Protection of workers' personal data in the European Union

Two studies

1. Study on the protection of workers' personal data in the European Union: general issues and sensitive data.

2. Study on the protection of workers' personal data in the European Union: surveillance and monitoring at work.

By Professor Frank Hendrickx
University of Leuven
University of Tilburg

The contents of this publication do not necessarily reflect the opinions or the position of the European Commission, Directorate General for Employment and Social Affairs.

FOREWORD

The emergence of the knowledge-based economy together with the increasing advances in technology and the growing role accorded to human capital exercise an important impact on working life.

While these developments are positive in terms of productivity and competitiveness, they give also rise to a certain number of concerns and risks. One of the issues which came to the foreground and is currently the subject of active discussions, law-making and research, at international, European and national levels, is the protection of workers' personal data in the employment context.

The questions relating to this issue are often not new. In fact, a great number of activities performed routinely at work already entail the processing of workers' personal data at all stages of working life. However, new dimensions have appeared recently.

In particular, current developments in human resources management aiming at enhancing the human capital of companies, in work organisation as well as in the use of information and communication technology in the workplace have intensified collection of workers' personal data. Marketing of cheaper and more efficient technological devices has facilitated, and is likely to further facilitate, intrusions to the workers' private sphere. Illustrative examples may be seen in the field of genetic testing as well as monitoring and surveillance of workers.

Against this background, there is, on one side, an increasing awareness of the importance of fundamental human rights, in particular the rights to privacy and to personal data protection and, on the other side, a growing consciousness of the role of work quality as a driving force for a thriving economy, more and better jobs and an inclusive society.

In this context, the Commission included in its Social Policy agenda an action concerning the protection of workers' personal data in the workplace and, subsequently, consulted the social partners, at a first stage, on the advisability and, at a second stage, on the content of a Community intiative in this area.

The present document reproduces two studies which were prepared for the Commission with the aim to provide a comprehensive picture of the relevant regulatory framework in the EU Member States. The first study deals with protection of workers' personal data in the EU: general issues and sensitive data, while the second focuses on the specific issue of workers' monitoring and surveillance at work.

These studies throw light on a complex regulatory framework, characterised by the interaction of legal provisions in various fields of law, and aim at providing the tools to allow better analysis of the existing situation as well as the identification of the challenges for the future.

Odile Quintin

Table of Contents

Protection of workers' personal data in the European Union: general issues and sensitive data.

Table of contents

Protection of workers' personal data in the European Union: surveillance and monitoring at work.

Protection of workers' personal data in the EU: general issues and sensitive data.

Professor Frank Hendrickx
University of Leuven
University of Tilburg

With the collaboration of:

Alberto Arufe Valera
Catarina Castro
Michele Colucci
Taufan Homan
Mark Jeffery
Leonidas Kanellos
Tom McGuire
Nora Melzer
Monica Nebelius
Nuriye Yildirim
Lynn Roseberry
Christophe Vigneau
Anders von Koskull

Manuscript completed in July 2002

Preliminary Remarks

This paper contains the general and final report of the project "**Protection of workers' personal data: general issues and sensitive data**". This project has been financed by the European Commission, DG Employment and Social Affairs and constitutes the final report of contract study VC/2002/0102. It is further referred to as "the study".

The main purpose of the study was to undertake a European comparative research on the issue of "Protection of workers" personal data in the European Union: general issues and sensitive data". The study has focused on the situation in the various Member States of the European Union.[1] It aims to give a picture of the Member States' laws in respect of workers' data protection in general, with particular attention to sensitive data, including health data (covering issues such as Hiv/Aids-testing, genetic testing, drug and alcohol, psychological testing), criminal record data and trade union membership data. The study does not cover the issue of electronic monitoring and surveillance, as this has been the subject of a former study ("Protection of workers' personal data in the European Union: the case of surveillance and monitoring", with contract reference VC/2001/0159).

The study has taken into account the policy background in light of which the research of employee data protection should be conducted. One of the main objectives outlined in the Social Policy Agenda of the Commission (COM2000/379final, 28.6.2000) is to ensure the development and respect of fundamental social rights as a key component of an equitable society and of respect for human dignity, including the protection of personal data of individuals in the employment relationship. With a view to reach these goals, the Social Policy Agenda defines as a major road of action the launching of a consultation of the social partners – on the basis of Article 138 of the Treaty of Rome – with regard to data protection.

The issue of employment privacy, including sensitive data and testing in the workplace indeed received an increased attention among the Member States of the European Union. It has been widely discussed amongst the media, governments, data protection authorities, academic institutions and business. There are some basic Community instruments which apply to the issue, such as Directive 95/46/EC of 24 October 1995 on data protection (*O.J.* 23 November 1995, L281/31). As this Directive (also referred to as "Directive 95/46") fully applies to the employment situation, it is used as the main reference point in the present study. It is common knowledge that the impact of this Directive has been paramount, as it caused a dynamic of amending/modifying Member States' data protection laws along the lines of its general rules and principles. Rules and principles to be found could be labelled as, a.o., *legitimacy* (personal data may only be processed for limited purposes), *finality* (personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes), *transparency* (information to the data subject is required regarding data processing relating to him or her), *proportionality* (personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed), *confidentiality and security* (technical and organisational measures to be taken), and *control* (supervision by data protection authorities).

[1] I.e. the Member States of the European Union as existing on 31 July 2002.

Furthermore, it should be noted that the issue of workers' data protection needs to be assessed in light of the Member States' social policy and labour law principles and traditions. In this respect, labour policy is confronted with new challenges and must adapt to new issues evolving in modern labour relations. Indeed, among both labour and privacy lawyers and policy makers within the Member States, it is realised that labour law principles play a role in respect of fundamental rights and human dignity, more in particular with regard to data protection. It is also found that there is a certain relation of labour and employment laws or principles with data protection laws or principles. As Directive 95/46 also covers the employment situation, the application of its general principles of data protection in the employment context, will be a focus of attention. In this respect, the present study will take into account Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001 by the Working Party that has been established by Article 29 of Directive 95/46).[2]

In light of the above, and in particular taking into account the objectives and actions laid down in the Social Policy Agenda, this study gives an overview of the content and the extent of workers' data protection as presently to be found in the laws and principles of the Member States, both in general as well as in particular on the issue of sensitive data. The study takes into account international (binding or non-binding) instruments in so far as relevant for the analysis of the Member States' situations and has not been designed to depict the full content of international guidance.[3]

The study has been realised on the basis of European-wide country research. The research has been undertaken under the supervision of the contractor with the Cupertino of a group of experts, specialised in the field of data protection and employment privacy. Each expert prepared country research regarding the situation in the relevant Member State. The national research activities have resulted in a general discussion at a closed expert meeting on 13 and 14 May 2002, organised at the Law Faculty of the University of Leuven (Belgium). During this seminar, country surveys were further explained and discussed among the experts. The group of experts, with country studied, is composed as follows: Nora Melzer (Austria), Frank Hendrickx (Belgium and Luxembourg), Lynn Roseberry (Denmark), Anders von Koskull (Finland), Christophe Vigneau (France), Nuriye Nuyildirim (Germany), Leonidas Kanellos (Greece), Tom McGuire (Ireland), Michele Colucci (Italy), Catarina Castro (Portugal), Alberto Arufe Valera (Spain), Monica Nebelius (Sweden), Taufan Homan (The Netherlands) and Mark Jeffery (United Kingdom). The above mentioned experts are further referred to as "the experts".

The present report departs from the horizontal approach of comparativism. This means that it integrates all relevant information regarding Member States horizontally, throughout the general theme and its appropriate sub themes. General comments regarding the Member States' situation are made, and added with components or items specific to particular Member States.

[2] Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, Adopted on 13 September 2001, 5062/01/EN/Final.
[3] An overview of relevant international instruments can be found in the Data Protection Working Party's Working Document on the surveillance of electronic communications in the workplace, Adopted on 29 May 2002, 5401/01/EN/Final.

*

Introduction

Both information and knowledge have become crucial factors in post-industrial labour markets. In this context, labour-management relations are characterised by an increasing and considerable flow of information. These developments are influenced by new management techniques, such as human resources management, in which the individual is identified as a key-element in business success. Furthermore, there is the globalisation of the economy, the increase of international corporate mergers and the unfolding of the network-society which goes hand in hand with technological innovations. This has put companies and labour relations under pressure and has multiplied the needs for information and the flow of data. As labour relations are specifically sensitive to information, they easily open the issue of the regulation of information, including the protection of workers' personal data.

The present contribution relates to the situation as regards the protection of workers' personal data. It will focus on laws, regulations, collective bargaining agreements, case law and other sources relating to this subject. A particular focus of the study is the issue of sensitive data. These include in the first place data concerning the worker's health and his personality. The question is whether there are specific principles of law which govern the collection or further use of such data by the employer or other involved persons or bodies. Self-evidently there are also other sensitive data than medical data, such as information regarding a worker's trade union membership or regarding his (past) criminal conduct. The question is not only what the current law is but also whether the current law is adequate in protecting the worker's rights and interest, like the worker's right to privacy.

The analysis below is divided into two main parts. The first part (chapter 1) concerns the general legal framework with regard to the protection of workers' personal data. The second part (chapter 2) deals with the particular issue of workers' sensitive data. The study will be closed with some general remarks.

Chapter 1. General legal framework of personal data protection in the employment context

1. Legal framework

A. General right to privacy

All member states protect, in general, the right to privacy. The concrete form given to such protection may however differ and is self evidently influenced by the respective national legal and political tradition. Some Member States have an express *constitutional* provision regarding the right to privacy or one of its aspects. For example, article 22 of the **Belgian** constitution and article 10 of the **Dutch** constitution both clearly protect the right to privacy. The same goes for **Spain**, where the constitution[4] recognises the right to privacy as a

[4] Constitution of 27 December 1978, BOE of 29 December.

fundamental right.[5] **Portugal** on the other hand, has a special constitutional provision on data protection[6] together with some other constitutional provisions connected with the right to privacy.[7] Other countries do not know an express general constitutional right to privacy (like e.g. **Austria**, **Denmark**, **France**, **Italy**, **Ireland**, **Luxembourg**, **Sweden**), although the fundamental right to privacy is protected on the basis of national constitutional case law or international legal obligations.[8] Even so, these countries still adhere to some form of fundamental privacy protection, e.g. by protecting specific issues like telecommunications or correspondence, the integrity of the home, and so on. The **Hellenic** Constitution[9] contains a set of fundamental rules covering privacy and the broader right to personality. In **Germany**, the constitutional doctrine on personality rights, privacy and data protection is essentially anchored in four articles forming part of the so-called basic rights part of the Constitution.

The specific position of the **U.K**. with regard to constitutions is broadly known. It does not have a written constitution, nor, until recently, could it be said to recognise a generic concept of 'constitutional rights'. However, the Human Rights Act 1998, which came fully into force on 2 October 2000, brings the U.K. closer to recognising a generic concept of `constitutional rights' by giving further effect in domestic law to rights and freedoms guaranteed by the European Convention on Human Rights. The Human Rights Act 1998 has the very ambitious aim of promoting a new culture of human rights within the U.K. and as part of this, the courts are now obliged, as far as is possible, to interpret and apply national law in a manner that is consistent with the requirements of the European Convention on Human Rights. Of particular interest for the present discussion is the extent to which the courts will be influenced by Article 8 of the Convention, which guarantees the right of individuals to have their private life respected. Again, English law will have to come to terms with the application of general principles. It may be a long time before we can be certain about the precise effect that the Convention will have, but the first signs are that the application of European Law has already allowed the courts to get over any 'culture shock' involved in applying external rules to the interpretation of national law; and that they will not have any ideological difficulties in adapting to the new 'quasi-constitutional' role that has been given them.

Apart from national constitutional laws it is evident that international legal instruments play a great role in protecting privacy.

The relevance of the existence of constitutional right for employee privacy (and personal data) protection varies. It seems that in Scandinavian countries *the fundamental rights protected by the constitution* have played a lesser role in shaping the conditions of the employment contract than in other parts of Europe. In **Finland** the situation is however gradually changing in this respect because of the slowly growing importance of constitutional and human rights arguments. In *1995 the set of constitutional fundamental rights was amended* and the provisions were adapted into the new *Constitution 2000* (1999:731, brought into force

[5] *Vid.* article 18 SC.
[6] Article 35 «Use of computerized data».
[7] The Portuguese Constitution was approved in 1976: *Constituição da República Portuguesa* de 1976; A brief comment on the Portuguese data protection constitutional framework, in English, can be found in MICHAEL, James, *Privacy and Human Rights – An international and comparative study*, Dartmouth Publishing Company, UNESCO Publishing, 1994, 115-117.
[8] The most relevant international instrument being the European Convention on Human Rights (1950).
[9] Constitution of 1975, as revised on 18 April 2001. The Hellenic Constitution was recently revised by resolution of the Parliament dated 6 April 2001, which was published in the Official Gazette on 18.4.2001.

1.3.2000). The number of rights was increased and they were formulated more distinctly than before. According to section 10 of the Finnish constitution everyone's private life, honour and the sanctity of the home are guaranteed. The protection of personal data falls under this provision and it is expressly said that more detailed provisions of that protection are laid down by an Act.

In many Member States, the doctrine of horizontal effect ('Drittwirkung') receives a growing importance. In countries like Belgium, France, Germany or Spain, it is more and more accepted that constitutional rights have effect in employment relationships. It is less clear however, to what extent individual employees can rely on a constitutional right and how possible violations are sanctioned.

The concrete development of the right to privacy is mostly realised through laws that are designed to govern private relationships, such as civil law and labour law. In most Member States, the relationship between an employer and an employee is governed by civil law (in so far as labour law does not provide specific derogations). It is therefore no surprise that privacy issues come up under civil law concepts or tort laws (e.g. **Austria**, **Portugal**), under rubrics as 'good faith', (e.g. **Belgium, France, Portugal**), 'loyalty' (**Finland**) or 'trust and confidence' (**U.K.**). For decades already, **German** case law has brought the general personality right under the scope of the basic tort law provision of section 823 (1) of the **German** Civil Code (*Bürgerliches Gesetzbuch*). The right of personality which is guaranteed by Articles 1 and 2 of the **German** Constitution has significance also for the employment relationship and the rights and duties which are the result of it.[10] Any violation of the right of personality of an employee by the employer is equivalent with a violation of contract obligations. In the case of an objectively illegal encroachment upon his personality right the employee has a right, based on an analogous application of sections 12, 862 and 1004 German Civil Code, to apply for an injunction. In **France**, article 9 of the Civil Code states that "everyone has right to have his private life respected".

Some countries have various specific laws, often enforced through criminal sanctions, protecting specific values that may be brought under the rubric of privacy. But keeping track with criminal traditions such as 'nullum crimen sine lege', it mostly concerns specific incriminations (such as e.g. in the sector of telecommunications).

B. Labour and employment laws

It is obvious that the issue of employment privacy and workers' data protection is covered by labour law. Not in all employment law books, privacy can be found as one of the main topics, but it is felt that this is increasing. As generally known, there is no common and harmonised labour law in the European Union. National traditions and practices may differ strongly throughout the Member States.

A common feature of employment tradition in the EU implies the concept that an employment relationship, i.e. the individual relationship between employer and employee, is a subordinate relationship. Indeed, leaving aside the details, **all** labour laws in the Member States define the

[10] *Bundesarbeitsgericht* BAGE 64, 308, 312; cf. BAGE (GS) 48, 122, 136, 139.

employment contract as a contract whereby the employee agrees to perform the work, for a certain wage, under the authority of the employer. The main labour law principle implies that subordination by the employee to the employer is not an 'economic' subordination, but a legal subordination. Furthermore, this subordination may be considered as the general rule in the employment context. In other words, the employment relationship has a significant impact on the employee's fundamental rights and the exercise of his right to privacy.

Some Member States' employment laws directly refer to the issue of privacy. But these Member States remain exceptions and the initiatives are recent or in a preparatory stage.

A quite unique case is **Finland** that recently adopted the *Act on Protection of Privacy in Working Life* (hereafter Employment Privacy Act).[11] This act was a move to strengthening the approach of sector specific regulation. With its relatively broad scope the act was a kind of pioneer attempt within the European Union. During the preparation of the Employment Privacy Act, models were pointed out from elsewhere in Europe such as for instance in **France** with the so-called Aubry law of 1993[12] and in **Denmark** with the law on treating health data in working life[13]. But, in Finland, the approach is much broader. Also the **Spanish** Employees´ Statute of 1995 dedicates some of its articles to the topic of the protection of the privacy and dignity of the worker, but it does not seem to offer a complete and coherent treatment in the protection of the worker's intimacy. Another act with a relatively broad approach specifically aiming at personal data regulation in working life is being prepared in **Sweden**. In March this year an official report from the data protection commission was completed.[14]

1. In the travaux préparatoires of the Employment Privacy Act the **Finnish** government evoked the need of special regulation in working life and therefore goes further with the implementation of Directive 95/46 on data protection. It was stated that the law on data protection could not fully meet with the special needs of regulation of the employment relations. The Employment Privacy Act is meant to supplement the data protection law and even has priority over this law in case of conflict.

The Employment Privacy Act has general provisions for *collecting* and other *processing* of employee data. Furthermore there are provisions about *personality tests, evaluation tests, medical tests* including alcohol and drug testing and genetic testing. Finally there are provisions about technical surveillance, monitoring of e-mail and other telecommunications. The regulative approach in the act is varying. The rules are mostly general concerning qualitative standards and alternatively on rules or procedure. Some of them are supplementary to provisions in other legislation or to custom approved by case law. For instance, the employer's formal competence to demand health testing or drug testing is not depending of the Employment Privacy Act. It is felt that this mode of regulation depends partly on the nature of the object of regulation, partly on the difficulty to match two or several fields of regulation and partly on the possibilities to find a political solution. When the Finnish

[11] 2000:477, into force 1.10. 2001, an unofficial translation (Ministry of Labour) obtainable at www.finlex.fi/pdf/saadkaan/E0010477.PDF
[12] Several articles concerning processing of data in recruitment, Chapter V of Code du Travail, Journal Officiel 1.1.1993.
[13] Act on use of health data in the labour market (1996:86)
[14] Statens offentliga utredningar (SOU) 2002:18.

Parliament accepted the Employment Privacy Act it required some of the gaps in the act to be filled. The Ministry of Labour has appointed a committee with the task to analyse the situation and if needed to prepare legislation on *drug testing in working life.*[15] The committee's mandate ends the 31st of December 2002.

2. Besides legislative work in Finland, the draft bill of law of **Sweden** on Personal Integrity in Working Life should be mentioned. This draft bill of law was presented in March 2002. It is based on the Personal Data Act. In relation to the Personal Data Act the draft law envisages a special act which means that, where appropriate, its provisions will take over the provisions set out in the Personal Data Act. However, this law will not be limited to developing and specifying the rules in the Personal Data Act of special interest to working life. It will have a somewhat broader scope. The draft law also covers methods for carrying out different measures that may involve violations of personal integrity. It is proposed, for example, that personal data primarily be collected from the employee him/herself. Only in cases where this is not possible an employer may, with the employee's consent, collect information from some other source. Furthermore, in order to protect the employee's personal integrity as far as possible, the draft law specifies the way in which medical examinations, drug tests and personality tests may be carried out. It is proposed that the law on protection of personal integrity in working life would apply to both the public and the private sectors of the labour market. Its aim is to strengthen not just the protection of the employee's integrity but also the protection of the integrity of job applicants and former employee's.[16]

3. In **Spain** the Employees' Statute of 1995 (ES) [17], refers to the right to privacy and dignity of workers. Furthermore, the Law 13/1995, of 8th November[18] on Prevention of Labour Risks declares that «the employer will guarantee to his employees a periodic surveillance of their state of health in function of the inherent risks to the job»[19], bearing in mind that the surveillance of the workers´ health will be carried out, as a rule, with their previous consent[20] and «respecting the worker's right to privacy and his dignity, and the confidentiality of all the information related to his state of health.[21] Also within the labour law field, the Royal Legislative Decree 5/2000, of 4th August[22], the employer's acts «contrary to the respect of the privacy and without due consideration to the dignity of the worker» shall be considered as a «serious infraction»[23], and are sanctioned with fine from 3.00 to 90.000 Euro.[24]

4. In **France** the Labour Code contains provisions on employment privacy. The specific rules have been adopted in 1992 following the publication of a report of Professor G. Lyon-Caen, which, however, rather dealt with computerised forms of monitoring of workers. This report underlined the risks that new technologies might pose with regard to personal freedom at work. Following the presentation of this report, the law was modified and specific provisions were adopted regarding monitoring of workers and workers' data processing.

[15] The work is to be done in co-operation with a Committee appointed by the Ministry of Social affairs and health analyzing the problems of narcotics.
[16] Where applicable, employee also refers to job applicants and previous employees in this passage on the draft law.
[17] Royal Legislative Decree 1/1995, of 24th march (BOE of 28th march).
[18] BOE of 10th November.
[19] Article 22.1, paragraph 1.
[20] Article 22.1, paragraph 2.
[21] Article 22.2.
[22] BOE of 22nd September.
[23] Article 8.11.
[24] Article 40.1.c).

