminal case under this section, it shall be a good defense for the editor of the newspaper that he took reasonable steps to prevent the publication of the infringement or that he did no know of the publication.

(c) In this section, “editor” of a newspaper includes an acting editor within the scope of the powers or functions of the body that transmits or receives the information.

31. Responsibility of printer and distributor

If an infringement of privacy was published in print, except in a newspaper published under a valid license at intervals of not less than forty days, then criminal and civil responsibility for the infringement shall also be borne by the possessor of the printing press, within its meaning in the Press Ordinance, on which the infringement was printed, and by the person who sells or otherwise distributes the publication; however, they shall not bear responsibility unless they knew or ought to have known that the publication contained and infringement of privacy.

31 A. Penalties in due diligence offenses

(a) If a person does one of the following, then he is liable to one year imprisonment:

(1) he operates, keeps or uses a data base in violation of section 8;

(2) he delivers false particulars in an application for the registration of a data base, an required in section 9:

(3) he does not deliver particulars or delivers false particulars in a notice attached to a request for information under section 11;

(4) he does not comply with the provisions of sections 13 and 13A, concerning the right to inspect information kept in a data base, or he does not correct a data base according to the provisions of section 14:

(5) he grants access to a data base in violation of the provisions of section 17 A (a). or does not deliverdocuments or an affidavit in accordance with the provisions of section 17 A (b) to the Registrar;

(6) does not appoint a security officer for the protection of information under section 17B.

(7) operates or keeps a data base used for direct mail services in violation of the provisions of sections 17D to 17F;

(8) delivers information in violation of sections 23B to 23E.

(b) An offense under this section does not require that criminal intent or negligence be proven.

31B. Civil wrong

An act or omission in violation of the provisions of Chapters Two or Four, or in violation of regulations made under this Law, shall constitute a civil wrong under the Civil Wrongs Ordinance (New Version).

32. Material inadmissible as evidence

Material obtained by the commission of an infringement of privacy shall not be used as evidence in Court without the consent of the injured party, unless the Court, for reasons which shall be recorded, permits it to be so used, or if the infringer, who is a party to the proceeding, has a defense or enjoys exemption under this Law.

33. Amendment of Civil wrongs Ordinance

Section 34A of the Civil Wrongs Ordinance (New Version) is hereby repealed.

34. Amendment of Criminal Procedure Law

In the Schedule to the Criminal Procedure Law 5725-1965, the following paragraph shall be added after paragraph (12):

"(13) offenses under the Protection of Privacy Law 5741-1981."

35. Saving of Laws

The provisions of this Law shall not derogate from the provisions of any other Law.

36. Implementation and regulations

The Minister of Justice is charged with the implementation of this Law and be may, with approval by the Knesset Constitution, Law and Justice Committee, make regulations on any matter that relates to its implementation and, inter alia, on -

(1) conditions for keeping and safeguarding information in data bases;

(2) conditions for transmitting information to or from data bases outside the boundaries of the State;

(3) rules of conduct and ethics for owners, possessors and operators of data bases;

(4) provisions on the deletion of information when a data base ceases to function.

36A. Fees

(a) The Minister may, with approval by the Knesset Constitution, Law and Justice Committee, set fees for registration and inspection under this Law.

(b) The fees collected under this section shall b allocated to the Registrar and to the supervision unit for their activities under this Law.

37. Effect

Chapter Two shall go into effect six months after the date of publication of this Law.

Unofficial translation:

Electronic Signature Law, 5761 - 2001

Chapter 1 : General

1. Definitions In this Act –

"Signature Verification Device" – unique software, object or information required for verifying that a secure electronic signature was created using a specific Signing device;

"Signing Device" – unique software, object or information required for creating a secure electronic signature;

"Certification Authority" – an authority that issues electronic certificates, and is registered in the Registry under the provisions of this Law;

"Foreign Certification Authority" - an authority recognized under section 22, and registered in the Registry under the provisions of this Law;

"Electronic Signature" – a signature that is electronic data or an electronic sign, that is attached to or associated with an electronic message;

"Secure Electronic Signature" – an electronic signature which meets all of the following requirements:

(1) It is unique to the owner of the Signing Device;

(2) it enables apparent identification of the owner of the Signing Device;

(3) it is created using a Signing Device that can be maintained under the sole control of the owner of the Signing Device;

(4) it enables identification of any change to the electronic message subsequent to signing;

"Certified Electronic Signature" – a secure electronic signature for which a Certification Authority has issued an electronic certificate regarding the signature verification device required for verifying it;

"Computer", "computer data", "output" and "penetration of computer material", as defined in sections 1 and 4 of the Computers Law, 5755-1995.

"Electronic Message" – information generated, sent, received or stored by electronic or optical means, while it is seen, read, heard or retrieved by aforesaid means;

"Registry" – the registry as described in section 9;

"Registrar" – the registrar appointed under section 9;

"Electronic Certificate" – an electronic message issued by a certification authority, under the provisions of Chapter 4, confirming that a certain signature verification device belongs to a certain person;

"Minister"- the Minister of Justice.

Chapter 2 : Validity of a Secure Electronic Signature

Signature Required by Law

2. (a) For any law requiring a signature on a document - such requirement may be fulfilled, in respect of an electronic message, by use of an electronic signature, provided that it is a certified electronic signature;

(b) The provisions of subsection (a) will not apply to laws which the Minister, following approval of the Constitution, Legislation and Law Committee of the Knesset, set forth in the First Schedule.

Admissibility of a Secure

Electronic Signature

3. An electronic message signed with a secure electronic signature is admissible in any legal procedure, and will constitute prima-facie evidence that :

(1) the signature is that of the owner of the signing device;

(2) the electronic message is that which was signed by the owner of the signing device.

Presumption Regarding Certified Electronic Signatures

4. A certified electronic signature is presumed to be a secure electronic signature.

Certification

Authority

Certificate

5. (a) A court of law may accept as evidence, unless it finds distortion of justice, any certificate signed by a manager of a Certification Authority or on his behalf, certifying that a certain electronic certificate was issued by that Certification Authority (hereinafter – Certification Authority Certificate);

Said certificate will be in such form as established by the Minister.

(b) A Certification Authority Certificate shall be considered Testimony for the purpose of Section 237 of the Penal Code-1977.

(c) The provisions of subsection (a) will not derogate from the court's authority to order that the Manager of the Certification Authority or any person on his behalf who signed the Certification Authority Certificate, be summoned for interrogation in court, and the court will grant request by any party to order so.

(d) If the court finds that the request for interrogation of the Certification Authority manager or any person on his behalf , as described in subsection (c), was vexatious or reckless, the court may impose interrogation costs on the requesting party.

Status of Computer

6. (a) Any output of an electronic message signed with a secure electronic signature, will not be regarded, in any legal proceeding,

Output as a copy of the electronic message based on which it was produced, but as the original message.

(b) The provisions of subsection (a) will not apply to any type of electronic message, categories of legal proceeding or any uses of data messages as set forth in the Second Schedule by the Minister and approved by the Constitution, Legislation and Law Committee of the Knesset.

Duties and Liability of Owner of Signing Device

7. (a) The owner of a signing device shall –

(1) Take all reasonable steps to protect his signing device and to prevent unauthorized use thereof;

(2) Notify, immediately upon the discovery that his signing device has been compromised, anyone who might reasonably rely on his electronic signature based on routine relations between them and anyone whom he knows will probably rely on his electronic signature;

(b) The owner of a signing device who fulfills his obligations as set forth is subsection (a), will not be liable for any damage caused by unauthorized use of his signing device.

Duties and Liabilities of Owner of a Certified Signature Signing Device

8. (a) The owner of a Certified Signature Signing Device shall –

(1) Comply with the provisions of section 7(a)(1);

(2) Provide the Certification Authority, upon such request, with information that is, to the best of his knowledge, correct and complete, as is required by the Certification Authority for carrying out its tasks under this Law;

(3) Notify the Certification Authority that issued the electronic certificate, immediately upon discovery that his signing device has been compromised.

(b)The owner of a certified signature signing device who fulfills his obligations as set forth is subsection (a), will not be liable for any damage caused by unauthorized use of his signing device.

Chapter 3 : Registration

Certification

Authority

Registrar

9. (a) The Minister shall appoint, from among the employees of the Ministry, a person qualified for being a Magistrates court judge, to be the Registrar.

(b) The Registrar shall maintain a Registry in which he shall register Certification Authorities and Foreign Certification Authorities under the provisions of this Law; The Registry shall be open to the public.

(c) The Registrar shall supervise Certification Authorities under the provisions of this law.

Application for Certification Authority Registration

10. (a) Applications for registration of a Certification Authority shall be submitted to the Registrar, and shall include the following:

(1) Name of applicant, name of intended Certification Authority manager, and address and identification details of each; In the event that the applicant is incorporated, the application shall also include documents of incorporation or documents on the basis of which it operates, names of controlling shareholders in the corporation, as well as names of managers, their addresses and identification details. For this purpose - "control" – as it is defined in the Securities law, 1968, and every term in such definition shall be inerpreted under said law;

(2) Information regarding additional occupations of the Applicant;

(3) Additional information as the Minister may prescribe.

(b) Documentation to indicate fulfillment of the required

conditions of application under section 11, shall be enclosed with the application.

(c) The Registrar may require the applicant to submit any additional information or documents necessary for review of application.

Conditions for Registration of Certification Authorities

11. (a) The Registrar shall register in the Registry any applicant who fulfills the provisions under this law as well as all of the following:

(1) He is a citizen or resident of Israel, a company incorporated in Israel or a Public Corporation or other Public Entity established by law, whose place of business or activity is in Israel, and among its objectives is conducting business or activity as a Certification Authority;

(2) He has trustworthy hardware and software systems, which provide reasonable protection from penetration, disruption, interference or damage to a computer or to computer material, and provide a reasonable level of availability and reliability;

(3) He filed a bank guarantee or other suitable guarantee, or insured himself with an Insurer as defined under the Law for Supervision of Insurance Businesses, 5741- 1981, all as will be prescribed by the

Registrar, for ensuring compensation for anyone suffering damage due to an act or omission of the Certification Authority.

(4) He registered his Electronic Certificate Databases, described in section 18(c), as databases under the Protection of Privacy Law, 5741-1981;

(5) The applicant as well as intended manager have not been convicted of a crime; If applicant is a corporation – no acting director or controlling shareholder has been convicted of a crime.

In this subsection –

"convicted of a crime" – including persons against whom an indictment has been filed and final judgement has not yet been given;.

"crime" – a crime that its nature, severity or circumstances are such that it is inappropriate for Applicant to be registered as a Certification Authority;

"control" – as defined in section 10.

(b) The Registrar may impose additional terms for registration as well as prescribe limitations on the activity of the Certification Authority pertaining to scope or type of activity, taking into consideration, inter alia, any additional occupation of the applicant.

Certification of Certification Authority

Signature

Verification

Device

Authority

12. The Minister may prescribe that the Registrar will certify the signature verification device of Certification Authorities, using his secure electronic signature; In regulations under this section, the Minister shall prescribe the manner and details of such certification.

Report of Changes to Registrar

13. In the event of any change in the information filed under sections 10 and 11, the applicant or the Certification Authority, whichever applicable, will so notify the Registrar within 15 days from the day he became aware of the change.

Deletion of Certification Authority

Registration or Suspension of its Effect

14. (a) If the Registrar finds that any Certification Authority does not comply with any of the provisions under this Law, he shall demand of the Certification Authority to correct whatever requires correction and he may, after having giving the Certification Authority opportunity to present its arguments, suspend the effect of its registration for a period no longer than 30 days, or to delete it from the Registry.

(b) In the event that the Registrar suspended the effect of registration under the provisions of subsection (a), and found that by the end of the period of suspension, the matter in need of correction had not been corrected, he may extend the period of suspension by an additional 30 days; In the event that the Registrar finds that by the end of the period of extension the matter in need of correction had not yet been corrected, he will delete registration of the Certification Authority in the Registry.

(c) The Registrar will publish a notice of suspension or deletion under this section, in the manner prescribed by the Minister.

Change of Circumstance

15. (a) If the Registrar finds that the hardware or software system maintained by the Certification Authority no longer complies with the conditions under section 11(a)(2), he may require that the Certification Authority make necessary adjustments under aforesaid conditions, within a period of time as he will prescribe.

(b) If the Registrar finds that circumstances have changed so as to require change of the guarantee or insurance provided under the provisions of section 11(a)(3), he may require change of the guarantee or insurance' within a period of time as he will prescribe.

(c) If the Certification Authority does not comply with the requirements under subsections (a) or (b), the Registrar may suspend the effect of registration or delete registration, according to the provisions of section 14.

Appeal of Registrar's Decision

16. Appeal on any decision of the Registrar under this law may be filed with the District Court by anyone against whom such decision was made, within 45 days from the day on which he was notified of such decision.

Authority of Registrar

17. (a) To enable carrying out his duties, the Registrar or a State employee whom he appointed, in writing, for such purpose (in this section – the Registrar), may supervise the activities of Certification Authorities, as follows:

(1) Demand of any person relating to the matter, to submit information and documentation referring to the activity of a Certification Authority;

(2) Enter, after identifying himself, into any place where a Certification Authority operates, and conduct an inspection; However, he may not enter into a place that serves solely for residential purposes, without a court order;

(3) Penetrate computer information and produce a printout thereof, provided that such penetration be conducted only by personnel trained in performance of such tasks;

(4) Seize any object, including documents, if he finds that seizure is required to assure implementation of this Law, or to prevent violation of its provisions;

Regarding seizure of any object that is a computer or computer information, the following provisions shall apply:

(a) The Registrar shall make a copy of the computer information, and will leave the original with the

owner;

(b) If the Registrar finds that leaving the original computer information with the owner might be disruptive to the supervision or its results, he will seize the original and leave a copy with the owner;

(c) If the Registrar finds that copying the computer information or leaving it with the owner might be disruptive to the supervision or its results, he will seize the computer information without making a copy thereof;

(d) The Registrar will not act under subsection (c) and will not seize any object that is a computer or a component thereof unless he obtains a court order;

(e) The court will grant an order under this section only if it convinced that seizure is necessary for conducting supervision; Such order will be in effect for no longer than 48 hours, and Saturdays and Holidays will not be taken into account; The court may extend the order, only after allowing the owner opportunity to state his claims.

(b) The Registrar will not appoint anyone under subsection (a), unless all of the following requirements are met:

(1) The Police Department has not given notice that it objects to the appointment for reasons of public security;

(2) He is skilled at conducting penetrations into computer systems and producing output as a result thereof;

(3) He received appropriate training, as prescribed by the Minister.

(c) When the Registrar acts under this section, the following provisions will apply:

(1) The Registrar shall maintain a list of all items seized in performance of the inspection, and the places in which they were found;

(2) The Certification Authority, or anyone on its behalf, will be allowed to be present during the inspection, and he will receive a copy of the list of seized items;

(3) The Magistrates Court under whose jurisdiction an object has been seized may, upon request of either the Registrar or anyone who claims rights in the object, order that the object be given to whoever claims rights to it or to anyone else or to act with it in any other manner, as prescribed by the court, and everything as under any conditions it may prescribe;

(4) A seized object will be returned as soon as possible, and no later than 15 days from the day it was seized.

Chapter 4 : Certification Authority

Activity of Certification

Authority

18. (a) A Certification Authority may issue an Electronic Certificate to a specific person, upon his request (hereinafter – the Applicant), indicating that a certain Signature Verification Device belongs to him.

(b) A certification Authority will not issue an Electronic Certificate unless it has taken reasonable measures to identify the Applicant, to check his Signature Verification Device and assure that the information in the application for issuance of a Certificate is accurate and complete.

(c) A Certification Authority shall maintain a database of Electronic Certificates that it issued, as well as a database of revoked Electronic Certificates, in accordance with the provisions of this law.

(d) In order to perform its obligations, a Certification Authority shall use only trustworthy hardware and software systems which provide reasonable protection from penetration, disruption, interference or damage to a computer or to computer material, and provide a reasonable level of availability and reliability.

