COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 23 June / juin 2011 T-PD-BUR(2011) 09 MOS

BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]

LE BUREAU DU COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNES A CARACTERE PERSONNEL [STE n°108]

(T-PD-BUR)

Compilation of relevant national legislation in personal data protection used for employment purposes

Compilation des législations nationales pertinentes en matière de protection des données à caractère personnel utilisées à des fins d'emploi

Secretariat document prepared by
The Directorate General of Human Rights and Legal Affairs

Document préparé par
la Direction Générale des affaires juridiques et des droits de l'Homme

INDEX / TABLE DES MATIERES

CZECH REPUBLIC

21.03.2011 - 08:27:53

Position No. 1/2006
January 2006

Operating Video Recording Systems in the Light of Data Protection Law

Operation of a video recording system is considered personal data processing, if besides the video surveillance itself **the captured images are recorded**, or information stored in the recording device and at the same time the recordings, or selected information **serve to the purpose of identification of individuals** in context with a certain conduct.

The video surveillance of individuals itself is not a personal data processing pursuant the Act No. 101/2000 Coll., as it does not falls within the meaning of Article 4(e) of the Act No. 101/2000 Coll. It does not eliminate, however, the application of other legal regulations, especially the provisions of the Civil Code regulating conditions for the protection of personality.

Data stored in a recording device, either images or sounds, are personal data on condition an individual might be identified directly or indirectly on the ground of these recordings (i.e. information from the image or sound recordings enable, if indirectly to identify a person). An individual is identifiable, if the image on which is he recorded reveals his distinctive marks (especially his face) and the full identification of a person is possible, if these characteristics are matched with other data at disposal. A personal data in its complexity then consists of those identifiers that make it possible to link the respective person with a certain conduct captured on the video shooting.

Personal data processing by means of a video recording system is legitimate:

a) in **fulfilling the tasks imposed by the law** (e.g. Act on the Police of the Czech Republic); in these cases it is necessary to observe the provisions of the law in question,

b) with **the data subject's consent**; it is virtually feasible only in very limited cases when it is possible to identify explicitly the group of persons frequenting within the reach of the camera,

c) without the data subject's consent under application of the **Article 5(2)(e) of the Act No. 101/2000 Coll.** The conditions, however, laid down in paragraph 4 are to be observed.

Obligations of a controller who operates a video recording system equipped with a recording device:

a) **Video surveillance must not excessively interfere with one's privacy.** A video recording system may basically be deployed, if the intended purpose cannot be achieved in another manner (a property, for instance, can be protected from robbery by a lock). Furthermore, it is not acceptable to install a video recording system in rooms used exclusively for private purposes (e.g. toilettes, showers). It is, of course, possible to offer the data subjects a choice between alternatives (it is possible, for instance, to monitor the cloak-room of a swimming pool on condition a space is reserved for changing that is not monitored).

b) **Specification of the intended purpose.** The purpose of recording must first be specified unambiguously and be in line with the important, legally protected interests of the controller (e.g. protection of property against robbery). The recordings may be used only in connection with investigation of an event harming these important, legally protected interests of the controller. The legitimacy of the usage of recordings for other purpose must be limited to a significant public interest, e.g. fight against street criminality.

c) **Retention period** for the recordings is to be fixed. The data retention period should not exceed the maximum time limit eligible for fulfilling the purpose of the video surveillance. Data should be stored within a time loop over, for instance, twenty-four hours, if a permanently guarded property is in question, or over a longer period not reaching over several days and they should be erased after this period elapsed. It does not apply for recordings made by the police pursuant a special law. Only in case of an existing security incident the data should be disclosed to the law enforcement authorities, the court or other entitled subject.

d) Appropriate security measures are to be ensured in order **to protect** the recording systems, transfer

ways and data carriers on which **recordings** are stored from unauthorized or incidental access, alteration, destruction, loss or other unauthorised processing – see Article 13 of the Act No. 101/2000 Coll.

e) **Data subject** must be **informed** in an appropriate manner that a video recording system is in operation (e.g. through a notice placed in the monitored space), see Article 11(5) of the Act No. 101/2000 Coll., except where special rights and obligations ensuing from a special law are being exercised.

f) Other data subject's rights are to be guaranteed, namely the right to access the data processed and the right to object to their processing, see Article 1 of the Act No. 101/2000 Coll.

g) **Personal data processing is to be registered** with the Office for Personal Data Protection except where special rights or obligations ensuing from a special law are being applied, see Article 18(1)(b) of the Act No. 101/2000 Coll.

Position No. 1/2007

June 2007

Position on the application of the right to personal data protection in the provision of information on the work of the public administration bodies

The Charter of Fundamental Rights and Basic Freedoms, which is part of the constitutional order of the Czech Republic, stipulates *inter alia* two human rights where the relation between them may not be entirely clear in interpretation. The Office for Personal Data Protection was established to supervise compliance with part of one of them: on one side there is the right to the protection of privacy and on the other the right to information.

The protection of privacy is governed in particular by the following two provisions in the Charter:

Article 7 paragraph 1: "The inviolability of the person and of her private life is guaranteed. They may be limited only in cases provided for by law."

Article 10 paragraph 3: "Everyone has the right to be protected from the unauthorized gathering, public revelation, or other misuse of his personal data."

The right to information is governed in general by Article 17 paragraph 1 of the Charter, which states: "The freedom of expression and the right to information are guaranteed." Paragraph 5 of the same Article extends the right to information to the principle of publicity for the public administration: "State bodies and territorial self-governing bodies are obliged, in an appropriate manner, to provide information with respect to their activities. The conditions and implementation thereof shall be provided for by law."

There is specific legislation on those constitutional principles in Act No. 101/2000 Coll., on the Protection of Personal Data and on amendments to certain acts, as subsequently amended (hereinafter "Personal Data Protection Act"), for the protection of privacy, and Act No. 106/1999 Coll., on Free Access to Information, as subsequently amended (hereinafter "Free Access to Information Act"), on questions of the general right to information and the application of the constitutional principle of the public nature of state administration.

Those constitutional principles can come into conflict, as the work of the bodies of the state administration and territorial self-governing bodies is performed by people, individuals, and in many cases their work is directed at individuals. All of those individuals have of course a right to the protection of privacy, which may however clash with the public's right to information on the work of state bodies and territorial self-governing bodies.

Both the aforementioned acts seek to resolve that potential ambiguity in the application of the law. Section 8a of the Free Access to Information Act states: "The legally-bound person shall communicate information concerning a personality, manifestations of a private nature, an individual's privacy and personal data only in accordance with legal regulations governing their protection." A footnote to that provision includes examples of other legislation, namely Sections 11 to 16 of Act No. 40/1964 Coll. (hereinafter "Civil Code") and Articles 5 to 10 of the Personal Data Protection Act.

The provisions in the Civil Code govern the right to the protection of personality. From our perspective Section 11 of the Civil Code is particularly interesting: "An individual shall have the right to the protection of his or her personhood, in particular his or her life and health, civic honour and human dignity as well as his or her privacy, name and manifestations of a personal nature." This is the general legislation on the constitutional principle of the protection of privacy, one aspect of which (and one that is crucial for our theme), the protection of personal data, is covered in the Personal Data Protection Act.

The other aforementioned provisions of the Civil Code govern the option of acquiring and publishing documents of a personal nature, portraits, pictures and visual and audio recordings concerning an individual or manifestations of a personal nature and the option for the protection of the individual against the unwarranted violation of his or her privacy.

Article 5 of the Personal Data Protection Act governs the rights and duties of the controller and processor in the processing of personal data, such as specifying the purpose, means and manner of personal data processing, processing only accurate personal data and only for the specified purpose. The second paragraph states that personal data processing is in principle only possible with the consent of the data subject, but it also lists a number of exemptions from that rule. For instance the controller may process personal data without such consent if processing is essential for fulfilment of a contract to which the data subject is a contracting party; if it relates to personal data that is lawfully published in accordance with

special legislation; if it is essential for the protection of vitally important interests of the data subject, etc.

For our theme the crucial provision is Article 5 paragraph 2 (f) of the Personal Data Protection Act, according to which the controller can process personal data without the subject's consent "if he provides personal data on a publicly active person, official or employee of public administration that reveals information on their public or administrative activity, their functional or working position."

Article 10 of the Personal Data Protection Act, to which the Free Access to Information Act refers in a footnote, and which reads "In personal data processing, the controller and processor shall ensure that the rights of the data subject are not infringed upon, in particular, the right to preservation of human dignity, and shall also ensure that the private and personal life of the data subject is protected against unauthorised interference," is more a statement of the general subject of the Personal Data Protection Act, but it is one of the most important provisions for the aforementioned conflict of rights.

In the provision of information on the work of the state administration or territorial self-governing bodies we can come into conflict with the right to the protection of privacy for two types of individuals:

1. Individuals who come into contact with bodies of the state administration or territorial self-governing bodies as citizens (petitioners, witnesses, injured parties, applicants, perpetrators, etc.);
2. Individuals who contribute directly to the work of the state administration or territorial self-governing bodies (officials and other employees of state administration bodies or territorial self-governing bodies, etc.).

For the first group of citizens it may seem that under the Free Access to Information Act information on them can in principle be provided. Section 2 paragraph 1 of the Act states: "The legally-bound persons, who under this Act have the duty to provide information related to their competencies, are the state agencies, territorial self-governing bodies and public institutions." The second paragraph in the list of legally-bound persons continues: "The legally-bound persons are further such entities who have been entrusted by law to decide on the rights, legitimate interests or duties of persons or legal entities in the area of public administration, namely to the extent of their decision-making activity only."

It may be deduced from the wording of the Free Access to Information Act that legally-bound persons may or should also provide information on, for instance, the parties in administrative proceedings, for administrative proceedings come under the competencies of many legally-bound persons. According to Section 2 paragraph 2 their disclosure duty is restricted, but the wording "to the extent of their decision-making activity" could be interpreted to mean that those legally-bound persons provide information on their entire decision-making activity, including on those individuals for whom their decisions established, amended or annulled rights or duties.

Of course, if a legally-bound person provides information on an individual so defined or definable, and therefore of necessity on their personal data, the reference by Section 8a of the Free Access to Information Act to the relevant provisions of the Personal Data Protection Act applies. In that situation it is necessary to apply Article 5 paragraph 2 of the Personal Data Protection Act, that personal data may only be processed with the consent of the data subject, where according to Article 4 (e) of the Act processing covers *inter alia* the disclosure, dissemination and publishing of personal data. The provision of personal data on those individuals is not covered by any of the exemptions in Article 5 paragraph 2. The aforementioned exemption in Article 5 paragraph 2 (f) of the Personal Data Protection Act covers a situation in which personal data on a publicly-active person, official or employee of the public administration may be provided without their consent, but not on other individuals who, while they have come into contact with the state administration or territorial self-administration, by no means work for it.

On that point it can be summarised that bodies or persons performing the state administration or territorial self-administration cannot publish or provide, in response to a request according to the Free Access to Information Act, personal data that they have obtained in connection with the performance of the state administration or territorial self-administration without the consent of the data subject, unless a special regulation stipulates otherwise, or unless a special regulation includes legislation on the publishing of information, including personal data (e.g. Act No. 183/2006 Coll., on the town and country planning and building code [the Building Act], Act No. 500/2004 Coll., the Administrative Code, or Act No. 56/2001 Coll., on the conditions for the operation of vehicles on roadways and on the amendment of Act No. 168/1999 Coll., on liability insurance for damage caused by the operation of vehicles and on amendments to certain related acts [the Motor Third-Party Liability Insurance Act], in the wording of Act No. 307/1999 Coll., including Decree No. 243/2001 Coll., on vehicle registration, etc.).

For the second group of persons presented above, when information is provided on the work of the state

administration and territorial self-administration, their right to the protection of privacy and personal data must be weighed against the necessity of applying the principle of making the work of the public administration public. Those persons are those who perform public administration at a body of the public administration, and those who have been entrusted by a special act to decide on the rights, legitimate interests and duties of other persons. Especially for those persons the aforementioned constitutional principles may conflict, when on one side there is the public's interest in information on the public administration, and on the other side the question of the privacy of a specific individual who contributes or has contributed to the performance of the state administration of territorial self-administration.