5. In **Italy**, the *Workers Statute* of 1970[25] is the most important source of regulation governing labour-management relations in Italy. It contains rules to safeguard the freedom and dignity of workers and the freedom of trade unions and their activity at the workplace.[26] In doing so, it sets narrow boundaries on managerial prerogatives in order to protect worker dignity and privacy.[27] For example, according to Article 8 of Act 30 (May 1970), No. 300: It shall be unlawful for an employer, for recruitment purposes or during the course of the employment relationship, to make enquiry or have enquiry made into *political, religious or trade union opinion of a worker or into facts that are irrelevant to the assessment of a worker's approach to his work*.

C. Data protection laws

Nearly all Member States (with some exceptions like **France** or **Luxembourg** or **Ireland** who are preparing new laws) have transposed European Directive 95/46 of 24 October 1995 ("the Directive") into national legislation. The Member States' data protection laws are commonly considered as quite technical and detailed. However, for most academics and practitioners, the general principles laid down in those laws show to be quite clear in their abstract meaning.

In all **Member States**, in conformity with the aforementioned European Directive, data protection laws are applicable to the employment relationship and to the processing of personal data of (present or future) employees by employers (in so far as employees can be considered as data subjects in the sense of the data protection legislation – and they often can). Therefore, the general data protection principles also apply to the employment relationship. However, it appears that the *concrete* application of the data protection principles *in practice* is not always clear and therefore leaves a degree of uncertainty. Therefore, in some Member States, Data Protection Authorities have formulated opinions or codes of practice or made studies regarding the applicability of some of the principles laid down in the data protection legislation to the employment relationship, often specifically involving the issue of electronic monitoring in the workplace. This is the case with **Belgium, France, The Netherlands** or the **U.K.** Also the **Greek** Data Protection Authority recently issued directive 115/2001, which specifies the conditions of the lawful processing of the workers' data in the employment context.[28] In **Ireland**, a code of practice, building on the work in this area which has done by the Article 29 European Working Party, is under consideration.

1. The **U.K.** Data Protection Act 1998 is the main source of law in this area in the U.K. It is both clearer and stronger than its predecessor (of 1984) and it is also backed up with the force of European Law – this may prove significant, as courts in the UK are now well-accustomed to interpreting national legislation in line with the purposes of the Directives which it must implement. The fact that the U.K. legislation on data processing contains a list of general and wide-ranging rules, often indicated as *data protection principles,* is an

[25] "Statuto dei Lavoratori," Act No. 300 (May 20, 1970), Title 1, Gazz. Uff. of May 27, 1970, No. 131, *available at* http://www.minlavoro.it.
[26] F. Douglas Scotti, *Il Dialogo Diretto tra L'azienda e il Singolo Lavoratore*, *in* STRATEGIE DI COMUNICAZIONE E STATUTO DEI LAVORATORI (P. Ichino ed., 1992).
[27] A. FRENI & G. GIUGNI, LO STATUTO DEI LAVORATORI (1971).
[28] All the above decisions are available in Greek on the Data protection Authority website *www.dpa.gr*

important departure from the normal practice in English law[29], where there are no codes and no written constitution, and where both legislation and common law tend to deal with specific and detailed rules. Although general principles may subsequently be identified from such rules, they are rarely set out from the start. Perhaps because of this, there remains some considerable room for doubt about how these principles might be applied in practice. The policy of the Information Commissioner, the public official responsible in the first instance for the enforcement of the law on data processing[30], is to settle questions of interpretation in an informal manner wherever possible; and – again possibly because of the room for doubt – most data processors seem also to prefer this approach. Although it might well be the best interests of the parties involved, the result is that very few cases reach the courts[31], and so lawyers have very few precedents on which to base their interpretations of the data protection legislation.

In the meantime, the best indication we have of how the law will apply to the processing of **workers' personal data** is the **Code of Practice** in this area, which at the time of writing (Spring 2002) is in the process of being published by the Information Commissioner. The Commissioner decided to exercise her powers to issue a code of practice precisely because of the increasing concerns of employers, workers and worker representatives over the how the newly-strengthened legislation would apply in practice. Nonetheless, the issuing of the draft version of the Code of Practice, in October 2000, provoked strong reaction from employers and employers' associations. It has been argued that the previous legislation had very little effect in practice upon the behaviour of employers[32], and so until the Draft Code was issued, many employers may have assumed that this situation would continue as before. Nevertheless, the Code does no more than provide advice to employers on how they may ensure that they fulfil the requirements of the law; however, as with all codes of practice issued by official bodies, this may then be a strong influence upon any court which has to decide the matter: so in effect, the advice in the code is likely to become the official judicial interpretation of the legislation. Moreover, the Commissioner's duties under the Act itself include the promotion of 'good practice'[33], so in her codes, she sometimes mixes the legal requirements (the minimum that an employer must do to obey the law) with her own recommendations (which are more demanding, but not legally-binding).

The issuing of the draft version of the Code of Practice, in October 2000, provoked an unexpectedly strong reaction from employers and employers' associations. Some of this was doubtless bluff (it may have suited employers to take an extreme – even unrealistic – position in the hope of being able to persuade the Commissioner to make changes to the draft); but equally, many employers may genuinely not have realized the extent to which the 1998 Act will affect workplace practices. It has been argued that the previous legislation had very little

[29] This discussion will be limited to English law: although much of it also applies to the rest of the United Kingdom, the legal context is different in Scotland and Northern Ireland.
[30] The Information Commissioner is the national supervisory authority as required by Article 28 of Directive 95/46/EC. When the post was first created in 1984, it was called the *Data Protection Registrar*; under the 1998 Act, this became the *Data Protection Commissioner*; and as of 2001 it is the *Information Commissioner*. The Commissioner's Web page <www.dataprotection.gov.uk> has a lot of interesting and useful information, including her Codes of Practice and Annual Reports.
[31] During the year to April 2001, the Information Commissioner took just one formal enforcement action: Information Commissioner's Annual Report, June 2001.
[32] Michael Ford, "The Data Protection Act 1998", (1999) 28 Industrial Law Journal 57
[33] Section 51, *Data Protection Act 1998*

effect in practice upon the behaviour of employers[34], and so until the Draft Code was issued, many employers may have assumed that this situation would continue as before.

In their responses to the Draft Code of Practice, the main employer's association (the CBI), as well as several employers, not infrequently reacted as if the Commissioner were proposing to create new laws, although in fact she was doing no more than recommending a particular interpretation of the law that already exists. The employers' calls for less-demanding rules are often not sustainable, given that neither the courts (which must uphold the legislation) nor the government (which is obliged to comply with the requirements of Directive 95/46/EC) – and less still the Commissioner herself – are able to take into account many of the employers' arguments that special exceptions to the law on data processing should be made for them. Nonetheless, these arguments have served to confuse the debate on how the law should be interpreted, and have succeeded in putting the Commissioner on the defensive. The controversy has been such that the publication of the final version of the Code has been subject to long delays.

2. **France** is currently revising data protection legislation in order to bring it in line with the requirements of the European Directive 95/46. In France, an act on Computers and Freedom[35] was adopted on 6 January 1978, dealing with the issue of the automated collection and processing of data. Article 1 of the 1978 Act states that computers must be at the service of the citizen, and so must not prejudice human identity, or human rights, or privacy, or private and public freedoms. The purpose of this legal instrument was to protect individual privacy against the computerised collection, storage and treatment of personal data. The 1978 Act was not aimed to prohibit but to regulate the automated collection and treatment of personal data. The objective was to conciliate the free movement of information with the individual right to privacy. The Act established the *National Commission for Computer Technologies and Personal freedom* as a state agency, independent of government, whose main tasks are to inform individuals about their rights, to monitor the application of the legislation, and to undertake research on the impact of computer technologies upon human rights. Under its powers to check on the application of the Act, the Commission may investigate any matter involving the collection and processing of personal data, and individuals, groups, and other bodies may also refer any claims relating to this area to it. The key provision of the 1978 Act is the requirement that any public or private body or individual who collects or processes any data concerning identifiable individuals must notify this to the Commission. The scope of this requirement covers not only databases where lists of names appear, but also all data that reveal by any means, whether directly or indirectly, the identity of the subject concerned. This may for example include software that checks on the productivity of workers, a computerised system of clocking-in, and systems that keep a record of the recipients of phone calls or e-mails. On 30 January 2002, the French Assemblée Nationale adopted the first reading of the new Bill of Law, transposing Directive 95/46 into French law and modifying the law of 6 January 1978.[36] A particular feature of the Bill of Law is that it requires prior authorisation of the French Data Protection Authority of personal data

[34] Michael Ford, "The Data Protection Act 1998", (1999) 28 Industrial Law Journal 57
[35] Loi Informatique et Liberté, 06/01/1978
[36] Texte adopté n°780, « Petite loi », Assemblée Nationale, session ordinaire de 2001-2002, 30 janvier 2002, Projet de Loi adopté par l'Assemblée Nationale en première lecture, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

processing, when it concerns a.o. sensitive data, genetic data, data regarding convictions, or when the processing is designed for the selection of individuals who are eligible for a right, a service or a contract.[37] In relation to the employment context, the French Data Protection Authority has issued reports on cyber surveillance at work (in March 2001 and February 2002), a code of practice regarding data processing in the framework of personnel recruitment (March 2002), including a model questionnaire to be used by employers in their relation with job applicants.[38]

3. In **Spain**, there is the Organic Act 15/1999, of 13th December 1999[39] on protection of personal data which develops article 18.4 of the Spanish constitution. It constitutes the main legal instrument of implementation of the Directive 95/46/EC, of 24th October, on data protection. This is an Organic Act —although it was declared partially unconstitutional by the aforementioned DCC 292/2000, of 30 November— applicable in the field of the labour relationships —as its precedent, the Organic Act 5/1992, of 29th October[40], on regulation of the automated processing of the data of personal character, now abolished—, since it has a strong general character, so it «will be applicable to the data of personal character registered in physical support that makes them capable of processing, and to every modality of later use of these data for the public and private sector»[41]. Besides, the same Organic Act contains several express references to the processing of personal data in the employment context, concerning the following issues: 1) «the creation of files of private ownership containing data of personal character will be allowed when it is necessary in order to achieve the activity or the legitimate objectives … of the company»[42]; 2) «the files created with the exclusive purpose of storing data of personal character that reveal the ideology, union membership, religion, beliefs, racial or ethnic origin, or sexual life are forbidden»[43]; and 3) for the processing of the data of personal character, «it will not be necessary the [worker's] consent when the data … refer to the parties of a … contract of employment … and they are necessary for its execution»[44].

4. In **Austria**, in the year 2000 the new Data Protection Act (Datenschutzgesetz 2000 = DSG 2000; BGBl I 1999/165), has brought data protection law, laid down in an Act of 1978, in conformity with the European Directive 95/46. The first section's paragraph 1 of the new Data Protection Act entitles everybody to secrecy of his/her personal data, as far as vital interests, in particular with regard to the right of privacy and family life, are concerned.[45] It does not only comprise protection of computer-aided data, but also manual ones (card indices etc). The Act is applicable to employment relationships. The Data Protection Act contains the general data protection principles as provided by the European Directive 95/46. While there is no specific guidance with regard to the application of these principles in the employment context, the data protection legislation makes reference to the possibility of making private codes (of conduct) in this area, through forms of social dialogue, for the application of the general data

[37] Section 2 Bill of Law.
[38] Délibération n°02-017 du 21 mars 2002 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement.
[39] BOE of 14th December.
[40] BOE of 31st Cctober.
[41] Article 2.1. On this matter, *vid.* J.J. FERNÁNDEZ DOMÍNGUEZ and S. RODRÍGUEZ ESCANCIANO, *Utilización y control de datos laborales automatizados*, Agencia de protección de datos (Madrid, 1997), *passim*.
[42] Article 25.
[43] Article 7.4.
[44] Article 6.2.
[45] *Berka*, Lehrbuch Grundrechte (2000), 99; *Adamovich/Funk*, Verfassungsrecht (1985), 364, 395ff;

protection principles[46] to the specific employment context. It is provided that the social partners may lay down directives (or codes or recommendations) laying down what is to be considered fair processing.[47] This may result in either non-binding or binding rules. An adequate legal instrument within labour law would be the collective bargaining agreement, concluded between employers' associations and employees' associations, whereby mandatory provisions (so called "Normwirkung") directly affect the individual employment relationship.[48] No illustrations of this were found in the undertaken research.

5. In **Italy**, the regulation of employees' information has been deeply affected by the entry into force of Act No. 675 of December, 1996,[49]on protection of individuals and other subjects with regard to the processing of personal data, and by the authorizations given in that regard by the *Autorita' Garante per la Protezione dei Dati Personali*, or simply the "*Garante*." This is the national watchdog authority for data processing and it has its offices only in Rome.[50] Act No. 675/96 aims to ensure that the processing of personal data is carried out in a manner that respects the rights, fundamental freedoms and dignity of natural persons (and, therefore, also employees), particularly with regard to privacy and personal identity; it also ensures the protection of the rights of legal persons and of any other body or association (Article 1).

6. In **Greece**, The Data Protection Act (Law 2472/1997 as subsequently amended by laws 2819/2000 and 2915/2001) which implements the EU Data Protection Directive 95/46/EC is designed to guarantee a basic level of protection of privacy in all activities, including the employment relationship. The Act, as supplemented by law 2774/1999 on data protection in the telecommunications sector, is in line with the European Data Protection Directive. It implements in Greece the general data protection principles, such as legitimacy, finality, transparency, proportionality, confidentiality and security as regards the use, processing, storage and export of personal data both in electronic and manual files. Electronic processing of personal data is placed under the control of an independent Personal Data Protection Authority (DPA).

7. In **Finland**, the main legal instrument for implementing the directive is the *Personal Data Act* (1999:523, in force 1.12.1999). The ambition was to very carefully adopt the pattern prescribed in the European directive.[51] That and some principally minor changes motivated by the experience of the "predecessor" *i.e.* the Personal Data File Act (1987:471) shaped the Personal Data Act. At this occasion and later on, acts have been changed or new ones have been enacted in order to have a more careful or complete implementation of the directive. The Data Protection Act is a *general act of secondary status*, meaning that special legislation

[46] For example, Section 6, paragraph 1 of the Data Protection Act states that personal data must be processed fairly, collected for specified, explicit and lawful purposes and not further processed in a manner incompatible with those purposes and stating that personal data must be adequate, relevant and not excessive in relation to the purposes for which they were collected.
[47] Section 6 par. 4 of the Austrian Data Protection Act.
[48] *Löschnigg*, Verarbeiten und Übermitteln von Arbeitnehmerdaten, in Jahnel/Schrammel/Staudegger, Informatikrecht (2000), 151.
[49] Act No. 675 (Dec. 31, 1996) (protection of individuals and other subjects with regard to the processing of personal data), *available at* http://www.privacy.it.
[50] The *Garante*'s website is *available at* http://www.dataprotection.org.
[51] Concerning the Personal Data Act and data protection in Finland, in English, see Saarenpää, Ahti, Finland. *Nordic Data Protection*. (Ed. Peter Blume). Copenhagen 2001, 39-78. An unofficial translation of the Personal Data Act is obtainable at www.finlex.fi/pdf/saadkaan.

(lex specialis) will overrule the Data Protection Act in case of a conflict (Section. 1 and 2.1). The law is relevant for regulating working life, but with a few exceptions it does not include any provisions especially designed for employment relations. However, with the *Act on Protection of Privacy in Working Life* (2000:477, into force 1.10. 2001, referred to as the 'Employment Privacy Act')[52] the implementation of the Data Protection Directive took a considerable step forward and strengthened the approach of sector specific regulation.

8. In the **Netherlands**, in 2000 a new Data Protection Act (the 'Wet Bescherming Persoonsgegevens 2000', hereafter WBP 2000), was adopted by the Dutch parliament.[53] It replaced the older version of the Dutch Data Protection Act of 1988, (the 'Wet Persoonsregistraties 1988', hereafter WPR 1988) per 1 September 2001.[54] The Dutch Data Protection Act is fully applicable to the employment relationship. It does not provide for specific employee rights in addition to the protection granted. As far as the employment context is concerned, the Dutch Data Protection Authority has issued a report and framework rules regarding electronic monitoring through internet and e-mail at work (April 2002). Furthermore, particular studies are undertaken, such as with regard to medical data and the issue of reintegration (a legal concept under Dutch social law) into the employer's company of workers with a (past-) work incapacity. It is presently unclear how medical data of workers are protected in the process of reintegration vis-à-vis their employer, reintegration companies and insurance companies. Both the group of reintegration companies ('Borea') as well as the group of insurance companies are examining the possibilities of a code of conduct in this respect.

9. **Germany** has implemented the European Data Protection Directive by adopting larger amendments to the Federal Data Protection Act which entered into force on 23 May 2001.[55] In addition to that, a general revision of German data protection law is planned, at least a master plan is expected by the end of 2002. In Germany, arguments have been made for specific exemptions for workers privacy, but a legislative initiative is not considered to be due very soon. The Federal Data Protection Act does not provide for additional rules on employee data protection.

10. In **Belgium**, a specific law came into force in 1992 with regard to the protection of personal privacy in relation to data processing. This is the Law of 8 December 1992 regarding data protection ('LDP'). This law also applies to labour relations. This law has been amended by the Act of 11 December 1998 so as to bring Belgian data protection legislation in line with European Directive 95/46 of 24 October 1995. The Belgian Data Protection Act does not provide for additional rules on employee data protection, except with regard to the consent requirement to process sensitive, including medical employee data (see below).

11. In order to bring **Luxembourg** law into conformity with Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, a new data protection law has been enacted. The bill of law was passed on, upon request of the Prime Minister, to the Consultative Commission on

[52] An unofficial translation (Ministry of Labour) obtainable at www.finlex.fi/pdf/saadkaan/E0010477.PDF
[53] Wet Bescherming Persoonsgegevens van 6 juli 2000, Stb. 2000, 301
[54] Wet van 5 juli 2001, Stb. 2001. 337
[55] Federal Law Gazette, BGBl. I, p. 904.

Human Rights in order to receive an opinion. The Consultative Commission gave its opinion on 11 June 2001.[56] This commission has formulated some remarks regarding the content of the bill of law, which probably would give rise to some modifications. The bill of law makes some references to the employment context, such as in the case of processing of medical data, including genetic data (see below), with regard to employee surveillance – not the subject of the present study – (limitation of legitimate purposes) and prior authorisation of data processing (e.g. in case of employee data processing) by the Data Protection Authority.

12. **Denmark** implemented the 1995 Data Protection Directive by passing the Act on Processing of Personal Data (Act No. 429) on 31 May 2000.[57] The law became effective 1 July 2000. Like the Directive, the scope of the Personal Data Act applies to the processing of personal data of all persons, including workers. Therefore, employers' processing of workers' personal data is primarily regulated by the Danish Personal Data Act. The Personal Data Act applies whenever an employer collects and stores personal data about persons who are or were employed or who are applying for a job. The relationship between data protection law and employment law is expressly recognised by the Danish data protection law. As other provisions within the area of employment and labour law also deal with certain aspects of employers' use of personal data, it is provided that to the extent these other provisions provide better protection, that they must be applied instead of the Personal Data Act.[58]

The Danish Personal Data Act follows the provisions of the Directive quite closely, although there are some variations. The two most obvious differences are in the provisions regarding the scope of the legislation and the exceptions. The scope of the Danish Personal Data Act is slightly broader than the Directive's. Section 1 of the Act is identical to article 3 of the Directive. It states that the "Act shall apply to the processing of personal data wholly or partly by automatic means and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system." However, § 1(2) of the Act goes beyond the scope of the Directive slightly by extending the Act's application "to other non-automatic systematic processing of data performed for private persons or bodies and including data on individual persons' private or financial conditions or other personal circumstances which can reasonably be claimed not to be made open to the public." It must be noted that the provisions on the duty to inform the data subject and the data subject's right to object do *not* apply to this latter category of data processing. As a general matter, essentially all of the professional processing of employees' personal data undertaken by employers will be covered by the Danish Personal Data Act.

13. **Ireland** has currently a Data Protection Act dating from 1988, which is however under revision. The Data Protection (Amendment) Bill 2002 – amending the 1998 Act – was presented in the Irish Parliament on 25 February 2002. The new bill of law follows very closely the language used in the Directive. Both existing and proposed data protection acts have no specific employee data protection provisions, but within the Irish Data Protection Authority a draft Code of Practice relating to the employment context and building on the work

[56] Commission consultative des droits de l'homme. Avis sur le Projet de loi 4735 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel, 11 juin 2001 ; Projet de loi relatif à la protection des personnes à l'égard du traitement des données à caractère personnel, www.eta.lu/SMA/protdon/loi.htm
[57] Law nr. 429 of 31.5.2000. English translation available from the Danish Data Protection Agency's home page at http://www.datatilsynet.dk.
[58] Cf. §2(1) of the Danish Personal Data Act.

in this area which has been done by the Article 29 European Working Party, is under consideration. The precise content thereof is not known yet. A new section is introduced by the bill of law with regard to prior checking by the Data Protection Authority, in view of data processing operations likely to present specific risks to data subjects. In such case, the Data Protection Authority may be of the opinion that prior checking is necessary before any processing takes place.

According to the Irish Data Protection Commissioner, the need for a sector-specific approach of personal data protection (e.g. employment context) is recognised, but has not been addressed yet. When the Data Protection (Amendment) Bill 2002 becomes law, the Commissioner will have the power to introduce codes of practice which will have statutory effect. In the views of the Data Protection Commissioner, the question of a code of practice for the employment relationship will require to be addressed in the context of the work programme necessary to oversee the new act. Besides this, the European Communities (Data Protection) Regulations, 2001 were signed by the Minister for Justice, Equality & Law Reform on 19 December 2001, and will bring into force some new data protection rules with effect from 1 April 2002. The Regulations give effect to some parts of the 1995 EU Data Protection Directive.