Specification of Electronic Certificate

19. (a) A Certification Authority shall include at least the following details in an Electronic Certificate:

(1) Name of Certificate owner and his identification number, or any other identifying detail, as may be prescribed by the Minister;

(2) Confirmation regarding inspection of the Certificate owner's Signature Verification Device;

(3) Serial number of the Electronic Certificate in the database it maintains;

(4) Notification of means of identification of Certificate owner;

(5) Notification of beginning and ending dates for validity of the Certificate;

(6) Name and address of the Certification Authority, and statement of registration in the Registry;

(7) Secure Electronic Signature of the Certification Authority;

(8) Information regarding restrictions on permissible uses according to the Certificate, as there may be, and in the event of a limit on transaction sum according to the Certificate – specification of said sum;

(9) Information regarding limitations of Certification Authority Liability, if any exist; (10) Reference to the revoked Electronic Certificate database, in accordance with section 18(c).

(b) The Minister may, with the approval of the Knesset Committee for Scientific and Technological Research and Development, prescribe additional details to be included in an Electronic Certificate.

Revocation of an Electronic Certificate

20. (a) A certification Authority shall revoke an Electronic Certificate in any of the following: (1) Upon request from the owner of the Certificate, immediately following receipt of said request and verification of identity of whoever so requested;

(2) Immediately upon discovery that part of the information in the Certificate is incorrect, or that the Certificate is no longer reliable for any other reason, or that the Signature Creation Device of the owner of the certificate is no longer reliable;

(3) Following death of owner of Certificate, and if owner is a corporation – following an order for its liquidation, immediately upon receipt of such notice, provided that the Certification Authority has been convinced of the credibility of said notice;

(4) Immediately upon discovery of fault with its Secure Electronic Signature or with its hardware and software system, that might derogate from the reliability of its signature or of the Certificates it issues.

(b) Upon revocation of an Electronic Certificate, a Certification Authority shall immediately notify owner of the Certificate thereof, and shall record the revocation in a database in accordance with the provisions of section 18(c), in a manner as will be prescribed by the Minister.

Certification Authority Liability

21. (a) A Certification Authority will not be liable for any damage caused due to reliance on an Electronic Certificate that it issued, if it ascertains that it took all reasonable measures for fulfillment of its obligations under this Law;

(b) In the event that the Certification Authority limits Certificate uses or sums of transactions for which Certificates may be used, the Certification Authority shall not be liable for any damage caused due to use that exceeded any such limitation, provided that said limitation was specified in the Certificate, in accordance with the provisions of section 19; The provisions of this section will not be construed so as to affect the Certification Authority's right to prescribe additional limitations on its liability, subject to any law.

Chapter 5: Other Certificates of Foreign Certification

Authorities

22. (a) The Registrar may recognize as a Certification Authority, any authority from outside the State of Israel that verifies Electronic Signatures, provided that he finds that it fulfills conditions similar to those required of anyone requesting registration under the provisions of this law; If the Minister prescribes additional conditions under subsection (d) – the Registrar must base his findings on fulfillment of any additional conditions as well.

(b) The Registrar will enter into the Registry any Foreign Certification Authorities recognized under subsection (a);

(c) An Electronic Certificate issued by any Foreign Certification Authority that has been recognized and registered under the provisions of this section, shall be treated as an Electronic Certificate issued by a Certification Authority in Israel, under this Law.

(d) The Minister may prescribe what constitutes similar conditions, for the purpose of subsection (a), as well as additional conditions for the recognition of a Foreign Certification Authority under this section.

Applicability to Governmental Entities

23. The minister of Justice may prescribe special conditions for the transmission of electronically signed messages to or from governmental entities, following approval of the Constitution, Law, and Legislation Committee of the Knesset.

Implementation and Regulations

The Minister of Justice is charges with the implementation of this Law, and he may make regulations for its implementation, as well as prescribe the following – (1) Fees for Registration in the Registry and viewing thereof;

(2) Information to be included in the Registry, and directions as to maintenance thereof;

(3) Means of viewing the Registry, including by way of electronic communication and the Government Internet Site;

(4) Provisions regarding insurance, bank guarantee or any other guarantee, including type of guarantee, its amount, and means of filing, changing and forclosing thereof, under sections 11(a)(3) and 15(b);

(5) Additional conditions for registration of a Certification Authority, provisions regarding type and means of restricting its activity, and requirements regarding its operation, under section 11;

(6) Provisions regarding management of valid and revoked or suspended electronic certificates, including means of viewing them, required period for retaining electronic certificates in the database and means of retention, under sections 14, 18 and 20;

(7) Details in request for obtaining an electronic certificate, under section 18;

(8) Information of which a Certification Authority must inform owner of the Signing Device, including information regarding the risks involved in using a Certified Electronic Signature, and the duties imposed on the owner of the Signing Device under this Law;

(9) Types of systems presumed to be trustworthy hardware and software systems under sections 11, 15 and 18, as well as types of Electronic Signatures presumed to be Secure Electronic Signatures;

(10) Methods for identification of applicant and inspections of his Signing Device, in order to obtain an Electronic Certificate, under section 18;

(11) Information to be included in Electronic Certificates, and ways of presentation thereof;

(12) Conditions for recognition of Foreign Certification Authorities, under section 22(d).

(b) (1) Regulations under subsections (1) through (8) shall be enacted with the approval of the Constitution, Law and Legislation Committee of the Knesset.

(2) Regulations under subsections (9) through (12) shall be enacted with the approval of the Knesset Committee for Scientific and Technological Research and Development.

Retention of Laws

25. This Law shall add and not derogate from the provisions of any other Enactment.

Requirement for Prescribing Regulations

26. Preliminary regulations under sections 2(b) and 6(b) shall be brought to the Constitution, Law and Legislation Committee of the Knesset for approval, within four months of publication of this Law.

Commencement 27. This Law shall come into force six months from date of its publication.

First Schedule

Section 2(b)

Second Schedule

Section 6(b)

Note: This is an unofficial translation. Only the Hebrew version of this law is binding.

Prohibition of Money Laundering Law, 2000 - התש"ס [1]

Chapter One: Interpretation

1. Settings [התשס"ב Amendment (No. 3)] of this law --

"Stock market" - as defined in Article 1 Securities Law;

"Bank Mail" - significant law bank mail, 1951- התשי"א;

"Member of Bursa" - on the stock exchange member who by the rules set forth in regulations under article 46 Habursa Securities Law, except for corporate banking;

"Penal Law" - Penal Law, Htsl"z -1977;

"Securities Law" - Law of Securities, Htsc"h -1968;

"Currency service providers" - who ovary it mandatory registration as stated in Article 11 c;

"Driver files" - as defined in Article 1 Law Practice arranging investment advice and investment files, 1995- התשנ"ה;

"Action property" - the purchase or receipt of ownership or other right of property, and in return and not in exchange, action and property that is delivered, receipt, possession, conversion, operation banker, investment, securities action or holding them, real, or giving obtaining credit, import, export, and loyalty, and

Mixing of the property with property of another is forbidden, even if he is not the property is prohibited;

"Ordinance dangerous drugs" - drugs dangerous Ordinance [New Version], Htsl"g -1973;

"Arrest and Search Ordinance" - the Criminal Procedure Ordinance (Arrest and Search) [New Version], 1969;

"Customs officer" - who the manager, as defined Customs Ordinance, Law of Proximity to this point;

"Property" - land, Mitltlin, money and rights, including property that he Tmorto

Of the property as stated, and any property or plant comes Spacious property, as stated;

"Currency Services" - a service as specified in Article 11 c (a) (1) to (5);

"Banking corporation" - as defined by law Banking (Licensing), 1981- התשמ"א, and the corporation

Helped the same law as defined, Shuagd Israel.

Chapter II: Offenses

2. Source offense

(A) of this section, "offense" - plus the offense as the first.

(B) the point of this chapter will see an offense also a crime as stated in paragraph (a) Snabra in another country as long as she is also a crime under the laws of that country.

(C) the condition which is a small section (b) Sifh, the matter shall not apply to criminal offenses listed in paragraph (18) more first point criminal offenses listed in paragraphs (19) and - (20) an offense related to the addition in paragraph (18).

3. Prohibition of Money Laundering

(A) doing an action property, property which is, as stated paragraphs (1) to (3) (this law - the property is prohibited), but the purpose of camouflage to conceal the source, the identity of owners of rights which, the location, movements, or the making of action in countries - ten years' imprisonment or a fine under the said section twenty fine 61 (a) (4) Penal Law --

(1) from the property, directly or indirectly, offense;

(2) property used for the execution of a crime;

(3) enabling property infringement.

(B) doing an action or property of morality false information, in order not to be reported under Article 7 or to not report under article 9, or to cause incorrect reporting, according to these provisions, countries - the punishment of

Small section (a); the point of this section, "submitting false information" - including the failure of delivery of the individual must update report.

4. Prohibiting the making of an action prohibited property

Doing action property, property, knowing that he must not, and he listed a property plus the second set in which countries - seven years' imprisonment or fines tenfold penalty provided in Section 61 (a) (4) Law of the Penal Code; the point of this article, "knowledge" - except for turning a blind eye, significant section 20 (c) (1) Penal Law.

5. Proof of knowledge

Relevant Sections 3 and 4 pretty if proven knowledge that makes the action property is the property is prohibited, even if you did not know what particular crime-related property.

6. Sage criminal liability

(A) No person shall be liable for a criminal by Article 4 if he did one of the following:

(1) reported by the police at the time determined before the making of the action property, the intention to do that action, and follow the instructions on the action, or the police report, as stated, after the making of the action property, near the thick of it as possible under the circumstances, after Ashiith;

(2) reported by the provisions of Section 7 - If the provisions of section apply to him.

(B) Minister of Internal Security, in consultation with the Minister of Justice, will determine the date and methods of reporting by a small paragraph (a) (1).

Chapter Three: obligations imposed on financial services provider 1

7. Imposing obligations on financial services providers [התשס"ב Amendment (No. 3)]

(A) there Acifto of law that the Bank of Israel Governor shoot order, after consultation with the Minister of Justice Minister of Internal Security, regarding the type of property and affairs will be order, that the banking corporation --

(1) do not do damage to property as part of the service provided by him unless the hands are the identification information, as detailed order, the receiving service from corporate banking; Hanagid determines who receives the service order that the matter; This may include enjoying the action and creates loyalty or take (In this section - get the service); was getting the service corporation or that the operation was done at the request of a corporation, or with an account of the corporation, could include the determination who has control over a corporation; point this paragraph --

(A) "benefit" - for which a person or property is held for the benefit of an action is done or property, or property in his power to direct action, and everything directly or indirectly;

(B) "control" - as defined by law securities, and setting the said term to be interpreted by the law in question;

(2) would be reported as determined on the order of actions of property receiving the service order will be;

(3) will conduct drawings maintain them periodically determined order, these swim:

(A) identification information as stated in paragraph (1);

(B) set of actions for which mandatory reporting as stated in paragraph (2);

(C) any other matter, determined order, required to Acifto of this law.

(B) there Acifto of law determines that the Minister order, the entities mentioned as the body plus a third that is responsibility, after consultation with the Minister of Justice Minister of Internal Security, Debt identifying, reporting, registration and, as a small section (a), apply it; Yes Minister determines As mentioned above the methods of debt Miloin

Established order.

(C) Despite the provisions of any law, order can be determined, reported Sgiloim types, or reference which is forbidden; המגלה or anything that allows browsing in reporting that contrary order by a small section of this, countries - a year in prison.

(D) reported by this section will be the pool of information as stated in Article 28.

(E) ways to transfer and pool the information reported will be determined by the Minister of Justice, in consultation with the Minister of Internal Security, and in consultation with --

(1) Governor of the Bank of Israel - the point Banking Corporation;

(2) Is it the minister take responsibility for body - the body of the entities mentioned the point that in addition to third.

---

1. The beginning of this chapter on 17.2.2002 (K"t התשס"ב, p. 756).

8. Responsible for the corporate debt

(A) corporate debt to diseases by the provisions of Article 7 is responsible for reliable refilling debts.

(B) is responsible for refilling work for debt obligations imposed on the corporation by the provisions of Article 7, training workers for the supervision of duties as stated Miloin.

Chapter Four: mandatory reporting on the funds while the entrance and exit from Israel 1

9. Mandatory reporting on the funds during entry or exit from

(A) In this chapter, "money" - cash, travelers checks bank checks.

(B) a person entering the State of Israel or from which funds have to report that during entry or exit from it, if value of money is in a permanent addition to the fourth.

(C) mandatory reporting on the funds to Israel and spend money outside of Israel said in a small section (b), the person shall also Hmcniss The money for Israel, or from funds, e or otherwise.

(D) (1) mandatory reporting under this section does not apply to these:

(A) Bank of Israel;

(B) corporate banking;

(C) a person Hmcniss money to Israel or The money from her bank or by a corporation who using lacquer Treasury, in consultation with the Minister of Internal Security, permanent order.

(2) No provisions of this section to exempt smaller reporting obligations under article 7.

(E) the Minister of Finance, in consultation with the Minister of Internal Security, the methods of reporting will be determined by this section, he may, in consultation with the Minister concerned, substitute for reporting the matter to determine the funds to Israel.

(F) Reporting for this section will be the pool of information as stated in Article 28 ways and determined Minister of Justice, in consultation with the Minister of Internal Security and Minister of Finance.

(G) to require reporting by this section and the authority under article 11 (a) will, whenever possible, the language must report in person by this section or person is turned Sclapio authority.

10. Violation of mandatory reporting

That mandatory reporting has been canceled on him by section 9 countries - six months' imprisonment or a fine in the said section 61 (a) (4) Law of the Penal Code, or tenfold the amount not reported on it, all by the higher amount.

11. Seizure authority and funds of funds

(A) fertilized mandatory reporting has been terminated according to Article 9, a police officer or officer may seize without a warrant duty of judging the amount of funds on the reporting exemption; funds will remain captured in maintaining police or customs by the provisions of this section.

(B) financial progress has not been canceled or not indictment was filed, within 10 days of the seizure of funds, the funds will be returned to the person from which were captured; however, the court may, on request according to a police officer or customs officer, to order the seizure of funds to continue for a period not exceeding 10 days on information to allow the imposition of financial progress or the filing of an indictment, according to the issue.

(C) The court, as stated Hdn please a small section (B), will decide after the request heard claims of the individual funds from which were captured, and who claims the right to funds if it is known.

(D) The court may, at any time, the team on the return of funds or part thereof, under conditions determined, after receiving the bond or without bond.

(V) indictment was filed against in violation of the provisions of Article 9, applied to the captured funds payable to the provisions of this chapter the fourth arrest and search changes committed; this point, "object" - including the funds, as defined in Section 9.

(F) The court convicted the violator to the fines, or imposed on him financial progress, and not paid monetary penalty or in progress at the time determined that, you can collect the fine or the progress of financial funds from Harovhsnitna or captured by a small section (d).

(M) funds captured by this section and not returned, the foundation will be established under article 36 of payable dangerous drugs.

---

1. The beginning of this chapter on 17.2.2002 (K"t התשס"ב, p. 756).

[התשס"ב Amendment (No. 3)]

Chapter Four: 1 service providers Currency

A 11. Settings

[התשס"ב Amendment (No. 3)] in this chapter --

"Criminal proceedings" - from opening an investigation by law;

"Currency" - including a bill of money, they are here is a valid state;

"Criminal scheme" - significant section 1 Criminal Law of the prescription you install Hsbim, - התשמ"א 1981;

"Faithful" - significant law of loyalty, 1979- התשל"ט;

"Having fun" - as defined in Section 7 (a) (1) (a);

"Officer corporation" - any one of the following: the owner of a corporation, the director general, other than a corporation, subject of a similar role or equivalent position in question;

"Control" - as defined in paragraph 7 (a) (1) (B).

11 In. Registrar of Currency Services providers [התשס"ב Amendment (No. 3)]

(A) the Minister of Finance reliable, among office workers, Registrar of Currency Services providers (this law - Register).

(B) Register will conduct a prescription, which will write a currency service providers, according to the provisions of this Law (hereinafter - the prescription); the prescription will be open to public review.

(C) Register Ifkh the currency service providers by this law.