The aforementioned provision of Article 5 paragraph 2 (f) of the Personal Data Protection Act is crucial for that question. According to it the controller can process personal data without the subject's consent "if he provides personal data on a publicly-active person, official or employee of the public administration that reveals information on their public or administrative activity, their functional or working position."

"Public or administrative activity" is not defined by the Act and is therefore problematic. According to the wording of the Act it concerns data other than functional or working position, therefore information other than the information that a specific person occupies a specific function or is assigned to a particular working position in the performance of public administration, which under the Free Access to Information Act can be provided on request without the consent of the person concerned.

The Judgement of the Constitutional Court I. US 453/03 offers some help in clarifying those terms. It states "All the agendas of state institutions, as well as the activity of persons active in public life, e.g. the activity of local and national politicians, officials, judges, attorneys, or candidates or trainees for these offices are a public matter. These public matters, or the public activities of individual persons, may be judged publicly." The public activity of specific persons that is crucial for our theme is then the performance of the agendas of state institutions (and of course the agendas of territorial self-governing bodies) and the related activities of officials. However, even then account must be taken of any amendment by special regulations. For instance, for territorial self-administration that is Act No. 128/2000 Coll., on Municipalities (the Municipal Order), which includes legislation on publishing minutes from sittings of the municipal board and municipal council, where according to Section 101 of that Act the minutes from a sitting of the board may only be viewed by members of the council, while minutes from proceedings of the council are, pursuant to Section 16 of that Act, available to all citizens in the municipality or individuals over 18 years of age who own property within the municipality.

According to the Constitutional Court ruling, the wording of Section 2 paragraphs 1 and 2 of the Free Access to Information Act and Article 5 paragraph 2 (f) of the Personal Data Protection Act can be summarised as saying that legally-bound persons shall provide information on individual persons who perform public activities at a legally-bound entity provided those public activities are related to their competencies. For legally-bound entities that public and administrative activity is the agendas of state institutions and territorial self-governing bodies, including the activities of their officials.

Each legally-bound entity is established on the basis of an act: ministries and other central administration bodies by Act No. 2/1969 Coll., on the establishment of ministries and other central state administration bodies of the Czech Republic; other central administration offices by special acts, e.g. the Office for Personal Data Protection by the Personal Data Protection Act, regional offices by Act No. 129/2000 Coll., on regions (Regional Government), municipal offices on the basis of Act No. 128/2000 Coll., on municipalities (the Municipal Order), etc. Those special acts then define for the legally-bound entities the subject and extent of their competencies and powers. In general therefore information can only provided on the activities of individual persons within the scope of the competencies of the legally-bound entities.

Of course, even with that narrower definition of the conditions for providing information on persons who contribute to public administration, it is not possible to formulate a general conclusion on how to proceed in specific cases of requests for the provision of information pursuant to the Free Access to Information Act; it is not possible to stipulate strictly which category of data a legally-bound entity can provide and which it cannot. The solution always depends on the given situation, on the unique content of the request for the provision of information and on the legally-bound entity's assessment of the entire matter.

Conclusion: Although the right to the protection of privacy for persons who contribute to the performance of the state administration and territorial self-administration is in part weakened, it definitely is not annulled, and when appraising each request it is necessary to consider carefully what can be disclosed on a specific person without excessive violation of his or her privacy. The Constitutional Court reached a similar conclusion in its Judgement I. US 321/2006: "The right to the protection of private life is an inalienable human right which unquestionably also includes the right of an individual to decide at his or her discretion whether, to what extent and in what manner the facts of his or her private life be made available to other parties. That right can nevertheless be restricted for the purpose of protecting the fundamental rights of

other persons, or for the purpose of protecting the public interest, which is contained in the constitutional order in the form of a principle or value. Simultaneously care must be taken to achieve the broadest possible exercise of both protected values."

It can be said that in principle it is possible to restrict the right to the protection of the privacy of a person contributing to the performance of the state administration or territorial self-administration for reason of the exercise of the constitutional right to information. That weakening does not however mean the forfeiture of the right to the protection of privacy and in every case the legally-bound entity that decides on the provision of information must seek to satisfy as far as possible both the principle of the protection of privacy and personal data, and the right to information on the activities of the state administration and territorial self-administration.

Position No. 8/2006
October 2006

Use of electronic cards

The recent period has witnessed spreading issuance of electronic (chip) cards, by various institutions and in many areas of everyday life, that enable e.g. enjoyment of discounts, entry of buildings or use of various services. Collection of personal data occurs practically in all instances of production of these cards. In response to these facts, the Office for Personal Data Protection has decided to publish its below position, expressing the core of the Office's approach to the issues.

Several types of electronic cards are issued currently. The simplest one is so-called white chip card, often erroneously referred to as anonymous. Anonymity of such card, however, consists in the fact that no visible identification data of the card holder (first name, family name, photograph…) are set out on it. In terms of the Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Acts, as amended (hereinafter "the Personal Data Protection Act"), anonymity of the card holder could be accepted only providing that the card enables its holder access into a building, to an information system (or, use of a service), while not permitting the holder's unambiguous identification at such use. Hence, the system would, instead of identifying the holder, check only for the level of access rights provided by the card to its holder, i.e. no personal data would be processed in connection with a use of the card within the meaning of Article 4(a) and (e) of the Personal Data Protection Act. In fact, however, majority of the white cards are personalised. That means they authorise use of specific services only for a specified user (such as issuance of lunch meals, retrospective checks of the authorisation to enter etc. The system is then able to monitor activities of the white card holder in the same manner as those of a holder of any other card. This would certainly satisfy the provision of Article 4(e) according to which processing of personal data shall mean any operation or set of operations that is systematically executed by the controller or a processor in relation to personal data by automatic or other means, and therefore processing of personal data does occur.

Another card type includes single purpose personalised cards, such as client, benefit or subscription cards. Upon issuance of these cards, personal data are also processed as the cards are dedicated to a specific user who is unambiguously identified in the card - most frequently by his or her first name, family name, or sometimes photograph.

The last, currently the most widespread type of electronic cards includes multifunctional cards, enabling use of multiple types of services provided by multiple entities.

In terms of personal data processing relating to a provided product (service), a card represents an outward means with reference to various defined purposes. What is important is personal data processing (a database) in relation to which the card has been issued and, in particular, the purpose of such processing, not the card itself. In most instances, cards serve as a tool of performance of a service, i.e. they are a medium chosen for the purposes of completion of a contract (a service contract) entered into by the service provider and data subject. Issuance of a card and personal data processing is therefore an expression of a contractual relationship entered into on the initiative of the data subject (lodging an application for the card issuance) to which an exception provided by Article 5(2)(b) of the Personal Data Protection Act applies. According to that provision, the controller may process the personal data without the data subject's consent if the processing is essential for fulfilment of a contract to which the data subject is a contracting party or for negotiations on conclusion or alteration of a contract negotiated on the proposal of the data subject. The foregoing therefore constitutes an acceptation of a product offer, with specified parameters.

In case an optional solution exists, i.e. an option to use the product also without a chip card, personal data processing will be possible without any formal consent of the data subject since, by having chosen the product, the client has acceded to the terms set by the service provider. In case the product provision is strictly preconditioned by the card holding requirement, it is essential to distinguish data processing for various purposes.

The above applies to processing of information necessarily required for a card to be issued and contract to be performed, i.e. there is the option of processing without consent. Where data to be processed go above the threshold of processing essential for fulfilment of a contract (recording of information such as from

processing by doing so.

Correct determination of statuses of separate project participants is a starting point for complying with the other obligations provided by the Personal Data Protection Act. In most of the cases, personal data processing upon issuance of cards is subject to the notification obligation provided by Article 16 of the Personal Data Protection Act and the personal data controller must comply with it. The controller will not be required to comply with the notification obligation only in the instances when any of the exceptions provided by Article 18(1) of the Personal Data Protection Act may be applied to the processing performed by it (e.g. if an employer issues cards to its employees in order to monitor their work attendance. The employer is complying with a legal requirement by that, while the card is merely a vehicle chosen for legal processing).

It is obvious from the above that, in most cases, electronic cards are just a vehicle or tool serving to processing personal data in connection with provision of services. In the event any personal data is processed in connection with the service, persons (entities) offering such technical means to their clients (customers) shall bear in mind that this involves personal data processing which is wholly subjected to the Personal Data Protection Act regime. They must be further aware of the fact that duties arise for them from that. This may involve, in particular instances, obtaining of consent to personal data processing. It needs to be kept in mind that the information duty shall apply to such persons in any case and that all other statutory obligations of the controller, or, processors must be obviously respected, in particular obligations provided by Article 5(1) and (2) of the Personal Data Protection Act.

Note: The above document is available at the web pages of the Office for Personal Data Protection at http://www.uoou.cz/uoou.aspx?menu=22&lang=en

where an to which destination the data subject travels, at what times he or she goes to lunch etc.), the position of the Office for Personal data protection is that consent of data subject is essential. However, even where such consent has been obtained, the principle of privacy and personal life protection defining the threshold of the personal data processing scope must be respected.

Considering the fact that the offered product (service) can be used only in conjunction with the card, and, if the scope of the processed data is obviously inadequate to the defined purpose, freedom of such given consent may be contested. It is however exactly freedom, in terms of Article 4(n) of the Personal Data Protection Act, that constitutes an indispensable attribute of the described act. Consent must be informed, too, as required by Article 5(4) of the Personal Data Protection Act, according to which, when giving his consent the data subject must be provided with the information about what purpose of processing, what personal data, which controller and what period of time the consent is being given for.

Informing the data subject, however, is not tied solely to the act of consent. It may be necessary to provide data subject with information also in the cases where the Personal Data Protection Act allows processing without consent. This obligation is provided by Article 11 of the Personal Data Protection Act. Compliance with the information duty towards the data subjects (card users) gains particular importance in the cases where the actual environment in practice “gives no other choice” to the natural persons but to acquire a card and use it within the actual system or community they live in.

Relating to issuance and subsequent use of cards, an extensive database is created or may be created in an overwhelming number of cases. Such database may include, in addition to the identification data required for the card issuance, also information on use of separate services provided by the card, obtained through information systems involved in the respective project. The system is then able to store all information, as enabled by the relevant technology, on the card holder's activities, such as information when or how often the card holder (a pupil or student) attends the lessons and goes to lunch while at school, when or how often the card holder moves around a certain building (not just, say, a school building but also e.g. a student dormitory, library etc.) - the system therefore enables an option of keeping highly demonstrable records of the school attendance etc.

Collection of personal data that occurs in relation to issuance of cards, or, based on collection of additional information connected to use of the card and subsequent processing of such information is indisputably subject to application of the Personal Data Protection Act. In view of that, attention should be paid to the below groups of issues.

In the first place, basic relations in the processing of personal data should be made clear, i.e. who is the controller and who processor within the meaning of Article 4(j) and (k) of the Personal Data Protection Act. This step will be more complicated with "multifunctional" cards. A clear determination is required whether the card issuer coincides with the controller and whether owners of individual applications or functions of the card and of information technology systems involved in the project are processors, or, if all of the participants have the “controller to controller” relationship, i.e. if a single (multifunctional) card is going to have, in terms of the Personal Data Protection Act, several controllers of the personal data processed while the card is used by its holder.

A setup of mutual relationships between the card issuer and other participating parties is at their sole discretion, so it cannot be envisaged, recommended or even regulated who should hold the controller or processor status. It is true in most cases that the card issuer is the controller. Separate participants involved in the system may be in the processor position, or, all participants may have the controller to controller status, and, it is even possible for the card issuer to have the controller status and at the same time that of the processor towards the other entities - independent controllers.

If a processor appears in a relationship, a processor contract must be concluded between the controller and processor as provided by Article 6 of the Personal Data Protection Act. Such contract must be made in writing and shall in particular explicitly stipulate the scope, purpose and period of time for which it is concluded. The contract shall further contain guaranties by the processor related to the technical and organisational securing of the protection of personal data.