14. The legislation on data protection in **Portugal** is laid down in the Data Protection Act (Law 67/98) of 26 October 1998 [59] and the Telecommunications Act (Law 69/98), that have incorporated into Portuguese legislation the provisions of the Directives on data protection[60]. The Data Protection Act does not have special provisions on the privacy of employees, besides the provisions on sensitive data, where reference is made to trade union affiliation, and the prohibition of automated individual decisions, which refers to performance at work. When sensitive data is concerned (health data, criminal record data), a prior authorisation by the Data Protection Authority is required. (i.e. a verification of compliance with the data protection principles).

15. In **Sweden**, the European Directive 95/46 was implemented by the Personal Data Act of 29 April 1998 (entry into force on 24 October 1998), which replaced the former Swedish data protection law of 1973. No specific provision exist in the data protection, specifically addressing employee data protection.

D. Collective bargaining

The present study did not discover widespread collective bargaining on the issue of workers' data protection. Although some examples are found in different Member States. In **Belgium**, recently a collective bargaining agreement was concluded within the framework of the National Labour Council, regarding the protection of workers' private life with regard to the control of electronic and online telecommunications data. This topic does however not lay in the ambit of the present study. Nevertheless, since 1983 there has been a collective bargaining agreement (nr. 38) regarding recruitment and selection of employees.

[59] The mentioned dates refer to the day of publishing in the official bulletin *Diário da República.*

[60] The Data Protection Act has transposed the 1995 Data Protection Directive (95/46/EC), and the Telecommunications Act has transposed the 1997 Telecommunications Data Protection Directive (97/66/EC). We have made special reference to the Telecommunication Directive and legal regulation in Portugal on the previous work: «Protection of workers' personal data in the European Union: The case of surveillance and monitoring», Portuguese Report for University of Leuven's (Law Faculty) Seminar of 4-5 October 2001.

On the following countries, some specific remarks can be made.

1. The **Swedish** draft law on the Protection of Personal Integrity in Working Life is worth mentioning, as it contains several provisions whose concrete application at the workplace is not categorically determined beforehand. The intention is that the law will be used as a basis on which social parties should be able to conclude collective agreements, containing provisions that define the jurisdiction of the law and take particular conditions within individual industries or local conditions at various workplaces into account. For the parties to be able to sign such explicit collective agreements, there is no need for special provisions in the law. The law points out the primary negotiation obligation of employers in accordance with the Act of Codetermination at Work.

2. In **Spain**, from one hundred collective bargaining agreements at branch level that were published officially in January and February 2002, six of them include some clause concerning processes of workers' selection, but none of them has a purpose of putting restrictions on the employers' data collection. These collective bargaining agreements have provisions like 1) «it is compulsory to undergo physical and intellectual tests introduced by the company»[61]; 2) « companies must carry out a medical examination previous to the worker's hiring»[62]; 3) «no worker will be hired without previous medical examination, which will have, among others, the following purposes: to value the candidate's competence for the work to be performed, to specify whether or not he has a predisposition for certain illnesses that could occur or increase due to job performance»[63]; 4) «companies can subject applicants to such selection tests as they consider necessary in order to verify their competence»[64]; 5) «in workers' selection, companies may require aptitude tests to assure the professional competence and the necessary physical and psychological conditions»[65]; or 6) «in each company the workers' legal representation will be informed about the conditions that the candidates should meet»[66].

2. Guiding Principles

From the above it is clear that the issue of employment privacy, more specifically workers' data protection, is covered by constitutional provisions, labour and employment laws, data protection laws as well as other specific laws, often enforced through criminal sanctions. These general constitutional, privacy and employment laws contain various principles which are used or are to be used in the context of workers' data protection.

A. Principle of relevancy: need for justification

Throughout the Member States, the main labour law principle to be found is the principle of *relevancy*. It implies that the employer's right to investigate is not absolute. It is designed to strike a balance between the respective legitimate interests that exist in the context of

[61] CBA to «Industrias de captación, elevación, conducción, tratamiento, depuración y distribución de agua» (Girona, 19-I-2002; *Información Laboral* 49/2002), article 8.
[62] CBA to «Materiales y prefabricados para la construcción» (Vizcaya, 21-I-2002; *Información Laboral* 118/2002), article 51.
[63] CBA to «Galletas» (Barcelona, 22-I-2002; *Información Laboral* 114/2002), article 19.
[64] CBA to «Industrias de la madera» (BOE of 24-I-2002; *Información Laboral* 204/2002), article 22.
[65] CBA to «Confección de peletería fina» (Madrid, 25-I-2002; *Información Laboral* 218/2002), article 31.
[66] CBA to «Comercio vario» (Madrid, 25-II-2002; *Información Laboral* 836/2002), article 10.

employment privacy. It departs from the idea that there is both a right to information (on the side of the employer) and a right to privacy (on the side of the employee, or applicant) and that these interests need to be reconciled. Therefore, the relevancy-test is made, implying that the employer's may only exercise his right to information – or his right to investigate and collect information – in so far as these collections or investigations are relevant for the employment. This is concerned with the protection of private or private life information and with the need for justification in information collection. The principle of relevancy receives many forms and formulations in the Member States.

1. Relevancy-principle in Member States' labour laws

The relevancy principle can be found in some of the Member States to the extent that privacy is addressed under labour law (see above). In the countries, mentioned hereafter, express reference to this principle is made in labour law.

1. In **Belgium**, the principle of relevancy is laid down in article 11 of Collective Bargaining Agreement n° 38 regarding recruitment and selection – and addressing the privacy issue – [67], providing that the private sphere of the applicant will be respected during the selection procedure and that questions with regard to the private life of the applicant may only be justified if such questions are relevant in light of the nature of the job and/or the conditions of performance of the function.[68]

2. A similar provision exists in **Italy**'s Workers Statute of 30 May 1970. According to its Article 8 it shall be unlawful for an employer, for recruitment purposes or during the course of the employment relationship, to make enquiry or have enquiry made into political, religious or trade union opinion of a worker or "*into facts that are irrelevant to the assessment of a worker's approach to his work"*. The prohibition on irrelevant information gathering covers all issues unrelated to the job description and required vocational aptitudes, including political, religious, and union choices; sexual habits and marital status; and, cultural or sports activities outside work. Investigations are allowed when there is an arguable link to expected job performance and, more importantly, to particular job requirement.[69] Article 8 is enforceable through criminal sanctions,[70] while in the more serious cases, fines and a term of imprisonment may both be imposed.[71] Also found to be irrelevant are family and marital status,[72] attire worn (apart from cases in which a uniform is required),[73] compliance with military service requirements,[74] and pregnancy.[75] The ban on investigation into employees' personal opinions is of a very general nature.[76] An employee's opinions about trade unions, politics and religion are irrelevant in evaluating her professional competency. Thus, the prohibition is broadly defined and includes all possible assumptions and consequences of an

[67] Concluded on national level and applicable in the whole private sector.
[68] Article 11 CBA nr. 38.
[69] M. De Cristofaro, *Il Divieto di Indagini su Fatti non Rilevanti ai Fini Della Valutazione Dell'attitudine Professionale del Lavoratore*, I R.I.D.L. 31 (1983).
[70] Breaches of Art. 8 shall be punishable (unless the offense is more serious) by a fine of not less than 50 Euros and not more than 500 Euros or a term of imprisonment of not less than fifteen days and not more than one year.
[71] Art. 38 of Act 300 (1970).
[72] *Id.* at 121.
[73] *Id.* at 123.
[74] *Id.* at 127.
[75] *Id.* at 128.
[76] E. Gragnoli, *La Prima Applicazione Della Legge "Sul Trattamento dei Dati Personali" ed il Rapporto di Lavoro Privato*, R.C.D.P. 673 (1997).

employee's opinions,[77] such as being a member of particular clubs, groups, or associations,[78] participating in cultural and sports activities, or being listed as a candidate for election.[79]

3. Expression of the relevancy-principle can also be found in French labour law. In **France**, the collection and storage of data have to be related to the evaluation of the workers' activity. On the basis of article L.121-6 of the Labour Code all information which employees are asked to provide must serve the purpose of assessing their professional abilities or the individual's capacity to do the job. Only data that have a *direct and necessary* link with the job being offered or with the evaluation of professional abilities being made, can be collected. The courts apply this rule very strictly and prohibit the collection of any data that are related to the employees' private sphere. The principle also applies during the recruitment process of the worker. On the basis of this principle, French law only authorises psychological investigation insofar that there are necessary and directly linked to the recruitment process. Applicants must be informed of the methods of recruitment used.

4. In **Finland**, on the basis of the Employment Privacy Act, a quite strict necessity requirement was introduced.[80] The employer is allowed to process personal data only when it is *directly necessary* for the employment relationship and concerns: 1) management of the rights and obligations of the parties to the relationship; 2) benefits provided by the employer for the employee; 3) or arises from the special nature of the work concerned. It is explicitly stated that no exceptions can be made to this provision, even with the employee's consent.

In a brochure accompanying the Finnish Employment Privacy Act drafted by the Ministry of Labour, it is stated that:

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

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

For practical reasons, it is impossible to list all of the personal data which an employer is entitled to process. Situations in working life vary according to sector or task. An employer requires an employee's personal data for a variety of reasons such as for the authorities when dealing with taxation and social security payments, for the management of the personnel administration and development of the organisation, for customers etc. As regards personal

[77] *See supra* note 24.
[78] L. GALANTINO, DIRITTO DEL LAVORO GIAPPICHELLI (1999).
[79] M. Magnani, *Diritti Della Persona e Contratto di Lavoro. Esperienza Italiana*, 15 Q.L. 47 (1994).
[80] Section 3 Employment Privacy Act.

data concerning the collecting of which some other act lays down separately, an employer no longer needs to consider the necessity of collecting the data.

Data that are necessary as regards managing an employer's and employee's rights and obligations include, for example, data relating to the performance of tasks, selection of an employee, working conditions and compliance with the regulations in collective agreements. Data relating to the benefits provided by an employer can relate, for example, to swimming pool tickets and discounts provided by an employer and to the use of these. Data based on the special nature of work can relate, inter alia, to the family circumstances of an employee who is to be transferred to assignments abroad whenever the employer is responsible for the education of the children or to pets in the home of a family day carer so that allergic children are not assigned to be cared for by that family.

In recruitment situations, an employer has to assess the necessity for data with regard to the job which the person has applied for. This mainly means data showing the applicant's competence and suitability and also a statement on the job applicant concerning his or her suitability health-wise for the job. The employer has to make sure that the job applicant knows what the data are to be used for."

5. The **Swedish** 2002 draft law on personal integrity in working life provides that the personal data collected must be *adequate and relevant* in relation to the purpose for which they are processed.

2. Proportionality

The principle of relevancy has primarily justification purposes, as it is related with the reasons or purposes for data processing. But as may be derived already from the above mentioned French example (a *direct and necessary link with the job), it may also give rise to* a proportionality test in various cases. This proportionality issue is a matter for assessment on a case-by-case basis. However, in **Portugal**, in the context of pre-employment, the Data Protection Authority has explicitly addressed the issue in deciding that personal data like name and profession of husband or wife, number of children, existing of deficiency on the family, and bank account, are excessive data for recruitment and selection procedures[81].

3. Tendency companies

In the framework of the relevancy-principle a specific concept is sometimes used in labour law, mostly in cases involving sensitive employee data. This is the concept of so-called '*Tendenzbetriebe*' or, literally translated as '*tendency companies*', whereby companies are indicated which are biased or show a certain social, ideological, political, religious, … affinity. Religious organisations are a clear example, like political parties, or various non-profit organisations. For such organisations, the employer's interest in collecting specific personal and sensitive information may increase in relation to the specific biased (but legitimate) business purposes. This principle is derived form **German** legal doctrine and is primarily applied in **Austria**, **Belgium** and the **Netherlands**. Also under the **Italian** Workers Statute of 30 May 1970, the exception to the broad prohibition of private life information gathering (cf. article 8 explained above) is found in connection with employers engaged in activities that are

[81] Decision 32/98, published on the Data Protection Authority Report of 1998.

ideologically oriented, for example, political parties, trade unions or religious foundations and associations.[82] Even in this case, a restrictive interpretation has been suggested. The ban on investigations would be lifted only for employees performing tasks that are directly linked to the employer's ideological stance.[83] For employees performing non-ideological functions, employer's investigations would continue to be illegal.

B. Data protection principles

As indicated above, the European Directive 95/46 on data protection has been transposed into national law in most Member States. It has also been pointed out that, without exception, the general data protection principles are applicable in the employment context (in so far as employees can be considered as data subjects in the sense of the data protection legislation – and they mostly can).

Hereafter, mention will be made of special measures or provisions in Member States' data protection laws, that would further develop on or deviate from the general data protection principles laid down in the European Directive. Additional and specific remarks regarding sensitive data will be addressed in another section of the present study (see below).

1. Legitimacy

Article 7 of the Data Protection Directive provides for criteria for legitimacy of data processing. It appears that normal data processing under employment contract or law is considered to constitute legitimate processing under the Member States' data protection legislation. Leaving the issue of consent aside (see below), justifications for employee data processing may be found in most grounds of legitimacy, but in particular in the requirements that "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (Cf. article 7, b) Directive 95/46), or "processing is necessary for compliance with a legal obligation to which the controller is subject" (Cf. article 7, c) Directive 95/46), or "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject" (Cf. article 7, f) Directive 95/46).

In order to determine whether there would or would not be legitimate (normal) data processing in the employment context, the principle of *relevancy*, developed under labour law and explained above, appears to be the most relevant test.

The **Portuguese** Data Protection Commission has had the opportunity to explicitly deal with some cases of legitimate processing necessary for compliance with a legal obligation. This was the case with the employers' obligation to disclose information on employees' pay, for social security and tax purposes, to social security and tax authorities,[84] or the obligation of the employer to communicate to the Labour Inspection the information on existing human resources (like their professional category, profession, social security number, data of

[82] F. SANTONI, LE ORGANIZZAZIONI DI TENDENZA E I RAPPORTI DI LAVORO GIUFFRÉ. (1983)
[83] *Id.*
[84] If employer is an institution with more than 10 workers it is obliged to send this information by e-mail: Decree-Law 106/2001, of 6th April 2001,and *Portaria* 1039/2001, of 27th of August 2001. Tax obligations come as a result of provisions established on Law 42/91, of 22nd January 1991.

admission, data of promotions, any kind of payments...).[85] There is no evidence to assume that these findings would not be applicable to the other Member States.

2. Consent

According the European Directive, and the Member States data protection laws, as far as ordinary (non-sensitive) data regarding workers are concerned, it is sufficient that the employee is *informed* of data processing. Therefore, Member States' legal systems typically do not have a general (either oral or written) consent requirement for all data processing by the employer, although, according to some experts, it may be argued that the conclusion of an employment contract *implies* a consent to normal, legitimate data processing. It seems, however, that the practical impact of the latter argument would be rather weak, having regard to the existence of other possibilities to justify the legitimacy of data processing. In other words, as far as the protection of (ordinary) employee data is concerned, Member States laws do not deviate from the general legitimacy requirements of Directive 95/46.

3. From consent to transparency

While individual consent is not put forward as a prerequisite for the processing of (ordinary, i.e. non-sensitive) employee data, the individual is involved via the transparency-requirement. Information requirements arise from the obligations laid down in articles 10 and 11 of Directive 95/46 and the corresponding implementing provisions in Member States' laws. The data controller (employer) must provide a data subject (employee) with a minimum amount of information, except where he already has it.

The European Directive leaves open the possible to obtain personal data from other parties than the data subject, in which case information needs to be provided to the data subject at the latest at the time of undertaking the recording of the data or at the time of first disclosure (cf. Article 11 Directive 95/46).

In examining the Member States laws and regulations, two sets of issues need to addressed: First, whether or not Member States would provide additional safeguards with regard to transparency when personal data regarding him or her are collected, or whether or not Member States would prevent the possibility that personal data are collected from other parties than the employee himself.

1. As far as additional safeguards on transparency are concerned, attention must be paid to some countries that implemented specific 'employment privacy' laws or provisions. Mostly, they repeat the transparency principle as already contained in data protection law, but sometimes do slightly deviate. This is the case in the following countries:

In **France**, in addition to the provisions of the data protection legislation, the employer's duty to inform the worker has been laid down in the Labour Code. Article L.121-8 of this Labour Code rules that no personal data may be collected without employee's first being informed, regardless of the used technique. This duty to inform does not mean that the data has to be collected directly from the data subject. The data may be collected from a third party insofar

[85] Decree-Law 332/93, of 25th September 1993. Opinion 7/2001, of Portuguese Data Protection Authority, to be published on Report 2001.

that the data subject is informed. This protection deriving from article L.121.8 of the Labour code does not have an equivalent in the 1978 Data Protection Act and differs slightly from the protection given by the Directive 95/46.

The **Finnish** Employment Privacy Act also contains some provisions in addition to the general data protection law. It provides that in case the employer is collecting personal employee data in order to establish the employee's reliability, the employer shall give the employee in question advance notice that such data will be collected.[86] If data regarding the employee have been collected from some other source than the employee himself, the employer has an obligation to notify the employee of these data. It cannot be used in making decisions concerning the employee before this duty is completed.[87]

In **Portugal**, the transparency requirement is also based on the employer's duty to provide information to the worker regarding the conditions of the employment contract.[88]

2. Member States' laws generally do not show any preference with regard to the source of information that employers obtain from prospective or current employees. Under the **Portuguese** data protection legislation however, obtaining personal data from the worker himself, is considered as the general rule. However, it still remains possible to collect personal data from other sources, but remains linked with the provisions on communication of workers' personal data (if the employer receives personal data from a third party, then this implies that workers' personal data are communicated by that third party to another third party). Communication of workers' personal data to a third party is possible either on the basis of a legal provision or on the basis of the Data Protection Commission's authorisation.

A similar provision exists in the **German** Data Protection Act. Section 4 of this act provides that personal data shall be collected from the data subject. They may be collected without his participation only if (1) a legal provision prescribes or peremptorily presupposes such collection, or (2) the nature of the administrative duty to be performed or the business purpose (of the controller) necessitates collection of the data from other persons or bodies, or collection of the data from the data subject would necessitate disproportionate effort, and (both for (1) and (2)) there are no indications that overriding legitimate interests of the data subject are impaired.

Also the **Finnish** law adds a component to employee data protection in this respect. Concerning sources for collecting data about the employee or a job applicant a clear provision in the Employment Privacy Act (Section 4.1) exists. The provision concerns any employee data that the employer collects. The main rule is that the employer shall collect data concerning the employee primarily from the employee him/herself. In order to ask information from elsewhere, the employer has to ask and obtain consent from the employee. Consent is defined in the Personal Data Act [Section 3 (7)] as any voluntary, detailed and conscious expression of will, whereby the data subject approves the processing of his/her personal data. This implies that the employee should be aware of what the consent concerns and its

[86] Employment Privacy Act, Section 4.2.
[87] Employment Privacy Act, Section 4.2.
[88] This is established by the Decree-Law 5/94 of 11 January 1994.

eventual implications. There are exceptions from the rule on consent. "... this consent *is not required* when an authority discloses to an employer to enable the latter to fulfil statutory function..." (Employment Privacy Act Section 4.1). The employee's consent is not necessary when the employer is collecting data on the employee's personal credit history or criminal record in order to establish the employee's reliability.

Some countries, albeit not prohibiting or discouraging employee data collecting from third party sources, limit this form of data processing by the employer. In **Austria**, there is a restricted right to gain employee information from the employee's former employer. It is provided that the so-called reference/certificate of employment[89] should deal with the duration of the employment relationship and the kind of services being carried out. It is also provided that any statement or use of phrases hindering the employee's future career, are forbidden. For example, information may not be given to a succeeding employer, if it concerns remarks with regard to the ground of the employee's dismissal, or negative assessment of his work or insights into his activities as works council or trade union member. The same applies to oral communications by (former) employers. A similar legal provision exists in **Belgium**. One particular case came up before the Belgian civil courts.[90] Person X is hired by employer Y. After a two-month trial period the employer decides to contact the former employer of X. This former employer provides in writing information regarding the period of employment of X, the reason of the termination of his employment as well as the number of persons whom X was supervising. Employer Y seemed to dislike the information provided by the former employer, as it decided to dismiss X. By accident, employee X is informed of the letter and the connection thereof with his dismissal and brings the case up before the courts. The court decides that the former employer has violated the law. Indeed, the Law on Employment Contracts provides that an employer should provide a certificate of employment to every ex-employee. But this should contain only the period of employment (beginning and end). The providing of any other information is prohibited, unless explicitly requested by the ex-employee. In this regard, a European Court-case may also be mentioned, where an employer was obliged to provide for honest references regarding its female ex-employee, who claimed that her contract was terminated for reasons related to her pregnancy.[91]

The **UK'**s Information Commissioner's draft Code of Practice provides that during the vetting process information might be sought from a third party, e.g. a previous employer that the applicant has not given as a referee. If the information is subject to a duty of confidentiality, the third party will need some basis on which to justify its release. The employer might obtain consent for this from the applicant in order to avoid the need for the third party to contact the applicant to seek consent.[92]

4. From transparency to access

It may be argued that another aspect of transparency, interpreted in its broad meaning, is the issue of *access* to (including the right to *rectification* of) personal data, as provided in article 12 of Directive 95/46. It is quite unclear under present Member States laws how the right of access is applied to and implemented in the employment context if personnel files containing

[89] Paragraph 39 AngG, Paragraph 1163 ABGB.
[90] Court of First Instance of Antwerp, 19 February 1993, not published.
[91] C-185/97 of 22 September 1998, NJB 1998, 1825.
[92] The Employment Practices DP Code, Part 1: Recruitment and Selection, March 2002, 27.

employee evaluations or, in general, judgmental data are concerned. It appears that, in practice, the employee's right to access and rectification of personal data concerning him is often misapprehended. In some countries, more clarification is given with regard to transparency and access to personal data by employees.