11 c .1. Mandatory registration of providers of prescription services coin [התשס"ב Amendment (No. 3)]

(A) any person who is one of involvement in providing the services listed below, even if it is not the only one of practice, (this law - giving currency services) have a prescription registry:

(1) currency exchange of one country's currency other country;

(2) Sale or redemption of the traveler's checks in any type of currency;

(3) receipt of financial assets in the country against one bringing financial assets

In another country; the point of this section, "financial assets" - cash,

Traveler's checks, bags, fresh Rates, fresh debt, securities Shirim,

Card or cash deposit;

(4) exchange of money bills;

(5) discount bags, Terry Terry debt exchange.

(B) Notwithstanding the small section (a), the registry does not have any one of the following:

(1) a public body established by law;

(2) corporate banking;

(3) reliance;

(4) working laborer when he gives currency services as part of his work at the employer that he gives currency services listed.

11 D. **.1. A request for registration giving currency services [התשס"ב Amendment (No. 3)]**

(A) a request for registration giving coin prescription services Togs Register, which will include all of these:

(1) applicant name, identifying information we heard, and if he runs true, even heard of identifying information like; the applicant was a corporation, will also request the documents on which the corporation or association which is working on, and the names of officers corporation, private Zyahuim Umanm ;

(2) of the branch Manm want to run Umanm of the applicant, with the main branch, and the names of branch managers, if there are any, information Zyahuim Umanm;

(3) Details regarding the practice of the other applicant, if he has;

(4) Additional information set by the Minister of Finance.

(B) the application documents will be appended Hmaidim on the conditions for registration, as stated in Article 11 the; the relevant sections 11 (a) (4) and - (b) -11 and Tet (a) (2) and - (d) to (f) - consent of the

applicant, officers of the corporation and the branch manager, according to the issue, the Registrar receives prescription information from the criminal, before listing a prescription

Any time then, so long as there is registration under this chapter.

_____

1. On 1.5.2002 who gave currency services may continue to provide these services to the decision by Registrar

Please register by Article 11 d, provided that the application submitted by no later dated 1.8.2002. Sign up

Will give its decision within 6 months from the date of submission of the application [Section 13 to correct התשס"ב (No. 3)].

(C) The Registrar may require the applicant listing any information or document information required for testing the application.

(D) of this section:

"Identifying information" - an identity card number; of a foreign citizen of the State of nationality policies and the state which is not a resident ID card - ID officially got another country to drive and a valid passport number and state issued it;

"Address" - Score of at least all of these: the street name, house number, name of the zip code, address, and if Israel does not even name the state.

The 11. Conditions listing services give currency [התשס"ב Amendment (No. 3)]

(A) Register will write a prescription requesting registration Hmkiim all of these, by the issue:

(1) the point that he seeks registration of a single - is adult Israeli citizen or resident of Israel;

(2) the point that he seeks registration of corporate organization in Israel - at least one officer is a corporation adult Israeli citizen or resident of Israel;

(3) the point that he seeks registration of a corporation organization outside Israel - in a country where there is a registered corporation prohibit Money Laundering legislation, the corporation duly registered in Israel;

(4) requesting registration offense is not convicted under Sections 3 and 4 Sldat Register or offense, due to death, or serious Nsibotih he is not giving proper services to serve as currency; was requesting registration corporation, was convicted of no offense, as stated also officer a corporation; paragraph This Article Small (B) --

"Convicted offense" - including a similar offense was convicted in another country;

"Requesting registration" - including having fun, if the applicant operates a trustee, and Branch, if there is.

(B) are against the Register learned that seeks registration or against the officer who requires a corporation to register one of the criminal proceedings in criminal offenses as stated in Section Small (a) (4), he may reject the registration request in connection with its decision to end the proceedings against him.

And 11. Register reported on the changes in [התשס"ב Amendment (No. 3)]

(A) change, in particular from the information provided by Sections 11 (d A) and the -11 (a), notify the Registrar currency service providers, in writing, within 7 days after which he learned about the change.

(B) has given the place of currency services activities or the location of one branch, notify the Registrar in writing within seven days of the change, meeting him the certificate of registration within thirty days from the said.

(C) worthless currency service providers to engage in providing currency services, notify the Registrar in writing within 7 days after meeting him that determines the registration certificate within 30 days from the

said; provides services coin operated several outlets, meeting the registration certificates of all branches; giving worthless currency services to give

Currency services at the branch, will return only the documents of the branch, as stated; this point, "which today" - the day on which the -101 worthless, continuously, to give currency services.

(D) service providers learned Register Currency died or was declared disqualified Din, fires on the return of certificate of registration and were closing; However, the Registrar may allow the continued provision of services to the currency in the name of the deceased or disqualified law, to protect the rights of service providers eligible currency or third party related

Practice; period starting business in this case shall not exceed 90 days; decision will determine who will register their services in local currency deceased or disqualified law (hereinafter - the temporary operator); after the said period the temporary operator will return the registration certificate register; decision to register the point that identifying information operator's temporary sign up a prescription.

(E) decided to give currency services, failure to engage in providing services coin, to return to practice in providing currency services, submit a new request for registration and will register in providing services to coin a new listing.

11 M. Certificate of registration and issuance of certificate [התשס"ב Amendment (No. 3)]

(A) the Registrar to register the applicant registry prescription currency service providers, will give him certificate of registration; were branches currency service providers - will register a separate certificate for each approved branch; certificate will be address and registration of branch; registration will be valid for the service providers for currency specified Certificate

Registration only.

(B) service providers will show the currency at any branch registration certificate, rather than conspicuous, that shows the registration number on each plate or any of his advertising and on every document that he spends.

(C) currency service providers announced the change in their place of Branch Register returned the certificate of registry branch, will register a new certificate of registration with the new address and registration number of the original certificate will cancel the previous certificate; changes to this article sign up for a prescription.

11 H. Refusal to register service providers currency [התשס"ב Amendment (No. 3)]

Registrar refused to register the applicant service providers currency Inmk the refusal would give him an opportunity to argue his claims before him within 30 days after which the decision requesting Humtzah Register.

11 Tet. Delete the prescription of the service providers or currency Hanging registry [התשס"ב Amendment (No. 3)]

(A) Registrar may delete a currency service providers in any one of the following prescription:

(1) worthless currency service providers exist in terms of conditions of registration by the Article 11 (a) (1) to (3);

(2) provides services to the currency, and if a corporation is, it has control, were convicted of offense, as stated in Article 11 the (a) (4);

(3) provides services currency breached by another provision of this chapter.

(B) before the Registrar decides to delete a currency gives the prescription services, as stated in Section Small (a), and would give him control of a corporation, by it, a chance to load the claims within 30 days after which the currency service providers Humtzah message written prescription.

(C) Given that the Registrar provides services currency breached another provision as stated in Section Small (a) (3), will require him, before it decides to delete the prescription, uploaded the patch to fix, he may, after giving service providers the opportunity to upload your currency claims, hang on the prescription records for a period not exceeding 30 days; violation not corrected within the said period, the Registrar to delete the violator

Prescription.

(D) learned Register are against giving currency services, recorded a prescription, and if a corporation is, even against the owner of a controlling, criminal offense procedures as stated in Article 11 the (a) (4), he may hang on the prescription records to the end of criminal proceedings; before it decides Hanging on the Register of Records gives the prescription currency services, and would give him control of a corporation by the issue, an opportunity to load the

Claims to within 30 days after which the service providers Humtzah currency message written prescription.

(E) Register officers learned that he gives to a corporation or service coin Director of the Branch provides services coin Convicted offense as stated in Article 11 the (a) (4), may register before deleting gives decides on the currency of the prescription services, to require him to dismiss those convicted offense, as stated, within a period determined; refused to let the currency services to do so, the Registrar may delete it from the prescription, after giving him an opportunity to claim those convicted before the claims within 30 days after which the currency service providers Humtzah message written prescription; small section of this Article a small (F), "officer corporation" - except with a control.

(F) the provisions of sections of small (D) and - (e) apply, the changes committed, the officer and director of a corporation Branch, proceedings against them are criminal offense as stated in Article 11 the (a) (4).

(M) service providers has announced that he was worthless currency Register engage in providing services to a currency, it will erase the prescription Register.

S 11. Message petition [התשס"ב Amendment (No. 3)]

(A) Register Imtzia service providers currency decisions on the written notice by the Articles 11 (b), and 11 (d), 11 H and 11 Tet.

(B) injured himself הרואה Registrar's decision about that small, as stated in Article (a), may petition a court of administrative affairs against the decision within 30 days after which Humtzah his decision.

K. **11. Public Message [התשס"ב Amendment (No. 3)]**

(A) Register Ifrsm records a message to all of these:

(1) records of service providers currency prescription, we heard his name in detail, including Manm of branches, if there are any;

(2) we heard of the change giving coin services, including change of address of the branch affiliates;

(3) deleting a currency service providers or affiliates Branch Hanging or prescription records;

(4) renewing the prescription records of service providers currency Hutlh records;

(5) to appoint a temporary operator under article 11 and (d).

(B) message, as stated paragraphs (1) to (3) a small section (a) Tforsm also on the Internet; website address where you can find information Tforsm as stated, a reasonable frequency, three daily newspapers with broad distribution in Israel, provided that at least one of them will be in Hebrew and one in Arabic.

11 Dib. Penalties [התשס"ב Amendment (No. 3)]

(A) provides services coin doing one of these countries - a year in prison or a fine by a factor of three in a fine of section 61 (a) (4) Penal Law:

(1) deals with the provision of services to coin a prescription without registration contrary to section 11 c and 11 and (e);

(2) not giving Registrar written notice as required by Article 11 and (a) to (c).

This translation is not an official translation

General Collective Agreement

Made and signed in 25 June 2008

Between

The New General Labour Federation (the Histadrut)

The most representative Labour Union which is a party to National and Sectorial Collective Agreements in all market Sectors

Hereby: Side A

and

The Federation of the Israeli Economic Organizations

A Federation comprising of the majority of Employers and Economic Organizations

of Israel[1]

Hereby: Side B

Since a computer in the Workplace is owned by the Employer and it's usage is a part of his Rights of Property, enshrined in the Basic Law: Human Dignity and Liberty.

And Since the Right to Privacy is a right enshrined in the Basic Law: Human Dignity and Liberty.

And Since the Employer's Right of Property and the Employee's Right to Privacy should be adequately balanced.

And Since making use of the Employer's computer for work related purposes has become an inseparable part of performing work in every workplace, in which computers are needed for that purpose.

And Since balancing the principles and rules of conduct regarding the usage of computers is deemed by the parties as vital, important and innovative, and in need of an agreed upon Normative Standard.

And Since For that purpose the parties have conducted a collective negotiation in order to reach an agreement as to the rules of conduct that shall apply concerning an employee's rights and how he may make use of his employer's computer.

Thereby the parties have agreed upon the following:

1. Definitions

In this Collective Agreement,

"Employee" - refers also to an actual user of the computer, including anyone who is required to make use of the employer's computer in order to perform work tasks, which are part of his work for that employer.

"Employer" - including a user undertaking, enterprise, management and any workplace in which computers are being used for work related purposes.

"Workplace" - any workplace in which the employer puts computers at the employees disposal for the enterprises purposes.

"Computer" - a computer that an employer has made available to his employees in order to perform their work.

[1] List of Organizations on whose behalf this Agreement is being signed appears at the end of this Agreement.

“Computer usage” - all computer applications, including Internet and mail boxes and everything specified in this agreement as usage of the computer by the employee.

“Rules of usage” - the rules specified in this agreement.

2. Agreed Principles

The following principles would apply as to rights and duties of employer and employee regarding computer usage:

A. The parties acknowledge the employer's Right of Property in his enterprise including his managerial prerogatives, and the right of the employee to privacy and private life in his Workplace all according to the Law, and all this in a reasonable, proportional and appropriate framework and in good faith, while respecting the employee's Right to Privacy concerning his Personal Data And according to this Agreement.

B. An Employee's use of the computer shall be made for work related purposes, according to the law and the rules that apply to all computer users in the enterprise, in fairness and good faith.

C. An employee's usage of his employer's computer shall be made fairly, reasonably and in good faith and according to the Law and this Agreement.

D. An Individual's private life is no one else's affair and his dignity and privacy in the workplace shall be preserved and respected, all according to the Law and this Agreement.

E. The Right to Privacy shall be examined together with the employer's prerogative to run his business according to his goals and interests.

3. Rules of Conduct

The following rules of conduct would apply in a workplace in which an employee is making use of his employer's computer:

A. Subject to the principles agreed upon in Article 2, an employer has the right to establish rules for use or disuse of the computer in the workplace, including the technology appropriate to the enterprises needs and the use of various soft wares, adopting known standards regarding Data Safety (ISO), policy of allocating mail boxes for employee's usage, connection or disconnection to Internet suppliers and websites, establishing a scheduled background copy process, taking data security and safety measures to prevent date leakage, guidelines for use or disuse of software, deletion of business or private material, and also all kinds of monitoring and maintenance needed to prevent invasion of the computer system including the use of Anti Virus programmes.

   The above mentioned rules shall be used for realizing the enterprise's goals and for a legitimate purpose, and shall be made known to the employees and in accordance with this Agreement and the Law.

B. The employee shall make use of the computer for work related purposes, and he may - according to this Agreement, to a proportional degree and for a reasonable length of time - make use of it also for personal and private purposes that are not work related and are subject to personal privacy principle but are not contrary to the Law and this Agreement.

C. The employer shall do all activities mentioned in section A above in good faith, reasonably, observing transparency and for a legitimate purpose, according to the enterprise's needs, and shall make no use of Personal Data of his employee in a harmful way that effects his dignity and his private life.

D. In circumstances in which a reasonable employer would have a cause to assume in good faith that an employee is making an illegal use of the computer or such use that could expose the employer to a legal suit by a third party or such that can harm the enterprise, the employer

shall be entitled to take actions to check the employee's computer, internet and/or e-mail, and it shall be done in a reasonable and proportional way, for a reasonable length of time and is compatible with the objectives specified above.

Any entry into a personal mail box bearing only the employee's mail address and his personal files requires an explicit consent by the employee, and shall be done in his presence of he so wishes.

E. All use of personal data or information gathered by the employer according to this article shall be made according to the rules while the employee's invasion of privacy shall be kept to a minimum. No use shall be made with data or information that has been obtained unlawfully and contrary to this Agreement.

F. The rules concerning the boundaries of computer usage according to this Agreement shall be made known to the members of the organizations on their behalf this Agreement has been signed.

4. <u>Third Party Actions</u>

An employer shall not be held liable for a breach of privacy as a result of actions or activities that have been done contrary to this Agreement or unlawfully, if such actions have been done by a third party who is not under the employer's control or by a computer maintenance personal who is not the employer's employee. The employer shall make no use of such personal data.

5. <u>Proceedings of conflict resolution</u>

A. Any deference of opinions arising between an employer and an employee regarding a topic that is subject to this Agreement would be dealt with within the framework established in a Sectorial Collective Agreement or a Specific Collective Agreement or a Collective Arrangement that apply to that Workplace. Topics that have to do with breach of discipline would be dealt with according to the Collective Agreement that applies to that Workplace.

B. If the parties at the Workplace would not reach an agreement within 60 days from submitting the application, each party shall be entitled to address the Joint Supreme Committee appointed by the Chairman of the Labour Committee of the Federation of the Israeli Economic Organizations and the Chairman of the trade union department in the Histadrut. The Committee shall consist of one representative of the employer sectorial organization and one representative of the representative employees organization in the Workplace and/or the Sector. The Committee's decision shall be given in writing and shall state the grounds that led to that decision.

In a Workplace that has no representative Labour Union, shall each side be entitled to apply directly to the Supreme Committee who shall act according to this article.

C. In case that the Committee shall not reach an agreement within 60 days shall each side be entitled to appeal to the Labour Court and he may affix to his application information concerning the parties positions, a summery of the hearing that took place that should include each party's position, agreements and deference of opinion.

D. Any deference of opinion regarding legal interpretation of a concept or provision in this Agreement, or any unclarity regarding the meaning or application of an article or the need to establish agreed upon rules as to it's application, including conforming of the rules established in this Agreement and or establishing specific rules to workplaces or sectors that due to the nature of he work performed require the establishment of such specific rules, would be dealt with by a Committee who's members shall be appointed by the parties by mutual agreement. The Committee shall give it's decision including legal arguments within 30 days. An appeal can be submitted to the Labour Court. Shall there be no appeal within 30 days of receiving the

decision, the decision shall then be send to the Registrar of Collective Agreements and shall become an inseparable part of this Agreement.