Furthermore, any personal data processed using the applications must be secured in the manner guaranteeing that information contained within separate applications may be accessed solely by its controllers, while each controller will be enabled access only to its own application. It is entirely inadmissible to make the data fully accessible to all of the controllers whose application is present in the card or to even grouping the data in any manner. The access setups must correspond to the mutual relationships setups at all times, guaranteeing compliance with all provisions of the Personal Data Protection Act, in this case particularly compliance with Article 13. The controller or, processor shall also make sure that the card manufacturer, upon completion of works, has liquidated all information provided to it and has terminated

POSITION No. 2/2001
October 2001

The Processing of Sensitive Personal Data - Trade Union Membership - in Connection with the Return of Membership Fees

The return of trade union membership fees is closely connected with the issues of personal data protection, because it concerns rights and responsibilities in the field of industrial relations. This field includes, in the wider sense, the relations between the employer and the respective trade union, the relations between the employer and the employee as a member of this union as well as the mutual relationship of the trade union and its individual members.

Under Article 4, Para.2 of the Act No. 1/1992 Coll. on Wages, Availability Payments[1] and Average Earnings, as amended (hereinafter referred to as "Wages Act"), the term "wage" applies to monetary payments or payments of monetary value (compensation in kind) received by the employee from the employer in return for work. Similar provision can be found in Article 3 of the Act No. 143/1992 Coll. on Salaries and Availability Payments in State-financed Organisations and Certain Other Organisations and Bodies (hereinafter referred to as "Salaries Act") under which law the employee is entitled to a salary for his or her work, the term "salary" referring to monetary payments received by the employee from the employer in return for work. A wage or a salary is therefore owned by the employee who has the right to dispose of it in the same way he or she disposes of other parts of his or her property.

Consequently, the basic pre-condition for wage or salary deductions made in accordance with the existing legislation is the consent of the employee which must be given in the form of a written agreement on payroll deductions.

A separate question is whether, in connection with the TU membership fees return, the employer would process sensitive personal data concerning trade union membership, and what rights and responsibilities the employer would have in such a position, particularly as regards the possible application of Article 9 of the Personal Data Protection Act.

Unless the authorisation to process sensitive personal data is granted by a special Act or unless at least one of the conditions stated in Article 9, letter b) and c) of the Personal Data Protection Act is fulfilled, the employer may process the sensitive personal data on trade union membership only in those cases where the subject of data has given the employer explicit written consent which conforms to all requirements of Article 9, letter a) of the Personal Data Protection Act. In relation to the personal data of the employees, the employer is always in the position of an administrator.

To implement the agreement on payroll deductions it is not necessary to process sensitive personal data, namely the data on trade union membership. The employer only has to process the information that a particular employee submitted to the respective department of the employer a duly concluded agreement on payroll deductions in which he or she gives consent to these deductions and states the amount to be deducted and the account to which the sum should be transferred. This consent must be expressed by the employee in a legally relevant form, in accordance with the provisions of Article 12, Para. 1 of the Wages Act, Article 18, Para.1 of the Salaries Act and Article 121 of the Labour Code. To bring into effect such duly concluded agreement on payroll deductions, the employer needs to process no further personal data about the employee except for the data already processed in connection with the keeping of employees' individual files, and, naturally, the information that the employee has concluded the agreement on payroll deductions, that he or she gives consent to the deductions, the amount deducted and the account to which the deducted amount should be transferred. If from this individual agreement the employer gains knowledge of sensitive personal data on employee's membership in trade unions, this knowledge is usually not processed further and it is not used in any systematic operations. The processing of "regular" personal data - including also payroll deductions - does not require a special consent of the subjects of data under the Personal Data Protection Act, because it is the processing referred to in Article 5, Para.2, letter a) or b) of the Personal Data Protection Act - the employer performs the duties imposed by special Acts or the duties ensuing from the contractual relationship between the employer and the employee. The consent of the employee would be evident from the submitted agreement on payroll deductions. As regards notification duty under Article

16 of the Personal Data Protection Act, the implementation of an agreement on payroll deductions does not oblige the employer to fulfil this duty with regard to the Office for Personal Data Protection for the purpose of registration of authorised cases of personal data processing. In accordance with the amended provision of Article 18, letter b) of the Personal Data Protection Act, in implementing the agreement on payroll deductions the employer processes the necessary personal data on the employee in connection with the fulfilment of duties stipulated by law or the relevant data are necessary for the exercise of rights stipulated by special Acts.

Conclusion:

In implementing the agreement on payroll deductions, the employer does not need to process the sensitive personal data on trade union membership. Unless the implementation of the payroll deductions agreement will result in (systematic) processing of the sensitive personal data on trade union membership, it is not even necessary to fulfil the notification duty under Article 16 of the Personal Data Protection Act.

The Office for Personal Data Protection assumes this position particularly with regard to the duty of the administrator, stipulated in Article 5, Para.1, letter d) of the Personal Data Protection Act, to gather only such personal data as correspond to the stated purpose and only to such extent as is necessary for the fulfilment of this purpose. Moreover, the aforementioned procedure is suitable, because the account number and the amount to be deducted do not necessarily identify membership in a trade union or in another social organisation. The conclusion of a payroll deductions agreement may be motivated also by the need to pay for legal or educational services or by a mere inclination to and support of the trade union on part of the employee.

---

[1] Payments for the employee's willingness to be available for work if needed.

The following material has been prepared in co-operation with the Czech-Moravian Chamber of Trade Unions.

POSITION No. 5/2004
May 2004

The amount of paid union dues as an income tax deductible

Act No. 586/1992 Coll., on Income Taxes, was amended by Act No. 438/2003 Coll. and a majority of the new provisions took effect on 1 January 2004. This is also the case of Article 15(14) and Article 38 l (1) (j) of the aforementioned Act. Under Article 15(14), the taxpayer who is a member of a trade-union organisation will at the end of 2004 for the first time have the opportunity to deduct from his or her tax base the amount of paid trade-union dues up to the maximum yearly limit stipulated by law. The first limit is set at 1,5 % of taxable income, the second is the maximum amount of CZK 3000 per tax year. Under Article 38 l (1) (j) the employee must claim the deduction within the statutory time limit with his employer by submitting to him a certificate issued by the trade-union organisation and certifying the amount of paid union dues.

The amendment is in line with the aims of the Czech-Moravian Chamber of Trade Unions, since it provides trade union members with an opportunity for tax reduction. However, the trade-union organisation must issue to its members on request a certificate stating the amount of paid union dues, as required by law. This procedure should pose no problem to those organisations that themselves regularly collect union dues from their members.

There is, however, a significant number of trade-union organisations for which the membership dues are collected by the employer who deducts the appropriate amount from the employees' wages and transfers the sum thus collected to the account of the trade-union organisation. If trade-union dues are paid in this way, it is necessary to consider the possibility of conflict with Act No. 101/2000 Coll., on the Protection of Personal Data. The problem of fee deduction in itself was addressed by the employers and trade unions in co-operation with the Office for Personal Data Protection (hereinafter referred to as "Office"). This led to the issuing of Position No. 2/2001 "Processing of the sensitive personal data -trade union membership - in connection with the return of membership fees". The aforementioned position was published in the Journal of the Office for Personal Data Protection, part 12 of 23 October 2001. However, in connection with the income tax law amendment the problem of potential collision arises again, in a different aspect.

Employer deducts trade-union dues on the basis of an agreement on wage deductions between the employee and the trade-union organisation, which has been submitted to him, and transfers the appropriate amounts to the account of the trade-union organisation. At this stage, the employer can opt between the following procedures:

1. Each month the employer provides the trade-union organisation with information on paid dues by submitting to it a written list with the names of the employees and the respective amounts of fee deductions;

2. The employer transfers to the account of the trade-union organisation only the total sum of deducted trade-union dues, without any concrete information on the members.

Case 1

In this case the trade-union organisation has no major problem with establishing on the basis of the submitted lists the total yearly amount of deducted trade-union dues and issuing the required certificates to its members.

Case 2

In this case the trade-union organisation must first find out how much each of its members has paid to the account. It may do so in one of the following ways:

Option A - If the amount of the membership fee is fixed and does not depend on wage (salary) level, the employer should without hesitation comply with the request of the trade-union organisation as a creditor and provide it with the required information on the respective amounts paid by individual "debtors" to meet the obligation in question (the "obligation" being the claim of the trade-union organisation to the corresponding sum of union dues). The same principle should also apply in those cases where the membership fee is defined as a percentage from the member's wages; however, here one may encounter the objection that the employer would thus provide another subject, though only indirectly, with personal data of the employee, i.e. the amount of his or her wage (salary). The consent of the employee with the processing of

the said data may be deduced from the agreement on wage deductions, which the employee concluded knowing that the trade-union organisation would learn the amount of his or her net income if the membership fee is defined as a percentage from this amount.

Option B - This option is in our opinion more "elegant" and in principle it also meets the requirements of Act No. 101/2000 Coll. Under Article 5(2) (a) of the said Act, the data controller may process the data even without the consent of the data subject, if the processing is expressly required by *lex specialis* (special law) or if it is necessary for the fulfilment of duties ensuing from a special law. In doing so he is only obliged under Para. 3 of the same provision to respect the right of the data subject to the protection of his or her private life. The special law in question here is the already mentioned Income Tax Act, which stipulates the right to deduct trade-union dues from the income tax base and in connection with this right imposes a corresponding obligation to submit a certificate stating the amount of union dues paid. If the deductions of trade-union dues are made by the employer and for the purpose of establishing their amount the trade union is obliged to issue the taxpayer a certificate, it is not a violation of the Act on Personal Data Protection if the employer provides the trade-union organisation with an annual report on union dues paid by individual taxpayers.

Under Article 18(b), the Income Tax Act also justifies the fact that the employer submitting such report need not notify the Office for Personal Data Protection about his intention to process sensitive personal data.

Option C - The employee = trade union member = taxpayer asks the employer to issue him a certificate stating the amounts that have been deducted from his wages and transferred to a specific account. It is not necessary to specify the purpose of the deductions; the number of the account provides all information needed by the trade-union organisation. The employee submits the certificate to the trade-union organisation and the organisation, after having checked its bank account, issues him an identical certificate in accordance with Article 38 l (1)(j) of the Income Tax Act. This procedure also meets the requirements of Act No. 101/2000 Coll., as well as the criteria laid down in the aforementioned position of the Office for Personal Data Protection. Since it may be expected that employees will be interested in ways to reduce their tax burden, it should not be a problem to persuade them to use this procedure.

Any of the three procedures described above provides the employee with a certificate of the trade-union organisation stating the amount of trade-union dues paid during the relevant tax year. The next step involves two possibilities:

1. the employee files his or her own tax return, or
2. the employee does not have this obligation and the calculation of the final tax amount is carried out by the employer.

Case 1

The employee deducts from his or her income tax base the sum stated in the certificate issued by the trade-union organisation; if the sum exceeds the limits stipulated by the Income Tax Act (i.e. it amounts to more than 1,5 % of the tax base or to more than CZK 3000), he or she deducts only the sums eligible for deduction. The certificate issued by the trade-union organisation forms an annex to the tax return form.

Case 2

At the end of the tax year, the employee asks the employer to take the sum of deducted trade-union dues into account when calculating the final amount of his or her income tax for the relevant year in the same way as it is done with money paid into supplementary pension schemes or life insurance.

Certificate issued by the trade-union organisation for the purpose of claiming a tax deduction on the basis of paid trade-union dues

Grassroots (local) trade-union organisation .....
.....
Office .....

certifies in accordance with Article 15(14) of the Act No. 586/1992, on Income Taxes, as amended, that its member

.....
(name and surname, personal identification number)
paid in the year ..... the amount of .....,

in writing .....,
in trade-union dues to the aforementioned organisation.

The present certificate is issued under Article 38 l (1) (j) of the same Act.
Date, signature and stamp of the trade-union organisation

Transfers of personal data of employees abroad

In practice, the Office for Personal Data Protection (hereinafter the "Office") often comes across cases of data controllers with contractual relations established with international entrepreneurs who require transmission of employees´ personal data to the management or other specialised departments of those international companies.