1. In a series of decisions issued in the past two years, the **Italian** *Garante* ruled that employees requesting access to their evaluation data in the reports drafted by employers were to be granted such access based on Article 13 of the Italian Data Protection Act, due to the fact that the data could be regarded as personal data. For example, a complaint was lodged in 1999 by some employees alleging that their employer (a bank) had only partly complied with their requests for access to their personal data. More specifically, they were not informed of the considerations and judgements underlying the summary rating of their performance (i.e. "excellent," "good," "poor"), which was the sole information disclosed yearly to the individual employees.[93] The decision given by the *Garante* focused on the legal nature of evaluation data for the purpose of possibly applying the Data Protection Act. Under Article 1(2)c of the Italian Data Protection Act, personal data means "any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number." According to the *Garante*, "Any information" is clearly meant to give the broadest possible scope to the definition of "personal data," including any item having an informational content, such as to add to the knowledge of a given identified or identifiable person. This applies both to objective information (i.e. information that can be objectively verified and challenged) and to descriptions, opinions, analyses or personal profiles (based on attitudes, characteristics, professional skills and conduct) leading to subjective evaluation and opinions also with a view to the overall evaluation of a given person. Still, under this Italian interpretation, the right of rectification cannot be exercised with respect to the subjective, discretionary considerations that are also included in an evaluation record. In the latter case, data subjects will be eventually entitled to supplement the information by having riders or personal notes added to their respective files.[94]

2. In **Germany**, section 83, subsection 1 of the *Betriebsverfassungsgesetz* (BetrVG) gives the employee a right to access to personnel files related to him. In this case, the employer has to reveal all information relating to the employee concerned. The employee is permitted to ask the works council for assistance in exercising the right to access. In addition to his access right, the employer has, according to section 83, subsection 2 BetrVG, a right to formulate statements regarding the content of the personnel file(s) relating to him. These comments are then to be included in the personnel file. The access rights under the BetrVG are considered as a *lex specialis* in relation with the right under section 34 of the Data Protection Act.

3. According to the **U.K.** draft Code of Practice 2002, interview notes have to be accessible by job-applicants. This means, according to the Information Commissioner, that

[93] Milan, July 1999. This decision is *available at* http://www.dataprotection.org.
[94] As per Article 13(1)c, No. 3 of the Data Proteciton Act

when an individual makes a request for access to the notes, it must be granted, unless the set of notes is so unstructured as to fall outside the Data Protection Act.[95]

4. According to the new **Irish** Data Protection (Amendment) Bill 2002, no-one can force an employee to make an access request, or to reveal the results of an access request, as a condition of recruitment, employment or provision of a service.[96]

5. Data quality

Article 6 of Directive 95/46, and accordingly national data protection laws, have provisions on data quality.

The above mentioned article provides that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.[97] This is sometimes indicated as the *finality-principle*. It involves the principle of purpose compatibility.

These data quality principles are quite essential with providing fair processing and the respect of the employee's privacy in this respect. The Member States' data protection law use the general terms of the European Directive in formulating these data quality principles. The Data Protection Working Party's Opinion 8/2001 on the processing of personal data in the employment context,[98] adopted on 13 September 2001, has indicated the importance of well applying the data quality principles in the employment situation. In the Opinion, with regard to the finality-principle, the example is given that "the personal addresses of workers collected for payroll purposes cannot be further used or processed for direct marketing purposes without specific consent. A compatible purpose could be, however, to further process these data in order to calculate and include new travel allowances in the salary".[99] No particular regulations are found in the Member States which make the finality-principle more concrete with regard to the employment relationship. It is felt that more concrete evidence should come from application of the general data protection principles.

In **Portugal**, examples have been put forward by the Data Protection Authority. If employees' addresses are collected for administrative management, those data cannot be disclosure to a third party for marketing purposes, except with employees' consent. The Portuguese Data Protection Authority has considered that data collected and processed for retirement pensions purposes may be disclosed and be used to process a complementary payment by a third party[100]. Although this is the case of data being processed for a different purpose, this new processing purpose was not considered incompatible with those original purposes[101]. It has also given authorisation on employees' data on working-related accidents and injuries to be

[95] The Employment Practices DP Code, Part 1: Recruitment and Selection, March 2002, 40.
[96] Amendment of Section 4 of the Principal Act, by section 5 of the Data Protection Amendment Bill 2002, introducing a new subsection 13 in Section 4 of the Principal Act.
[97] Article 6, 1, b) Directive 95/46.
[98] Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, Data Protection Working Party, 5062/01/EN/Final, 28p.
[99] Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, Data Protection Working Party, 5062/01/EN/Final, 20.
[100] Authorisation 15/2000, published on Data Protection Report of 2000.
[101] Article 5.1.b of Data Protection Act; article 6.1.b of Data Protection Directive 95/46/CE.

processed for a different purpose: data may be disclosed by the Hospital to the insurance companies to ensure future medical diagnosis, or the provision of care or treatment. This is also the case of a new processing purpose that was not considered incompatible with the original purpose[102]. Another decision on purpose's compatibility, that has not considered a new purpose incompatible with the original one, was a decision on information disclosure to Labour Courts. Although the employee's medical data had been collected and processed for preventive medicine, medical diagnosis, the provision of care or treatment, it may be disclosed to labour court.

Another aspect of data quality in the sense of data protection legislation (and Directive 95/46) is the period of keeping data. In **France**, Article L.121-6 of the Labour Code implies that employers are not allowed to keep records or information on former employees: so at the end of employment relationships, employers must destroy all information that they have collected about their employees. And in its report of 2001, the French Data Protection Authority (CNIL) recommended that a code of conduct should establish the length of time for which personal data may be stored, and should stipulate what will be done with the data at the end of the employment relationship.

C. Collective guarantees

An additional dimension in employee data protection is formed by collective guarantees. Collective guarantees typically arise from the Member States' labour laws rather than data protection laws. Obviously, collective labour law provisions are strongly linked with national tradition.

A distinction can be made between, on the one hand, Member States that provide specific collective guarantees in workers' data protection, through the involvement of trade unions or works council, and, on the other hand, Member States where such collective guarantees are implied or derived from general collective labour provisions providing for – mostly – the involvement of works councils in human resources or work organisational matters. In the latter group of countries (i.e. those not mentioned hereafter) it concerns information and consultation rights. Particular attention needs to be paid to the **U.K.** In the U.K., workers' representatives have no rights to participate in decision-making regarding the processing of workers' personal data. It is not impossible, however, that a significant change in an employer's policy on the processing of such data will in the future be caught by the legislation which must implement Article 4(2)(c) of Directive 2002/14/EC on Information and Consultation of Employees.

In another group of countries, works councils have general competencies to be informed of and discuss employers' policies involving employee data processing.

1. In **France**, Article L.432-2-1 of the Labour code imposes an obligation to consult the Works Council whenever new techniques of recruitment are introduced and whenever new computer technologies are used in human resource management. More generally, the employer is under a duty to consult the Works Council over all introductions of new

[102] Decision 6/2000, published on the Data Protection Authority of 2000.

technology within the company if these may affect the employees' working conditions, employment, pay, training and qualifications.

2. In **Austria**, there is an obligation on information concerning data collection. According to § 91 par 2 of the Labour Constitution Act[103] the employer is obliged to inform the works council about computer-aided data processing.[104] The information must comprise the categories of employee data as well as the intended processing, including transfer. The works council is not granted an automatic right to investigate into employee data by the above mentioned legal provision.[105] However, like in other Member States, in Austria, the works council has a comprehensive right to obtain information on all matters concerning economic, social, sanitary or cultural interests of employees.[106] Several rules comprise specific information to be given by the employer, sometimes with and sometimes without the representatives' request. It is also relevant to mention that, according to the Labour Constitution Act, the works council representatives have a certain right to investigate the data as well as the technological bases of data processing (e.g. the programme documentation). However, if the representatives want to inspect personnel files, they need the concerned employee's consent.[107]

3. In **Finland**, the main legal framework concerning information and consultation with regard to processing of employee data is to be found in the Co-operation within Undertakings Act (1978:725, into force 1979).[108] References to this "Co-operation Act" are included in the Employment Privacy Act. The Co-operation Act concerns the right to information, consultation and co-decision. In most cases of compulsory co-operation the prescribed model of co-operation is information and consultation. The new Act on Employment Privacy, which is linked to the procedure of co-operation (Employment Privacy Act Section 4.3), provides that the co-operation procedure shall cover *"*(...) the principles of recruitment, its methods, the data collected in connection with recruitment and during an employment relationship (...)".[109] The obligation imposed on the employer regards information and consultation, not co-decision (Section 7.5). It must be noted that, with regard to data processing, a lack of personal and individual consent cannot be compensated through a collective co-operation procedure.

4. In the **Netherlands**, the Works Councils Act gives an important role to the works council when it comes to the use and processing of personal data of employees by the employer.[110] According to article 27 of the Act, the employer needs the positive consent from the works council when he intents to implement, change or withdraw rules about processing personal data.[111] The works council's consent cannot, however, replace individual employee consent.

[103] ArbVG (Arbeitsverfassungsgesetz = Labour Constitution Act)
[104] *Melzer-Azodanloo*, Tele-Arbeitsrecht [2001], 175.
[105] *Löschnigg*, Verarbeiten und Übermitteln von Arbeitnehmerdaten, in Jahnel/Schrammel/Staudegger, Informatikrecht (2000), 155.
[106] § 91 par 1 ArbVG
[107] *Strasser/Jabornegg*, ArbVG[3](1999), § 91 Nr 14.
[108] For a presentation of the act, see Bruun op.cit. 2002, 200-203 and Suviranta op.cit. 155-163.
[109] The Co-operation Act Section 6, pt. 8, as amended by the act 2001:478.
[110] See: S.F.H. Jellinghaus and M. Korpershoek, OR en de Wet Bescherming Persoonsgegevens, Sociaal Beleid 2000, nr. 3a, Special Privacy-edition
[111] Wet op de Ondernemingsraden of 28 January 1971, Stb. 54, last revision of 18 March 1999, Stb. 184.

5. In **Denmark**, the Medical Data Act[112] it is provided, among other exceptions mentioned in the Act, that the employer may collect employee health information after agreement with the union, in order to satisfy essential interests connected with the running of the business or concern. If a medical examination is necessary, additional individual informed consent remains necessary (see below).

D. Notification exemptions for human resources

Article 18 of Directive 95/46 concerns the notification of the national supervising authority. This obligation has been transposed into the respective national data protection laws. However, several countries (see hereafter) have made use of the possibility to exempt human resources related data from the notification duty (under Article 18, paragraph 2 of the Directive). In **Greece**, where this is done, this already has been officially criticised by unions. In their opinion, the exemption from prior notification makes control over legitimacy and adequacy less realistic. Also in **Belgium**, there is a wide category of exempting HR-data from notification. In this country, it is also felt that notification duties are not well lived up to anyway. Likewise, **Portugal**'s Data Protection Authority has exempted data processing of remuneration, pay and subsidies of employees, and of the administrative management of staff, employees and service contractors.[113] A general feeling remains that matter of control by the data protection authority remains difficult, even in case where notification is obliged. In **Denmark**, private employers have no duty to notify data processing made necessary by a collective agreement. In **Germany**, the employer is not bound to the duty of notification if the data subject has been instructed otherwise. Regarding data which have been collected on the course of an employment situation, this is conceivable In **Finland**, if the processing concerns an employment relationship, there is no duty of notification, but if the processing concerns sensitive data such duty of notification exists. In the **Netherlands**, on the basis of the so-called Exemption Decision, various human resources related data processing activities are, under certain conditions, exempted from the notification duty, such as data regarding job applicants, temporary workers, personnel administration, salary administration, indemnities upon termination, data regarding retirement and pre-pension.

Chapter 2. Sensitive data protection in the employment context

Sensitive data are protected under section III of Chapter II of Directive 95/46 on data protection, regarding special categories of processing. In article 8 of Directive 95/46 it is provided that Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. To this general prohibition, various exceptions are applicable.

[112] Law n° 86 of 24 April 1996.
[113] All the exemption notices were published in the official bulletin *Diário da República* of 27th January 2000. There are other exemption not related with employees' data.

1. Justification of processing

All Member States have implemented this idea of *general prohibition* to process sensitive data, with formulation of exceptions, as provided in the European Directive. The system therefore allows to indicate justification grounds that may justify the processing of sensitive personal data.

1. A most important exception is the *explicit consent* of the data subject, laid down in article 8, paragraph 2, a) of the Directive. According to article 2, h) of the Directive the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

2. Another important exception for the employment context is laid down in article 8 paragraph 2, b) of Directive 95/46, providing that the prohibition of sensitive data processing shall not apply where the processing is necessary for the purposes of carrying out the *obligations and specific rights of the controller in the field of employment law* in so far as it is authorised by national law providing for adequate safeguards.

Both grounds of exception are commented hereafter on the basis of the available Member State information. They are however added with specific protection under some Member States' data protection legislation. Some countries, for example, know a system of prior authorisation by the Data Protection Authority for the processing of sensitive personal data.

A. Consent or authorisation

With some qualifications or exceptions (see hereafter) Member States' data protection laws, like the European Directive 95/46, provide consent of the employee as data subject as a non-exclusive (meaning that sensitive data processing can also be justified on other grounds) base of legitimate sensitive data processing. National laws, therefore, follow the general pattern of the European Directive in providing for other grounds of sensitive data processing, albeit much more limited than in the case of ordinary (non-sensitive) data processing.

Some countries however know more restrictive approaches or provide specific protection or features in this respect, which require closer examination, as shown hereafter:

1. In its implementing measures **Belgian** data protection law has added some elements to the protection offered by the European Directive. The Belgian Law on Data Protection does not know a system of prior authorisation (by the Data Protection Authority) of sensitive data processing, but provides that processing of sensitive data is allowed if the data subject has given his written consent to the processing of those data, yet in the understanding that the consent may be withdrawn by the data subject at any time. According to the Law on Data Protection[114] consent is defined in the sense of the Directive and means "any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating him being processed".

[114] Article 1, §8 LDP.

Like in other countries, also in Belgium the question has arisen whether workers can lawfully give their consent in the individual employment contract. In principle, the answer is affirmative. Apart from the issue of the 'freedom' of consent, data protection law does not prevent contractual clauses in the employment context whereby the informed consent is given by an employee. However, with the introduction of Royal Decree of 13 February 2001[115] an important nuance should be made with regard to sensitive and health-related data. Indeed, the Belgian data protection law provides that a Royal Decree may indicate the cases in which the prohibition of data processing, referred to above, may not be lifted by the explicit consent of the data subject. In Belgium, article 27 of the Royal Decree of 13 February 2001 stipulates that if the processing of personal data relates to sensitive or health-related data and is only made lawful on the basis of the consent of the data subject, this processing is still prohibited if the controller of the processing is the current or potential employer of the data subject. This prohibition is lifted in case the data processing has the purpose of providing an advantage to the data subject.[116]

In an official explanation of this Royal Decree[117] it was argued that in article 2, h) of Directive 95/46/EC consent is understood as a 'free expression of the will'. According to the said explanation, such free will is often absent in the relationship between an employer and an employee. However, the Belgian data protection authority is of the opinion that the quite strict rule of aforementioned article 27 was not necessary as the current system of data protection already protects workers satisfactorily.[118]

As indicated above, the prohibition laid down in the Royal Decree of 13 February 2001 is lifted in case the data processing has the purpose of providing an advantage to the data subject.[119] The preparatory works of the Royal Decree give the example of the payment of trade union allowances, or the situation whereby an employer has to provide specific facilities to employees who follow the practice of a particular religion.[120] The latter examples could also be viewed as justifications under article 8, paragraph 2, b) of Directive 95/46.

2. In **Italy**, individual consent is needed for the processing of sensitive data of employees. The employee needs to give this consent in writing. Consent is however not requested with regard to a person applying for a job on his own initiative. An additional guarantee is the prior authorisation of the *Data Protection Authority (*or the *'Garante')*[121] to proceed with sensitive data processing. The *Garante* shall communicate its decision concerning the request for the authorisation to process such data within 30 days; in default of such communication at the expiry of that period, the request shall be regarded as denied. Along with this authorisation or thereafter, based also on appropriate checks, the *Garante* may provide for measures and precautions in order to safeguard the data subject, which the controller shall be bound to apply. The Italian system of prior authorisation brings self-evidently many practical application problems, such as increased workload for the *Garante* or additional formalities or administrative burden for employers. Taking this into account and due

[115] Giving effect to the amended LDP.
[116] Article 27 Royal Decree 13 February 2001.
[117] Report to the King, Preparatory Works, *Belgian State Gazette,* 13 March 2001, 7859.
[118] Opinion 8/99 of 8 March 1999, *B.S.* 13 March 2001, 7878.
[119] Article 27 Royal Decree 13 February 2001.
[120] Report to the King, Preparatory Works, *B.S.* 13 March 2001, 7859.
[121] *Autorita' Garante per la Protezione dei Dati Personali.*

to the fact that, in Italy, employers may only process sensitive data upon authorisation by the Data Protection Authority (and after obtaining the data subjects' consent in writing), the *Garante* has granted authorisations *ex officio* either to individual controllers (i.e. employers) or, by means of a general provision, in respect of specific categories of controllers or processing operations (see below).

The general authorisations, such as No. 1/1998, No. 1/1999 and No. 1/2000,[122] issued by the *Garante*, relying upon Article 41 of Act 675/96, aim to lay down and harmonize measures and safeguards for the benefit of data subjects, by taking account of the rights and interests of data controllers deserving protection, as the need to apply for individual authorizations would place an excessive burden on the latter. They have been considered necessary to further simplify the obligations imposed under Act No. 675/1996 on certain categories of data controllers, enhance operation of the Office of the Garante and streamline the provisions to be made through said authorizations. They are time-limited, partly on account of the provisions included in the regulations on organisation and operation of the Office of the Garante as issued by Presidential Decree No. 501 of March 31, 1998. Following the same rationale behind the Workers Statute and Act. No. 675/96, these authorisations aim to minimize the risk of affecting or endangering, through the processing, fundamental rights and freedoms and human dignity—especially with regard to privacy and personal identity. One authorisation underlines that the processing of sensitive data is carried out to a considerable extent for the fulfilment of obligations applying to labour relations, with regard to accounting, salaries, social security, assistance, taxation and insurance. Such processing must therefore be the subject of a general authorisation. On the basis of these considerations, the *Garante* expressly authorized the processing of sensitive data for employment purposes. The scope of the authorisations is quite broad.

It is important to stress that these authorisations are without prejudice to the requirement of obtaining the data subject's consent in writing and informing him or her as a data subject.

3. Comparable to Italy, **Portugal** also knows a system of prior authorisation of sensitive data processing by employers (data controllers). Under Portuguese data protection law, sensitive data are defined as those personal data revealing philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data. The Portuguese Data Protection Act provides that the processing of such sensitive data shall be permitted by a legal provision or by the authorisation of the Data Protection Authority when, on important public interest grounds, such processing is essential for exercising the legal or statutory rights of the controller or when the data subject has given his explicit consent for such processing, in both cases with guarantees of non-discrimination.[123] Like the Italian *Garante* (see above), and apparently at least partly inspired by a practical rationale, the Data Protection Authority has issued some abstract authorisations in certain employment fields (e.g. the use of trade union data; the use of medical data).

122 *Garante*, *Authorization Concerning Processing of Sensitive Data for Employment Purposes (Provision No. 1/2000)*, *available at* http://www.dataprotection.org.
[123] Article 7, Data Protection Act 26 October 1998.

4. Under the **Hellenic** Data Protection Act, the collection and processing of sensitive data, as well as the establishment and operation of the relevant file, also needs to be permitted by the Data Protection Authority, even in combination with the individual's consent, under one or more specified conditions.[124] However, the authorisation requirement is quite widely abandoned for the employment related purposes. It is provided that the prior authorisation of the Data Protection Authority is not required when processing is carried out exclusively for purposes relating directly to an employment or project relationship and is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the aforementioned relationships, and upon prior notification of the data subject.[125]

5. The new **French** Bill of Law on data protection also introduces a system of prior authorisation by the Data Protection Authority. This is provided for the processing of genetic data, as well as for the automated processing of data aiming at selection of persons eligible for the benefit of a right, a service or a contract.[126] The latter wording would suggest that data processing following many forms of personnel selection would need prior authorisation by the French Data Protection Authority, even if it does not concern sensitive data. The new Bill of Law on data protection allows for standard authorisations,[127] but as this law is not yet operative, it is difficult to assess at this moment whether or not employment related general authorisations will be provided. It is argued that this flexible approach makes governmental control (or control by the Data Protection Authority) difficult in assessing the lawfulness of sensitive data processing by employers. Justification appears to be, in the first place, to be determined by the data controller (employer).