6. Agreement Registration

This Agreement shall be registered by the Collective Agreements Registrar as a Collective Agreement and the parties will apply to the Minister of Industry, Commerce and Employment to issue an Extent Writ making it binding on all employers and employees in Israel.

7. Joining this Agreement

A. An Employers Organization who is not a party to this Agreement can inform the parties of his joining, and following the notice send by the parties to the Registrar of Collective Agreements all it's members shall be bound by it.

B. An Employer to whom this Agreement does not apply but is a party to a General Collective Agreement or a Collective Arrangement can announce that he is joining this Agreement and following a written notice of consent by the parties, shall be bound by it.

8. General

This Agreement is not contrary to all laws concerning information and Data secrecy and Protection of Privacy.

We hereby undersign, in Tel-Aviv 25 June 2008

The Federation of the Israeli Economic Organizations
on behalf of the following organization:

Manufacturers Association of Israel.
Federation of Israeli Chamber of Commerce.
Federation of Building Contractor's Association of Israel.
Farmers Federation of Israel.
The Israel Diamond Manufacturers Associations Ltd.
Israel Hotel Association.
General Association of Merchants in Israel.
Ceneral Union of Artisan & Manufacturers of Israel.
National Federation of Trade in Israel.
Cinema Owners Association in Israel.
The Federation of The Israel Self Employed Organizations.
The Association of Security Enterprises in Israel.
The Association of Cleaning and Maintenance Enterprises in Israel.

The New General Labour Federation (the Histadrut)

Shelley Wallach[2]

IXth European Congress of Labour and Social Security Law
Freiburg Congress of International Society of Labour
Law and Social Security

General Collective Agreement

Establishing principles and rules of conduct regarding employee's usage of his employer's computer and the Right to Privacy.

On 25 June 2008, a General collective Agreement, establishing principles and rules of conduct regarding employee's usage of his employer's computer has been signed in Israel.

The parties to this Agreement are The New General Labour Federation (the Histadrut) which is the most representative Labour Union in Israel, and the Federation of the Israeli Economic Organization, a federation comprising of the majority of employers and economic organizations of Israel - who also signed it on behalf of many and major employers associations specified at the end of the Agreement.

The purpose of this General Agreement, which is only the second collective agreement on this topic (the first one has been signed in Belgium on 26 April 2002 - and is referred to as National collective Agreement No.81) is to set clear norms for employers and employees, regarding their mutual rights and boundaries concerning employee's usage of the computer that his employer puts at his disposal, which has become in this modern age an inseparable part of performing work in almost every workplace, accept the low-tech sectors, with the aim of seeking to strike a balance between employers legitimate rights of property and his managerial prerogatives on the one hand, while respecting and preserving as much as possible the employee's right to privacy - which modern technology makes very easy to invade if no clear norms and boundaries are there to prevent it.

This topic of employee's Privacy vis-à-vis his employer in the workplace, as once prof. Weiss has pointed out to me, is not only a question of conflicts of Rights - the right of property on the employer's side versus the employee right to Privacy, but of boundaries. Therefore it is by the rules and norms that we put in place by which we draw those boundaries.

It is also important to stress, that this Agreement deals only with the situation in which the employee is making use of the computer that his employer puts at his disposal, and not when the employee is using his own computer whether at home (even if he performs work that is work related) or his own laptop that he brings to work.

We have no time, of course, to go over all the articles of the collective Agreement, but I would like to draw your attention to what I think are the most important points in it:

I. The opening statements and declarations at the very beginning makes it very clear that it aims to strike a fair balance between the employer's Rights of property (as the computer he puts at the employee's disposal is his property) on the one hand, and the employee's Right to Privacy when doing so. Both rights, as stated there, are enshrined in Basic Law: Human Dignity and Liberty (Basic Laws in Israel are like the German "Grund Gesetze").

II. Article 2: Agreed Principles, in which both parties acknowledge the employer's right of property and managerial prerogative and that the employee's use of the computer shall be made: "for work related purposes, fairly reasonably and in good faith according to the Law and this Agreement", but also stresses in subsection D that: "an Individual's Private life is no one else's affair and his dignity and privacy in the workplace shall be preserved and respected".

[2] The following is the summary of my lecture given as one of the panelists of the round table on the topic of the impact of information and communication in the field of Labour Law.

III Article three deals with Rules of Conduct, of which the most important are subsection B, C & D. Sub Section B makes it clear that although the use of the computer is for work related purposes, the employee may "to a proportional degree and for a reasonable length of time" make use of it also for personal and private purposed that are not work related.

While subsection C makes it clear that the activities made by the employer in subsection A. (which deals with uses, maintenance and soft wares), shall be done in "Good faith, reasonably, observing transparency and for a legitimate purpose" and shall make "no use of personal Data of his employee in a harmful way that effects his dignity and private life."

But perhaps the most important subsection is D: "in circumstances in which a reasonable employer would have a cause to assume in good faith that an employee is making an illegal use of the computer or such use that could expose the employer to a legal suit by a third party or such that can harm the enterprise, the employer shall be entitled to take actions to check the employee's computer, internet and/or e-mail, but it shall be done in a reasonable and proportional way, for a reasonable length of time and for the above mentioned purposes.

Any entry into a personal mail box bearing only the employee's mail address and his personal files requires an explicit consent by the employee, and shall be done in his presence if he so wishes."

- that deals with situation in which the employer shall be entitled to check the employee's computer, internet and or E-mail, the key words being in the beginning of this section: "In circumstances in which a reasonable employer would have a cause to assume in good faith…", that means that this right of the employer to actively monitor or check the employee's computer: internet and or E-mail - should not be used on a whim, arbitrarily or out of pure unfounded suspicion but has to be well grounded on reasonable causes and in good faith.

It is important to stress in this context that this subsection deals with two situation: the first one in which the mail box is allocated by the employer and bearing the mail address at work (i.e.: shelleywallach@court.gov.il), and the second, in which case the mail address has been chosen as a private address by the employee but while using the employers server and on the computer made available to him by his employer (i.e.: shelleywallach@gmail.com).

In the later case, any entry or checking of this mail box can be done only subject to the employee's consent and also in his presence if he so wishes.

Again it is worth to point out, that this subsection, as indeed the Agreement itself, does not touch on a situation whereby the computer itself and the mail box is on a computer owned by the employee himself but only the one owned by the employer.

I assume that in future when disputes that have to do with the application of this Collective Agreement would be brought before the Labour Courts, it is most likely that this will be the one article or subsection they will have to deal with, and I hope they will give the interpretation that gives as much protection to employee's Right of Privacy as is clearly manifested in the spirit of this Agreement.

The Agreement also deals with Proceedings of conflict resolution (in article 5). I have no time to go into the details specified there at length, but the important thing to notice is that a mechanism is established by which representatives of the parties - employer & employee, shall try first to resolve any conflict or deference's of opinions regarding this Agreement before bringing the matter before the Labour courts when all else fails.

This is not only good news for the overloaded Israeli courts, but on a more serious note, very appropriate and in line with the spirit of the parties mutual cooperation on those issues.

In this context it is also worth mentioning that article 5 also deals with deference of opinion regarding legal interpretation of a concept or provision in the Agreement or unclarity regarding the meaning or application of an article, establishing a mechanism which refers such interpretation first to a committee

who's members shall be appointed by the parties by mutual agreement. This committee's decision may be subject to an appeal to the Labour Court.

However, if no appeal has been made, the decision after being registered by the registrar of Collective Agreements, becomes an inseparable part of the Agreement, thereby a mechanism is created that allows for amendments to this Agreement shall the need for it arises in the future, again in the spirit of co-operation between the parties for as much as possible.

This mechanism also gives the Agreement an added dimension of flexibility.

Other articles deal with third party actions, (in article 4) whereby the employer shall bear no responsibility for actions of a third party, such as computer maintenance personal, that is not his employee and not under his control, but on the other hand, he may not make any use of personal data regarding the employee that he obtained by the actions of the third party, hence the protection of employee's personal data remains in place. Agreement registration and the possibility for joining this Agreement by employers or employers organizations who are not a party to it already (articles 6 and 7).

The key words in this Agreement are: legitimate purpose, proportionality, transparency, reasonably and good faith. This is the first time that concepts taken from the European Law that are an inseparable parts of it's legislation, EU directives and important documents like the Charter of Fundamental Rights, are incorporated into Israeli Law.

This important topic, that has to do with internet and E-mail use and monitoring is also a very topical issue in the EU and the subject of a Pending Directive (mentioned in the 5 Year Agenda in 2005).

In Israel, unlike some other countries, Collective Agreements are subject to a specific Law (Collective Agreements Law 1957).

Therefore, although Collective Agreements are usually considered to be Soft Law, in Israel once such an Agreement has been registered by the Registrar of Collective Agreements, it has become hard Law.

In my opinion, such an arrangement as has been done is Israel, which although as explained above, is hard law, but it does still retain some of the features of soft law by the relative ease in which it can be amended as needed by the parties, thus lending. It more flexibility than a typical hard law, may well be a very suitable way of setting clearer guidelines for both employers and employees to deal with the issues arising from computer use.

Slovenia

Judge Miran Blaha
Supreme Court of the Republic of Slovenia

Part 1: The regulatory context

1 Does your legal system possess any general definition of "privacy"?

Our legal system does not have any general definition of privacy.

- **If so, please indicate the content and source of that definition. If not, how have notions of "privacy" been approached in your country conceptually, in academic writings, or as matters of socio-legal policy?**

Privacy is, due to its subjective character, not unambiguously or clearly defined; however, in each individual case of judicial action, the right to privacy is weighed against other rights. The right to privacy is otherwise defined as a personality right encompassing a series of rights related to human persons and their personal relationships, and, like any other personality right, it is personal and non-pecuniary. It belongs to

individuals as an integral part of their personality, protecting it at the same time, whereby their relationships toward others are protected as well.

The notion of privacy appears in several areas, among others:

- information privacy: includes personal data collection and management and is also known as personal data protection,
- physical privacy: covers the field connected with genetic and other searches of body fluids and/or tissues and openings,
- communication privacy: guarantees the privacy of postal items, telephone conversations and other forms of communication, and
- spatial privacy: restricts invasions of one's privacy at the workplace or at home.

2. Does your country have a Constitution, and does this make any provision in relation to "privacy" for citizens (whether at work or otherwise)?

Slovenia has a Constitution, which regarding privacy contains provisions on the protection of privacy and personality rights (Article 35), inviolability of dwellings (Article 36), protection of the confidentiality of correspondence and other means of communication (Article 37), and on the protection of personal data (Article 38).

3. Does your country adhere to International Instruments which contain provisions relating to "privacy" (*e*.g. at the level of the Council of Europe, *etc*.)?

- **If so, please indicate which instruments and when your country signed up to, or ratified, each of those instruments.**

UN Documents (the Republic of Slovenia take over these instruments through the Act of Notification of the SFRY Succession of 1 June 1992):

- Universal Declaration of Human Rights,
- International Covenant on Economic, Social and Cultural Rights,
- International Covenant on Civil and Political Rights

THE COUNCIL OF EUROPE:

European Convention for the Protection of Human Rights and Fundamental Freedoms (1994),

Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data,

Council of Europe Convention 164 on Human Rights and Biomedicine

EUROPEAN UNION

- Directive 95/46/EC
- Directive 2006/24/EC
- Directive 2002/58/EC
- European Council Regulation no. 45/2001

4. As a general matter, how are norms established at the international level transposed into protections or rights at the domestic level for citizens in your country?

- **Please illustrate this by reference to any International Instruments mentioned in relation to Q.3.**

Regulation no. 45/2001 is directly applicable, and directives are implemented. The Personal Data Protection Act therefore means the implementation of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Other legal sources, notably the UN instruments, are binding on Slovenia following the accession and ratification of these instruments. Individuals may invoke the rights conferred by them.

5. Are public sector workers/officials in your country subject to a different regime from private sector staff in relation to rules on "privacy"? If so, please indicate what the differences are, and whether there can be said to be broad equivalence between the different regimes.

No. Certain specific features apply only to state officials (including judges and state prosecutors), who are obliged to disclose data on their financial status. Data concerning the officials' income and financial status are publicly available despite the restrictions imposed by the Act for protecting personal data and tax confidentiality. Where the comparison of the supplied data with the actual situation gives reasonable grounds to suspect that the officials may have transferred their property or income to family members in order to evade verification, they must supply data on their family members as well (i.e., spouses, common law partners, biological or adopted children).

6. Are any groups of workers (other than public sector workers/officials) treated differently from the "normal model" in relation to rules on "privacy"?

No.

7. Please describe briefly your national framework of rules dealing with issues of "privacy"?

- **Where these are contained in legislation or administrative regulations, please indicate the sources *[and, if possible, please attach a copy/version of the relevant provisions].***

  Constitution

  Personal Data Protection Act (PDPA - Official Gazette of the Republic of Slovenia 86/2004 and 113/2005)

  Information Commissioner Act (Official Gazette of the Republic of Slovenia, no. 113/2005)

  Health Care and Health Insurance Act (Official Gazette of the Republic of Slovenia, no. 72/2006, 114/2006, 91/2007), governing an employer's familiarisation with a worker's state of health

  Labour and Social Security Registers Act (Official Gazette of the Republic of Slovenia 40/06 - LSSRA) defines what records can be held and what personal data can be entered in these records.

Part 2: The State and the Employer

8. Please outline the areas in which the State authorities in your country are entitled to obtain personal information from an employer about a member of its workforce.

- **In particular, please indicate whether the State authorities possess such powers in relation to nationality or national origins; residence status; work permit status; previous employment records; criminal records; tax status; family/marital status; medical records, health and/or disability-related material; bank account information (*e.g.* for payment of wages); trade union membership.**

The State authorities can obtain from the employers certain personal data about their employees in the following cases:

- The (National) Employment Office holds a data base on foreigners employed in Slovenia under the **Employment and Work of Aliens Act**. The data base contains data on their sex, tax number, citizenship, residence, passports, work permits;
- Under the **Tax Procedure Act**, the tax authority may obtain any personal data required for tax collection;

- Under the **Defence Act**, the Ministry of Defence may, within the framework of so-called security clearance of personnel (i.e. regularly employed and applicants for jobs in the military), obtain data on immediate family members, former employers and criminal records, without being obliged to inform thereof the individuals these data refer to;
- Under the **Private Protection Act**, the Ministry of the Interior holds records of persons providing security services, which also includes personal data such as citizenship, residence, proof of no criminal record, etc;
- Policemen also have certain powers under the **Police Act** to obtain personal data from employers about their employees; and
- The Office for the Prevention of Money Laundering is also authorised to obtain personal data from employers about their employees under the **Act on the Prevention of Money Laundering and Terrorist Financing**.

In order to confirm the representativeness of trade unions, the State (or the Minister of Labour) may in certain cases request data on the number of union members, but only aggregate data, not by name.

9. Please indicate whether the State authorities in your country are entitled, under any circumstances, to implement surveillance of a workplace (electronic, video, visual observation, *etc*.) for the purpose of obtaining personal information about any member of the workforce?

- **In particular, please indicate whether the State authorities possess any special powers of this kind in the context of measures intended for "combating terrorism" or in relation to investigation of serious criminal activities (*e*.g. drug dealing, "money laundering", *etc*.).**

Special provisions apply to video monitoring in the area of national defence, national intelligence and security activities, and the protection of classified information (with no obligation to inform employees of video surveillance in advance). Otherwise in general, equal rules regarding video monitoring of persons employed in state bodies apply to state authorities.

State authorities entitled to obtain personal data (for example, police), may, within the limits of the powers conferred upon them, also obtain video or other electronic data from employers who are monitoring their employees. Thus, for example:

- the pharmaceutical inspector of the Agency for Medicinal Products and Medical Devices is entitled to examine audiovisual recordings of persons, rooms and premises;
- it is possible to examine recordings from audio and video surveillance in gambling establishments (casinos) provided for under the Gambling Act.