The Office shall review such cases of personal data transfer not only in the sense of the application of Article 27 of Act No. 101/2000 Coll., on the protection of personal data and on amendment to some acts, as amended (hereinafter the "Act"), but also in view of other legislation governing the processing of employees´ personal data, also including their potential transmission abroad. Therefore, it is necessary to take into account particularly the provisions of labour law and to assess whether such transfer of personal data complies with the purposes stipulated therein.

In some cases of personal data transfer, in particular, if it is subjected to international treaties the ratification of which has been approved by the Parliament of the Czech Republic (e.g., Convention No.108 for the protection of individuals with regard to automatic processing of personal data published in the Collection of International Treaties No. 115/2001), or if they are covered by decisions of an institution of the European Union, it is not necessary to seek a permit of the Office for such transfer of personal data.

If an application for a permit to transfer personal data to other countries is filed, it is obligatory to launch an administrative proceeding pursuant to Article 27 of the Act in order to examine the application for the transfer of personal data. In assessing the statutory conditions applicable to such transfer of personal data, therefore, it is essential to review both legality and efficiency of such transferred personal data, their extent, and/or format, because it involves transfer of personal data to other parties, which usually have no relationship (including no employment relationship) with the employees (data subjects) of a certain employer established in the Czech Republic.

International business entities, which are interested in economic results achieved by some local companies, may receive economic summaries containing anonymous data relating to certain employees, and they may also receive – as part of contractually guaranteed cooperation (i.e., in particular make random collections of) individual data about specific employees in relation to their performances. Any potential economic interest of such international entities, however, is not relevant in respect of the legal position of employees employed in the Czech Republic because, in keeping with the Labour Code, the employer is always authorised to assess employees' conduct and evaluate their performances (both of those activities undoubtedly also involve processing of personal data). Therefore, controllers intending to transfer personal data of employees abroad should be recommended to take into consideration also the following criteria:

1. The issue of transfer of employees´ data abroad is limited not only by the conditions stipulated in the terms and conditions as per Article 27 of the Act but also by the fact that the said processing of the employees´ data must be in keeping with certain additional provisions of the Act because they often are activities, which have been governed by special legislation. It must also be in keeping with the rules stipulated in that legislation, and those additional rules must be viewed as specifications of the principles of personal data protection as stipulated in the Act. Therefore, it should not happen that any allegedly "legal" transfer of personal data for such processing abroad takes place, which, however, runs counter to the conditions of such processing as stipulated in the laws of the Czech Republic (legal provisions and decisions of authorities of the European Union).

2. As long as labour law is considered to be part of private law, it should be stated that, in the given case, the purpose and any potential restrictions applicable to handling employees´ data have been stipulated in legislation. They are both cases explicitly stipulated in the Labour Code, e.g., the provision of Article 60, as well as some general cases allowing for processing certain paperwork in relation to special legislation, e.g., personnel matters and wages (namely for the purposes as characterised by the very name of such case). Also, it is possible to mention in this connection applications of certain special legislation, which may not explicitly stipulate handling of personal data but which have such handling of personal data is necessarily inherent in them; here, too, we talk about activities whose nature specifies the purpose of processing of personal

data as required by the Act.

3. Employees' personal data do not serve exclusively certain matters related to employment relations between employees and their employers but they also may represent background materials for other activities, e.g., assessment of works rationalisation efforts, labour efficiency and future trends within the employer's business. In such cases, though, it is necessary to make such employees´ personal data anonymous because such processing of personal data serves the purposes of achieving economic goals of the employers. Processing non-anonymous data, although they may be in direct relation to employees but serve in the first place to immediate economic purposes of the employers, obviously is over and above the framework (purpose) of the handling of employees' personal data as stipulated in the legislation.

4. Undoubtedly, some cases of the handling of employees´ personal data, particularly in areas which have not been governed or directly restricted by the legislation, may only be performed with the employees' consent. In any such cases, however, also other provisions of the Act must be complied with, including the requirement that any such specific case of personal data handling must have a clear purpose. It is obvious that such a consent by the employee cannot heal any potential conflict between the employer's requirements and the rules and purposes stipulated in the legislation. Last but not least, such consent can be considered as being outside acts in keeping with labour law since it needs not be conditioned thereby. At the same time, it is necessary that employers keep their employees informed about any such processing of their personal data abroad, namely in such manner so that it is obvious that their consent with such personal data processing for the purposes of such transfer has been voluntary, and that they are free to refuse to give it.

5. In many cases, such transfers of personal data to other countries are required because such processing is performed by certain specialised or professional offices situated with so-called "parent" companies located abroad, which are regarded as processors by the Act. Then, it is essential to comply in particular also with the provision of Article 6 of the Act, that is, to enter into an agreement between the controller and the processor. The said processor, however, is not authorised to process the relevant personal data for any other purposes and for any other controller (however, it is allowed to make the data anonymous for such other purposes).

6. Often, transfers of personal data abroad are performed for the purposes of increasing qualifications of certain selected groups of employees, and if they are dispatched for abroad business trips. In such cases, one of the conditions pursuant to Article 27 of the Act has usually been complied with. However, if such employer should also process personal data of an employee's family members in connection with such international secondment, usually if the employee and his/her family should re-settle there, it also is essential to seek those family members' consent.

In conclusion, it should be pointed out that the identified areas of issues also apply to cases of processing of personal data which do not fall under the category covered by personal data transfer permits issued by the Office because those cases are subject to the Office's supervision (including sanction). Therefore, the above-described criteria should also be considered in case of any transfers of employees´ personal data abroad.

Act on the use of health data etc. on the labour market

Act No. 286 of 24 April 1996

Ministry of Labour
Denmark

Act on the use of health data etc. on the labour market

Act No. 286 of 24 April 1996

Ministry of Labour
Denmark

Act on the use of health data, etc. on the labour market

Part I

Purpose and scope of the Act

1. - (1) The purpose of the Act is to ensure that health data are not used wrongfully to limit the possibilities of employees for obtaining or maintaining employment. This shall apply irrespective of whether the data relate to genetic tests, ordinary examinations or come from any other sources.

(2) The Act shall apply to the use of health data on the labour market. However, the Act shall not apply to the extent that rules on the use of health data have been laid down by special legislation or by provisions issued on the basis of such legislation.

(3) In this Act requests for and collection of health data shall also be taken to mean the carrying out of examinations to the extent that these are required in order to obtain the health data concerned.

Part II.

Collection of data

2. - (1) In connection with recruitment or during the duration of an employment relationship an employer shall only be entitled to request health data to be provided for the purpose of ascertaining whether the employee in suffering from or has suffered from a disease or has or has had symptoms of a disease if the disease will be of significant importance for the employee's capacity for work in the job function concerned, cf., however, sections 3 to 6.

(2) However, the employer may only request information, cf. subsection (1), of which the employee is not himself informed, if the conditions in connection with the work concerned specifically justify that such data should be provided.

(3) When requesting data under subsections (1) and (2) the employer shall inform the employee of the diseases or symptoms of diseases on which he seeks information.

(4) An employer shall not - in connection with recruitment or during the duration of an employment relationship - request, collect, receive or make use of health data for the purpose of ascertaining the employee's risk of developing or contracting diseases, cf., however, section 3.

(5) The provisions laid down in subsections (1) to (4) shall also apply to consultants and other persons acting on behalf of the employer.

3. - (1) An employer may offer that health data are collected for the purposes mentioned in section 2 (1) and (4) if working environment conditions make it reasonable and appropriate to do so for considerations of the employee himself or other employees.

(2) Collection of data under subsection (1) shall be instrumental in the prevention of work-conditioned diseases or improvements in the working environment conditions. The rules and guidelines laid down in the working environment legislation on examination methods and use of experts shall be correspondingly applicable.

(3) The employer shall notify the local working environment service before such examinations are carried out. The notification shall include detailed information on the examination, including its extent, method, etc. and on the persons assisting in and in charge of the examination. The examination may not take place until 4 weeks after the working environment service has received the notification.

(4) When a health examination takes place the employer shall -

(1) give the person who carries out the examination any necessary information to be used in this connection,

(2) pay the costs in connection with the examination, and

(3) ensure that the examination can take place without any loss of income for the employee and, if possible, during normal working hours.

(5) The Director of the National Working Environment Service may decide that an examination should not be carried out or should be suspended if it does not satisfy the requirements laid down in subsection (2).

(6) An appeal may be brought against the decisions of the Director in accordance with the same rules as those applying to decisions under the Working Environment Act. However, an appeal shall not have suspensive effect in relation to the decision.

4. - (1) The Minister of Labour may - after having obtained the opinion of the Council mentioned in section 8 - permit that an employer arranges for data to be provided on whether the employee is suffering from a disease, has symptoms of a disease or may be infectious, to the extent that this is necessary in the interest of

(1) the safety and health of consumers or other persons,
(2) the external environment, or
(3) other community interests.

(2) It is a condition for requesting health data that the interests concerned outweigh the interests of the employee and that it is not possible for the enterprise to take these interests into consideration in any other way.

(3) Health examinations shall be carried out by using the least radical method which will serve the purpose.

(4) Section 3 (4) shall be correspondingly applicable.

5. - (1) An employer may arrange for provision of data on whether the employee is suffering from a disease, has symptoms of a disease or may be infectious when this is considered necessary for considerations of the operation of the enterprise, cf., however, subsection (2).

(2) It is a condition that the employer or the organisation of the employer concludes an agreement about this with the opposite employee organisation(s), cf., however, subsection (3). The agreement shall be sent to the Minister of Labour for the purpose of information.

(3) In those cases where no agreement can be concluded according to subsection (2), the Minister of Labour may - after having obtained the opinion of the Council mentioned in section 8 - give permission to a request for provision of health data.

(4) Section 3 (4) and section 4(2) and (3) shall be correspondingly applicable.

Part III.

The employer's duty of disclosure

6. Before the recruitment the employee shall of his own will or if questioned by the employer inform the employer whether he is cognizant of suffering from a disease or has

symptoms of a disease which would be of significant importance for the employee's capacity for work in the job function concerned.

7. If the employer should - on the basis of the data obtained by virtue of section 4 and section 5 - take special measures in connection with the work or make other dispositions, the employee shall ensure that the employer is informed hereof.

Part IV.

The Council of Experts

8. - (1) The Minister of Labour shall set up a Council which shall submit opinions at the request of the Minister of Labour or on its own initiative in cases which are sent to the Minister in accordance with section 4 (1) and section 5 (2) and (3).

(2) The Minister of Labour shall appoint the chairperson of the Council. In addition to the chairperson, the Council shall be composed of 16 members to be appointed by the Minister of Labour at the recommendation of the following authorities and organisations:

1 representative of the Ministry of Labour,
1 representative of the Working Environment Institute,
1 representative of the Ethical Council,
1 representative of the Directorate of the Working Environment Service,
1 representative of the Ministry of Business and Industry,
1 representative of the Association of General Practitioners,
1 representative of the Ministry of Justice,
1 representative of the National Board of Health,
1 representative of the Central Organisation of Professional Associations,
1 representative of the Federation of Salaried Employees' and Public Servants' Organisations,
1 representative of the Main Organisation of Managers,
1 representative of Federation of Danish Trade Unions,
1 representative of the Danish Employers' Confederation,
1 representative of the Ministry of Finance, the National Organisations of Municipal Authorities and the National Organisation of County Authorities, jointly,.
1 representative of the Association of Employers in the Finance Sector,
1 representative of the Association of Employers in Agriculture.

(2) The members shall be appointed for a term of 3 years at a time. They may be re-appointed.

(4) The Council shall lay down its own rules of procedure.

Part V.

Informed consent

9. - (1) Before an examination is carried out for the purposes mentioned in section 2 (1) and (4), cf. section 3, the person who carries out the examination shall ensure that the employee has been informed in writing and orally about:

(1) the purpose and nature of the examination,
(2) the examination method,
(3) any risks in connection with the examination,
(4) any consequences which the results of examination may have for the employee,
(5) the nature of the information which may result from the examination, including the degree of the risk of future disease, etc.,
(6) the conditions for passing on data, cf. sections 7 and 11,
(7) follow-up to the examination, including notification of the employer,
(8) how the results of the examination will be stored,
(9) where warranted by the nature of the examination, also the possibility that the result of the examination may have an impact upon the expectations to life and self-opinion of the person examined.