6. An interesting feature with regard to consent is the **Austrian** concept of works agreements, i.e. agreements concluded between an employer and a works council, in relation to staff questionnaires.[128] In some cases, the works council's agreement (approval) is necessary in order to make such staff questionnaires lawful. In principle, the collection of general information about a person or his/her qualification need no consent and can be obtained by the employer without a works agreement. This is the case for information such as names, birthdays, addresses, family status, education, job experience. On the other hand, some questions or investigations are not allowed, even with the works council's consent, namely in case the (employee's) private life is too much involved, e.g. on questions regarding pregnancy. Another series of information, or possible questions, comprising more than general information on a person may require the consent of the works council. This may involve information on an employee's trade union membership or religion in so called *Tendenzbetrieben* (see above) or questions on an employee's previous convictions in an area in which the undertaking is working.

[124] Article 6 Hellenic Data Protection Act.
[125] Article 7 Hellenic Data Protection Act
[126] Section 25 of the French Bill of Law.
[127] Section 25, II.
[128] See *Grillberger*, Ein umstrittener Personalfragebogen, DRdA 1979, 148; *Schwarz/Löschnigg*, Arbeitsrecht[9](2001), 856ff.

The Austrian Data Protection Act provides for lawful sensitive data processing with the consent of the individual concerned. This is defined as unambiguous consent, which can be revoked at any time, the revocation making any further use of the data illegal.[129]

7. As indicated above, the **Finnish** Employment Privacy Act provides that employee data have to be collected primarily from the employee himself. There are some exceptions to this rule (see above). Health-related data collection is, however, more restrictive. In this case, the employer must collect the data directly from the employee concerned and with the employee's written consent. The data may only be collected from another source than the employee with the latter's written consent.[130] The Finnish data protection legislation leaves alternatives for individual consent as far as sensitive data processing is concerned.

B. Rights and obligations under employment law

In relation to individual consent as an important exception to the prohibition of sensitive data protection, related grounds of justification should be examined. The most general exception to the prohibition of sensitive data processing, besides consent, is laid down in article 8 paragraph 2, b) of Directive 95/46, providing that the prohibition of sensitive data processing shall not apply where the processing is necessary for the purposes of carrying out the *obligations and specific rights of the controller in the field of employment law* in so far as it is authorised by national law providing for adequate safeguards.

The approach of article 8 (referring to legitimacy of sensitive data processing) is more restrictive than the one used in article 7 (referring to general legitimacy of data processing) of Directive 95/46, where in particular requirements are provided that "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (Cf. article 7, b) Directive 95/46), or "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject" (Cf. article 7, f) Directive 95/46).

Not all Member States have implemented the exception of article 8 paragraph 2, b) of Directive 95/46 in the same manner. In some case, other – and more restrictive wording – is used. In other cases, this general justification ground has been made more specific or clear. It should be noted that the relevance of individual (or other forms of) consent becomes increasingly pertinent to the extent that the other grounds of justification (of sensitive data processing) become more restrictive. Therefore, the issue of consent can only be fully assessed if attention is paid to other (alternative) justifications provided for labour or employment situations.

1. Under **French** law, as already indicated above, a rather strict relevancy-test is used. On the basis of the relevancy principle, the processing of personal data must show a direct and necessary link with employee evaluation in light of the workers' activity in order to be lawful. It is still under discussion as to how far this rule would deviate from the principle laid

[129] Section 9, 1, 6 Austrian Data Protection Act.
[130] Employment Privacy Act, section 4.1 and section 8.1.

down in article 8, paragraph 2, b) of Directive 95/46. However, the new Bill of Law on data protection does not provide for a general exception under labour or employment laws with regard to the processing of sensitive data.

2. In **Germany**, according to Section 28 of the Data Protection Act – generally taken as the main article referring to justifications in the employment context – uses rather restrictive grounds for sensitive data processing in its paragraph 6. The restrictive cases in which collection, processing and use of sensitive data for own business purposes would be admissible – when the data subject has not consented – do not generally refer to rights or obligations under an employment situation.

3. It is also relevant to point to **Italy** where the *Garante* must authorise the processing of sensitive data (see above) and to cases where it has granted authorisations *ex officio* in respect of specific categories of controllers or processing operations. In assessing these authorisations, it appears that the *Garante* has taken account of the provision in article 8, paragraph 2, b) of Directive 95/46. Indeed, the general authorisations, No. 1/1998, No. 1/1999 and No. 1/2000,[131] issued by the *Garante*, relying upon Article 41 of Act 675/96, aim to lay down and harmonise measures and safeguards for the benefit of data subjects, by taking account of the *rights and interests of data controllers* deserving protection, as the need to apply for individual authorisations would place an excessive burden on the latter. They have been considered necessary to further simplify the obligations imposed under Act No. 675/1996 on certain categories of data controllers, enhance operation of the Office of the Garante and streamline the provisions to be made through said authorizations. They are time-limited, partly on account of the provisions included in the regulations on organisation and operation of the Office of the Garante as issued by Presidential Decree No. 501 of March 31, 1998.

The *Garante* has taken into account the *specific context of the employment relationship*. One authorisation underlines that processing of sensitive data may be carried out, to a considerable extent, for the fulfilment of obligations applying to employment relations, with regard to accounting, salaries, social security, assistance, taxation and insurance. Such processing must therefore be the subject of a general authorisation. On the basis of these considerations, the *Garante* expressly authorised the processing of sensitive data for employment purposes.

The *Garante* applies the principle of necessity. The processing of sensitive data must be necessary:
a) to perform or enforce performance of specific obligations, or to discharge specific functions as provided for by laws, Community legislation, regulations or collective agreements, even when related to individual businesses, particularly with a view to complying with provisions related to social security and assistance, occupational or population health and safety, taxation, health care, public order and security;
b) for accounting purposes or the payment of salaries, allowances, premia, other kinds of remuneration, gifts or fringe benefits, even apart from the cases referred to under a), provided

[131] *Garante*, *Authorization Concerning Processing of Sensitive Data for Employment Purposes (Provision No. 1/2000)*, *available at* http://www.dataprotection.org.

this is in compliance with the laws in force and serves specific, legitimate purposes. In that regard, the *Garante* has interpreted this provision to mean that an employer contracting with an outside accountant for payroll services needed the consent of each employee whose payroll would have been transmitted.
c) for the protection of life or bodily integrity of the data subject or a third party;
d) for the establishment or defence of a legal claim, even by third parties, including administrative proceedings and arbitration or settlement in the cases provided for by laws, Community legislation, regulations or collective agreements, on condition that said claim is of an equal level as compared with the data subject's one, if the processing concerns data disclosing health and sexual orientation;
e) to exercise the right of access to administrative records in compliance with the relevant laws and regulations;
f) to perform obligations resulting from insurance contracts against risks related to employers' liability for occupational health and safety and occupational diseases, or against any damage caused to third parties in the exercise of labour or professional activities;
g) to ensure equal opportunity actions.

In respect of the justification of the processing of sensitive data, specific use of the relevancy principle is often made when justifying data processing on the basis of rights or obligations under the existing (or prospective) employment *relationship*.

A first series of justifications related to so-called *Tendenzbetrieben*. In many countries it is accepted that employers that can be regarded as companies with a specific ideological, philosophical, etc. purpose, could argue for the processing of sensitive data, e.g. data regarding religion or political or ideological beliefs. For example in the context of the employee's religion, schools, kindergartens or hospitals kept by the Catholic or other Churches, employer's may be allowed to asks for the (prospective) employee's attitude towards religion and which church he/she is member of.

In **Italy**, it is provided that data processing may concern the data that are closely relevant to the following obligations, tasks or purposes: with regard to data disclosing religious, philosophical or other beliefs, or membership of associations or organizations with a religious or philosophical aim, any data concerning leave of absence, religious holidays or use of canteen services, as well as those relating to conscience objection where this is provided by the law. Processing may concern the data that are closely relevant to the following obligations, tasks or purposes: with regard to data disclosing political opinions, membership of parties, trade unions, associations or organizations with a political or trade-union aim, any data concerning exercise of public functions and holding of political offices (provided data processing is carried out in order to grant a temporary leave of absence pursuant to laws or collective agreements, even when related to individual businesses) or the organization of public initiatives, as well as any data relating to trade-union activities or offices and the deduction of fees due for trade-union services.

4. In **Austria**, the Data Protection Act also seems to be more restrictive than the Directive 95/46 in allowing sensitive data processing where the Act demands that "the use is required according to the rights and duties of the controller in the field of employment law and

civil service regulations *and* is legitimate according to specific legal provisions (…)". A link with the rights and obligations under the employment relationship seems to be only established in specific cases where employers need sensitive data for personnel administration purposes. This is the case with deduction of union dues (check off clause), the taking of specific measures (e.g. with regard to pregnant or disabled workers), the granting of leave for private purposes, etc. For example, in Austria, several rules concerning public holiday rest lay down that members of other churches than the Catholic one (e.g. the Protestant, the Old Catholic) have additional days off[132].

5. In the **U.K.**, according to the Data Protection Act, the processing of sensitive data is allowed if it is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment. There is one interesting addition: the *Data Protection Act 1998* includes as one of the legitimate reasons for processing sensitive personal data, any processing of personal data on race or ethnic origin that is necessary for equal opportunities monitoring, where this is done in order to promote or maintain racial and ethnic equality[133]. These exceptions will therefore allow in a rather flexible way for processing to be done without the express consent of the data subject.

6. In **Finland**, the Personal Data Act seems to regulate the derogations from the prohibition to process sensitive data more strictly than Directive 95/46. According to section 12 of this Act, the prohibition (of sensitive data processing) does not prevent, among others (and leaving health data aside):

- processing of data where the data subject has given an express consent;
- processing of data on the social, political or religious affiliation or trade-union membership of a person, where the person has himself/herself brought the data into the public domain;
- processing of data necessary for the safeguarding of a vital interest of the data subject or someone else, if the data subject is incapable of giving his/her consent;
- processing of data necessary for drafting or filing a lawsuit or for responding to or deciding of such a lawsuit;
- processing of data where based on the provisions of an Act or necessary for compliance with an obligation to which the controller is subject directly by virtue of an Act;
- the processing of data on religious, political or social affiliation in the operations of an association or corporation professing such affiliation;
- the processing of data on trade-union membership in the operations of a trade union or a federation of trade unions; or where necessary for the observation of the special rights and duties of the controller in the field of labour law;

In the wording used in the Finnish Personal Data Act, the purpose of "carrying out the obligations and specific rights of the controller in the field of employment law" is not found.

[132] *Schnorr*, Erfüllung arbeitsvertraglicher Pflichten und Persönlichkeitsschutz des Arbeitnehmers, in Festschrift Strasser (1983), 113.
[133] Paragraph 9, Schedule 3 of the Data Protection Act 1998.

7. Under **Dutch** data protection law, no general employment exception is provided with regard to sensitive data processing. Some particular references exist, but these are not necessarily employment related. According to the Data Protection Act, data regarding *race* may be processed in view of identification of an individual or in order to give a person from an unrepresented group a privileged position. A particular reference in this respect must be made to the Employment of Minorities Promotion Act,[134] which has as its general goal the reduction of race inequalities in the workplace, the employer should inquire and process data regarding the employee's place of birth, of his parents and some other related information. The employee can refuse to give this information but such refusal has to be given in writing. The ultimate purpose of this registration is that the employer has to draw up a, official report to give governmental authorities, works councils and other representative organs insight into the amount of minority employees employed in his company. Data regarding *political opinion* can only be processed in an employment context of employers with a certain political affiliation, in so far as this is also relevant and linked with the function to be performed. Sensitive data may only otherwise be processed – besides consent – after authorisation of the Data Protection Authority and if they serve a more important interest.

8. In **Sweden**, the Data Protection Act provides that sensitive data may be processed "in order to fulfil obligation or to exercise rights within the field of labour law".

9. In **Portugal** there is no general reference to rights and obligations under employment law in order to permit sensitive data processing (above, reference has already been made to the system of prior authorisation by the Data Protection Authority).

10. In **Ireland**, under the draft legislation, provision is made for lawful sensitive data processing if "the processing is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment".[135]

11. According to article 6, paragraph 2, b) of the **Belgian** Data Protection Act, sensitive data may be processed if "if processing is necessary for the purposes of carrying out the specific obligations and rights of the controller in the field of employment law".

12. The **Luxembourg** draft Bill on Data Protection is somewhat more strict than the Belgian Data Protection Act, in providing that sensitive data may be processed "if the processing is necessary for the fulfilment of the specific obligations and rights of the controller, in particular in the field of labour law, to the extent that it is authorised by a legal provision".[136]

13. In **Denmark**, the Data Protection Act does not provide a general employment law exception to the prohibition of processing of personal data. There is only a specific exception

[134] Wet van 9 april 1998 tot wijziging van de Wet bevordering evenredige arbeidsdeelname allochtonen in verband met het vergroten van de effectiviteit van de wet (Wet stimulering arbeidsdeelname minderheden, Stb 1998, 241 and stb. 1998, 242

[135] Section 4 of the Data Protection (Amendment) Bill 2002, inserting section 2B, 1, b, (ii) after section 2 of the Principal Act.

[136] Article 6, 2, b) of the Draft Bill on data protection.

in section 7,(3) Data Protection Act under which "processing of data concerning trade union affiliation may further take place where the processing is necessary for the controller's compliance with labour law obligations or specific rights". In addition to this, the Danish Employment Discrimination Act (1996) also prohibits employers from requesting, collecting, receiving or using information about race, colour, religion, political opinion, sexual orientation or national, social or ethnic origin of an employee in connection with his or her hiring or during his or her employment.

14. The **Spanish** Data Protection Act does not provide for general exceptions under employment law with regard to the processing of sensitive data.

15. It has been indicated above that, under the **Hellenic** Data Protection Act, the collection and processing of sensitive data, as well as the establishment and operation of the relevant file, needs to be permitted by the Data Protection Authority, when one or more specified conditions occur.[137] However, it is further provided that the prior authorisation of the Data Protection Authority is not required when processing is carried out exclusively for purposes relating directly to an employment or project relationship and is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the aforementioned relationships, and upon prior notification of the data subject.[138]

2. Specific categories of data processing

A. Health or medical data

As far as medical data is concerned, Directive 95/46 mentions 'data concerning health' in article 8, paragraph 1. The regime of protecting personal data concerning health follows that, in principle, of other sensitive data. Still, some elements are added.

In addition to the exceptions under the second paragraph of article 8 of the European Directive, the justifications of the third paragraph of article 8 may become increasingly important with regard to the processing of health-related personal data. According to said paragraph 3, the prohibition of processing sensitive data "shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy".

In this respect, mention has to be made of various labour law traditions in the Member States, in which the concept of occupational medicine exists, as a form of preventive medicine in the employment context, organised through a company practitioner or occupation health services. It is obvious that, besides company health justification, consent will remain an important justifier.

[137] Article 6 Hellenic Data Protection Act.
[138] Article 7 Hellenic Data Protection Act

Self evidently, the issue of health related data does not only pose the issue of legitimacy of processing, but also other principles. Key in the discussion is the issue of data quality, with requirements of finality, fairness, proportionality, accurateness, and so on.

1. General comments and grounds of justification

1. In general in the **U.K.**, consent is almost certain to be the most important condition for legitimising the processing of most medical records. The Data Protection Commissioner has repeatedly insisted that this consent must be 'freely given' This is the definition of consent that is set out in Article 2(h) of Directive 95/46/EC, and although it was not transposed into the UK legislation, the courts will presumably take it to apply. Her interpretation of this requirement is that consent cannot be freely given if employees will lose their jobs for not consenting: in other words, there must be a right to refuse, otherwise the consent will not be valid, and the processing will be unlawful. By contrast, lawyers for the CBI have argued that such consent automatically follows from the employee's agreement to the contract of employment[139]. Although the Commissioner's argument appears the better interpretation of the law, some authors argue that a right to refuse would only exist in practice for workers who are already employed: the explanation is that any applicant for a job who exercised a right not to produce medical data might simply not receive a job offer, and would probably not have any realistic means of redress.

The **U.K.** Data Protection Act also includes that processing of health data is allowed if such processing is necessary for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by – (a) a health professional (as defined in the Act); or (b) a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

In the **U.K.**, a test to determine whether a particular employee is fit for a particular job is a case foreseen by both the ILO and the Commissioner. Under English law, the main limits on the processing of data which this may involve are the general principles of data protection. Exactly how these principles apply will depend very closely on the circumstances in each individual case – of particular interest may be the nature of the medical data, the nature of the job and how these two relate. To take some examples: medical information that has nothing to do with the capacity of the worker to do the job in question will be both irrelevant and excessive; but at the other extreme, where the health of a particular worker might put other people at risk, then this would surely be a relevant concern; and where the testing is for a potentially relevant reason, but then the manner in which the testing is done involves an invasion of the worker's privacy out of all proportion to this reason, then the processing might be unfair.

In cases where there is a legal requirement for health testing – such as in the case of pilots, who must pass medical examinations in order to have their licence renewed – this would

[139] See for example part one of the final draft of the Information Commissioner's "Employment Practices Data Protection Code", March 2002; the comments of the CBI's legal officer were reported as a news item on www.lawdirect.co.uk, 28th March 2002.

probably allow for medical testing without the express consent of the worker; and although the fact of there being a legal requirement would probably satisfy the requirements of fairness and relevance, there would still be scope for review by the Information Commissioner and the courts – especially in cases where the employer goes beyond what is strictly necessary for compliance with the legal requirement in question.

In the U.K., there are important legal limits upon the access that employers may have to existing medical records, but to a lack of clarity remains with regard to medical doctors hired by the employer to conduct employee medical examinations. In principle, section 57 of the 1998 Act renders automatically void any contract term which requires a data subject to provide someone with a copy of his or her health records. Furthermore, if an employer wants a medical report from a medical practitioner who *cares* for the data subject, then he or she will have to follow all the rules and procedures set out in the *Access to Medical Records Act 1988* (employers must have the consent of each data subject before receiving any such report, and in asking for this consent, they must inform the data subjects of their rights under the Act; These rights include the right to see the report before it is sent to the employer; and, having seen it, the right to withhold consent, or to ask the doctor to amend the report before it is sent). However, both of these laws are aimed at medical records from a medical professional who *already treats* the worker. In other words, if the employer hires a different doctor in order to make a report, then this will not be covered by this law. It remains to be seen what will be the position of such reports made by company doctors, as they are considered to be in-between these two positions.

2. **Portuguese** employment law imposes the creation of occupational health services that should cover all workers, viewing the protection of the workers against sickness, disease and injury. These services are responsible for the employees' medical examination and also for applicants' examination on the admission procedure.[140] Besides admission examination to verify workers' fitness, law also determines the tasks of these services: health assessment of workers before their assignment to specific tasks which may involve a danger to their health or that of others, health assessment on resumption of work after a prolonged absence for health reasons (more than 30 days) for the purpose of determining its possible occupational causes, of recommending appropriate action to protect the workers and of determining the worker's suitability for the job and needs for reassignment and rehabilitation[141]. This is complemented by the Portuguese Data Protection Act, also admitting explicit consent as a justification on health data processing but brings in an additional role of the Data Protection Authority. According to article 7.4 of the Data Protection Act and in line with the Directive, the processing of health, sexual and genetic data may be permitted if it is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services. However, when the processing of these data does not have one of these purposes, and if there is no other legal rule allowing it, an authorisation of the Data Protection Authority is necessary (article 7.2 of Data Protection Act). The Data Protection Authority will authorise the processing to the employer when the employee's

[140] Decree Law 441/91, of 14th November 1991, article 13.
[141] Decree-Law 26/94, Article 19.2.c., and 21.1. These rules obey the recommendation concerning occupational health services of OIT - Recommendation 171.

consent has been given or when, on important public interest grounds, such processing is essential for exercising the legal or statutory rights of the controller.

The health professional performs his functions with technical independence, and he is bounded by a medical code of practice. The Decree-Law 26/94 of 1 February 1994 protects the practitioner's independence (article 24.5).[142] The **Portuguese** Data Protection Authority has made some decisions on the subject in which it has determined that only the examination result – fit or not fit for the job – may be disclosed.[143] Fitness is assessed with regard to current illness and to the activity concerned.

3. As regards **Italy**, it must be remembered that the *Garante* must authorise the processing of sensitive data (see above). However, Authorisation No. 1/2000 gives private employers the ability to process data disclosing health, occupational diseases, disability, sickness, pregnancy, child-bearing or breast-feeding, accidents, risk factor exposure, physical and mental qualification to perform specific functions and title to the special protection afforded by law to certain disadvantaged categories. Article 23 of Act No. 675/96 states that health professionals and public health institutions may, even without authorisation from the *Garante*, process personal data disclosing health exclusively, with regard to the data and operations required to safeguard the data subject's bodily integrity and health.

In **Italy**, an employee or prospective employee may only be asked questions concerning his state of health and be medically examined to determine the suitability for his present or future employment. The medical examination can only be made by health professionals or public health institutions.[144]

4. Under the **French** Bill of Law on Data Protection preventive medicine is provided as a category of lawful sensitive data processing, as long as the processing is executed by a health professional or a person who owes a duty of confidentiality.