Part 3: <u>The Employer and the Worker</u>

10. Does a worker in your country enjoy any form of "right to privacy"?

- **If so, what form or forms does this right take? How is that right reflected in the legal system of your country?**

Yes. The Constitution guarantees to everyone – thus including the employers - the protection of the rights to privacy, and the protection of personal data (Articles 35 and 38 of the Constitution). The Personal Data Protection Act governs the protection of individuals against unlawful encroachments on the privacy in the processing of personal data.

The Employment Relationship Act (Official Gazette of the Republic of Slovenia no. 42/2002 - ERA) stipulates that the employer must protect and respect the worker's personality and take into account and safeguard the worker's privacy, and governs the protection of the worker's personal data. The employer is liable for damages he caused to the worker by violating the rights arising from the employment relationship (including the right to privacy and the protection of personal data). The Information Commissioner is

authorised for supervision of the implementation of the provisions of PDPA and can impose sanctions. Interfering into the right to privacy is sanctioned also by the provisions of the Penal Code.

11. To what extent (if at all) is any "right to privacy" for a worker more limited when that person is at work than any "general right to privacy" enjoyed by citizens in general?

In principle, the employer's right to privacy is not restricted more than the right of any other citizen. In practice one has to take into account the nature of the employment relationship, and the rights and duties arising from such relationship. For reasons of employment, the requirements related to safety at work and the exercise of rights, the employees are disclosing various types of personal data; for example on their state of health, disability, family situation, membership in trade unions, etc.

12. Under what conditions (if at all) is an employer in your country entitled to obtain (*e.*g. by way of questions contained in job application forms) personal information about a member of its workforce?

The ERA specifies what exactly the employers may or may not ask the applicant for employment. As a rule, the employer may only demand the applicant to submit documents proving the fulfilment of conditions for carrying out work.

According to the ERA, the employer may not demand the applicant to provide information on the family and/or marital status, pregnancy, family planning nor on other information, unless they are directly related to the employment relationship, and the applicant is not obliged to answer questions which are not directly related to the employment relationship. The border between what is and what is not related to the employment relationship, is generally rather thin (see also the answer to question 11).

– **In particular, please indicate the position in relation to the following specific areas (and please add information about any other matters which are of particular significance in your country):**

• Information about the address, telephone contact numbers, *etc*. of the worker

Employer can collect only those data on employees that can be found on their personal documents and which are stated in Article 13 of the LSSRA, for example single personal identification number, permanent residence address, tax number, citizenship, place of birth, education.....).

• Information about the marital status of the worker

See above, answers 11 and 12.

• Information about the health and medical condition of the worker (including, for example, details of the worker's personal doctor)

Such data may be relevant for exercising the rights and duties from the employment relationship, therefore in these cases the employer may obtain such data. For the purposes of the necessary and permissible control of the sick leave, the details on the employees' personal doctor and the address of their outpatient unit may in certain cases actually be necessary to supervise the exercise of rights and duties from the employment relationship.

• Information about the sexual orientation of the worker

No

• Information about the religion of the worker

No

• Information about the political affiliation or activities of the worker

No

• Information about the tax (fiscal) affairs of the worker

No

• Credit information about the worker

Not directly, only when the employer pays the bank directly the liabilities of the employees from their salary. In this case the employer obtains this information upon the employee's consent or approval.

• Court information (*e*.g. for enforcement of court orders by way of deductions from salary – "attachment of earnings")

The same as above.

• Information about any criminal convictions which the worker may have

A number of applicable acts request the applicants to supply evidence of non-conviction because this is the condition for employment, for example:

- Police Act (OG RS no. 3/2006)
- Judicial Service Act (OG RS no. 94/2007)
- Defence Act (OG RS no. 103/2004)

Data on employees' membership in trade unions qualify under sensitive personal data under the PDPA which can only be processed in eight cases stipulated there. In the public sector, the processing of such data requires not only the explicit personal consent (as a rule it must be in writing), but also an explicit foundation in law governing the particular sphere. A direct foundation in law for the processing of data on the trade union membership can be found in the provision of the ERA stating that 'upon the request of the trade union and in compliance with the regulation of the trade union the worker is a member of, the employer shall ensure the technical execution of settlement and payment of a trade union membership fee for the worker concerned'.

13. Under what conditions (if at all) is an employer in your country entitled <u>to retain</u> (whether in the form of personal files, or electronically) personal information about a member of its workforce?

In particular, please indicate the position in relation to the specific areas mentioned in Q.12 (and please add information about any other matters which are of particular significance in your country).

Personal data of workers can be gathered, processed, used and provided to third persons only if the ERA or other laws stipulate, and if it is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship. This means that the employers may create also those records on the employees which are not provided by law but are obliged to explain in detail and present the purposes for which certain personal information on the employee is necessary. If the employers fail to present that certain personal information on the employee is necessary in order to exercise the rights and obligations arising from the employment relationship, they may not demand it from the employees.

– Is an employer in your country obliged to tell the worker that it is holding personal information about that worker and/or to make any such information available to the worker for inspection (*e.g.* to ensure the accuracy of the information)?

The Constitution itself guarantees individuals the right of access to the collected personal data that relates to him (own personal data) and the right to judicial protection in the event of any abuse of such data.

PDPA contains provisions regarding the right of the individual to information on personal data processing. Employer, as controller of personal data, shall on request of the individual enable consultation of the filing system catalogue, supply an extract of personal data, and provide a list of data recipients to whom personal data were supplied (when, on what basis and for what purpose). The data controller must enable the individual to consult, transcribe or copy no later than within 15 days, or within 15 days inform the individual in writing of the reasons why he will not enable consultation.

- **Are there any provisions in your country which require the employer to handle such information in a particular way?**

– For example, is the employer required to register the fact that it holds such information with a public official (a "data protection commissioner" or the like)?

– Does the employer personally/physically have to retain such information under its control at the workplace, or can it employ specialist companies to hold and manage any such data?

– Is the employer required to destroy such information after a certain period of time? - Are there provisions in your country which regulate the freedom of the employer to disclose or pass such information to third parties (including to the public authorities)?

The PDPA contains a number of clauses preventing the personal data abuse, and the LSSRA Act has special provisions on personal data processing which are binding on the administrator of the personal data related to employment. They define what records the employers may hold and what these may comprise (e.g. the records of employees, the records on the use of working time). They also define that employers may hold records for the purposes of exercising the rights under the social security and social care system, for the purposes of statistical monitoring, and for the needs of inspection supervision. The records that the employers may hold in the field of labour and social security with respect to employees who entered the employment relationship are stipulated in detail in Article 13 of the LSSRA Act.

Information Commissioner has to be informed of the existence of all personal data records processed by the employers. The entry in the register is not obligatory for data controllers with less than 50 employees (with some exceptions for the personal data collections in the public sector, notaries public, attorneys, detectives, bailiffs, private security providers, private healthcare workers, and healthcare providers).

When legal grounds for holding personal data on the employees cease to exist, these data should be promptly deleted and withdrawn from the use.

Personal data can be forwarded to other persons only in the following cases:

- there are explicit legal grounds in one of the laws,

- the individuals have given consent to the forwarding of their personal data,

- the forwarding of personal data is necessary for the purpose of implementing the contract or exercising the rights arising from the contract,

- exceptionally also when the forwarding of personal data is inevitable for the exercise of lawful competences, duties or obligations by the public sector, provided that this does not encroach on the justified interests of the individual,

- when forwarding of personal data is essential for the fulfilment of the lawful interests of the private sector and these interests clearly outweigh the interests of the individual to whom the personal data relate.

14. In addition to the situations mentioned and Q.12 and Q.13, are there any circumstances under which an employer in your country is entitled to obtain (or to demand) medical details about a member of its workforce?

The ERA does not explicitly stipulate a general health capacity of the employee as a condition for concluding an employment contract. However, it states that in order to establish the applicant's health capacity for carrying out work, the employer shall at his costs refer the applicant to the preliminary medical examination.

The details on the employees' personal doctor and the address of their outpatient unit may be important in certain cases, for example in order to supervise the exercise of rights and duties from the employment relationship, therefore the employer may obtain them. The control of exercising the prescribed sick leave arrangements and the related activities of personal data processing may be performed by the employer himself, or may by contract be entrusted to a data processor in line with provisions of the PDPA. The employer must give detailed grounds for the need of processing particular data. The control on behalf of and for the account of the employer may be performed only by legal or natural persons who are registered

to perform security activities. The control has to be performed in compliance with the Detective Activities Act.

Employers are not entitled to be informed of the employee's diagnosis. In order to be able to verify justified absence from work, they are entitled however, to be informed of the occurrence of sick leave and free movement arrangements, but not of the treatment arrangements. The certificate of justified absence from work may not state the diagnosis or detailed description of the patient's situation. It may only contain data which are necessary and permissible for the needs of the employer or the health insurance agency (e.g. whether there is a professional disease or injury at work).

- **In particular, please indicate whether there are any situations in which an employer is obliged to obtain information about the health of the worker (*e.*g. before permitting that worker to perform tasks at heights, or where there may be exposure to dangerous substances or radiation during the course of performing the job)**.

There is a number of regulations which, for a (safe) performance of certain tasks, require from the employees not only to have specific qualification but also to prove a suitable health shape. Employers may define special health requirements the employees have to meet for a particular job, working process, or in order to use particular means of work. Their health state is established on the basis of a professional opinion of an authorised doctor. Therefore the law not only prescribes the preliminary medical examinations for establishing a general health capacity for work, but also preventive and mandatory periodical medical examinations for all types of work connected with increased risk for the workers' health, or in other justified cases (for example work with foodstuff). The workers are allowed to undertake work at such workplaces or in the conditions with increased risk for injuries and health damage only on the conditions defined in special regulations, and following the authorised doctor's professional opinion that they are capable of undertaking such work.

- **Is there any procedure laid down for an employer in your country to obtain the formal consent of a worker to accessing such personal medical information?**

No.

- **Is an employer in your country entitled to ask specific questions about whether a member of its workforce is "disabled"? – If so, what are the consequences if the worker refuses/fails/chooses not to disclose such information?**

The workers are obliged to inform the employer about the category of their disability and the resulting restrictions (prohibition to lift burdens, prohibition to work at a height), so that the employer may establish whether they are suitable for a particular job, or if this job can be adapted to the working abilities and needs of the disabled; or if some professional or technical support have to be provided. The workers can prove this with a document issued by a competent authority. It has to show the category of disability and provide the explanation of the kind of work the workers are capable of doing, or what they can not be asked to do. The workers may address the Pension and Invalidity Insurance Agency (ZPIZ) which issues a certificate on the facts from its official records. Such a certificate can be enclosed to the application for employment.

– Can an employer in your country require a worker to submit to a medical examination, and subsequently have access to the results of that medical examination (*e.g.* where the employer is considering dismissing the worker on grounds such as "capacity", or "fitness to do the job", or because of a high level of absences from work for medical reasons)?

The preliminary medical examination does not imply performing a general exam or establishing the complete health state (of the applicants); what is examined is only their health capacity to perform the work which is the subject of the employment contract.

The medical certificate only proves their capacity to work. The employer is in no way familiarised with the results of testing.

– Is an employer in your country entitled to make use of (and act on the basis of information obtained as a result of) techniques such as "psychological testing" or "genetic testing"?

Employer may use psychological testing or have the applicants tested in the phase of selecting the applicants. The purpose of psycho-diagnostical testing is to find out the applicants' personal qualities and skills, their advantages and eventual obstacles for successful performance in a certain field of work and for the future development of their career. There are no special restrictions in this sphere, and the employers often choose these forms to check the applicants. The results of psychological testing are part of the personal records (e.g. the personnel file or the lists of applicants for a certain job…) which create the personal data collection related to the individual.

15. Is an employer in your country entitled to implement any forms of surveillance of workers at the workplace?

– in particular, please indicate whether there are any situations in which an employer is entitled to make use of the following:

1. • CCTV (video surveillance)

• Monitoring and inspection of web-browsing by the worker

• "Keystroke monitoring" of workers performing computerised tasks

• Monitoring and inspection of a worker's electronic communications (eMail, social networking websites, *etc*.)

• Monitoring and inspection of a worker's traditional communications (post, telephone calls, *etc*.)

As regards video surveillance at the workplace, the PDPA stipulates that video surveillance within work areas may only be implemented in exceptional cases when necessarily required for the safety of people or property or to protect secret data and business secrets, and where such purpose cannot be achieved by milder means. Video surveillance may only be implemented for those parts of areas where the interests from the previous paragraph must be protected, and is prohibited in work areas outside of the workplace, particularly in changing rooms, lifts and sanitary areas. Employees must be informed in advance in writing prior to the commencement of implementation of video surveillance. Prior to the introduction of video surveillance, the employer is obliged to consult the representative trade union at the employer.

The contents of private electronic mail is protected directly under Article 37 of the Constitution which guarantees the privacy of correspondence and other means of communication. In all the cases where the employers allow the use of communication means (computer, telephone, car) both for official and private purposes, they are obliged to respect the privacy and protect personal data. Legitimate control of communication for the protection of the employers' interests (protection of their business secrets, appropriate or rational use of the means of work and costs, use of working time, etc.) may not invade the privacy of their employees.

16 Are there any circumstances where an employer in your country may be entitled to conduct (*e.g.* by security staff belonging to the enterprise) a physical (possibly including intimate) body search of a member of its workforce? – What would be the consequences if the worker refused to submit to such a search? – What would be the consequences if an employer carried out such a search without the consent of the worker?

No. Body search can be carried out only when it is reasonable to suspect that a person has engaged in a criminal offence and it is probable that the search will provide traces and items of value for the criminal procedure. The search is ordered by the court with a substantiated warrant in writing. Policemen can perform body search without the search warrant and witnesses when they are enforcing the production or arresting a person, if there is a suspicion that this person is armed for attack, or that this person is going to reject, hide or destroy the items which have to be seized for evidence in the criminal procedure.

Private security officers hired by the employer can not perform body search, either. They are only authorised for a surface inspection of upper clothes, interior of the car and luggage of a person at entering or exiting the secured area, if this is necessary for the safety of people and property which are being protected, and if the person agrees with this. If the person refuses the search, the security officer may prevent such person from entering or exiting the secured area, and has the right to hold such person until the arrival of police, if the person has been caught in committing a criminal act.

17. Is an employer in your country subject to any recognised "duty of confidentiality" in relation to members of its workforce and/or others? – If so, what is the extent of any such duty, what form or forms does this duty take, and how is that duty reflected in the legal system of your country?

18. Under what circumstances can an employer in your country justify breaching the "privacy" of a member of its workforce or any "duty of confidentiality" owed to a worker and its employment?

– in particular, please indicate how this might be the case in relation to:

- **• The employer's business interests (*e*.g. protection of trade secrets)**

• Supervision of security at the workplace

• Prevention of criminal activity (others abuse, *etc*.)

• When required to act under instructions from the public authorities (*e*.g. as part of a police investigation)

The rights of individuals to be informed about the processing of their personal data and to the protection may exceptionally be restricted by statute for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, the exercise of the responsibilities of the police, the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others.

19. Is it possible for an employer in your country to justify intrusions into the privacy of members of its workforce by giving clear notice that particular measures are and use (*e*.g. signs stating that the workplace is subject to CCTV surveillance)?

Yes. Employees must be informed in advance in writing prior to the implementation of video surveillance. Exceptions are provided in the field of national defence, national intelligence and security activities, and the protection of classified information.

The Electronic Communications Act (ECA, Official Gazette RS, no. 13/07) regulates the confidentiality of and stipulates that a subscriber or user may record the communication, but they must inform the sender or recipient of the communication thereof or adjust the operation of the recording device so as to inform the sender or recipient of the communication of its operation. This Act also defines who and under what conditions can obtain the information on communications (relating to the communication contents, the transactions and the location information).

20. Is it possible for an employer in your country to include contractual provisions in the terms of the employment relationship which effectively permit the employer to breach the privacy of a member of its workforce?

In principle, no.

21. Are there any special rules in your country concerning "personal" files created by a worker on a computer belonging to the employer at the workplace? – Is there any guidance in relation to who "owns" any rights in relation to such "personal" files?