(2) Before the examination is carried out, the employer shall ensure that the employee is informed about any possible consequences which a refusal to undergo the examination may have for the employee.

(3) The examination may only be carried out, if the employee has given his consent in writing. The employee shall be given a time limit of at least 2 working days for giving his consent after having been informed as mentioned in subsection (1).

(4) If an employee expresses a wish for restrictions in the data concerning the evaluation of the consequences which the results of the examination may have for the employee or if the examination will have an impact on the expectations of life and the self-opinion of the person examined, the person who informs the employee about the results and interpretation of the examination under section 10 (4) shall respect such a wish.

Part VI.

Experts

10. - (1) A request for the carrying out of an examination under sections 2, 4 and 5 shall be made by the employee and at the employees own choice either to the general practitioner normally used by the employee concerned or to a similar expert in the occupational health service to which the enterprise may be attached.

(2) The person who receives the request shall involve the necessary and sufficiently qualified medical or other expertise, including occupational hygiene, clinical-chemical, genetic or biochemical expertise, both in connection with the actual examination as well as the interpretation of the clinical consequences of the examination.

(3) Any person who - on the basis of an examination -issues a certificate concerning an employee's state of health and risk of developing or contracting diseases shall at the same time give an evaluation which illustrates the degree of uncertainty in connection with the interpretation of such examinations.

(4) Certificates concerning the results of an examination shall be passed on to the employee of the person who received the request under subsection (1), cf., however, section 9 (4).

Part VII.

Professional secrecy, etc.

11. - (1) Physicians, clinics, laboratories, public authorities, etc. are not allowed to pass on health data covered by this Act to other persons that the person to whom the data relate, cf., however, section 2.

(2) However, passing on of the data mentioned in subsection (1) may take place to the extent that this is necessary in order to serve the purpose. It is further a condition that the passing on of data -

(1) follows from another Act or provisions issued on the basis of such acts,
(2) takes place for the research purposes with the consent of the person concerned, or
(3) is necessary to avoid risks of the type mentioned in section 4 (1).

(3) The employer may not request or receive and use a power of authority to obtain health data.

Part VIII.

Sanctions

12. Persons whose rights have been violated by infringements of the provisions laid down in sections 2 and 9 may be awarded compensation.

13. Any person who acts in violation of section 2, section 3 (3) or sections 9 to 11 will be liable to a fine, unless a more severe sanction applies under other legislation.

14. If the violation has been committed by a company, an association, an independent institution, a fund or a similar body the fine may be imposed upon the legal person as such. If the violation has been committed by the state, a municipal authority or a municipal association, the fine may be imposed upon the state, the municipal authority or the municipal association as such.

Part IX.

Commencement

15. The Act shall not extent to the Faroe Island and Greenland.

16. The Act shall come into operation on 1 July 1996.

Given at Christiansborg Castle, 24 April 1996

Under our royal hand and seal

MARGRETHE R.

/Jytte Andersen

A new act on the protection of personal privacy in working life

There is a prevailing consensus, both at national and international level, that the right to respect for private life and personal privacy is a human right, and that the state has a responsibility to maintain effective protection against violations of that right.

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 and the meaning of certain statutory provisions must be regarded as unclear. Moreover, protection for employees in the private sector differs to some extent from that afforded to public sector employees. In addition, job applicants have no means of taking effective action against privacy invading background checks conducted by an employer for whom they wish to work.

Given the deficiencies in the existing regulatory framework, protection of personal privacy in working life needs to be clarified and strengthened through appropriate legislation. In our view, this should be done through the introduction of a single, self-contained act. To ensure that the act is as clear as possible to those responsible for its application, it should be patterned on known labour law models. The regulations we propose should also be generally applicable to all areas of working life.

The legislation we propose mainly entails the following provisions:

As regards surveillance and background checks involving the processing of personal data, the provisions in the Personal Data Act should continue to apply in all but three areas, where we propose changes which in our view will serve to strengthen employee protection. We propose the introduction of special provisions governing some of the surveillance and background checks specified in our terms of reference, namely concerning certain records checks and medical tests. In addition, we propose a blanket provision – to be applicable under certain conditions – prohibiting surveillance and background checks in general where these are deemed to have a palpable effect on personal privacy. The provisions we purpose regulating medical tests and the proposed general provision are constructed as discretionary norms. As such they restrict the adoption of surveillance and background checks to

purposes which are authorised and which, on the basis of a proportionality assessment, are seen to constitute an admissible intrusion. A party guilty of breaching the provisions in the proposed act will be liable for damages.

Purpose and scope of the proposed act

The proposed act is prefaced by a declaratory paragraph stating its purpose – to protect the personal privacy of employees in working life.

The act only concerns measures implemented by employers and directed at employees.

Under the proposal, the term employee also embraces in principle certain other categories, namely job applicants, people seeking or undertaking work experience placements and those who perform work as hired or borrowed labour. Where reference is made to employees in the present summary or in the report as a whole, the term is to be understood to apply equally to job applicants and the other categories of persons protected under the act, unless otherwise indicated.

Processing of personal data

The Personal Data Act (1998:204) contains provisions intended to protect against invasion of personal privacy through the processing of personal data. We hope that the relatively extensive account of the content of the act included in our report will afford a better understanding of its application in working life. Our review of the provisions has led us to the conclusion that the act provides relatively good protection of personal privacy in working life. We have accordingly proposed that the Personal Data Act should, unless otherwise stated, apply to the processing by employers of personal data. We do not therefore propose the adoption of separate regulations governing employer surveillance involving, for example, logs or digital camera surveillance, as these come under personal data processing as defined by the act. However, the protection in working life afforded by the act should be more clearly defined and, to some extent, strengthened. We therefore propose the inclusion in our act of a provision modifying the

Personal Data Act as follows in cases where an employer's purpose in processing an employee's personal data is to check up on or monitor the employee.

In the first place, the misuse rule in Section 5 a of the Personal Data Act would not be applicable; instead all the provisions of the act are to be applied.

In the second place, an employer would not be permitted to process an employee's personal data solely on the basis of consent; under the act, some other ground for action would need to exist for processing to be admissible.

Finally, processing by an employer of an employee's personal data should only be admissible under the act if it is stated, when the data has been collected, that the purpose of the processing was to check up on or monitor employees in some specific respect. Thus the act explicitly guards against purpose drift. However, under the proposed act, exceptions may be made where exceptional grounds exist and provided the employer promptly informs employees affected by the processing about its new purpose.

Regulation in collective agreements of issues relating to the processing of personal data in working life could in our view serve to clarify the provisions of the act and facilitate their application. However, although the provisions of the act cannot be departed from by collective agreement, the limits of the area which may be covered by such an agreement can be difficult to define. We therefore propose that a provision also be introduced into the Personal Data Ordinance (1998:1191) as a means of promoting the establishment of collective agreements. Under the proposed provision, the Data Inspection Board would be required, at the joint instance of the parties to the agreement, to deliver an opinion on a draft collective agreement with respect to its compatibility with the Personal Data Act and other statutes governing the type of personal data processing in question.

Prohibition against obtaining certain data extracts

Criminal records include information on people who have had sanctions brought against them for crimes committed. The overriding purpose of these records is to provide authorities, primarily law-enforcement agencies, with speedy, relatively trouble-free access to the information they need to carry out their work. Data

of this kind compiled and stored in a register is extremely sensitive and is therefore subject to the strictest secrecy. However, individuals are entitled to full access to the records with regard to data about themselves.

It is in the public interest that a person who has served his/her sentence be able to play an active part in the community on the same premises as everyone else. With certain types of jobs, however, the need to protect others from the risks that may be associated with previous crimes committed by an employee is deemed to constitute grounds for accessing data from the records. Careful consideration has therefore been given to the incorporation in statutes governing access to criminal records or register checks of provisions specifying which employers are permitted and/or required to conduct register checks. Also specified is the extent of the information that may be obtained in such checks.

According to reports by *inter alia* the National Police Board, employers are increasingly making use of the individual's right to access data about him/herself to request that job applicants themselves produce extracts from the records. Such extracts contain all the information about the individual stored in the register. To prevent employers from exploiting the individual citizen's right to access data about him/herself in a way which is neither intended or desirable, we propose that employers be prohibited from requiring job applicants to produce criminal record extracts about themselves unless there is legal sanction for doing so. It is proposed that the prohibition also cover requests without legal sanction for extracts from the register of suspected offenders.

It has also come to our attention that employers have been known to require job applicants to produce extracts from the Swedish Social Insurance Agency showing previous periods of absence from work due to illness or to care for a sick child. The agency does not normally release this kind of information to prospective employers in accordance with the secrecy rules governing social insurance set out in the Secrecy Act. In order to prevent circumvention of the rules in the Secrecy Act designed to protect personal privacy, it is proposed that employers may not without legal sanction require job applicants to produce extracts from data registers kept by the Social Insurance Agency if the extract contains information to which the employer has no right of access under the Secrecy Act.

However, the proposed new act does not contain specific provisions prohibiting employers from obtaining a prospective employee's credit rating from a credit rating agency or from requiring a job applicant to produce an extract from the Swedish Enforcement Authority's data register. This information is normally in the public domain. Moreover, credit rating agencies and their operations are governed by the Credit Information Act (1973:1173), a special statute intended to protect people against improper invasion of personal privacy. What is more, there is no indication that employers are acting in such a way as to justify special regulation in this regard. As regards obtaining data of the kind referred to above in ways that would constitute an unwarrantable invasion of privacy – such as a request for or access to any data subject to secrecy under the Secrecy Act – our proposal provides for action to be taken under the proposed general provision in our new act otherwise prohibiting encroachments on personal privacy.

Medical tests

Employer background checks in the form of medical tests are particularly sensitive from a privacy standpoint and should therefore be conducted very restrictively.

There is an observable tendency today towards the use of background medical checks in working life, particularly with regard to drug tests. A review of existing law in this area shows that there is no comprehensive regulation regarding an employee's obligation to undergo a medical test, and the legal situation is unclear in a number of respects. Employee protection in this respect varies between private and public sectors and protective regulations for job applicants are largely absent.

We accordingly propose special legislation regulating background medical checks. This would replace the provision on regular medical check-ups currently applying to employees in the public sector under Section 30 of the Public Employment Act.

The proposed act would regulate the right of an employer to request medical tests. By this is meant a request to undergo such a check or to inform an employer of its results. Medical tests are defined under our proposal as a medical examination or any form of alcohol, or narcotic or other drug test. However, this provision

would not apply to alcohol tests administered in connection with alcolocks in vehicles.

The proposed act would permit an employer to request a medical test only if the test was for an authorised purpose within the meaning of the law, and if the test could be said to be an admissible invasion of an employee's personal privacy having regard to the said purpose.

Purposes for which a medical test would be deemed appropriate are specified in the proposed act. These include in the first instance cases where tests are conducted for security reasons. An authorised purpose in such a case would, under our proposal, be the need to assess the medical condition of an employee who has duties where health problems or the influence of alcohol, drugs or medical preparations could entail a risk to human lives, personal security or health, or significantly damage the environment or property.

A request for a medical test would also be for an authorised purpose under our proposal if the test formed part of a rehabilitation plan for the employee.

Finally, the purpose of a medical test would be authorised if it was conducted to assess the state of health of an employee and if said test was of critical importance to the operation of the entity concerned owing to its special character. Checks of this kind are needed primarily in order to conduct drug tests. The basic principle here should be that checks of this type should be essential to or form a vital part of the operation of the entity concerned.

It is proposed that the provision specifying the purposes for which a medical test may be requested by an employer be semi-discretionary, thereby allowing for a decision to establish another authorised purpose than that specified in the act through a collective agreement at national level.