In the Bill of law, it is also provided that the processing of *genetic data* needs the prior authorisation of the Data Protection Authority, unless such processing is necessary for the purposes of preventive medicine, medical diagnosis or the administration of medical care or treatment.[145]

In **France**, employers are not entitled to appreciate whether the workers' health makes him fit to perform his work. Before entering into any job a worker must be declared capable of doing the job by a *médecin du travail* who is a civil servant. It is only this medical practitioner who is entitled to access medical information concerning the worker. He is therefore the only one to appreciate whether a worker is fit. An employer who does not respect the opinion given by this doctor is liable under criminal law. Any decision taken by the employer based on medical

[142] Data Protection Authorisation 6/2000, published on Data Protection Report of 2000, makes reference to this practitioner independence.
[143] Authorisation 9/96 and 112/96, published on Portuguese Data Protection Authority Report of 1996. Decision 32/98, published on Portuguese Data Protection Authority Report of 1998, Authorisation 9/96, of 3rd January, published on Portuguese Data Protection Authority Report of 1996, Authorisation 91/96 of 11th July, Authorisation 104/97, of 2nd October 1997, published on Portuguese Data Protection Authority Report of 1997, Authorisation 114/97, of 30th October, published on Portuguese Data Protection Authority Report of 1997.
[144] Art. 5 of the Workers' Statute.
[145] New version of Article 25, I, 2° Data Protection Act.

data collected by himself has no legal value and cannot sustain any claim for dismissal or justify a disciplinary measure. Furthermore, any discriminatory treatment based on health is prohibited. In general, the employer is not entitled to collect medical data about the employee and not allowed to ask a worker to provide a medical certificate.

5. Medical examinations of workers or applicants is also lawful under **Spanish** law, but again, under specific conditions. The Data Protection Act includes preventive medicine as a legitimate purpose of data processing.[146] In practice, justification of medical examinations may be found in the fact that it concerns a job which necessitates certain physical abilities, or in the words of the Spanish Supreme Court 'an indispensable requirement for the employment relationship'.[147] Furthermore the employer can obtain personal data on the basis of an explicit and specific legal provision. In some cases the employee is legally obliged to undergo a medical examination as a condition for (further) employment in which case an employee can be sanctioned in the event of his refusal to co-operate.

As far as employee medical examinations are concerned, the Act 13/1995 on Prevention of Labour Risks of 8 November 1995 (henceforth, PLRA) has to be mentioned. Its article 22 — on "surveillance of the health" — provides that «the employer will guarantee to his employees the periodic surveillance of their state of health in function of the inherent risks to the job». Moreover — according to the same article 22 — "the measures on surveillance and control of the workers' health must be carried out by a specialist medical service". The surveillance of the workers' health will be carried out, as a rule, on the basis of previous consent and "always respecting the worker's right to privacy and dignity as well as the confidentiality of all the information related to his state of health".

As far as subjecting job candidates to previous medical examination, the Spanish labour case law seems to be favourable towards this option, at least when this examination appears either legally or conventionally established. This is usually the case with jobs that require a given physical ability. To be mentioned are the Decision of the Supreme Court of 9 June 1987 concerning the medical examination for jobs on board of fishing and merchant crafts — established in a Ministerial Order of 1st March 1973 —; secondly, the Decision of the Superior Court of Justice of Castilla and León-Valladolid of 21 April 1998, regarding the obligatory pre-hiring medical examination for candidates to a job position in the prevention and extinction of forest fires —on the basis of a collective bargaining agreement» —; and, thirdly, the Decision of the Superior Court of Justice of Asturias of 11 June 1999, in connection with prior medical examination in companies belonging to the mining sector — according to article 2 of the Royal Decree 3255/1983, of 21st December, on the Miner´s Statute.

Spanish case law established that an employer couldn't have access to medical files or to any medical diagnosis of employees. This was decided in a case where the employer kept an automated medical data file regarding absence of workers due to illness.[148] In Spain the Law

[146] Article 7, 6 of the Spanish Data Protection Act.
[147] Decision of Supreme Court (henceforth, DSC) of 9th June 1987, *Aranzadi* 4315.
[148] DCC 202/1999, of 8th November, BOE of 16th December; about this decision, *vid.* A. MONTOYA MELGAR, «Ficheros de datos automatizados sobre la salud del trabajador y derechos a la intimidad y la libertad informática», on M. ALONSO OLEA y A. MONTOYA MELGAR, *Jurisprudencia Constitucional sobre Trabajo y Seguridad Social*, t. XVII, Civitas (Madrid, 2000), pags. 300 and ff. Although it was a supposition caused during the validity of the Organic Act 5/1992, of 29th October, nowadays abolished, its teaching stays at the present time.

13/1995, of 8th November[149] on Prevention of Labour Risks declares that «the employer will guarantee to his employees a periodic surveillance of their state of health in function of the inherent risks to the job»[150], bearing in mind that the surveillance of the workers´ health will be carried out, as a rule, with their previous consent[151] and «respecting the worker's right to privacy and his dignity, and the confidentiality of all the information related to his state of health.[152] This law provides several additional guarantees: 1) «the results of the surveillance … will be communicated to the worker concerned»[153], «the access to the medical information of personal character will be limited to the medical practitioner and is not being accessible by the employer or any other person without the worker's express consent»[154]; 2) the employer «will only be informed about the conclusions that are derived from the examinations concerning the worker's fitness to work»[155]; and 3) «data regarding the examination of the workers' health will not be used with discriminatory purposes or to the detriment of the worker»[156].

6. In **Greece**, the Data Protection Act allows lawful health data processing when it is carried out by a health professional subject to the obligation of professional secrecy or relevant codes of conduct, provided that such processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services. According to the guidelines of the Data Protection Authority, medical data may only be collected directly from the employees for justified reasons and specified purposes; such data may be collected in order to comply with specific health and safety regulations in workplaces (workers in restaurants, hospitals, hotels etc.), in order to assess an employee's qualifications for a particular job or task (pilots, drivers etc) or even to prove disabilities or special needs justifying the grant of subsidies from social security funds. As a general rule, all personal data should be obtained, as far as possible, from the individual worker himself and processed on the basis of his informed consent.

7. In **Finland**, particular guarantees were introduced by the Employment Privacy Act. In the first place, the principle of consent is used for the processing of employee health related data. In order to have the right to process employee health data, the employer must collect the data directly *from the employee* and with the employee's *written conse*nt. The data may also be collected from elsewhere, but again only with the employee's written consent (Employment Privacy Act Section 8.1). In addition, there are other safeguards than consent. The processing (including collecting) is allowed only if the objective if it is needed "... in order to pay sick pay or other comparable benefits, or to establish whether there is a justifiable reason for absence, or if the employee expressly wishes his ability to work to be assessed on the basis of data concerning the employee's personal health" (Employment Privacy Act Section 8.1).

[149] BOE of 10th november.
[150] Article 22.1, paragraph 1.
[151] Article 22.1, paragraph 2.
[152] Article 22.2.
[153] Article 22.3.
[154] Article 22.4, paragraph 2.
[155] Article 22.4, paragraph 3.
[156] Article 22.4, paragraph 1.

The employer can organise a compulsory work health care service. This is done in three alternative ways: (1) by acquiring the services from a health centre (referred to in the Primary Health Care Act 1972:66), or (2) by arranging a health care services himself or together with other employers, or (3) by acquiring these services from another unit or person entitled to provide occupational health care services (private sector, mostly).

The Finnish Employment Privacy Act regulates the conduct of examinations or tests, requiring that they shall be carried out by health professionals and laboratory workers with proper training (there is a system of authorising health care personnel laid down by law.). Strictly speaking, an employer may require an employee to furnish him with a doctor's opinion concerning his fitness for work. The requirement of necessity for processing (cf. also Data Protection Act) should nevertheless be met. Normally this assessment regards a prognosis about the person's medical ability to cope with the foreseen work tasks. The data on the job applicant / patient in the register of patients is covered by secrecy according to statutory law. The health care personnel cannot legally hand over or disclose data to the employer, without the consent of the job applicant. The health professional may, however, have an obligation to inform the employer regarding particular circumstances that should be observed at work or in the work environment. In addition, there are specific provisions concerning the possibility of the work health professionals to disclose medical facts normally covered by secrecy. One of these exemptions concerns work that causes special health risks.[157]

Only persons who prepare, make or implement decisions regarding employment relationships on the basis of such data may process data concerning the employee's health. An additional requirement is that the employer shall nominate such persons or specify functions involving that kind of data. It is also required that persons with access to such information may not disclose any of it to third parties either during, or after an employment relationship. (Employment Privacy Act Section 8.2-3). The employer has an obligation to keep any data concerning an employee's health separate from any other personal data collected. (Section 8.3)

8. The **Swedish** draft bill of law on Personal Integrity in Working Life, contains a general prohibition on employers' processing personal data of employees. The regulation makes no provision for consent of the employees. Exemptions are proposed, however, for example if it is necessary for an employer to process personal data on an employee's health in order to ascertain whether the employee is capable of carrying out tasks required by the job. This exemption is intended to be applied when it is necessary for the security of the employee him/herself, of other employees, the workplace or the general public. The employer is also entitled to process personal data on an employee's state of health in order to be able to assess whether the employee has the physical capacity, regarding, for example, sight or hearing, required for the job. Exemptions from the prohibition may also be made for the employer to be able to assess an employee's right to benefits, providing, for other benefits than legal, that the employee him/herself has requested this.

[157] Work Health Care Act Section 18 pt. 1 as an exemption from the Patient's Rights Act

As a general rule, employers should refer to an occupational health service, although the employer could collect medical data on an interview basis. According to the regulations of the Swedish Official Secrets Act, no health related information can be passed over to the employer without the employee's agreement.

9. A most important law in the field of employee medical data protection in the **Netherlands** is the Medical Examinations Act 1997, dealing with employment selection from the angle of personal data protection.[158] Before the implementation of this law there was no comprehensive arrangement on medical examinations in employment, but instead, a major diversity of fragmented rules.[159]

The Medical Examinations Act 1997 provides that:

- Examinations are only allowed if this can be justified by the job itself. If this is the case then an employer can ask job-related questions about the health of the applicant;
- The applicant himself also has the obligation to disclose relevant medical information if he is aware that his medical situation may cause problems with the job he applies for;[160]
- Medical examinations should be limited by the purposes for which they are used and gathered information can only be used for the purpose of the examination. Any interference with the right to privacy has to be in a reasonable proportion to the purpose of the examination;
- Examinations in the pre-employment (i.e. application) phase are prohibited. An Examination can only take place if the employer has decided that, in view of all the other criteria, the person will be hired;
- The employer must communicate in writing the purpose of the examination, the questions that are going to be asked and the planned medical examinations. The medical examiners should be independent and be subject to a policy of secrecy. They only should disclose information to the employer that is necessary for the purpose of the examination.

According to article 4 of the Medical Examinations Act, medical fitness for a job or function includes the protection of the health and safety of the examined individual as well as of third parties at the occasion of the executing of the concerned job.

Primarily, the company medical service (and not the employer himself) is involved in the actual employee medical examinations. However, practice shows that human resources officers are able to collect medical and other sensitive data directly from job applicants or employees during interviews or assessments. In general medical information regarding the

[158] Law 5 July 1997, , Stb. 1997, 365, in force on the 1st January 1998, Stb 1997, 636

[159] See: J.K.M. Gevers, Medische keuringen aan juridische banden, Sociaal Recht 1987-5, p. 159-163, J.K.M. Gevers, Medische Keuringen: de rol van de wetgever, Sociaal Recht 1992, nr. 2 p. 36-40 in particular p. 37, H.E.M. Duynstee-Bijvoet and F.C.B. van Wijmen, Regulering van de medische keuring, Sociaal Recht 1994, nr. 12 p. 345-350

[160] See for example: Hoge Raad 20 March 1981, NJ 1981, 507, (bronchitis), Centrale Raad van Beroep, 26 July 1990, TAR 1990, 195 (alcohol), Kantongerecht Rotterdam 16 March 2001 and 20 July 2001, Jar 2001, 182 in which a waiter did not mentioned his medical problems of his knee while he was aware that the job involved walking long distances and climbing stairs. See also Hoge Raad 2 November 1984, NJ 1985, 192.

employee can only be passed over to the employer with the consent of the concerned employee.

In case of sickness, in the **Netherlands**, the employer can request detailed employee information in order to deal with the question if the employee is still able to work and, if so, what kind of suitable work the employee is still capable of doing. The search for suitable work is an obligation based on the Law on Reintegration of Disabled Workers, but also on the principle that an employer always has to act in good faith ex article 7:611 of the Civil Code.[161] Offering suitable work results in most cases in adjusting the actual workplace. For this purpose, there is a larger need for additional information. Furthermore, the penalty is the civil liability of the employer on the basis of article 7:658 of the Civil Code providing that an employer who has neglected his responsibility of care has to pay for any damages caused by it to the employee.[162]

It is quite evident that the needs of processing medical data bear a strong relation with concerns of cost-control. Budget operations in social security have made the issue of medical testing in employment more important in the Netherlands during the last years. With putting larger responsibilities on employers and '*rerouting*' the financial consequences directly to employers, employers appear to be stimulated to select their new employees on medical criteria.[163] In this perspective employers also want medical information of employees that are already a member of the working staff. These developments are providing tensions in the processing of medical data.[164] In an advisory opinion, the Council of State (*Raad van State*) explained that increased selection on health criteria is a highly unwanted effect of the measures to make the employers more responsible for their sick and disabled employees.[165] In this respect, measures on health-related selection were introduced. First of all there are measures incorporated in different social security acts which have to be regarded as a financial incentive to hire partial disabled employees. Secondly, different acts protect personal medical data. Within a short period of time, a third solution will come into force in the form of Anti-discrimination Act.[166]

10. In **Belgium**, under the Data Protection Act, one of the grounds which make the processing of sensitive data lawful, is the situation where processing is necessary for the purposes of preventive medicine or medical diagnosis, the provision of care or treatment to the data subject or one of his relatives, or the management of health-care services operating in the interest of the data subject, and if those data are processed under the supervision of a health professional.

Labour law imposes a duty of care on the employer with regard to health and safety.[167] However, the performance of medical examinations in the employment context are delegated

[161] See article 46 WAO; See Hoge Raad 3 February 1978, NJ 1978, 248, Hoge Raad 8 November 1985, NJ 1986, 309 and Hoge Raad 13 December 1991, NJ 1992, 441.
[162] S.D. Lindenbergh, Arbeidsongevallen en beroepsziekten, W.E.J. Tjeenk Willink 2000, see for example p. 93 and further.
[163] See about selection on health criteria and the use of medical data: T.C.B. Homan, Risicoselectie van werknemers, hun medische gegevens en hun privacy, Arbeid integraal 2002 nr. 2 p. 46-53
[164] J.C.J. Dute, W.E.M. Duynstee-Bijvoet and I.A.W. de Jong, Gezondheidsrechtelijke aspecten van Wulbz en Pemba, Sociaal Recht 1996-12, p. 336-342
[165] Tweede Kamer 1995-1996, 24 439 p. 8
[166] Tweede Kamer 2001-2002, 28 169 nrs. 1-2
[167] Cf. article 20,2° Law of 3 July 1978 on Employment Contracts.

to a specific corporate medical practitioner. Belgian labour law specially regulates so-called 'company medicine'. This is an arrangement introduced by the law in order to enhance the health and safety or the well being of employees in the workplace. It is concerned with prevention. This company medicine is realised by the company practitioner ('*médecin du travail*'). This is a medical doctor hired or paid by the employer,[168] who takes care of the health of the employees. The relevant provisions can be found in the General Rules on Labour Protection ('GRLP'). In particular, the GRLP regulates medical examinations.

In some cases, a medical examination is prescribed by the law. This is the case for staff that is hired and comes under specific legal categories, which are often indicated as 'functions with an increased risk': workers who are exposed to professional diseases; workers who are entrusted with security tasks; workers who deal with food; disabled workers; workers who have not reached the age of 21. It concerns a general clinical examination. The law determines in more detail which medical data exactly are examined. As it concerns a medical examination during the hiring stage, the granting of a contract of employment is often made conditional upon the medical fitness of the employee as established by the company practitioner conducting the examination. During the employment relationship, there are also several medical examinations which are prescribed by the law. There are periodical examinations for staff employed in 'functions with an increased risk' (see above), as well as ad hoc examinations, e.g. in certain cases of modification of the job, in case of pregnancy, etc. The law also gives an important voice to the health and safety committee.[169] This employee representative body may decide to extend the prescribed medical examination to *all* employees of the company (and not only staff with 'risk functions').

As far as all these legally prescribed medical examinations are concerned, it must be noted that every employee is obliged to undergo the examination (if he or she wants to keep his or her job). The idea is, however, that these examinations are unconcerned with selection, but are provided for the own interests of the workers as well as for society at large.

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

11. As indicated above, the **Luxembourg** Bill of Law on data protection allows sensitive data processing on the basis of specific rights and obligations under employment law. As far as health data are concerned, the processing thereof is allowed for the purposes of preventive medicine, albeit, in principle, with the prior authorisation of the Data Protection Authority, unless it concerns a relationship between a medical doctor and his patient.

The processing of genetic data cannot be justified on the basis of 'specific rights and obligations under employment law'; but would be lawful under the conditions of 'preventive medicine' (as a rule, in this case, with the prior authorisation by the Data Protection Authority).

[168] Depending on whether there is an internal or an external service of prevention operative for the enterprise.
[169] To be established in every company employing at least 50 workers.

12. In general, **Austrian** labour law does not lay down any restrictions concerning "requirements of recruitment", which gives the employer a wide range of freedom to recruit or not recruit a person on the ground of fulfilment of requirements. Under the Data Protection Act, apart form the employment law exception ("rights and duties of the controller in the field of employment law") sensitive data may be processed if the data are required for the purposes of preventive medicine, medical diagnosis, the provision of health care or treatment or the management of health-care services, and the use of data is performed by medical personnel or other persons subject to an equivalent duty of secrecy.

The employer may ask for a medical attest stating that the employee is fit for the job. The standard used for "fitness" is the capability to carry out the job. However, a medical doctor is not allowed to transfer the exact results of a medical examination to the employer. The doctor may only comment on the general state of health in context with the envisaged job.[170] Nevertheless, the (potential) employee can allow *expressis verbis* the disclosure of the examination and all its results to the employer. The doctor may be released from his/her medical secrecy by the patients expressly declaration (see § 54 par 2 nr 3 ÄrzteG). In this case the employer is legitimised the access to the medical files.

Health professionals or medical personnel involved in medical assessment of employees may be the employee's family doctor in a practice (or at health centre of the health insurance institution), an official doctor (Amtsarzt = doctor working for the health authorities), a, company doctor/health centre or persons working for the physician (nurses etc).

13. In **Ireland**, the Data Protection (Amendment) Bill 2002 provides that the processing of health data may be justified on the basis that the processing is necessary for medical purposes and is undertaken by a health professional, or a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health professional. Medical data therefore should be held in the custody of a health professional. In Ireland, it would not be considered employers have access to the employee's medical files or even that the employee's consent would legitimise the access of the employer to the entire medical file.

14. In **Denmark**, the Data Protection Act provides that the prohibition of processing sensitive data shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where those data are processed by a health professional subject to a statutory obligation of professional secrecy.

Far more relevant in the Danish case, is specific legislation regarding health data, referring to medical examinations in the employment context. The Medical Data Act (1996) [171] delimits the conditions under which an employer may have access to and process workers' medical data. It does not deal with the use of aptitude tests, interviews or any other kind of investigation which has the objective of confirming that the candidate for employment has the necessary abilities and skills to perform the work or how good the candidate is in comparison

[170] *Köck*, Arbeitsrechtliche Konsequenzen von Aids (I), RdW 1987, 329.
[171] Law nr. 86 of 24.4.1996.

with other applicants. Nor does this law deal with the extent to which an employer may introduce control measures, such as drug or alcohol tests.

The Act permits the employer to collect information about the employee's health in certain circumstances:

- when the information is relevant to the employee's ability to perform the work in question (Paragraph 2);
- with the permission of the Minister of Labour in order to satisfy essential interests in the safety and health of consumers or others, the environment or other social interests (Paragraph 4);
- after agreement with the union or with permission from the Minister of Labour in order to satisfy essential interests connected with the running of the business or concern (Paragraph 5);
- as a service to the employee, if the circumstances of the working environment make it reasonable and efficient with regard to the employee himself or others (Paragraph 3).

The employee must give the employer, on his own initiative, any information about his health of which he is aware and that is relevant to his ability to perform his job.

The employer may not collect information about the employee's health when the information is not relevant to the employee's ability to perform the work (Paragraph 2(1)) or when the information concerns the extent to which the employee may suffer from an illness in the future.

In addition to rules about when health information may and may not be collected, the Act contains rules intended to ensure the quality of the information collected. These rules concern the co-operation of people with the necessary expertise in examinations, the duty to hold information confidential, and informed consent.

With regard to the cupertino of an expert, the employee may choose either his doctor or a comparable expert who is connected to the workplace in some capacity. It is also essential that expertise is guaranteed with regard to both the performance of the examination itself and the interpretation of the clinical results of the examination.

With regard to informed consent, the law requires that the person who undertakes the examination shall ensure that the employee is informed both orally and in writing about a series of issues. These issues concern the purpose, type and method of the examination, any risks associated with it, eventual consequences that the results of the examination may have for the employee, storage of the results, and the conditions under which this information may be released to others. The employee must also be informed about the possibility that the examination results may affect the employee's self-image and expectations.

The Medical Data Act is based on the principle that the employee must have the possibility to refuse an examination that might reveal a serious illness-such as cancer. The law does not, on the other hand, prevent the employer from taking any action should the employee refuse to participate in such an examination.