As a general rule, mere ownership of the computer does not entitle the employer to violate the workers' rights to the privacy of documents stored on their computers. A case from recent practice: in order to secure evidence on the coordinate actions for restrictive agreements, the Competition Protection Office seized and copied hard disks of some employees in large trade companies. The Information Commissioner prohibited the use of part of the seized documentation related to the e-mail and the web browsing, as it allegedly concerned unlawful processing of personal data.

Part 4: Miscellaneous Procedural and other Matters

22. Please provide a brief overview of the mechanisms in place in your country to deal with the regulation of "privacy" as between employers and workers.

INFORMATION COMMISSIONER

If the worker thinks that the employer has violated the provisions of the personal data protection law, he can make a declaration to the Information Commissioner about the abuse of personal data. The Information Commissioner monitors the implementation of the provisions of the Personal Data Protection Act and ensures harmonised enforcement of measures in the field of personal data protection.

LABOUR INSPECTOR

The labour inspector has a mandate to impose a fine on the employer and a responsible person at the employer. The fine is defined in the penal provisions of the ERA: a fine between EUR 3,000 and 20,000 shall be imposed on the employer who has acted contrary to Article 26 of the ERA Act when concluding an employment contract; and a fine between EUR 450 and 2000 shall be imposed on the responsible person of the employer. In particularly justified cases, the labour inspector may decide to pronounce a reprimand or warning to the offender. Beside issuing (administrative) decisions during the inspection procedure and pronouncing sanctions (fines), the labour inspector may also mediate in the dispute between the workers and the employer. Both parties have to agree to it, and thus concluded agreement has executory title (this concerns special forms of out-of-court settlement).

LABOUR COURTS

Should a worker think that the employer does not fulfil his obligations arising from the employment relationship or that he violates any of his rights arising from employment relationship, he shall have the right to request in writing that the employer abolish the violation and/or fulfils his obligations.

Should the employer not fulfil his obligation arising from the employment relationship and/or not abolish the violation within eight working days upon the receipt of the worker's written request, the worker may request judicial protection before the competent labour court within 30 days from the expiry of the time limit stipulated for the fulfilment of obligations and/ or abolishment of violation by the employer.

Filing of application for the removal of offence is a procedural assumption for judicial protection. Deadline for instituting the action is a preclusive deadline; any delays result in the rejection of the complaint.

If individuals have suffered damage due to unlawful processing of their personal data, they may claim indemnity from the perpetrator. Since this case concerns pecuniary claim under the employment relationship, the worker may claim it directly at the Labour Court. In this case, the Court will only take into account the limitation period of five years applicable to labour disputes. The employer is liable to pay the worker the compensation under the general rules of the civil law based on the principle of total compensation.

For suffered mental pain due to a decrease in living activities, defamation of goodwill and honor or okrnitve freedom or personality rights and for the fear suffered by the victim, if the circumstances of the case, in particular if the degree of pain and fear and their length justify this, a fair monetary compensation independent from the reimbursement of pecuniary damage, but also if not of pecuniary damage. The amount of compensation for non-pecuniary damage depends on the importance of the goods and the

purpose of this compensation, but it may not support the aspirations which are not compatible with its nature and purpose.

23. Do issues of "privacy" arise before the Labour Courts/Tribunals in your country, and, if so, what form to these tend to take?

The issues of invading the privacy (and personality) of employees occasionally occur in labour disputes. There were some cases where the question was raised of accepting evidence on serious misconduct in disciplinary procedures, and the termination of the employment contract, if such evidence was obtained by recording of business premises (concretely, casinos). The issue of evidence obtained by invading the privacy also occurs in determining the alcohol consumption at the workplace (alcotests, blood samples), or compliance with the instructions for the treatment during the sick leave.

The Supreme Court judgement VIII Ips 160/2001 of 9.4.2002; from the statement of grounds:

„... upon committing a criminal offence prosecuted ex officio, the worker has to be caught either at work or in connection with work. It is not important how, or in what way he was caught, and who caught him at committing a criminal offence. It can also be presented through video records, since visual recording of the business (the working) premises of the employer during working time is not prohibited. If the employer has good grounds for it, such recording is acceptable, although the workers were not informed thereof in advance. This does not mean invasion of the workers' privacy. The work is performed in the premises and with the means of the employer, therefore the latter cannot be banned to use technical means to perform the control of how his employees work and how they handle the means entrusted to them. Whether these video clips can be used as evidence in the criminal procedure and whether they can serve as a basis to prove the alleged offense to the plaintiff is the matter of a criminal procedure and not of this labour dispute ..."

The Supreme Court judgement VIII Ips 217/2003 of 18.5.2004, from the statement of grounds:

„As regards the use of evidence obtained with the help of the contractual engagement of the private detective J.P., the court of first instance entirely agrees with the reasons stated by the court of the second instance in the statement of grounds for its final decision. As the defendant was in charge of paying the wage compensation for the time of the plaintiff's absence from work during the sick leave, he had to comply with the rules of control over the exercise of the health insurance rights as defined in the Rules on statutory health insurance. These rules explicitly defines the possibility of controlling the temporary absence from work due to illness through a contractually engaged legal or natural person. Information obtained by such person from the contract-based observation of the movement of persons on a sick leave, in the sense of controlling their temporary absence from work, may be used as evidence in a disciplinary proceeding, and also at the court unless it has been proven that they were obtained illegally (e.g. by breaching the privacy of home, correspondence, etc.). Since in this case the plaintiff did not prove that the information supplied by the detective on the plaintiff's work on a farm and his private exits during the days in issue was obtained in such unlawful manner, the defendant could use it as evidence in the disciplinary procedure and the court in its legal procedure, together with the explanation of his doctor what such practices imply in the sense of the plaintiff's absence from work due to sick leave."

The Supreme Court judgement VIII Ips 345/2006 of 29.5.2007; extract from the statement of grounds:

„The plaintiff's position that video recordings constitute illegally obtained evidence is unfounded. The court of the first instance agrees with the assumption of the lower courts that the audio video control in the premises of the defendant is explicitly allowed under the Gaming Act (Official Gazette RS, no. 27/95). Such control is prescribed as statutory control of gamblers (in Article 78), gaming tables, cashiers and safe (Article 80). It results from these provisions that the statutory video control Nazor includes both gamblers and employees, and even more clearly from Article 79(4) and (5) which allows (not excludes) the video control also for identifying irregularities on gaming devices and accessories, and in the performance of games. The defendant had to prescribe detailed methods of performing such controls. The actual findings of both courts is that the defendant accepted the relevant regulations and that the plaintiff was or must have been aware of them. Video surveillance in the areas where irregularities in the gaming devices might occur

(playing cards) was therefore not in contravention with law; evidence through consulting such video recordings was therefore not produced in an unlawful way...”

24. Do the procedures of the Labour Courts/Tribunals in your country make provision for private/secret hearings in particular circumstances:

– in particular, please indicate whether this might be the case in relation to:

• National security

• Cases involving disability or medical records of an intimate or embarrassing nature

• Cases where allegations are made that criminal acts been committed by a party or witness

• Cases where allegations are made of sexual or other abuse, and/or where the records may involve disclosure of intimate sexual or other acts by a party or witness

Pursuant to the provisions of the Labour and Social Courts Act (LSCA), the public shall be excluded from the oral hearing in disputes on the rights to and from the disability and health insurance; the hearing may be attended by persons authorised by the Court for justified reasons on the proposal of the insured.

Pursuant to the provisions of Article 230 of the Civil Procedure Act (CPA) if, by giving a testimony, a person might violate his duty to keep official or military secret, he may not be examined as a witness as long as the competent authority releases him from such duty.

Pursuant to Article 231 of CPA, a witness may refuse testimony:

1. on what the party has shared with him as his counsel;

2. on what the party or other person has confessed to him as their confessor;

3. on facts of which he has learnt as a lawyer or a doctor or in pursuance of other activity, if he is bound to protect the secrecy of what he learns in the practice of legal or medical profession or pursuing such other activity.

In line with the provisions of Article 233 of the CPA, witnesses may refuse to answer the asked question, if they have detailed grounds to do so, especially if their answer to those questions might cause severe embarrassment and considerable property damage or lead to the criminal prosecution of themselves or the persons in direct family kin line on any level, family kin steps up to the third level; their spouse or the person with whom they have been living in a lasting cohabitation as stipulated by the law governing the marriage and family relations; or the persons in in-law family relationship up to the second level even where such marital relationship has terminated; or their adoptive parent or direct descendant or adopted child.

25. Are there any provisions in your country which enable particular proceedings in the Labour Courts/Tribunals not to be disclosed in the press and/or not to be available to the general public as part of official records of judicial proceedings? – If so, please indicate under what circumstances this might arise, and whether there is any special form of appellate or supervisory jurisdiction in relation to exercise of any such powers.

Publicity of the main hearing is one of the basic principles of the procedure also at labour and social disputes. The exception is the previously stated Article 60 of the LSCA which stipulates that the public is excluded in disputes on the rights to and under the disability and health insurance.

The panel may, pursuant to the provisions of Article 294 of the CPA, exclude the public from the entire main hearing or its part also in other disputes, where that is required by the official, commercial or personal secrets, the interests of public order or reasons of morality. The exclusion of public from hearings does not apply to the clients, their legal representatives, counsels and intervenients; the Panel may give permission the main hearing from which the public is excluded be attended by certain designated officials, court personnel, scholars or public representatives, if this is necessary for performance of official tasks, scientific activity, or a public service. Those persons shall be warned by the presiding judge of their obligation to

keep secret information learned at the trial, and of the consequences of disclosing of such secret information (Article 295 of the CPA).

The exclusion of public shall be decided by the court in a substantiated and publicly announced decree. No special appeal shall be allowed against this decree; it can only be appealed together with the final decision (Article 296 of the CPA).

Visual recording of main hearings is regulated separately. The President of the Supreme Court may exceptionally allow visual recording of a main hearing in a criminal case, but the Courts do not issue permits for recording other hearings (e.g. civil proceedings and non-judicial proceedings, commercial law cases, etc.). Recording may be limited to the beginning of the trial, or to the declaration of judgments in a particular criminal case. The use of visual material or recordings from the main hearing can be limited to one single publication or dissemination in the media covering this criminal case. Visual recording of the judge or the Panel members is not allowed without their explicit consent. Despite the permission, the Judge may allow recording only to the extent necessary for the proper information of public and in a way that is least disturbing to the course of the trial.

Constitution of the Republic of Slovenia

Article 35

(Protection of Right to Privacy and Personality Rights)

The inviolability of the physical and mental integrity of every person, his privacy and personality rights shall be guaranteed.

Article 36

(Inviolability of Dwellings)

Dwellings are inviolable.

No one may, without a court order, enter the dwelling or other premises of another person, nor may he search the same, against the will of the resident.

Any person whose dwelling or other premises are searched has the right to be present or to have a representative present.

Such a search may only be conducted in the presence of two witnesses.

Subject to conditions provided by law, an official may enter the dwelling or other premises of another person without a court order, and may in exceptional circumstances conduct a search in the absence of witnesses, where this is absolutely necessary for the direct apprehension of a person who has committed a criminal offence or to protect people or property.

Article 37

(Protection of the Privacy of Correspondence and Other Means of Communication)

The privacy of correspondence and other means of communication shall be guaranteed.

Only a law may prescribe that on the basis of a court order the protection of the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time where such is necessary for the institution or course of criminal proceedings or for reasons of national security.

Article 38

(Protection of Personal Data)

The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited.

The collection, processing, designated use, supervision and protection of the confidentiality of personal data shall be provided by law.

Everyone has the right of access to the collected personal data that relates to him and the right to judicial protection in the event of any abuse of such data.

Employment Relationships Act

Obligation to Protect the Worker's Personality

Article 44

(General)

The employer must protect and respect the worker's personality and take into account and safeguard the worker's privacy.

Article 45

(Protecting the Worker's Dignity at Work)

(1) The employer shall be obliged to provide such a working environment in which none of the workers is subject to employer's, superior's or co-worker's undesired treatment of sexual nature including undesired physical, verbal or nonverbal treatment or other sexually based behaviour which creates intimidating, hostile or humiliating relationships and environment at work and offends the dignity of men and women at work.

(2) The concerned worker's rejection of the treatment referred to in paragraph (1) may not represent the reason for discrimination in employment and at work.

(3) If in case of dispute the worker states facts which justify the assumption that the employer behaved contrary to paragraphs (1) and (2), it is the employer who has to supply the evidence.

Article 46

(Protection of the Worker's Personal Data)

(1) Personal data of workers can be gathered, processed, used and provided to third persons only if this Act or other laws stipulate, and if it is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship.

(2) Personal data of workers can only be gathered, processed, used and provided to third persons by the employer or the worker who is specially authorised to do so by the employer.

(3) If the legal basis for gathering personal data of workers does not exist any more, they shall be deleted immediately and no more used.

(4) The provisions of the first three paragraphs shall also apply to personal data of applicants.

Personal Data Protection Act

Full text (and other relevant documents) at the home page of the Information Commissioner http://www.ip-rs.si/ (English version).

Spain

Antonio Martín Valverde,
Supreme Court Judge

Miguel Ángel Limón Luque
Legal Counsel of the Supreme Court

José María Ríos Mestre
Labour lawyer

Part 1. The regulatory context

62. Does your legal system possess any general definition of "privacy"?

- If so, please indicate the content and source of that definition. If not, how have notions of "privacy" been approached in your country conceptually, in academic writings, or as matters of socio-legal policy?

No, it does not. The definition has been constructed under the influence of both legal decisions and academic papers. Right to privacy , "implies the existence of a reserved area and own space to interact with others, according to the lines of our culture, in order to maintain a minimum standard of life" (STC 209/1988, of October, 27th).

63. Does your country have a Constitution, and does this make any provision in relation to "privacy" for citizens (whether at work or otherwise)?

The Spanish Constitution, passed on 1978, protects the right to privacy under its section 18.1. This right is strongly related to the right of the dignity of the human being recognized in section 10.1 of the Spanish Constitution.

64. Does your country adhere to International Instruments which contain provisions relating to "privacy" (e.g. at the level of the Council of Europe, etc.)?

- If so, please indicate which instruments and when your country signed up to, or ratified, each of those instruments.

Reference standards are the European Human Rights Convention and the International Covenant on Human Rights. At the EU level, it has to be mentioned the Regulation 45/2001 of the European Parliament and the European Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data. Its purpose is to establish a legal framework in which the institutions and bodies shall ensure the protection of fundamental rights and freedom of individuals, including their right to privacy with respect to the processing of personal data, without limiting the free flow of personal data between Member States and Community institutions and bodies or between the institutions and bodies. It is also subject of the regulation creating an independent supervisory authority known as the European data Protection Supervisor to monitor the implementation of this standard to all processing operations carried out by the Community institutions and bodies.

The rationale for this regulation lies in the requirement for Member States of Directive 95/46 CE to ensure the protection of fundamental rights and freedom of individuals, including the rights to privacy in regard to the processing of personal data in order to ensure the free flow of personal data in the Community. The Directive was complemented and refined by Directive 97/66 CE of the European Parliament and the European Council of December 15, 1997, concerning processing of personal data and privacy in the telecommunications sector.

65. As a general matter, how are norms established at the international level transposed into protections or rights at the domestic level for citizens in your country?

- Please illustrate this by reference to any International Instruments mentioned in relation to Q.3.

The International Covenant of Human Rights was ratified on April 27, 1977. After being published at the Spanish Official Newspaper the Convention is in force and it is not necessary to make any transposition of its content.

The Directive 95/46 CE was transposed by the Royal Decree 156/1996, of 2nd February, establishing an Agency created in 1992 called "Agencia de protección de datos", as the Spanish Authority to protect personal data.

66. Are public sector workers/officials in your country subject to a different regime from private sector staff in relation to rules on "privacy"?

- If so, please indicate what the differences are, and whether there can be said to be broad equivalence between the different regimes.

Our Constitutional Court has ruled that the worker has not a contractual obligation of loyalty regarding to the employer and his/her interests, but constitutional rights of the worker at the company are limitated by the good faith principle that governs the employment contract. Civil Servants are also entitled to the protection of their privacy in connection with their work. However, public employees are in a situation of "special subjection" and this position carries special duties, as their realtionship is not governed by an employement contract. This means that the public servant must be loyal in a broader sense than a worker under a private employment contract.