A further condition under which an employer may request a medical test is, as previously mentioned, that the test must be seen to be an admissible intrusion in relation to its purpose. Here the circumstances of each case must be taken into account. However, our proposal also specifies as a basic requirement that medical tests are only admissible if performed by health and medical care personnel, and provided samples taken for alcohol and narcotic and other drug tests are analysed by a laboratory accredited for the purpose under the Technical Conformity Assessment Act (1992:1119), or by an equivalent laboratory in another EEC country. However, the requirement concerning health and medical

care personnel and accredited laboratories does not apply to tests involving breath samples.

Prohibiting privacy invading measures in general

To ensure comprehensive protection against unauthorised invasions of privacy, we also propose, in addition to the special provisions outlined above, a provision prohibiting privacy invading measures in general. Under the proposed provision, an employer would be prohibited from conducting surveillance or background checks that constitute a manifest infringement on an employee's personal privacy unless the measure was taken for an authorised purpose and was seen to be an admissible intrusion into an employee's personal privacy having regard to the purpose justifying the measure. The proposed provision is designed to target qualified cases of surveillance or background checks from a privacy perspective. Examples of measures which would constitute a clear case of privacy invasion – and which in effect are prohibited unless properly justified and proportional – include wiretapping employees' telephone calls, subjecting employees to bag and other searches when leaving work premises, going through lockers, drawers or other spaces an employee normally has sole use of, and analogue camera surveillance in toilet areas.

Ordinary work supervision measures are not covered by the proposed provision. Nor do they concern such measures as obtaining employee references in the normal way or oral questioning of an employee or job applicant.

One measure which however must normally be deemed to fall under the scope of the proposed provision is the use by employers of personality tests or similar evaluations. Implementation of such tests as well as their results must be regarded as sensitive from a privacy standpoint. For the reasons set out in our report, we have not proposed a special, separate provision governing such cases. In our view these would be regulated most appropriately by the proposed general provision prohibiting privacy invading measures.

In accordance with our terms of reference, we also considered regulating the right of employers to question employees about their political convictions and trade union membership. However, we found no compelling justification for such a proposal. If, however, an employer's questioning were to constitute the kind of

improper infringement of personal privacy targeted by the general provision prohibiting privacy invading measures, action could be taken against such a measure under that provision.

Obligation to negotiate

An important element in a regulatory framework intended to protect personal privacy in connection with surveillance and checks in working life is that it be able to guarantee that any measures adopted are thoroughly discussed and transparent. The obligation to negotiate under the Co-Determination at Work Act (1976:580) is already applicable in many cases where an employer is considering the introduction of surveillance and background checks that will involve significant changes in the entity's operations, or will have a specific bearing on working conditions or terms of employment. In order to make it clear that the primary obligation to enter into negotiations applies whenever an employer intends to decide on the introduction of a surveillance and background checks liable to constitute a manifest infringement of the personal privacy of one or more employees, we propose the introduction of an explicit provision enjoining the employer to negotiate beforehand with the relevant employees' organisation in the manner prescribed in Sections 11–14 of the Co-Determination at Work Act. In addition, we propose that it should be permitted to depart from this provision if such a departure is negotiated through a collective agreement.

Other provisions

It is proposed that the penalty for breaches of the terms of the act be payment for damages.

Under the proposed act, cases would be handled in accordance with the Labour Disputes (Judicial Procedure) Act, except where these involve personal data processing, and concern categories of persons, other than employees, who are protected by law.

Except as regards the proposed provision governing personal data processing, prosecution under the Labour Disputes (Judicial Procedure) Act would be subject to the provisions on statutory

limitations set out in Sections 64–66 and 68 of the Co-Determination at Work Act.

We propose that the provisions of the act be mandatory. Thus that part of an agreement which acts to restricts the protection afforded to an employee under the proposed act would have no legal force. As mentioned previously, however, it is proposed that two of the provisions in the act be semi-discretionary, namely the provision establishing the purposes for which a medical test may be requested, and the provision on the obligation to negotiate.

Act on the use of health data etc. on the labour market

Act No. 286 of 24 April 1996

Ministry of Labour
Denmark

Act on the use of health data, etc. on the labour market

Part I

Purpose and scope of the Act

1. - (1) The purpose of the Act is to ensure that health data are not used wrongfully to limit the possibilities of employees for obtaining or maintaining employment. This shall apply irrespective of whether the data relate to genetic tests, ordinary examinations or come from any other sources.

(2) The Act shall apply to the use of health data on the labour market. However, the Act shall not apply to the extent that rules on the use of health data have been laid down by special legislation or by provisions issued on the basis of such legislation.

(3) In this Act requests for and collection of health data shall also be taken to mean the carrying out of examinations to the extent that these are required in order to obtain the health data concerned.

Part II.

Collection of data

2. - (1) In connection with recruitment or during the duration of an employment relationship an employer shall only be entitled to request health data to be provided for the purpose of ascertaining whether the employee in suffering from or has suffered from a disease or has or has had symptoms of a disease if the disease will be of significant importance for the employee's capacity for work in the job function concerned, cf., however, sections 3 to 6.

(2) However, the employer may only request information, cf. subsection (1), of which the employee is not himself informed, if the conditions in connection with the work concerned specifically justify that such data should be provided.

(3) When requesting data under subsections (1) and (2) the employer shall inform the employee of the diseases or symptoms of diseases on which he seeks information.

(4) An employer shall not - in connection with recruitment or during the duration of an employment relationship - request, collect, receive or make use of health data for the purpose of ascertaining the employee's risk of developing or contracting diseases, cf., however, section 3.

(5) The provisions laid down in subsections (1) to (4) shall also apply to consultants and other persons acting on behalf of the employer.

3. - (1) An employer may offer that health data are collected for the purposes mentioned in section 2 (1) and (4) if working environment conditions make it reasonable and appropriate to do so for considerations of the employee himself or other employees.

(2) Collection of data under subsection (1) shall be instrumental in the prevention of work-conditioned diseases or improvements in the working environment conditions. The rules and guidelines laid down in the working environment legislation on examination methods and use of experts shall be correspondingly applicable.

(3) The employer shall notify the local working environment service before such examinations are carried out. The notification shall include detailed information on the examination, including its extent, method, etc. and on the persons assisting in and in charge of the examination. The examination may not take place until 4 weeks after the working environment service has received the notification.

(4) When a health examination takes place the employer shall -

(1) give the person who carries out the examination any necessary information to be used in this connection,

(2) pay the costs in connection with the examination, and

(3) ensure that the examination can take place without any loss of income for the employee and, if possible, during normal working hours.

(5) The Director of the National Working Environment Service may decide that an examination should not be carried out or should be suspended if it does not satisfy the requirements laid down in subsection (2).

(6) An appeal may be brought against the decisions of the Director in accordance with the same rules as those applying to decisions under the Working Environment Act. However, an appeal shall not have suspensive effect in relation to the decision.

4. - (1) The Minister of Labour may - after having obtained the opinion of the Council mentioned in section 8 - permit that an employer arranges for data to be provided on whether the employee is suffering from a disease, has symptoms of a disease or may be infectious, to the extent that this is necessary in the interest of

(1) the safety and health of consumers or other persons,
(2) the external environment, or
(3) other community interests.

(2) It is a condition for requesting health data that the interests concerned outweigh the interests of the employee and that it is not possible for the enterprise to take these interests into consideration in any other way.

(3) Health examinations shall be carried out by using the least radical method which will serve the purpose.

(4) Section 3 (4) shall be correspondingly applicable.

5. - (1) An employer may arrange for provision of data on whether the employee is suffering from a disease, has symptoms of a disease or may be infectious when this is considered necessary for considerations of the operation of the enterprise, cf., however, subsection (2).

(2) It is a condition that the employer or the organisation of the employer concludes an agreement about this with the opposite employee organisation(s), cf., however, subsection (3). The agreement shall be sent to the Minister of Labour for the purpose of information.

(3) In those cases where no agreement can be concluded according to subsection (2), the Minister of Labour may - after having obtained the opinion of the Council mentioned in section 8 - give permission to a request for provision of health data.

(4) Section 3 (4) and section 4(2) and (3) shall be correspondingly applicable.

Part III.

The employer's duty of disclosure

6. Before the recruitment the employee shall of his own will or if questioned by the employer inform the employer whether he is cognizant of suffering from a disease or has

symptoms of a disease which would be of significant importance for the employee's capacity for work in the job function concerned.

7. If the employer should - on the basis of the data obtained by virtue of section 4 and section 5 - take special measures in connection with the work or make other dispositions, the employee shall ensure that the employer is informed hereof.

Part IV.

The Council of Experts

8. - (1) The Minister of Labour shall set up a Council which shall submit opinions at the request of the Minister of Labour or on its own initiative in cases which are sent to the Minister in accordance with section 4 (1) and section 5 (2) and (3).

(2) The Minister of Labour shall appoint the chairperson of the Council. In addition to the chairperson, the Council shall be composed of 16 members to be appointed by the Minister of Labour at the recommendation of the following authorities and organisations:

1 representative of the Ministry of Labour,
1 representative of the Working Environment Institute,
1 representative of the Ethical Council,
1 representative of the Directorate of the Working Environment Service,
1 representative of the Ministry of Business and Industry,
1 representative of the Association of General Practitioners,
1 representative of the Ministry of Justice,
1 representative of the National Board of Health,
1 representative of the Central Organisation of Professional Associations,
1 representative of the Federation of Salaried Employees' and Public Servants' Organisations,
1 representative of the Main Organisation of Managers,
1 representative of Federation of Danish Trade Unions,
1 representative of the Danish Employers' Confederation,
1 representative of the Ministry of Finance, the National Organisations of Municipal Authorities and the National Organisation of County Authorities, jointly,.
1 representative of the Association of Employers in the Finance Sector,
1 representative of the Association of Employers in Agriculture.

(2) The members shall be appointed for a term of 3 years at a time. They may be re-appointed.

(4) The Council shall lay down its own rules of procedure.

Part V.

Informed consent

9. - (1) Before an examination is carried out for the purposes mentioned in section 2 (1) and (4), cf. section 3, the person who carries out the examination shall ensure that the employee has been informed in writing and orally about:

(1) the purpose and nature of the examination,
(2) the examination method,
(3) any risks in connection with the examination,
(4) any consequences which the results of examination may have for the employee,
(5) the nature of the information which may result from the examination, including the degree of the risk of future disease, etc.,
(6) the conditions for passing on data, cf. sections 7 and 11,
(7) follow-up to the examination, including notification of the employer,
(8) how the results of the examination will be stored,
(9) where warranted by the nature of the examination, also the possibility that the result of the examination may have an impact upon the expectations to life and self-opinion of the person examined.

(2) Before the examination is carried out, the employer shall ensure that the employee is informed about any possible consequences which a refusal to undergo the examination may have for the employee.

(3) The examination may only be carried out, if the employee has given his consent in writing. The employee shall be given a time limit of at least 2 working days for giving his consent after having been informed as mentioned in subsection (1).

(4) If an employee expresses a wish for restrictions in the data concerning the evaluation of the consequences which the results of the examination may have for the employee or if the examination will have an impact on the expectations of life and the self-opinion of the person examined, the person who informs the employee about the results and interpretation of the examination under section 10 (4) shall respect such a wish.

Part VI.

Experts

10. - (1) A request for the carrying out of an examination under sections 2, 4 and 5 shall be made by the employee and at the employees own choice either to the general practitioner normally used by the employee concerned or to a similar expert in the occupational health service to which the enterprise may be attached.

(2) The person who receives the request shall involve the necessary and sufficiently qualified medical or other expertise, including occupational hygiene, clinical-chemical, genetic or biochemical expertise, both in connection with the actual examination as well as the interpretation of the clinical consequences of the examination.

(3) Any person who - on the basis of an examination -issues a certificate concerning an employee's state of health and risk of developing or contracting diseases shall at the same time give an evaluation which illustrates the degree of uncertainty in connection with the interpretation of such examinations.

(4) Certificates concerning the results of an examination shall be passed on to the employee of the person who received the request under subsection (1), cf., however, section 9 (4).

Part VII.

Professional secrecy, etc.