The person performing the examination must observe the rules on confidentiality. The employee is the one who receives the examination result and the employer does not have the possibility of collecting information from anyone but the employee. In some circumstances, the employee is obliged to give the information to the employee.

Another relevant law in Denmark is the Work Environment Law of 11 October 1999.[172] Chapter 11 of this law includes provisions authorising the minister of labour to promulgate administrative regulations regarding medical examinations of employees in specific sectors, trades, businesses, or other groups of employees whose work is associated with health risks. The Minister is authorised to require medical examinations before, during and after employment, or even regular examinations. The employer must ensure that the examinations can take place without loss of income for the employees and, as far as possible, during work hours. The employees and former employees have a legal duty to co-operate according to the regulations established by the Minister. The Minister can issue special regulations for young people under the age of 18 with regard to the beginning of their employment with an employer. The Minister can require a school doctor to provide a statement disclosing whether the young person has had any illness or physical problem that might be relevant to his safety and health at work.

Another law to be mentioned is the White-Collar Workers Act of 20 July 1999.[173] This Act applies to all persons employed in the private sector in non-technical or industrial occupations and who work on average more than 8 hours per week and are subject to the employer's management and control. Sections 5 and 7 impose duties on white-collar workers to inform their employers of any illnesses or physical conditions that may prevent them from working. Section 5 provides that absence from work due to illness does not provide legal justification for termination of a white-collar workers' employment unless the worker failed to inform the employer that he or she suffered from that illness at the time he or she was hired. Section 5(4) gives the employer the right to require information, from the worker's medical doctor, about the likely length of time the worker will remain ill. If the worker does not provide the requested information (or consent for release of such information), the employer can legally dismiss the worker. Section 7 concerns a worker's duty to inform the employer at least 3 months before giving birth of the expected date of delivery and when she plans to begin her maternity leave.

15. In **Germany**, the Data Protection Act provides that the collection of sensitive data shall be admissible if this is necessary for the purpose of preventive medicine, medical diagnosis health care or treatment or the administration of health services and the processing is carried out by medical personnel or other persons who are subject to an obligation to maintain secrecy.[174]

Medical examinations are performed by a company practitioner or an occupational health service. Health related information is permitted to be asked from employees if it shows a

[172] Lovbekendtgørelse nr. 784 af 11.10 1999 om arbejdsmiljø.
[173] Consolidated Act (Lovbekenddtgørelse) nr. 622 of 20. 7.1999 regarding the legal relationship between employers and white collar workers.
[174] Section 28, 7 Data Protection Act.

necessary link with the workplace. There is no specific or other criterion to determine fitness. Inquiries with regard to contagious diseases may be made in order to safeguard the health of other employees. Medical examinations require the consent of the individual concerned. The health professional is not allowed to disclose personal data (to the employer) but with the employee's consent. The company practitioner may report the employer concerning the employee's ability to do the work, but will not pass over the medical diagnostics, which remains in the company practitioner's own records.

2. Specific medical examinations

a. General comments

The collection of medical data is regarded as particularly sensitive when individuals are subject to medical examinations (medical testing or screening). Indeed, medical information is not necessarily communicated by an applicant or an employee to an employer. A medical record is usually established on the basis of a medical examination by a medical doctor. In the Member States, such examinations may take place within the framework of the employment relationship by the company practitioner (*'médecin du travail'*) or in the framework of a medical service. It is widely accepted in the Member States that this requires additional guarantees.

With regard to medical testing opens and the principle of finality of data collection and processing is concerned, the issue of discrimination in employment should be mentioned. Indeed, an assessment of the lawfulness of medical data collection by the employer shall be closely connected with the possible illegitimate purpose of employment discrimination. The same is true for most sensitive data collection and use.

In general, the guidance on issues regarding specific forms of examinations, such as drugs and alcohol testing, Hiv and Aids testing, genetic testing, or psychological testing, is considered to be rather weak in the Member States. Sometimes the issue is not regulated, or left open to the general appreciation of the employer, or the medical doctor who is involved in employment related health services.

b. Drugs and alcohol

Drugs and alcohol at the workplace is considered to be an issue in all Member States, but the issue of legal regulation of drug and alcohol data processing by the employer concerning employees, is not always specifically regulated. In some countries, the issue has been specifically addressed by (draft) legislation, in others it is solved on a case by case basis by the competent data protection authority, and still in others it is not addressed. Mostly, lawfulness of drug and alcohol testing will be considered on the basis of the relevancy test and on the condition that sufficient guarantees for the individuals concerned are put in place.

1. In her draft Code of Practice, the **U.K.** Information Commissioner argues that drug and alcohol tests will only be lawful if they are part of a voluntary health programme; or if they are part of an assessment of how drugs and alcohol might affect a particular employee's

capacity to perform his or her job, and such an assessment is justified on the grounds of safety. She stresses that in this second case, the testing must look at *all* drugs that might affect the employee's capacity, including legal medicines: testing for criminal drugs should only be done as part of a police enquiry.

2. In **Greece**, the Data Protection Authority's Code of conduct provides that alcohol and drugs testing in the workplace must be carried out with the prior informed consent of the employees concerned, be a clear element in their individual employment contracts and form part of an explicit health information, education and rehabilitation policy.

3. In **Portugal**, a rule on the commercialisation of alcohol on Public Administration workplaces imposes workers a co-operation duty on preventing accidents related with alcohol abuses[175]. The Portuguese Data Protection Authority has considered that the registering of data on the results of alcohol and drug control should not be a rule for all employees.[176] The systematic registering of these data may be excessive. The register on the results of a control test on alcohol or drug abuses may be proportionate when it comes to some special workers, which may put at risk on other peoples' health and safety. For all other workers whose professional activity does not endanger other people's life or integrity, registering drug or alcohol tests' results may be excessive. Occupational health departments may increase test frequency as a preventive measure.[177]

4. The **Finnish** Employment Privacy Act or any other statutory provision does not directly, explicitly regulate the general admissibility of drug tests at the work place. In the *travaux préparatoires* commenting on Section 6 of the Employment Privacy the constitutional protection of privacy is evoked. With a reference to the Constitution it is noticed that the employer has no right *per se* to oblige a job applicant or an employee to take a drug test. Consequently there should be no harm for the applicant or the employee if he or she refuses a test. Nevertheless it is admitted that the reality might be different. It is also stipulated that only persons who are authorised in health care can do testing for alcohol and narcotics. In addition there are provisions for safeguarding reliable analysis of the samples. The general debate neglected a thorough discussion concerning what ought, should and should not happen when somebody's test is positive.

5. Under the **Swedish** draft bill of law on Personal Integrity in Working Life, exemptions to the prohibition on data protection are proposed, for example, if it is necessary for an employer to process personal data of an employee's health or drug use in order to ascertain whether the employee is capable of carrying out tasks required by the job. This exemption is intended to be applied when it is necessary for the security of the employee him/herself, of other employees, the workplace or the general public. But also in other cases involving the use of alcohol or drugs with clear negative effects on the capacity of the employee to work or on the working environment of other personnel, where it is considered necessary to assess whether the employee is capable to undertake his/her tasks.

[175] *Portaria* 390/2002, of 11th April 2002, Article 7.b.
[176] Authorisation 59/97, published on Portuguese Data Protection Report of 1997; Authorisation 114/98, published on Portuguese Data Protection Report of 1998.
[177] As permitted by article 19.4 of Decree-Law 26/94, of 2nd February.

6. In the **Netherlands**, it is generally accepted that, on the basis of his instruction-prerogative, the employer can state that no alcoholic beverages are to be consumed during working hours. The same goes for the use of drugs. It is obvious that such use can influence the quality of work in a serious way.[178] Although it is the prerogative of the employer to ban alcohol and drugs of the workplace, he has not the unlimited prerogative to test every employee.[179] The Medical Examinations Act is first of all relevant. Questions, test or other examinations on drug- or alcohol use are only allowed if there is a justifiable cause connected with the job itself. If the job can be qualified as dangerous (risks for the employee himself of for third parties) it is possible for the employer to implement an alcohol test as an additional security measure.[180] A contractual clause giving the employer a right to test the employee is not considered to be sufficient in this respect.[181] This can be different if the circumstances of the case are special. An example is a case in which it was agreed by contract that the employer had the right to test the employees on alcohol and drugs at any time he wanted. As this case dealt with a rehabilitation centre for alcohol- and drug addicts, the Court stated that this was allowed on grounds of special circumstances.[182]

7. In **Belgium**, the issue of alcohol and drug testing is not specifically regulated. With regard to drug and alcohol testing, various situations are possible. It is unclear whether a general drug and alcohol screening policy would be valid under Belgian law. Still, in specific circumstances, alcohol tests may lawfully be used in order to prove the drunkenness of an employee in order to establish a valid reason for dismissal.[183] In this case, it is still necessary to obtain the consent of the individual concerned and to involve a medical practitioner.[184]

8. In **Denmark**, drug and alcohol testing is not specifically addressed in the law. The issue will be solved on a case-by-case basis. An industrial arbitration case was reported of 23 February 2000 with regard to drug and alcohol testing. The issue was whether DFDS, a shipping company, could require, without advance warning, the employees on board its ships to provide urine samples for alcohol and drug testing. The drug tests were introduced for safety reasons and involved spot-checking all employees regardless of whether any concrete basis of suspicion existed. Information about the employees who tested positive for drugs or alcohol was then recorded in the ship's diary. It is not clear from the panel's findings whether there was any electronic data processing involved. Nevertheless, it seems that the collection and registration of information about the presence of drugs or alcohol in employees' urine would fall within the scope of the personal Data Directive. The panel accepted the urine testing as falling within the employer's legitimate rights of management and control according to Danish collective labour law practice. The panel's decision did not refer to the Personal Data Act or the Personal Data directive. The employees invoked Article 8 of the European Human Rights Convention (which had been implemented in Danish national law by this time), but it was not discussed in the panel's findings.

[178] See Th.M.G. van Berkestijn, R.J.M. Dillmann and R.M.S. Doppegieter, Het testen van werknemers op gebruik van alcohol en drugs, Medisch Contact 1991, p. 439-442, A.J.C.M. Geers and J.K.M. Gevers, Het alcohol- en drugsgebruik in ondernemingen NJB 1992, p.85-89.
[179] See: H. Uhlenbroek, Werknemers en alcoholgebruik, Arbeidsrecht 1998, 3 p. 18-20.
[180] See also: A.J.C.M. Geers, Alcohol en drugsgebruik in de onderneming, Sociaal recht 1991-5, p. 139.
[181] See: A.M. Luttmer-Kat, De goede werknemer, een achterhaald begrip of dynamisch concept?, in Sociaal Recht de Grenzen verkend, 1994, p. 317.
[182] Kantonrechter Rotterdam, 22 February 1993, JAR 1993, 103.
[183] Arbh. Luik 17 December 1981, J.T.T. 1982, 118.
[184] Idem.

9. In **Austria**, **France**, **Germany**, **Ireland**, **Italy**, **Luxembourg** and **Spain**, the issue of alcohol and drug testing is not specifically addressed. The use of drug and alcohol testing in the employment context follows the general regime of medical data processing in the employment context.

c. Hiv /Aids

As far as Hiv and Aids data are concerned, it is often felt that this issue is not as big as the case for drugs and alcohol. Still, some concrete problems arise in Member States. As regards regulation of Hiv/aids data, mostly, lawfulness will be considered on the basis of the relevancy test and on the condition that sufficient guarantees for the individuals concerned are put in place. The manner in which the issue is addressed may differ strongly from one Member State to another. Sometimes, there is no additional guidance.

In most countries, the issue falls under general principles of data protection, combined with relevant employment law provisions. The common opinion is that information regarding Hiv or Aids primarily follows the regime of health data and medical examinations in the workplace (undertaken by assigned specialists, such as company practitioners or health services) and should not be used to exclude individuals from jobs or to discriminate individuals already employed. The relevancy would remain applicable. The common opinion is, however, that any relevancy of Hiv or Aids for an employment relationship, is determined by a medical practitioner. It is considered as a controversial issue. Secret HIV-testing would be considered as unlawful.

The only countries from which Hiv-related rules may be reported are Italy and Belgium. In **Italy**, Act No. 135/1990 forbids employment discrimination against HIV-infected persons, both in hiring and dismissal, and allows medical investigation only with individual consent. The law also prohibits employer's inquiries about HIV status, both for employment candidates and current employees. The Constitutional Court, however, decided that this law is unconstitutional, insofar as it lacks provisions that make HIV-tests compulsory whenever employee activity is potentially dangerous for third parties. The case arose because a hospital employee refused to submit to an HIV-test and consequently was suspended from her job, albeit with continued payment of her salary. The Court observed that the protection of health runs parallel to the enforcement of a constitutional right, implying not only an active position on the side of the individual who demands to be protected, but also an obligation not to endanger other individuals' health.[185]

In **Belgium**, new legislative initiatives have been taken in order to address the issue of Hiv-testing in the employment context (also addressing genetic testing, but see below). Hiv-testing is in principle prohibited in a double draft bill of law.[186] The Introductory Explanation of the double Bill of law states that the proposal is made in order to tackle abuses of Hiv-related information in employment screening. The principle therefore is that Hiv-testing is prohibited, unless the law provides for explicit exceptions (this still needs to be developed in the Bill of

[185] M. Di Lecce, *Test Anti HIV e Possibili Discriminazioni del Lavoratore Sieropositivo*, *in* L80 596 (1988).
[186] Parl. Doc. Senate, B.Z. 1999, 2-20/1 (employment testing), 1999/2000, 2-116/1 (pre-employment testing).

law). Genetic testing or the collection of genetic information cannot be done before any definite decision regarding the recruitment of job candidates is made. The company practitioner (*médecin du travail*) is indicated as the only player who determines the necessity of a medical (Hiv) test. The employer cannot have access to the actual medical diagnosis.

d. Genetic tests

There is little evidence to suggest that employers are requiring their staff to undergo genetic tests. However, genetic data are considered as a category of extremely sensitive information. As a general rule Member States' laws, either on the basis of specific laws, or on the basis of the general right to privacy (e.g. in the constitution), are rather reluctant with regard to predictive genetic testing in the employment context. Some Member States have addressed the issue of genetic testing in their existing or draft legislation, either in the data protection law, or through specific laws.

As far as genetic testing is concerned, a distinction should be made between 'genetic screening' and 'genetic monitoring'. Both involve genetic testing, but from a different angle. Genetic screening involves predictive genetic examinations, namely the examination of human materials in order to assess particular deviations or specific qualities that may influence the individual's future health. Genetic monitoring is rather concerned with examinations that aim to establish whether the individual genetic structure has been modified or damaged over a period of time, or is such as to provide evidence of potential or past exposure of the individual to certain risks.

While genetic monitoring may still be seen as (at least partly) serving the interests of the individual concerned, genetic screening would come within the framework of predictive medicine, serving the screening of the fittest employee or job applicant. Only in minor cases, as shown below, do Member States' laws make (sometimes implicitly) this distinction.

1. In **Austria**, on 1 January 1995 the Act on Genetic Technology (Gentechnikgesetz) was brought into force, intending to rule on the various aspects of genetic technology. According to Paragaph 67 of the Act, employers are not allowed to raise, ask for, accept or exploit in any way results of genetic analyses of their employees. If the employer demands, accepts or exploits in any way or tries to demand, accept or exploit in any way results of genetic analyses of employees, he commits an administrative offence and has to pay a fine (up to 36 300 €; see Paragraph 109, par 1 n° 1 of the Act on Genetic Technology). Furthermore, genetic tests or analyses are only allowed in case of consent of the concerned person after broad information about the aim and sense of such a test by a medical doctor (see Paragraph 65, Act on Genetic Technology). Paragraph 71 of the Act on Genetic Technology lays down that the institution carrying out the genetic test is allowed to disclose by transmission the results of such a test to employees of the institution whose work is to raise, process or evaluate the data of the examined person. Other persons may be allowed access, if the examined person agrees *expressis verbis* in writing to the disclosure by transmission. The institution has to keep the data in an adequately away from unauthorised persons. Any act contrary to this requirement will be qualified as an administration offence (and fined up to 7 260 €; Paragraph 109, par 3 n° 37 Act on Genetic Technology).

2. Under the current **Hellenic** data protection legislation, genetic testing is not specifically addressed, but is generally considered that the performance of such tests for purposes of employment should be forbidden, on the motives that this constitutes a severe intrusion of the right of personality and human dignity. Articles 2 par. 1, 9A and 5 par. 5 of the revised Hellenic Constitution impose that any legislation allowing genetic testing (or other tests identifying susceptibility to disease) could only do so for objectively justified strong public, or employee health and safety grounds.

3. As for genetic testing, the **U.K.** Information Commissioner notes that there is concern about the potential for such testing, but that there is little evidence of its being used in the United Kingdom; and she argues that it could only be justified where a specific employee has an identifiable genetic condition that could put others at risk, or where it is part of a voluntary screening programme related to the effect that the conditions in a particular workplace might have upon workers with a particular genetic configuration. She also notes that genetic testing are not always reliable, and so in order to meet the legal requirement of fairness, these should be done carefully and under the supervision of a medical specialist.

4. In the **French** Draft Bill of Law on data protection, it is provided that the automated processing of genetic data needs the prior authorisation of the Data Protection Authority, unless such processing is undertaken by medical practitioners or biologists and such processing is necessary for the purposes of preventive medicine, medical diagnosis or the administration or medical care or treatment.[187] No further (specific) conditions are put in place with regard to such processing. It can be noted that under the Draft Bill of Law on data protection, the processing of medical data (not making exception for genetic data) preventive medicine or medical diagnosis does not require individual consent.

5. In **Finland**, the employer is not under any condition permitted to require the employee to take part in genetic testing during recruitment or during the employment relationship. Furthermore, the employer has no right to get to know whether or not the employee has ever taken part in such testing. The provision (Employment Privacy Act, Section 7) is mandatory and cannot be modified by the employment contract (and therefore, individual consent) or a collective agreement.

6. As indicated above, **Belgium** knows new legislative initiatives in order to address the issue of genetic testing in the employment context. Genetic testing is in principle prohibited in a double draft bill of law.[188] The Introductory Explanation of the double Bill of law states that the proposal is made in order to face possible unrest that may exist among employees with regard to possible use of genetic information in the employment context. The double Bill takes as central viewpoint that medical assessment of employees or applicants may only be performed for the purpose of the protection of the public health and not for the purpose to socially exclude people (from employment). Predictive genetic testing is considered to be unlawful. The company practitioner (*médecin du travail*) is indicated as the only player who determines the necessity of a medical (genetic) test. Genetic testing or the collection of

[187] New version of Article 25, I, 2° Data Protection Act (when amended).
[188] Parl. Doc. Senate, B.Z. 1999, 2-20/1 (employment testing), 1999/2000, 2-116/1 (pre-employment testing).

genetic information cannot be done before any definite decision regarding the recruitment of job candidates.

7. In **Germany**, it is generally assumed that genetic testing in employment screening is legally unacceptable. There seems however to be no express legal provision prohibiting the individual's consent to genetic testing, although it may be argued that such consent is not valid.

8. In **Sweden**, there are no specific rules on the processing of genetic data. At the moment, there is a governmental committee that will present a report with proposals for legislation on the protection of genetic integrity. This report is expected to come out before 2004.

9. In **Denmark**, there are no express rules on the processing of genetic data in the employment context. The collection and processing of such data remains nevertheless governed by the Medical Data Act (see above). Indeed, the Medical Data Act itself is based on a 1994 report drawn up by the Gene Test Commission, which was established in 1993 to work out regulations on genetic information. In particular, the Commission was charged with the task of proposing laws or regulations that would prevent employers from selecting employee (or applicants) on the basis of unregulated or arbitrary use of genetic data. The Medical Data Act, which came out as a result, must therefore be considered to cover both genetic as well as other categories of health data. As explained above, the Medical Data Act prohibits, among other things, the processing of information on the employee's health when this information would concern the extent to which the employee may suffer from an illness in the future. This Act, therefore, clearly excludes predictive genetic screening.

10. In the law of **Spain**, the issue of genetic testing is not particularly addressed and seems to follow the general principles of health data processing.

11. The **Luxembourg** Draft Bill of Law on data protection, makes express reference to the processing of genetic data. Genetic data are defined by the draft bill of law as "every type of data that relates to the hereditary characteristics of an individual or relates to characteristics constituting the patrimony of a group of individuals".[189] Genetic data may not be processed for the fulfilment of rights and duties under employment law, even with the express consent of the individual concerned. The Bill of Law still makes exception for data processing in relation to preventive medicine. Such processing, however, still needs the prior authorisation of the Data Protection Authority (unless it is used in a pure patient-practitioner relationship).

12. In **Ireland**, genetic testing has not been raised yet as an issue. The Irish Data Protection Commission has no evidence that such testing is used in the employment context.

13. In the **Netherlands**, genetic testing is considered as an issue, but has not been expressly addressed by the law.

[189] Article 6, 1, b) Draft Bill of Law on data protection.

14. In **Portugal**, genetic data are considered as a specific category of health data. The Portuguese Data Protection Act makes express reference to genetic data. Article 7, referring to the prohibition of sensitive data processing, provides that "the processing of personal data revealing philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, *including genetic data*, shall be prohibited". According to section 4 of said article 7, the processing of data relating to health, including genetic data, shall however be permitted if it is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, provided those data are processed by a health professional bound by professional secrecy or by another person also subject to an equivalent obligation of secrecy and are notified to the Data Protection Authority.