67. Are any groups of workers (other than public sector workers/officials) treated differently from the "normal model" in relation to rules on "privacy"?

In general, worker behaviour after work time and outside the work centre is not subject to control by the employer. However ideological companies such schools, newspapers, trade unions and the like would take into account the behaviour of their workers after work time whether it could be opposed to its ideological goals. For example, cases have arisen where the religion teacher's contract was not extended or terminated because of his/her behaviour in private life (such as maintaining a relationship out of catholic marriage or doing "top less" in a public beach at the same city in which the teacher carries out her duties).

68. Please describe briefly your national framework of rules dealing with issues of "privacy". Where these are contained in legislation or administrative regulations, please indicate the sources *[and, if possible, please attach a copy/version of the relevant provisions]*.

The most relevant regulation is Act 15/1999, of December 13th, on the Protection of Personal data. This Act governs the matters relating to personal data, and abrogated the previous Act 5/1992, of October, 29th, of automated processing of personal data. Additional regulation is scattered and entail lack of entity; it is also important the Case Law of the Tribunals. Partially, it can be argued that in Spain there is not a national framework of rules dealing with issues of "privacy".

Also important is the Act 1/1982, of May 5th, for the Civil protection of fundamental rights to honour, personal and family privacy and image. The Act governs the procedure for the exercise of legal actions to protect the right to privacy. For workers and employers the procedure is regulated in the Labour Procedure Act.

The Act 1/1995, of March 24th, regulating the Statute of the Workers, recognizes to the worker the right to privacy at work at section 4.2.e), and provides some rules regarding body search or the search of worker personal belongings at work in section 18; also in section 20 the Act regulates the powers of the employer in order to control the behaviour of the employee. This power is limitated according to the principles of good faith and the preservation of the dignity of the worker.

Section 4.2.e): "*Artículo 4. Derechos laborales. (…)2. En la relación de trabajo, los trabajadores tienen derecho: (…) e) Al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo".*

Section 18: "*Artículo 18. Inviolabilidad de la persona del trabajador. Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible".*

Section 20: "*Artículo 20. Dirección y control de la actividad laboral. 1. El trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien éste delegue. 2. En el cumplimiento de la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquél en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres. En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe. 3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso. 4. El empresario podrá verificar el estado de enfermedad o*

accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones".

It is also important to mention the section 22 of the Act 31/1995, of November 8th, for the Prevention of Risks at work, that regulates health controls at the workplace.

Section 22: "*Artículo 22. Vigilancia de la salud. 1. El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo. Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento. De este carácter voluntario sólo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad. En todo caso se deberá optar por la realización de aquellos reconocimientos o pruebas que causen las menores molestias al trabajador y que sean proporcionales al riesgo. 2. Las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud. 3. Los resultados de la vigilancia a que se refiere el apartado anterior serán comunicados a los trabajadores afectados. 4. Los datos relativos a la vigilancia de la salud de los trabajadores no podrán ser usados con fines discriminatorios ni en perjuicio del trabajador. El acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador. No obstante lo anterior, el empresario y las personas u órganos con responsabilidades en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva. 5. En los supuestos en que la naturaleza de los riesgos inherentes al trabajo lo haga necesario, el derecho de los trabajadores a la vigilancia periódica de su estado de salud deberá ser prolongado más allá de la finalización de la relación laboral, en los términos que reglamentariamente se determinen. 6. Las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo por personal sanitario con competencia técnica, formación y capacidad acreditada".*

Part 2: The State and the employer

69. Please outline the areas in which the State authorities in your country are entitled to obtain personal information from an employer about a member of its workforce.

    - In particular, please indicate whether the State authorities possess such powers in relation to nationality or national origins; residence status; work permit status; previous employment records; criminal records; tax status; family/marital status; medical records, health and/or disability-related material; bank account information (e.g. for payment of wages); trade union membership.

In order to guarantee public interests, the different public Administrations are entitled to obtain directly or under Judicial authorization personal information from the citizens. Judicial authorities are empowered to authorize other Authorities in other to get sensitive information as well as to protect the right to privacy.

Judicial authorities, the State Attorney's Office and the Security Forces have access to all information necessary to prevent and punish crime. There are few exceptions to the judicial authority to obtain data (such as lawyer's duty of confidentiality). Obviously there are areas particularly sensitive as the secrecy of communications and the inviolability of the home that require judicial authorization. Also, the Internal Revenue Service and the managing bodies of the Social security System have access to all information assets. Health Administration also has important powers. Finally, the remaining Public Administrations have also allowed access to personal data to fulfil its own purposes.

It is important to note that individuals are entitled to obtain all information necessary for the exercise of judicial actions. This power includes even sensitive information (i.e. health information). The information is obtained by application to the judicial authority.

70. Please indicate whether the State authorities in your country are entitled, under any circumstances, to implement surveillance of a workplace (electronic, video, visual observation, etc.) for the purpose of obtaining personal information about any member of the workforce?

    - In particular, please indicate whether the State authorities possess any special powers of this kind in the context of measures intended for "combating terrorism" or in relation to investigation of serious criminal activities (e.g. drug dealing, "money laundering", etc.).

See response to question 8 above.

Part 3. The employer and the worker

71. Does a worker in your country enjoy any form of "right to privacy"?

    - If so, what form or forms does this right take? How is that right reflected in the legal system of your country?

Regarding the possible infringement of privacy rights in the context of an employment relationship, it should be noted that the signature of an employment contract does not mean in any way the deprivation by the employee of the rights that Constitution recognizes to the workers as citizens, including the right to personal privacy.

Business organizations are not separate worlds from the rest of society. Free enterprise does not legitimize those who run a business to withstand unjustified restrictions of the fundamental rights and civil liberties of the workers, which have a central value in the constitutional legal system (Constitutional Court decision 88/1985, July 19th). As we said above, the constitutional rights of the worker at the employment relationship are also limitated by the good faith principle, that governs the employment contract. The effectiveness of the fundamental rights of workers in the field of industrial relations must, therefore, take into account reciprocal limits that may arise between them and the corporate powers, which are also an expression of constitutional rights recognized in the Spanish Constitution.

This matter is also ruled by section 18 of the Act 1/1995, regulating the Workers Statute, under the title "Inviolability of the individual worker". According to it, "the employer is only entitled to make a body search or an inspection on the lockers and private belongings of the workers, when necessary to the protection of business or other workers, at the workplace and during working hours. In its full implementation the employer shall respect the dignity and privacy of the worker and shall be assisted by a legal representative of the workers or, in his/her absence at the workplace, by another worker of the company wherever possible".

It is important to remark a decision of the Spanish Constitutional Court that declared that an employer is not authorized to use information for different purposes of which they were disclosed. Therefore, the employer is not allowed to use the data regarding the workers that are affiliated to a specific Trade Union in order to discount salaries during a strike organized by the Union, when the data were obtained for check off purposes, taking also into account that the employer had other internal data stating that the worker did not join the strike (STC 11/1998, of January, 13th). Regarding computer

control by the employer, see also comments to STS September, 26th, 2007, R. 966/06 made in question 15.

72. To what extent (if at all) is any "right to privacy" for a worker more limited **when that person is at work** than any "general right to privacy" enjoyed by citizens in general?

See responses to questions 13, 14 and 15.

73. Under what conditions (if at all) is an employer in your country entitled **to obtain** (e.g. by way of questions contained in job application forms) personal information about a member of its workforce?

- In particular, please indicate the position in relation to the following specific areas (and please add information about any other matters which are of particular significance in your country):
  - information about the address, telephone contact numbers, etc. of the worker
  - information about the marital status of the worker
  - information about the health and medical condition of the worker (including, for example, details of the worker's personal doctor)
  - information about the sexual orientation of the worker
  - information about the religion of the worker
  - information about the political affiliation or activities of the worker
  - information about the tax (fiscal) affairs of the worker
  - credit information about the worker
  - court information (e.g. for enforcement of court orders by way of deductions from salary – "attachment of earnings")
  - information about any criminal convictions which the worker may have

See responses to questions 13 and 14.

74. Under what conditions (if at all) is an employer in your country entitled **to retain** (whether in the form of personal files, or electronically) personal information about a member of its workforce?

In a general sense, the employer is entitled to obtain and retain any information regarding the employee that relates directly to the job performed by the employee. The information must be congruent with the work performed and the goal of keeping the information has to be directly related to the reason that justified the data collection. In any case, the employer can keep information regarding the employee if he/she has given his/her express consent. This means that the employee consent permits to the employer to maintain and retain any data without fulfilling the above mentioned requirements.

To our opinion, a) it is not necessary to have previous consent of the employee in order to have the following data:

- information about the address, telephone contact numbers, etc. of the worker

b) it is not necessary to have previous consent of the employee in order to have the following data if the goal is directly related to the employment relationship:

- information about the marital status of the worker (exceptionally, in order to recognize employment rights or tax deductions)

- information about the health (only in cases specified by Law)

- information about the tax (fiscal) affairs of the worker

- credit information about the worker

- court information (e.g. for enforcement of court orders by way of deductions from salary – "attachment of earnings")

c) it requires previous consent of the employee:

- information about the medical condition of the worker (including, for example, details of the worker's personal doctor)

- information about the sexual orientation of the worker

- information about the religion of the worker

- information about the political affiliation or activities of the worker

- information about any criminal convictions which the worker may have.

- Is an employer in your country obliged to tell the worker that it is holding personal information about that worker and/or to make any such information available to the worker for inspection (e.g. to ensure the accuracy of the information)?

Yes, and the employee has the right to modify it if it is not accurate.

- Are there any provisions in your country which require the employer to handle such information in a particular way?

Yes, the employer is obliged to maintain the secrecy of the data, and not to disclose them to a third party, unless the data were sent to a company that provides to the company the services of holding and managing them.

- Is the employer required to destroy such information after a certain period of time?

If the information were not useful to the purposes of which it was obtained, the information should be destroyed. See also answer to question 10 (STC 11/1998, of January, 13th).

- Are there provisions in your country which regulate the freedom of the employer to disclose or pass such information to third parties (including to the public authorities)?

Yes. In general, to disclose or pass the information it is necessary the previous consent of the employee. One of the exceptions are Public Authorities when they require data in the exercise of their public powers.

75. In addition to the situations mentioned in Q.12 and Q.13, are there any circumstances under which an employer in your country is entitled to obtain (or to demand) medical details about a member of its workforce?

In general, the employer is not entitled to keep medical information to the employee without his/her previous consent. Anyway, there are some exceptions that we explain below. Under those exceptions, the employer may compel to an employee to pass a medical examination, after previous favourable opinion of the employee's representatives, but in general it is not allowed to keep data, that must be retained by medical personnel or public authorities. The employer –as well as the employees representatives– has only access to the conclusions of the medical examinations in order to prevent health risks at work.

- In particular, please indicate whether there are any situations in which an employer is obliged to obtain information about the health of the worker (e.g. before permitting that worker to perform tasks at heights, or where there may be exposure to dangerous substances or radiation during the course of performing the job).

The employer does not need previous consent of the worker and may compel to the worker in order to pass a medical examination when:

a) the employer needs to evaluate the effects of the conditions of work on the workers´ health;

b) the employer needs to verify that the worker's health is not a risk for himself, for the other workers, or for other people related to the company;

c) there is a specific legal measure in order to avoid special risk at work.

- Is there any procedure laid down for an employer in your country to obtain the formal consent of a worker to accessing such personal medical information?

No.

- Is an employer in your country entitled to ask specific questions about whether a member of its workforce is "disabled"? – If so, what are the consequences if the worker refuses/fails/chooses not to disclose such information?

Only in the cases above mentioned.

- Can an employer in your country require a worker to submit to a medical examination, and subsequently have access to the results of that medical examination (e.g. where the employer is considering dismissing the worker on grounds such as "capacity", or "fitness to do the job", or because of a high level of absences from work for medical reasons)?

There has been a case brought to the Spanish Constitutional Court (STC 196/2004, of November, 15th) in which a flight attendant was dismissed during a probationary period because she passed an urine test and the test showed a substantial presence of drugs (cannabis), and she was not told that the urine test included drugs control. The Constitutional Court ruled that the dismissal was null and void because the employer has the obligation to inform her of the purposes of the test and obtain her consent, because the information obtained was not proportional to the purposes of the test (a generic medical test), and the employer profited of this information in order to terminate the contract during the probationary period. It was a very polemic decision, as the drug control was performed in an airline company, and could be justified because of the special risk of flying under drug effects.

- Is an employer in your country entitled to make use of (and act on the basis of information obtained as a result of) techniques such as "psychological testing" or "genetic testing"?

It is common to pass "psychological testing" before being hired, but we understand that the employer needs the employee consent in order to obtain the data, unless exceptionally it could be a reason very closed to the job performed.

76. Is an employer in your country entitled to implement any forms of surveillance of workers at the workplace?

Yes, in public areas, and for safety reasons or reasons directly related to work. In general, it is possible to input all the measures of control mentioned below, but the employee must be previously informed and with the exception of inspection of electronic and personal communications (telephone calls out of the company, etc) –monitoring would be permitted–, as well as personal files contained in the computer. There was a very important decision of the Supreme Court (STS September, 26th, 2007, R. 966/06) that stated that the control of the computers given to the employee by the employer are governed by good faith rules, so the employer must inform previously to the workers that a specific control will be implemented and the measures that the employer will take in order to correct misconducts. Also, the employer is entitled to disconnect the employee of certain communication nets (for example, installing internet filters, etc).

- In particular, please indicate whether there are any situations in which an employer is entitled to make use of the following:
  - CCTV (video surveillance)
  - Monitoring and inspection of web-browsing by the worker
  - "Keystroke monitoring" of workers performing computerised tasks

- Monitoring and inspection of a worker's electronic communications (email, social networking websites, etc.)
- Monitoring and inspection of a worker's traditional communications (post, telephone calls, etc.)

16 Are there any circumstances where an employer in your country may be entitled to conduct (e.g. by security staff belonging to the enterprise) a physical (possibly including intimate) body search of a member of its workforce?

Under section 18 of the Statute of the Workers, the employer is only entitled to conduct a body search for the worker or his/her personal belongings and his/her locker, whether necessary to the property of the company or to protect the wealth of the other workers, at the workplace and during the work time. During the search the employer must be respectful with the worker dignity and privacy as much as possible, and a worker representative has to be present, and in his/her absence at the workplace, other worker, if possible. An intimate search would be possible only if there is no other way to respect dignity and privacy and is proportional to the purposes of the search.

What would be the consequences if the worker refused to submit to such a search?

If the worker refuses to do so, it could be considered a worker disciplinary misconduct, and if it is considered of special importance, it could justify a fair dismissal.

What would be the consequences if an employer carried out such a search without the consent of the worker?

Unless justified in extreme cases it could be considered a violation of the fundamental rights of the worker and maybe a crime. The employee could be entitled to damages. If the employee refuses to collaborate, the employer or his agents might call a public authority to conduct the search.

17. Is an employer in your country subject to any recognised "duty of confidentiality" in relation to members of its workforce and/or others?

The employer must keep confidentiality regarding to any private information regarding the worker to which he/she might have access. See responses 13 and 14 for more details.

If so, what is the extent of any such duty, what form or forms does this duty take, and how is that duty reflected in the legal system of your country?

This duty is guaranteed by good faith in the employment contract and also by Act 15/99, of data protection.

18. Under what circumstances can an employer in your country justify breaching the "privacy" of a member of its workforce or any "duty of confidentiality" owed to a worker in its employment?

- In particular, please indicate how this might be the case in relation to:
  - the employer's business interests (e.g. protection of trade secrets)

No.

  - supervision of security at the workplace.

At the very limit.

  - prevention of criminal activity (drugs abuse, etc.).

No. See STC 196/2004.

  - when required to act under instructions from the public authorities (e.g. as part of a police investigation)

Yes, as provided in Act 15/99.

19. Is it possible for an employer in your country to justify intrusions into the privacy of members of its workforce by giving clear notice that particular measures are in use (e.g. signs stating that the workplace is subject to CCTV surveillance)?

See question 15.