11. - (1) Physicians, clinics, laboratories, public authorities, etc. are not allowed to pass on health data covered by this Act to other persons that the person to whom the data relate, cf., however, section 2.

(2) However, passing on of the data mentioned in subsection (1) may take place to the extent that this is necessary in order to serve the purpose. It is further a condition that the passing on of data -

(1) follows from another Act or provisions issued on the basis of such acts,
(2) takes place for the research purposes with the consent of the person concerned, or
(3) is necessary to avoid risks of the type mentioned in section 4 (1).

(3) The employer may not request or receive and use a power of authority to obtain health data.

Part VIII.

Sanctions

12. Persons whose rights have been violated by infringements of the provisions laid down in sections 2 and 9 may be awarded compensation.

13. Any person who acts in violation of section 2, section 3 (3) or sections 9 to 11 will be liable to a fine, unless a more severe sanction applies under other legislation.

14. If the violation has been committed by a company, an association, an independent institution, a fund or a similar body the fine may be imposed upon the legal person as such. If the violation has been committed by the state, a municipal authority or a municipal association, the fine may be imposed upon the state, the municipal authority or the municipal association as such.

Part IX.

Commencement

15. The Act shall not extent to the Faroe Island and Greenland.

16. The Act shall come into operation on 1 July 1996.

Given at Christiansborg Castle, 24 April 1996

Under our royal hand and seal

MARGRETHE R.

/Jytte Andersen

ITALY

The Italian Data Protection Code (Legislative decree 196/2003 http://www.garanteprivacy.it/garante/document?ID=1219452), which obviously covers data processing in the employment sector, must be applied jointly with sector-related rules concerning employer-employee relationships and the use of technologies in such sectors, where data protection legislation is either left unprejudiced or expressly referred to.

(*Distance monitoring of workers)* In particular, the Data Protection Code states that the provisions laid down in Section 4 and 8 of Act 300/1970 are left unprejudiced (Article 113 and 114 of DPCode). http://www.garanteprivacy.it/garante/document?ID=1219452 . The Act 300/1970, so called "Workers' Statute, gives special consideration *inter alia* - to the distance monitoring of employees and the inquiries on employees' opinions carried out by the employer. Article 4.1 states that it is forbidden to use devices aiming at distance monitoring of workers' activities. However, Article 4.2 provides that those devices that are required by specific management and production needs, or by workplace safety and that can lead to distance monitoring of the workers can be used but only after the agreement with trade unions has been reached. Article 8 forbids inquiries carried out by the employer on the employee's opinions regarding politics, religion or trade union or on other elements that are non relevant for the evaluation of the workers' skill. These provisions have been considered in several decisions of the Italian Dpa (see below).

(*Evaluation data)* The DP Code takes into account evaluation data in connection with data subject's rights. In particular it allows the exercise of the rights by the data subject with regard to data of non-objective character on condition that it does not concern rectification of or additions to personal evaluation data in connection with judgments, opinions and other type of subjective assessment (Section 4).

(Sensitive data) The DP Code –as a general rule- provides that sensitive data can be processed only with the data subject's written consent and the Garante's prior authorization. However, this provision is not applicable if the data processing is necessary to comply with specific obligations and/or tasks laid down by laws, regulations or Community legislation in the employment context within the limits provided for by the DPA authorization. (Section 26)

(Notification) The DP Code states a positive list of specific type of data processing that must be notified to DPA (there is not a general obligation to notify). Processing of sensitive data stored in data banks for personnel selection purposes on behalf of third parties is among the categories of processing that must be notified to DPA. The same applies to the processing of biometric data or geo-localization data (Section 37)

(Telework) The DP Code also gives consideration to the telework by stating that in the context of home-based work and telework, employers shall be required to ensure that the employee's personality and moral freedom are respected.

DPA's decisions

(General Principles) With two different decisions the Italian Dpa has issued Guiding Principles on the Processing of Employees' Personal Data in the Private Sector (23 November 2006, http://www.garanteprivacy.it/garante/doc.jsp?ID=1364099) and in the Public Sector (14 june 2007, http://www.garanteprivacy.it/garante/doc.jsp?ID=1693793). The two Documents, respectively for private and public sector, *inter alia,* recall personal data protection principles employers must

comply with (including the respect for data subjects' rights), clarify the roles of data controllers and processors, deal with secrecy obligations of physicians in charge of health controls, limit the access of employers to the employees' health records, deal with data processing in relations with trade-union organizations, give indications on ID badges worn by workers, provide that biometric systems in the workplace must be deployed only for specific access control need to special workplace areas in which elevated security levels must be ensured and that the blanket use of automatic recognition systems to establish the presence of employees by means of collecting biometric data is not allowed.

(*Monitoring of e-mail and Internet use)* The DPA issued a general decision (dated 1 March 2007) applying to the monitoring of e-mail and the Internet carried out by both public and private employers http://www.garanteprivacy.it/garante/doc.jsp?ID=1408680. According to the Guidelines employers are required to afford reasonable privacy to their employees in order to ensure that their personality can develop freely and without constraints. The guidelines attempt to reconcile the interests at stake by reaffirming, on the one hand, the employer's right to lay down the usage arrangements for the IT equipment committed to employees – including proportionate disciplinary measures – and, on the other hand, employees' right to be the subject of controls carried out in a stepwise, proportionate manner and be adequately informed about the processing of their data, which must be minimised.

(*Electronic Health Records)* On the "Guidelines on the Electronic Health Record and the Health File" (date 16 july 2009 http://www.garanteprivacy.it/garante/doc.jsp?ID=1672821) the Dpa has stated that given the purposes underlying creation of an EHR/HR, access should only be allowed for the purposes of prevention, diagnosis, and treatment of the data subject; only health care practitioners should be enabled to access the data - which does not include, inter alia, employers.
(*Whistleblowing)* Regarding the issue of whistleblowing, a written submission to Parliament was made in December 2009 by the DPA concerning advisability of passing ad-hoc legislation to regulate whistleblowing in the corporate sector. The DPA drew attention in particular to the need for regulating the lawful use of personal data collected via the "good faith" reports lodged by whistleblowers as well as access by data subjects to their own data as collected in this manner.

PORTUGAL

Article 16

Right to privacy

1 – Both the employer and the employee must respect each other personal rights, mainly as regards the respect to the right to privacy.

2 – The right to privacy encompasses either the access to or the disclosure of facts pertaining to the private and personal life of the parties and, in particular, those related to family life, sentimental and sexual life, health status and to political and religious convictions.

Article 17

Personal data protection

1 – The employer shall not require the applicant or the employee to provide information related to:

a) His/her private life, save when such is strictly necessary and considered relevant to determine his/her ability for the exercise of the work, and provided that such request is well grounded and is done in writing;
b) His/her health or pregnancy state unless, due to the nature of the professional activity, there are some specific requirements that so justify it, and provided that such request is well grounded and is done in writing.

2 – The information foreseen in item b) of the preceding number is provided to a doctor, who only lets the employer know whether or not the employee is fit to perform the work.

3 – The applicant or the employee that has provided personal information has the right to control his/her personal data, know of its contents and its purpose, as well as to require such information to be rectified and updated.

4 – The files and electronic accesses used by the employer for the processing of the applicant's or the employee's personal data are subject to the law on personal data protection, currently in force.

5 – Breach of the provisions set forth in numbers 1 or 2 is considered a very serious administrative offence.

Article 18

Biometric data

1 – The employer may only process the employee's biometric data after the National Data Protection Authority has been notified.

2 – The processing of biometric data is only allowed when the information to be used is deemed necessary, adequate and proportional to the purpose to be achieved.
3 – The biometric data are retained during the period strictly necessary for the purpose to be achieved, and must be destroyed as soon as the employee is transferred to another work location or whenever the work contract ceases.
4 – The notification referred to in number 1 must be followed by a Worker's Committee's opinion or, if this one is not available within 10 days after the consultation process, by a document certifying that such request has been made.
5 - Breach of the provisions set forth in number 3 is considered a serious administrative offence.

Article 19
Tests and medical exams
1 – In addition to the situations foreseen in legislation on health and safety at work, the employer shall not, for admission or work purposes, require the applicant or the employee to have tests or medical exams, of any nature, in order to confirm their physical or psychical status, except if they aim at the protection or safety of the employee or third parties, or whenever specific requirements inherent to the professional activity so justify it, and provided that such request, well grounded and done in writing, is addressed to the applicant or to the employee.
2 – The employer shall not, in any circumstances, require the applicant or the employee to have or provide tests or pregnancy exams.
3 – The doctor responsible for the tests and medical exams only lets the employer know whether or not the employee is fit to perform the work.
4 - Breach of the provisions set forth in numbers 1 or 2 is considered a very serious administrative offence.

Article 20
Remote surveillance means
1 – The employer shall not use remote surveillance means at the workplace, through the use of technologic equipment, with the purpose to control the employee's professional performance.
2 – The use of the equipment referred to in the previous number is deemed legal whenever such aims at the protection and safety of persons and property, or whenever special requirements inherent to the professional activity so justify it.
3 – In the cases foreseen in the preceding number, the employer informs the employee of the existence and purpose of the surveillance means used, and shall affix in the areas subject to them,

the following, as appropriate: “This area is under a closed circuit video surveillance” or “This area is under closed circuit video surveillance, where images and sounds are recorded”, followed by an identifiable symbol.
4 - Breach of the provisions set forth in number 1 is considered a very serious administrative offence, whereas breach of the provisions set out in number 3 is considered a less serious administrative offence.

Article 21
Use of remote surveillance means
1 – The use of remote surveillance means at the workplace depends upon authorization of the National Data Protection Authority.
2 – The authorization may only be granted if the means used are deemed necessary, adequate and proportional to the purpose to be achieved.
3 – The personal data captured by the remote surveillance means are retained during the period strictly necessary for the purpose to be achieved, and must be destroyed as soon as the employee is transferred to another work location or whenever the work contract ceases.
4 - The authorization referred to in number 1 must be followed by a Worker’s Committee’s opinion or, if this one is not available within 10 days after the consultation process, by a document certifying that such request has been made.
5 - Breach of the provisions set forth in number 3 is considered a serious administrative offence.

Article 22
Confidentiality of messages and of access to information
1 – The employee has the right to privacy and confidentiality as regards the contents of messages, of a personal nature, as well as of access to information, of a non-professional nature, that he/she may send, receive or consult, in particular, through electronic mail.
2 – The provisions set forth in the preceding number do not hinder the employer to implement, in his/her own company, rules regarding the use of communication means and, in particular, those related to electronic mail.

Summary

The remit

We have been commissioned to draw up proposals for legislation to protect the personal privacy of the individual in working life.

According to our terms of reference, we are required *inter alia* to propose legislation to regulate certain measures – namely monitoring of private email and internet use, and surveillance through other computer-aided means, e.g. logging, monitoring of employees and job-applicants via health and drug tests – and establish the conditions under which employers would be entitled to view extracts from criminal records.

In addition, we have been instructed to consider and, if necessary, propose legislation governing the admissibility of employers requesting to view extracts from the National Social Insurance Agency's records, the Swedish Enforcement Authority's register of debt recoveries and credit ratings compiled by credit-rating agencies. We are also required to consider whether grounds exist for further regulation of camera surveillance and telephone tapping in the workplace. Finally we are instructed to consider whether there are grounds for introducing legislation governing the use of personality tests and the admissibility of asking employees or job applicants about their political convictions or trade union membership. We are also free to put forward proposals on other aspects of working life that could have a bearing on personal privacy.

A new act on the protection of personal privacy in working life

There is a prevailing consensus, both at national and international level, that the right to respect for private life and personal privacy is a human right, and that the state has a responsibility to maintain effective protection against violations of that right.

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 and the meaning of certain statutory provisions must be regarded as unclear. Moreover, protection for employees in the private sector differs to some extent from that afforded to public sector employees. In addition, job applicants have no means of taking effective action against privacy invading background checks conducted by an employer for whom they wish to work.

Given the deficiencies in the existing regulatory framework, protection of personal privacy in working life needs to be clarified and strengthened through appropriate legislation. In our view, this should be done through the introduction of a single, self-contained act. To ensure that the act is as clear as possible to those responsible for its application, it should be patterned on known labour law models. The regulations we propose should also be generally applicable to all areas of working life.

The legislation we propose mainly entails the following provisions:

As regards surveillance and background checks involving the processing of personal data, the provisions in the Personal Data Act should continue to apply in all but three areas, where we propose changes which in our view will serve to strengthen employee protection. We propose the introduction of special provisions governing some of the surveillance and background checks specified in our terms of reference, namely concerning certain records checks and medical tests. In addition, we propose a blanket provision – to be applicable under certain conditions – prohibiting surveillance and background checks in general where these are deemed to have a palpable effect on personal privacy. The provisions we purpose regulating medical tests and the proposed general provision are constructed as discretionary norms. As such they restrict the adoption of surveillance and background checks to

purposes which are authorised and which, on the basis of a proportionality assessment, are seen to constitute an admissible intrusion. A party guilty of breaching the provisions in the proposed act will be liable for damages.

Purpose and scope of the proposed act

The proposed act is prefaced by a declaratory paragraph stating its purpose – to protect the personal privacy of employees in working life.

The act only concerns measures implemented by employers and directed at employees.

Under the proposal, the term employee also embraces in principle certain other categories, namely job applicants, people seeking or undertaking work experience placements and those who perform work as hired or borrowed labour. Where reference is made to employees in the present summary or in the report as a whole, the term is to be understood to apply equally to job applicants and the other categories of persons protected under the act, unless otherwise indicated.

Processing of personal data

The Personal Data Act (1998:204) contains provisions intended to protect against invasion of personal privacy through the processing of personal data. We hope that the relatively extensive account of the content of the act included in our report will afford a better understanding of its application in working life. Our review of the provisions has led us to the conclusion that the act provides relatively good protection of personal privacy in working life. We have accordingly proposed that the Personal Data Act should, unless otherwise stated, apply to the processing by employers of personal data. We do not therefore propose the adoption of separate regulations governing employer surveillance involving, for example, logs or digital camera surveillance, as these come under personal data processing as defined by the act. However, the protection in working life afforded by the act should be more clearly defined and, to some extent, strengthened. We therefore propose the inclusion in our act of a provision modifying the

Personal Data Act as follows in cases where an employer's purpose in processing an employee's personal data is to check up on or monitor the employee.

In the first place, the misuse rule in Section 5 a of the Personal Data Act would not be applicable; instead all the provisions of the act are to be applied.

In the second place, an employer would not be permitted to process an employee's personal data solely on the basis of consent; under the act, some other ground for action would need to exist for processing to be admissible.

Finally, processing by an employer of an employee's personal data should only be admissible under the act if it is stated, when the data has been collected, that the purpose of the processing was to check up on or monitor employees in some specific respect. Thus the act explicitly guards against purpose drift. However, under the proposed act, exceptions may be made where exceptional grounds exist and provided the employer promptly informs employees affected by the processing about its new purpose.

Regulation in collective agreements of issues relating to the processing of personal data in working life could in our view serve to clarify the provisions of the act and facilitate their application. However, although the provisions of the act cannot be departed from by collective agreement, the limits of the area which may be covered by such an agreement can be difficult to define. We therefore propose that a provision also be introduced into the Personal Data Ordinance (1998:1191) as a means of promoting the establishment of collective agreements. Under the proposed provision, the Data Inspection Board would be required, at the joint instance of the parties to the agreement, to deliver an opinion on a draft collective agreement with respect to its compatibility with the Personal Data Act and other statutes governing the type of personal data processing in question.

Prohibition against obtaining certain data extracts

Criminal records include information on people who have had sanctions brought against them for crimes committed. The overriding purpose of these records is to provide authorities, primarily law-enforcement agencies, with speedy, relatively trouble-free access to the information they need to carry out their work. Data

of this kind compiled and stored in a register is extremely sensitive and is therefore subject to the strictest secrecy. However, individuals are entitled to full access to the records with regard to data about themselves.

It is in the public interest that a person who has served his/her sentence be able to play an active part in the community on the same premises as everyone else. With certain types of jobs, however, the need to protect others from the risks that may be associated with previous crimes committed by an employee is deemed to constitute grounds for accessing data from the records. Careful consideration has therefore been given to the incorporation in statutes governing access to criminal records or register checks of provisions specifying which employers are permitted and/or required to conduct register checks. Also specified is the extent of the information that may be obtained in such checks.

According to reports by *inter alia* the National Police Board, employers are increasingly making use of the individual's right to access data about him/herself to request that job applicants themselves produce extracts from the records. Such extracts contain all the information about the individual stored in the register. To prevent employers from exploiting the individual citizen's right to access data about him/herself in a way which is neither intended or desirable, we propose that employers be prohibited from requiring job applicants to produce criminal record extracts about themselves unless there is legal sanction for doing so. It is proposed that the prohibition also cover requests without legal sanction for extracts from the register of suspected offenders.

It has also come to our attention that employers have been known to require job applicants to produce extracts from the Swedish Social Insurance Agency showing previous periods of absence from work due to illness or to care for a sick child. The agency does not normally release this kind of information to prospective employers in accordance with the secrecy rules governing social insurance set out in the Secrecy Act. In order to prevent circumvention of the rules in the Secrecy Act designed to protect personal privacy, it is proposed that employers may not without legal sanction require job applicants to produce extracts from data registers kept by the Social Insurance Agency if the extract contains information to which the employer has no right of access under the Secrecy Act.

However, the proposed new act does not contain specific provisions prohibiting employers from obtaining a prospective employee's credit rating from a credit rating agency or from requiring a job applicant to produce an extract from the Swedish Enforcement Authority's data register. This information is normally in the public domain. Moreover, credit rating agencies and their operations are governed by the Credit Information Act (1973:1173), a special statute intended to protect people against improper invasion of personal privacy. What is more, there is no indication that employers are acting in such a way as to justify special regulation in this regard. As regards obtaining data of the kind referred to above in ways that would constitute an unwarrantable invasion of privacy – such as a request for or access to any data subject to secrecy under the Secrecy Act – our proposal provides for action to be taken under the proposed general provision in our new act otherwise prohibiting encroachments on personal privacy.

Medical tests

Employer background checks in the form of medical tests are particularly sensitive from a privacy standpoint and should therefore be conducted very restrictively.

There is an observable tendency today towards the use of background medical checks in working life, particularly with regard to drug tests. A review of existing law in this area shows that there is no comprehensive regulation regarding an employee's obligation to undergo a medical test, and the legal situation is unclear in a number of respects. Employee protection in this respect varies between private and public sectors and protective regulations for job applicants are largely absent.

We accordingly propose special legislation regulating background medical checks. This would replace the provision on regular medical check-ups currently applying to employees in the public sector under Section 30 of the Public Employment Act.

The proposed act would regulate the right of an employer to request medical tests. By this is meant a request to undergo such a check or to inform an employer of its results. Medical tests are defined under our proposal as a medical examination or any form of alcohol, or narcotic or other drug test. However, this provision

would not apply to alcohol tests administered in connection with alcolocks in vehicles.

The proposed act would permit an employer to request a medical test only if the test was for an authorised purpose within the meaning of the law, and if the test could be said to be an admissible invasion of an employee's personal privacy having regard to the said purpose.

Purposes for which a medical test would be deemed appropriate are specified in the proposed act. These include in the first instance cases where tests are conducted for security reasons. An authorised purpose in such a case would, under our proposal, be the need to assess the medical condition of an employee who has duties where health problems or the influence of alcohol, drugs or medical preparations could entail a risk to human lives, personal security or health, or significantly damage the environment or property.

A request for a medical test would also be for an authorised purpose under our proposal if the test formed part of a rehabilitation plan for the employee.

Finally, the purpose of a medical test would be authorised if it was conducted to assess the state of health of an employee and if said test was of critical importance to the operation of the entity concerned owing to its special character. Checks of this kind are needed primarily in order to conduct drug tests. The basic principle here should be that checks of this type should be essential to or form a vital part of the operation of the entity concerned.

It is proposed that the provision specifying the purposes for which a medical test may be requested by an employer be semi-discretionary, thereby allowing for a decision to establish another authorised purpose than that specified in the act through a collective agreement at national level.

A further condition under which an employer may request a medical test is, as previously mentioned, that the test must be seen to be an admissible intrusion in relation to its purpose. Here the circumstances of each case must be taken into account. However, our proposal also specifies as a basic requirement that medical tests are only admissible if performed by health and medical care personnel, and provided samples taken for alcohol and narcotic and other drug tests are analysed by a laboratory accredited for the purpose under the Technical Conformity Assessment Act (1992:1119), or by an equivalent laboratory in another EEC country. However, the requirement concerning health and medical

care personnel and accredited laboratories does not apply to tests involving breath samples.

Prohibiting privacy invading measures in general

To ensure comprehensive protection against unauthorised invasions of privacy, we also propose, in addition to the special provisions outlined above, a provision prohibiting privacy invading measures in general. Under the proposed provision, an employer would be prohibited from conducting surveillance or background checks that constitute a manifest infringement on an employee's personal privacy unless the measure was taken for an authorised purpose and was seen to be an admissible intrusion into an employee's personal privacy having regard to the purpose justifying the measure. The proposed provision is designed to target qualified cases of surveillance or background checks from a privacy perspective. Examples of measures which would constitute a clear case of privacy invasion – and which in effect are prohibited unless properly justified and proportional – include wiretapping employees' telephone calls, subjecting employees to bag and other searches when leaving work premises, going through lockers, drawers or other spaces an employee normally has sole use of, and analogue camera surveillance in toilet areas.

Ordinary work supervision measures are not covered by the proposed provision. Nor do they concern such measures as obtaining employee references in the normal way or oral questioning of an employee or job applicant.

One measure which however must normally be deemed to fall under the scope of the proposed provision is the use by employers of personality tests or similar evaluations. Implementation of such tests as well as their results must be regarded as sensitive from a privacy standpoint. For the reasons set out in our report, we have not proposed a special, separate provision governing such cases. In our view these would be regulated most appropriately by the proposed general provision prohibiting privacy invading measures.

In accordance with our terms of reference, we also considered regulating the right of employers to question employees about their political convictions and trade union membership. However, we found no compelling justification for such a proposal. If, however, an employer's questioning were to constitute the kind of

improper infringement of personal privacy targeted by the general provision prohibiting privacy invading measures, action could be taken against such a measure under that provision.

Obligation to negotiate

An important element in a regulatory framework intended to protect personal privacy in connection with surveillance and checks in working life is that it be able to guarantee that any measures adopted are thoroughly discussed and transparent. The obligation to negotiate under the Co-Determination at Work Act (1976:580) is already applicable in many cases where an employer is considering the introduction of surveillance and background checks that will involve significant changes in the entity's operations, or will have a specific bearing on working conditions or terms of employment. In order to make it clear that the primary obligation to enter into negotiations applies whenever an employer intends to decide on the introduction of a surveillance and background checks liable to constitute a manifest infringement of the personal privacy of one or more employees, we propose the introduction of an explicit provision enjoining the employer to negotiate beforehand with the relevant employees' organisation in the manner prescribed in Sections 11–14 of the Co-Determination at Work Act. In addition, we propose that it should be permitted to depart from this provision if such a departure is negotiated through a collective agreement.

Other provisions

It is proposed that the penalty for breaches of the terms of the act be payment for damages.

Under the proposed act, cases would be handled in accordance with the Labour Disputes (Judicial Procedure) Act, except where these involve personal data processing, and concern categories of persons, other than employees, who are protected by law.

Except as regards the proposed provision governing personal data processing, prosecution under the Labour Disputes (Judicial Procedure) Act would be subject to the provisions on statutory

limitations set out in Sections 64–66 and 68 of the Co-Determination at Work Act.

We propose that the provisions of the act be mandatory. Thus that part of an agreement which acts to restricts the protection afforded to an employee under the proposed act would have no legal force. As mentioned previously, however, it is proposed that two of the provisions in the act be semi-discretionary, namely the provision establishing the purposes for which a medical test may be requested, and the provision on the obligation to negotiate.