20. Is it possible for an employer in your country to include contractual provisions in the terms of the employment relationship which effectively permit the employer to breach the privacy of a member of its workforce?

Theoretically, the answer is yes, but it is not common. As it is a general renunciation of a fundamental right the possibility has to be interpreted strictly. It should be more reasonable a particular renunciation in a case by case basis.

21 Are there any special rules in your country concerning "personal" files created by a worker on a computer belonging to the employer at the workplace? Yes, see answer to question 15.

- Is there any guidance in relation to who "owns" any rights in relation to such "personal" files?

According to the Case Law this particular side of the employment relationship is regulated by good faith between the parties. In this sense, the employer should at least inform to the employee that he/she is going to monitor the creation of the files. According to Case Law the employer has not right to access to personal files.

Part 4. Miscellaneous procedural and other matters

22. Please provide a brief overview of the mechanisms in place in your country to deal with the regulation of "privacy" as between employers and workers.

Act 15/99; STC 196/2004 and STS September 26th 2007, R. 966/2006.

23. Do issues of "privacy" arise before the Labour Courts/Tribunals in your country, and, if so, what form do these tend to take?

Yes, they usually arise at Labour Courts, and concern dismissals, damages, disciplinary measures, fundamental rights.

24. Do the procedures of the Labour Courts/Tribunals in your country make provision for private/secret hearings in particular circumstances:

The Labour Judge is allowed to conduct the hearing without public if this is necessary to guarantee the dignity and privacy of the parties. In some cases, the Supreme Court has decided not to publish in the General Collections some data of the procedures in order to not make them public [for example, in a case in which the defendant was a transsexual, the Supreme Court ruled that it was prohibited the publication of any data identificating the procedure (including procedure number)].

- In particular, please indicate whether this might be the case in relation to:
  - national security

At the very limit.

  - cases involving disability or medical evidence of an intimate or embarrassing nature

Yes.

  - cases where allegations are made that criminal acts been committed by a party or witness

No.

  - cases where allegations are made of sexual or other abuse, and/or where the evidence may involve disclosure of intimate sexual or other acts by a party or witness

Yes.

25. Are there any provisions in your country which enable particular proceedings in the Labour Courts/Tribunals not to be disclosed in the press and/or not to be available to the general public as part of official records of judicial proceedings?

Yes, see question 24.

- If so, please indicate under what circumstances this might arise, and whether there is any special form of appellate or supervisory jurisdiction in relation to exercise of any such powers.

Sweden

The Labour Court
Stockholm

Swedish reply to the Questionnaire on Privacy

Part 1. The regulatory context

1. The Swedish legal system does not possess a general definition of "privacy".

2. Sweden has a written Constitution which contains provisions on fundamental rights (Chapter 2). Especially one provision is worth mentioning in this context: Article 6 means that an individual is protected from certain measures of the state, i.a. investigation of letters and other confidential information, secret screening, recording of telephone conversation and other confidential utterances.

3. Sweden, like most other countries in Europe, is bound by the European Convention on Human Rights. This convention was ratified by Sweden in 1952.

4. The European Convention on Human Rights was incorporated in Swedish law in 1994.

5. Nowadays, the relationship between public employer and its employees are in most respects governed by the same rules that are applicable on the private labour market. However, there are some exceptions i.a. concerning an employee´s duty to undergo medical investigation. According to the 1994 Act on Public Employment, an employee is in some cases obliged to undergo such an investigation.

6. Apart from what is mentioned above, there are no groups of workers that are treated differently from the "normal model".

7. The main legal source in this field is the 1998 Personal Data Act, which is based on EU law. There is at present no special act concerning privacy in working life. However, in May this year such an act has been proposed by a commission appointed by the government.

Part 2. The State and the employer

8–9. This question is not in the field of labour law.

Part 3. The employer and the worker

10–11. There are no cohesive rules for protection of personal integrity in working life. One can say that the existing regulatory framework intended to protect the personal privacy of employees in the workplace is elaborate and difficult to overview. It comprises a disparity of regulations and legislative enactments. Protection is only partially regulated by law.

12. There are no rules on what sort of information an employer is entitled to obtain. Some of the areas pointed out in the question is possible to get hold of according to the principle of free access to public

records. The question is rather if it is appropriate to ask a job applicant about information which is not related to the work or the workplace.

13, 19 and 21. If the information is filed electronically there are special rules in The Personal Data Act. The Personal Data Act, which applies to all automatic processing and registration, currently provides the best protection in connection with the processing of personal data.Through the Personal Data Act, the EC Directive on the protection of individuals has been introduced into Swedish legislation. The act contains special rules on processing data such as health and medical status, sexual orientation, religion of the worker, political view and membership in a trade union.

According to the directive and the The Personal Data Act an employer, as anybody else who is processing personal data, is obliged to inform the person, the employee, about the information he has in for instance a register.

The regulation in the directive and the The Personal Data Act covers the situation where information is passed on to a third party.

According to the act on camera surveillance one is obliged to inform about the surveillance.

There are no special rules on "personal" files, the The Personal Data Act is applicable.

14. There are no general rules which entitles an employer to obtain medical information.

As already mentioned employees in the public sector are under certain circumstances - security reasons - obliged to undergo medical investigation.

An employer in the private sector also have under certain circumstances, according to case-law, the right to ask an employee to undergo medical tests. The demand to undergo a test is accepted if the interest of the employer outweigh the interest for the employee not to undergo the test.

There are also special rules according to rules on safety and health at the workplace and concerning special types of work, e.g. railroad, aircraft and skips.

There are no rules concerning how to obtain a formal consent.

There is an act on genetic integrity from 2006. According to that act an employer is not allowed to ask a job-applicant or an employee to undergo a genetic test or to use information from such a test.

There are no specific rules on psychological testing and no case-law in the matter. If the test is done electronically or information from such a test is processed electronically or in a register The Personal Data Act is applicable.

15. The examples in the question are all, apart from the last one, some sort of processing of personal data on which The Personal Data Act is applicable. Even telephone calls can fall under this regulation if the telephone system is electronically.

Concerning traditional communication as post, letters, and telephone calls that is private there are special rules in the criminal law.

16. There are no specific rules on this matter. It is possible to regulate this in a collective agreement. If a worker refuses to submit to such a search a question of dismissal can arise. If an employer carried out such a search without agreement it could be considered a criminal act.

17. The employer is not subject to any generally recognised duty of confidentiality. An employer in the public sector have to consider some rules in the Secrecy Act, for instance concerning economy and health conditions.

18. For a private employer there are no rules of interest in relation to the examples mentioned. A public employer has in all these examples to apply rules in the Secrecy Act.

20. If applicable it is possible for an employer to breach a workers privacy by agreement or in accordance with a collective agreement.

Part 4. Miscellaneous procedural and other matters

22. There are no special mechanisms in place in Sweden to deal with the regulation of "privacy" as between employers and workers. Matters concerning privacy in working life are dealt with in the same way as other matters concerning the relationship between employers and employees. A dispute relating to a rule in a collective agreement concerning e.g. duty to undergo medical investigation is handled the same way as other disputes about interpretation of or breach of a collective agreement which means that in the end such disputes could be tried in the Labour Court.

23. Issues of privacy could arise in for instance disputes relating to a collective agreement or as part of a dispute concerning the legitimacy of a dismissal or a notice to quit the employment.

24. The procedure in the Labour Court follows the same rules in this respect as the procedure in the general courts. The Code of Judicial Procedure thus provide provisions for keeping parts of the hearings behind closed doors on special conditions. If it can be assumed that at a hearing information will be presented to which secrecy applies in court under the Swedish Secrecy Act, the court may direct that the hearing be held behind closed doors insofar as it relates to the information. That is if it deems to be of extraordinary importance that the hearing be held behind closed doors. The examples given in the question at dash one, two and four describe situations where – if the detailed conditions in the Secrecy Act and the condition of extraordinary importance exist – the provision for secret hearings could be considered applicable. (There are also some other cases – if secrecy applies under the Secrecy Act – when a hearing may be held behind closed doors without that special requirement of extraordinary importance. Those cases are mostly related to criminal cases though.) As far as the situation described at dash three is concerned The Code of Judicial Procedure provides provisions according to which a witness or a party may decline to testify concerning a circumstance that should reveal that he, or a close relative, has committed a criminal or dishonourable act.

25. No there are no such provisions.

Questionnaire on

Privacy at the workplace

Part 1. The regulatory context

1. Does your legal system possess any general definition of "privacy"?
   - If so, please indicate the content and source of that definition. If not, how have notions of "privacy" been approached in your country conceptually, in academic writings, or as matters of socio-legal policy?
2. Does your country have a Constitution, and does this make any provision in relation to "privacy" for citizens (whether at work or otherwise)?
3. Does your country adhere to International Instruments which contain provisions relating to "privacy" (eg. at the level of the Council of Europe, etc.)?
   - If so, please indicate which instruments and when your country signed up to, or ratified, each of those instruments.
4. As a general matter, how are norms established at the international level transposed into protections or rights at the domestic level for citizens in your country?
   - Please illustrate this by reference to any International Instruments mentioned in relation to Q.3.
5. Are public sector workers/officials in your country subject to a different regime from private sector staff in relation to rules on "privacy"?
   - If so, please indicate what the differences are, and whether there can be said to be broad equivalence between the different regimes.
6. Are any groups of workers (other than public sector workers/officials) treated differently from the "normal model" in relation to rules on "privacy"?
7. Please describe briefly your national framework of rules dealing with issues of "privacy". Where these are contained in legislation or administrative regulations, please indicate the sources *[and, if possible, please attach a copy/version of the relevant provisions]*.

Part 2: The State and the employer

8. Please outline the areas in which the State authorities in your country are entitled to obtain personal information from an employer about a member of its workforce.
   - In particular, please indicate whether the State authorities possess such powers in relation to nationality or national origins; residence status; work permit status; previous employment records; criminal records; tax status; family/marital status; medical records, health and/or disability-related material; bank account information (eg. for payment of wages); trade union membership.
9. Please indicate whether the State authorities in your country are entitled, under any circumstances, to implement surveillance of a workplace (electronic, video, visual

observation, etc.) for the purpose of obtaining personal information about any member of the workforce?

- In particular, please indicate whether the State authorities possess any special powers of this kind in the context of measures intended for "combating terrorism" or in relation to investigation of serious criminal activities (eg. drug dealng, "money laundering", etc.).

Part 3. The employer and the worker

10. Does a worker in your country enjoy any form of "right to privacy"?
    - If so, what form or forms does this right take? How is that right reflected in the legal system of your country?
11. To what extent (if at all) is any "right to privacy" for a worker more limited **when that person is at work** than any "general right to privacy" enjoyed by citizens in general?
12. Under what conditions (if at all) is an employer in your country entitled **to obtain** (eg. by way of questions contained in job application forms) personal information about a member of its workforce?
    - In particular, please indicate the position in relation to the following specific areas (and please add information about any other matters which are of particular significance in your country):
        - information about the address, telephone contact numbers, etc. of the worker
        - information about the marital status of the worker
        - information about the health and medical condition of the worker (including, for example, details of the worker's personal doctor)
        - information about the sexual orientation of the worker
        - information about the religion of the worker
        - information about the political affiliation or activities of the worker
        - information about the tax (fiscal) affairs of the worker
        - credit information about the worker
        - court information (eg. for enforcement of court orders by way of deductions from salary – "attachment of earnings")
        - information about any criminal convictions which the worker may have
13. Under what conditions (if at all) is an employer in your country entitled **to retain** (whether in the form of personal files, or electronically) personal information about a member of its workforce?
    - In particular, please indicate the position in relation to the specific areas mentioned in Q.12 (and please add information about any other matters which are of particular significance in your country).
    - Is an employer in your country obliged to tell the worker that it is holding personal information about that worker and/or to make any such information available to the worker for inspection (eg. to ensure the accuracy of the information)?

- Are there any provisions in your country which require the employer to handle such information in a particular way?
  - For example, is the employer required to register the fact that it holds such information with a public official (a "data protection commissioner" or the like)?
  - Does the employer personally/physically have to retain such information under its control at the workplace, or can it employ specialist companies to hold and manage any such data?
  - Is the employer required to destroy such information after a certain period of time?
- Are there provisions in your country which regulate the freedom of the employer to disclose or pass such information to third parties (including to the public authorities)?

14. In addition to the situations mentioned in Q.12 and Q.13, are there any circumstances under which an employer in your country is entitled to obtain (or to demand) medical details about a member of its workforce?
    - In particular, please indicate whether there are any situations in which an employer is obliged to obtain information about the health of the worker (eg. before permitting that worker to perform tasks at heights, or where there may be exposure to dangerous substances or radiation during the course of performing the job).
    - Is there any procedure laid down for an employer in your country to obtain the formal consent of a worker to accessing such personal medical information?
    - Is an employer in your country entitled to ask specific questions about whether a member of its workforce is "disabled"? – If so, what are the consequences if the worker refuses/fails/chooses not to disclose such information?
    - Can an employer in your country require a worker to submit to a medical examination, and subsequently have access to the results of that medical examination (eg. where the employer is considering dismissing the worker on grounds such as "capacity", or "fitness to do the job", or because of a high level of absences from work for medical reasons)?
    - Is an employer in your country entitled to make use of (and act on the basis of information obtained as a result of) techniques such as "psychological testing" or "genetic testing"?
15. Is an employer in your country entitled to implement any forms of surveillance of workers at the workplace?
    - In particular, please indicate whether there are any situations in which an employer is entitled to make use of the following:
      - CCTV (video surveillance)
      - Monitoring and inspection of web-browsing by the worker
      - "Keystroke monitoring" of workers performing computerised tasks
      - Monitoring and inspection of a worker's electronic communications (eMail, social networking websites, etc.)
      - Monitoring and inspection of a worker's traditional communications (post, telephone calls, etc.)

16. Are there any circumstances where an employer in your country may be entitled to conduct (eg. by security staff belonging to the enterprise) a physical (possibly including intimate) body search of a member of its workforce?
    - What would be the consequences if the worker refused to submit to such a search?
    - What would be the consequences if an employer carried out such a search without the consent of the worker?
17. Is an employer in your country subject to any recognised "duty of confidentiality" in relation to members of its workforce and/or others?
    - If so, what is the extent of any such duty, what form or forms does this duty take, and how is that duty reflected in the legal system of your country?
18. Under what circumstances can an employer in your country justify breaching the "privacy" of a member of its workforce or any "duty of confidentiality" owed to a worker in its employment?
    - In particular, please indicate how this might be the case in relation to:
        - the employer's business interests (eg. protection of trade secrets)
        - supervision of security at the workplace
        - prevention of criminal activity (drugs abuse, etc.)
        - when required to act under instructions from the public authorities (eg. as part of a police investigation)
19. Is it possible for an employer in your country to justify intrusions into the privacy of members of its workforce by giving clear notice that particular measures are in use (eg. signs stating that the workplace is subject to CCTV surveillance)?
20. Is it possible for an employer in your country to include contractual provisions in the terms of the employment relationship which effectively permit the employer to breach the privacy of a member of its workforce?
21. Are there any special rules in your country concerning "personal" files created by a worker on a computer belonging to the employer at the workplace?
    - Is there any guidance in relation to who "owns" any rights in relation to such "personal" files?

Part 4. Miscellaneous procedural and other matters

22. Please provide a brief overview of the mechanisms in place in your country to deal with the regulation of "privacy" as between employers and workers.
23. Do issues of "privacy" arise before the Labour Courts/Tribunals in your country, and, if so, what form do these tend to take?
24. Do the procedures of the Labour Courts/Tribunals in your country make provision for private/secret hearings in particular circumstances:
    - In particular, please indicate whether this might be the case in relation to:
        - national security

- cases involving disability or medical evidence of an intimate or embarrassing nature
- cases where allegations are made that criminal acts been committed by a party or witness
- cases where allegations are made of sexual or other abuse, and/or where the evidence may involve disclosure of intimate sexual or other acts by a party or witness

25. Are there any provisions in your country which enable particular proceedings in the Labour Courts/Tribunals not to be disclosed in the press and/or not to be available to the general public as part of official records of judicial proceedings?

    - If so, please indicate under what circumstances this might arise, and whether there is any special form of appellate or supervisory jurisdiction in relation to exercise of any such powers.