It must be remembered that section 2 of article 7 of the Data Protection Act also allows for health data processing (including genetic data) if the processing of the data is permitted by a legal provision or by the authorisation of the CNPD when, on important public interest grounds, such processing is essential for exercising the legal or statutory rights of the controller or when the data subject has given his explicit consent for such processing, in both cases with guarantees of non-discrimination and with appropriate security measures.

15. In **Italy**, as explained above, a system of prior authorisations by the Data Protection Authority exists. Genetic data also follow this regime. In principle, genetic data may be processed with the consent of the individual concerned. Failing such consent, the processing may be undertaken only upon specific authorisation by the Data Protection Authority, if the processing concerns data that are exclusively relevant to the obligations, tasks or purposes recalled in the authorisation. Genetic data fall under such (prior) authorisation. It concerns genetic data necessary to safeguard bodily integrity and health of the data subject, a third party or the community as a whole. In other words, genetic data that would be processed for preventive medicine, diagnosis or treatment, may only be used for the above mentioned purposes.

e. Psychological tests

Psychological tests or aptitude tests are widely used in the Member States in recruitment and selection policies and practices. A main issue, in this regard, is whether psychological tests can be considered as health data as understood in the Directive 95/46 and whether psychological testing of workers should follow the same regime as medical testing. It seems that according to most Member States' laws psychological testing may come under the concept of health or medical data. Still in practice the collection and processing of data obtained from personality, aptitude or psychological tests do not always follow the medical regime. It would appear that mostly the employer himself would determine the necessity of a particular psychological or aptitude test on the basis of the relevancy principle, leaving therefore a flexible system with regard to psychological tests.

In sum, where the system of medical data would primarily prohibit and only in limited circumstances allow data processing, in practice, psychological testing is used and often considered to be lawful if responding to the general data protection principles as well as the

relevancy-principle used under labour and employment law. Two main groups of countries may be mentioned.

1. A first group consists of countries with no specific, or mere sporadic, references in the law relating to psychological testing (all Member States are meant here, besides Finland and Sweden – see below). These countries tend to include psychological data in the concept medical data. For this reason, psychological testing is considered to follow the regime of medical data processing. In some countries, this has been expressly mentioned in regulations or cases. In **Ireland**, where the Data Protection (Access Modification) (Health) Regulations (1989) includes "psychologist" in the definition of "health professional". In the **Netherlands**, case law has confirmed that personality or psychological tests in general fall under the scope of medical data so that the regime as discussed above applies.[190]

In **Denmark**, psychological data processing would only follow the regime of medical data processing, if the test is designed to discover psychiatric "illnesses" or the signs of an emerging psychiatric illness. In this case, it will be covered by the Medical Data Act (discussed above), since it covers employers' requests for information about their employees' present and past illnesses. It is argued that the problem of distinguishing between a psychological test that is designed to discover an "illness" and one that is simply designed to reveal psychological characteristics may be resolved by considering the type of health professional involved in administering the test. If it is someone with medical training — such as a psychiatrist or neuro-psychologist, one may presume that it is covered by the Medical Data Act. Otherwise it will be covered by the Data Protection Act and general labour law principles (where the relevancy-principle would probably be the main guidance).

In the **U.K.**, data regarding personality, psychometric and handwriting tests – will be considered medical data to the extent that they claim to reveal information about the subject's mental or physical health or condition. Whether or not they are so defined, all such tests will have to satisfy the requirements of fairness and accuracy. The U.K. Information Commissioner takes the view that this means they must always be interpreted by a suitably qualified person; and that the test itself must be sufficiently accurate and predictive to permit a fair and accurate decision to be taken. This restriction may however be difficult to enforce in practice, since such tests are usually made as part of the recruitment process, and, as we have seen, although job candidates might well be able to exercise a right not to take an unfair or inaccurate test, they would have little practical legal redress against an employer who then decided not to employ them because they had refused to take the test.

In the first group of countries, not specifically addressing psychological information, psychological testing or employee assessment, a legal assessment of the lawfulness of psychological data processing is made by applying general principles of law and the general right to privacy. In practice, most problems concern procedural questions, such as the right to have access to psychological reports by job-applicants or employees, rather than the lawfulness or justification (relevancy) of such tests. There is also a lack of case law in order to give much guidance on the issue. In **Portugal**, it is argued that some professions may depend on psychological stability of the worker, like a plane pilot. Some psychological tests

[190] See for example: Centrale Raad van Beroep, 31 January 1991, TAR 1991. p. 138.

may be required to defend a very relevant public interest like other people safety[191]. On the basis of article L.121-6 of the **French** Labour Code all information which employees are asked to provide must serve the purpose of assessing their professional abilities or the individual's capacity to do the job. Only data that have a *direct and necessary* link with the job being offered or with the evaluation of professional abilities being made, can be collected. The courts apply this rule very strictly and prohibit the collection of any data that are related to the employees' private sphere. On the basis of this principle, French law would only authorise psychological investigation insofar that there are necessary and directly linked to the recruitment process. Applicants must be informed of the methods of recruitment used.

In **Spain**, the most significant ruling regarding psychological tests in workers' selection is the Decision of the Superior Court of Justice of Castilla and Léon-Valladolid of 3 December 1996.[192] The Court considered a psychological test lawful under the following conditions: the test consisted of 236 written questions, to be answered in writing; instructions indicated that the questions could only be interpreted with the help of a correction key owned by the psychologist of the company, who is subject to professional secrecy; workers would be able to refuse the test, in which case the psychologist would carry out an interview instead of the test; the test was evaluated by the psychologist of the company by means of a template that does not disclose the names but only if, after evaluation of the complete results, the psychologist would discover any trace of pathology, upon which he would carry out a personal interview with the person concerned; all test results were destroyed by the psychologist afterwards.[193]

In **Italy**, on the basis of Article 8 of the *Workers Statute* of 1970, case law has decided that an employer's inquiries into an employee's appearance, manner of speaking, and "character" are irrelevant to a professional evaluation.[194]

2. Only a few countries expressly address the issue of psychological or aptitude tests.

The use of personality and aptitude assessments has grown to be quite common in **Finland**, in a very wide range of occupations. The tests may be used both in recruiting and later on for planning career and training for the employee. In the Finnish media there has been clear indications that some of the enterprises selling its test services have not used very adequate methods. This was in fact one of the starting points when the Employment Privacy Act was prepared. It seems that there was some discussion about some authorization for the test services. However the solution was another.

Personality and aptitude assessment of the employee's capacity to perform work or need for training and other occupational developments *requires consent* of the employee (Employment Privacy Act Section 5.1). Formally the employer cannot force the employee to take such a test. The actual situation is of course that the employee has reasons to figure that he might make his position considerable weaker by refusing. In order to have some assurance of the

[191] This same opinion may be found on PINTO, Paulo Mota, «Protección de la vie privé et Constitution», G.E.R.J.C. – Groupe d'Etudes et de Recherche sur la Justice Constitutionnelle, Aix-en-Provance, Septembre 2000.
[192] *Aranzadi Social* 3998.
[193] Fact 3.VI.
[194] L. De Felice, *La Tutela Della Persona del Lavoratore (La Giurisprudenza Sugli Artt. 1, 2, 3, 5, 6 e 8 dello Statuto)*, 6 Q.L. 111 (1990).

quality of the tests the employer is compelled to assure himself that the test methods in use are reliable, the persons conducting the assessment are experts and that the findings of the assessment are free from error. In principle and may be also in practice the regulation gives the employee a standing for asking about the quality of the test service.

The practice of personal assessment as a tool of human resource management has also been a concern of the Finnish Psychological Association. Within the frame of the association a manual including an *ethical code* was introduced, especially for personnel assessment and with an explicit reference to the directive and the Employment Privacy Act.[195] One may say that the legitimised psychologists are taking care of their professional and business interests. At the same time it is a question of assessing professional including ethical standards. It is also an activity which can help to make poor quality testing less usual – for the mutual benefit of the employers and the employees/job applicants.

The **Swedish** draft law on the Protection of Personal Integrity in Working Life, proposes a provision stipulating that the processing of personal data collected through personality tests may only be carried out with he consent of the employee. This means also that the employee maintains control over the information resulting from the test. In order to further reduce the risk for violations of the personal integrity, it is also proposed that employers should ensure that personality tests are only undertaken in a satisfactory manner, using reliable test instruments and performed by persons with adequate training.

B. Criminal record data

According to Directive 95/46 the processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law. This principle has been implemented in the Member States' data protection laws. However, this does not take away that in the Member States' practice and within the employment context, use is made of data related to past or present criminal conduct of employees or job-applicants. Employers normally do not have autonomous and direct access to criminal record information. But employers may receive criminal record related data from applicants or employees themselves, often using governmental services to obtain the data concerned. Furthermore, some professional areas have legally laid down requirements regarding past convictions, for example in order to get the authorisation for carrying out a certain profession. It would seem that the practice of employers asking their (future) employees for a certificate of good conduct or a summary from their official criminal file, is not uncommon and primarily serves the employer's business interests. It is clear that this is a useful tool for employers, for instance in light of the employer's duty of care. However, account needs to be taken also of civil liabilities, health and safety of personnel or the public, the protection of goods and materials, the image of the company, etc. It seems that also here, above all, the relevancy-principle is applied.

[195] (Ed.s) H. Honkanen and K. Nyman The Handbook of Good Practice in Personnel Assessment (2002). Finnish Psychological Association.

Besides **Luxembourg** and **Spain**, who implemented the prohibition of processing of criminal data and for which no other specific comments have to be made, the following information may complement the general findings.

1. In **Ireland**, the Garda Síochána (Irish Police) provide a vetting service in respect of prospective employees in a number of areas including child care or other jobs involving child access. Vetting requests by employers or prospective employers are processed with the written consent of the individual concerned and the information supplied is in the form of a "convictions/no convictions" response.

2. Also in **Belgium**, a so-called 'certificate of good conduct and morals' can be obtained from the municipal authorities, which delivers them as a form of public service. These reports show limited details of the criminal record. A person with a 'blanco' certificate does not have a criminal record.

3. Employer access to the criminal records of workers has for some time been an important concern in the **U.K.** Problems arose because the first legislation on data protection – the 1984 Act – gave data subjects a right of access to publicly-held records, such as their criminal record, but did not impose any restrictions upon employers' actions in this area. Employers were then able lawfully to insist that job candidates use their rights of access in order to obtain a full copy of all the data that the police held about them, and that they then pass this record on to the employer (a process called 'enforced subject access'). Moreover, because the 1984 Act obliged the police to give the data subject a copy of all the records that they held, this information included old convictions that were no longer valid under the laws on the rehabilitation of offenders. Efforts have been made to change this situation: the *Police Act 1997* provided for the creation of a special agency – the Criminal Records Bureau – which will keep precise and updated records and disclose only the appropriate data when employers make requests. When this system starts working, new provisions in the *Data Protection Act 1998* will take effect: these will make 'enforced subject access' of certain public records (including criminal records) a criminal offence; and they will render automatically void any contract term that requires such access[196]. The Criminal Records Bureau is due to start issuing 'disclosures' in 2002: but the process has already been subject to long delays, and there remain serious concerns about whether the Bureau's computer system will be able to produce records that are sufficiently accurate and up-to-date to satisfy the requirements of the Data Protection Act[197].

4. In **France**, although there is no specific case law in this area, it is widely accepted amongst legal commentators that employers should not ask job applicants for details of their criminal records, except in very specific circumstances where such information is relevant to the job. Therefore, the employer is entitled to ask only in very few situations where the nature of the job requires checking the workers' morality (transport of money for example). Moreover, the fact that a candidate does not reveal a criminal conviction, even when asked directly about this, does not justify a dismissal if the employer subsequently finds out this once the candidate has been employed.

[196] Sections 112 to 116 of the *Police Act 1997*; sections 55 and 56 of the *Data Protection Act 1998*.
[197] See for example, the Information Commissioner's concerns in her Annual Report for 2001.

5. In **Portugal** lawful inquiries into the employee's past conviction concern mostly situations connected with law professions (lawyers, judges), security related work (night guards[198], private security guards, bodyguards[199], policemen[200]) or military activities[201], health connected professions (doctors, other health staff)[202], or teaching activities.

6. In **Italy**, the *certificato penale* contains information including arrests, offence reports, indictments, convictions, deferred prosecutions, and deferred sentences. It can be requested by the prosecutor, by those directly interested and by public bodies following the conditions enumerated in Article 686-689 of the Italian Criminal Procedure Code (that is, for criminal conviction and security measures). As a general rule, inquiry about an employee's criminal record before recruitment may be allowed.[203] Similarly, criminal convictions may be a just cause for dismissal, as well as for refusal to hire, whenever a connection can be shown to employee contractual obligations.[204] A requirement to disclose one's criminal record has been permitted only when a link can be established to the obligations of the job.[205] Some judges have considered legitimate the request of such records by the employer with regard to those occupations involving childcare, nursing, education, and industrial security.[206] Similarly, criminal records have been considered important in order to justify the employee dismissal, especially for security and police agents in a bank who have past convictions for robbery.[207]

7. In the **Finnish** parliament a government bill of law is under scrutiny (Travaux préparatoires 3/2002). The suggested legislation would concern certain defined jobs where the employee fosters, teaches or takes care of persons under age. According to the proposal the hiring employer has a duty to demand the job applicant to present a criminal record concerning certain crimes defined in the Penal Code. Put in general terms these crimes are sex crimes, crimes involving violence or drugs. The idea is to protect the personal integrity and promote the personal security of persons under age. In the preparation of the project of law there has been an emphasis on balancing the job applicant's privacy rights with the children's protected interests in good care. Also the existing legislation of the same kind of several countries is noticed in the travaux préparatoires (mostly member states of the European Union).

8. In **Sweden**, the committee drafting the bill of law on personal integrity at work, proposes a provision prohibiting the processing by employers of personal data on employees' criminal offences. Exemptions from the law are only proposed for cases in which processing is necessary in order to ascertain an employees' reliability with regard to public security or the security of employer's operations, which also includes security for other employees and for the workplace. Applications of this exemption should be extremely restrictive, according to the proposal.

---

[198] Decree-Law 316/95, of 28th November 1995, article 3.2. Portaria 394/99, of 29th May 2000, article 6.2.C.
[199] *Portaria* 970/98, of 16th November 1998, article 12.C.
[200] E.g., *Portaria* 101/95, of 2nd February 1995, article 3.C; *Portaria* 122/2000, of 8th March 2000, article 24.2.
[201] Decree-Law 289/2000, of 14th November 2000, article 33.5.
[202] E.g., *Portaria* 43/98, of 26th January 1998, article 18.1.C
[203] *See supra* note 17, at 131.
[204] G. Di Pietro, *I Dati Sensibili e la Privacy nel Rapporto di Lavoro*, I D.L. 449 (1998).
[205] V. Frosini, *La Protezione Della Riservatezza Nella Societa' Informatica*, *in* PRIVACY E BANCHE DEI DATI (N. Matteucci ed., 1981).
[206] *See supra* note 24, at 484; c*ontra* Pret. Milan, June 17, 1980, R.g.lav. 82, IV, 148 (comment by Pulitano).
[207] Cass. C 90/2683, C 85/6371, C 82/3592.

9. In **Denmark**, the Ministry of Justice issued a new regulation, based on the new Personal Data Act, on 27 March 2001 regarding processing of personal data in the Central Criminal Register.[208] According to this regulation, the police may issue a statement regarding the criminal record of an individual who is 18 years old or more when that individual requests it. The police may provide the same information to another private person or entity with the written consent of the person whose record is requested. The consent must contain information about what kind of information can be released, to whom the information can be released, and how the recipient can use the information. The information that can be released — whether to the subject or a third party — is listed in the regulation. Time limits ranging from 2 years to 5 years apply, depending on the seriousness of the charge or conviction. For example, dropped charges or acquittals are not included if it has been more than 2 years since approval by the court. Criminal fines are not included if more than 2 years have elapsed since the final judgement. Convictions punished with prison sentences are included up to 5 years from the time of release. There are no regulations or any legislation regarding the extent to which an employer can require such information of an employee. In general, job applicants have a duty to respond to the employer's questions during the hiring process. Whether an employer has the right to require information about an applicant's criminal record should be analysed according to the basic requirement of the Personal Data Law and the case law on the employer's rights of management and control. A minimum requirement may be that the collection of such information must serve a specific and objective purpose.

10. In the **Netherlands**, the Data Protection Act interacts with labour law provisions. With regard to the prohibition of processing data concerning personal criminal behaviour, it provides that the processing of these data concerning personnel shall take place in accordance with the rules established in compliance with the procedure referred to in the Works Councils Act. In the Explanatory Memorandum of the Data Protection Act it is suggested that this article implies an instruction to come to a sort of self-regulation between employer and works council.[209] Reference is made to article 27 of the Works Councils Act. It must be pointed out that, in general works councils are quite reluctant in giving their consent to the processing of personal data concerning past criminal behaviour of employees. The general finding is that one another will depend on the circumstances of the case. In high risk jobs employers are able to demand a full background check. Examples are money transport firms, security firms and financial companies. If there are not special circumstances, employers are not allowed to ask questions about the past criminal behaviour.[210] The so-called certificate of good behaviour, showing the (possible) criminal background of the applicant in question, may directly be obtained by the employer.[211] However, a request for such a certificate has to be sent to the Mayor and should include a written motivation of the employer on the grounds on which he wants such certificate regarding a particular employee.[212] Quite little attention has been paid to the issue of criminal record information in

[208] Justitsministeriets Bekendtgørelse nr. 212 of 27 March 2001.
[209] Tweede Kamer 1997-1998, 25 892, nr. 3 p. 121
[210] See (still up to date): J.D. van de Meulen, De verklaring omtrent gedacht en het strafblad, in Help, ik word geholpen. Na 150 jaar reclassering (1823-1973), Deventer 1973, p. 41-55
[211] Article 19 of the Judicial Records and Certificates of Good Behaviour Act.
[212] See: H. Singer-Dekker, Justitiele documentatie en de verklaring omtrent het gedrag, Tjeenk Willink Zwolle 1991, p. 43 and further

the case law or in the legal literature.[213] In a recent case the Supreme Courts stated that under certain conditions an employer has a right to inquire into the criminal background of an applicant, but this right is severely limited once he hired a job-applicant.[214]

11. The **Hellenic** data protection law has implemented the prohibition of criminal data processing. Still, it is accepted that employers inquire regarding the criminal history of job-applicants if this can be justified on reasonable grounds. The relevant data may only be processed from the candidate himself.

12. In **Austria**, criminal convictions are collected in the Register of Criminal Convictions ("*Strafregister*"), which is kept by the Bundespolizeidirektion Wien (Federal Police Department Vienna) and shows evidence concerning current valid convictions in Austria. Information about the content of the record of criminal convictions may be given to authorities, police, army etc. Persons sufficiently identifying themselves may ask for a certificate of criminal convictions ("*Strafregisterbescheinigung*"), containing the convictions or stating that the record does not comprise criminal convictions. A deleted conviction cannot be part of any communication, nor be disclosed or mentioned in any way.

Many years case law has held that an employee is not obliged to answer questions about criminal convictions or current procedures.[215] This was criticised in the literature.[216] It was argued not to overstate the generality of the Court's statements and it was argued that according to the principle of "*Recht und Glauben*" (good faith, bona fide), applying in the field of labour law, employees are obliged to respond truthfully when asked by employers about a past situation. Current opinion in literature is that the employer may ask a job-applicant or employee about criminal convictions when it inquires for aspects that are included in the envisaged employment of the employee concerned. According to recent case law, an employee is not obliged to give any information concerning deleted convictions.[217] In practice, applicants are asked to show the so-called "*Strafregisterbescheinigung*" (certificate of criminal convictions, see above). In some occupations, there are specific requirements of trustfulness, of which evidence is given by showing a recent "*Strafregisterbescheinigung*". Examples are tradesmen (§§ 13, 62, 339 Gewerbeordnung), midwives (see § 19 par 2 nr 3 Hebammengesetz), psychologists (§ 16 Psychologengesetz) etc.

13. In **Germany**, inquiries regarding an applicant's criminal record may be justified if it relates directly to the job offered. According to section 53 subsection 1 BundeszentralrG *(Gesetz zum Bundeszentralregister)* the applicant may have access to a report regarding criminal convictions and pass it over to employers. Only the concerned individual has an access right to his criminal report. This is based on the individuals' right to decide on his own personal data.

[213] Some examples are Hoge Raad 10 June 1966, NJ 1966, 390, Rechtbank Dordrecht 10 August 1983, NJ 1984, 592 and Rechtbank Den Haag, 26 September 1990, KG 1990, 329 and Nationale Ombudsman 12 August 1985, TAR 216
[214] See: Hoge Raad 29 October 1999, JAR 1999, 255
[215] OGH April 26th, 1983 ZAS 1984, 38; 4076,4569, 10.092.
[216] *Müller*, ZAS 1984, 189; *Petrovic*, DRdA 1986, 209;
[217] OGH 18.10.1994, DRdA 1995, 397 mit Bespr v *Mazal*; *Schwarz/Löschnigg*, Arbeitsrecht9[2001], 226.

C. Trade union data

The collection and further processing of trade union data is obviously related with the fear of employment discrimination. Because of this most Member States prohibit the use of trade union data processing, except for very specific purposes. Obviously, this is strongly connected with national traditions in labour relations. It appears that in **Scandinavian** countries (with rather co-operative collective labour relations) this is not a strong issue, as equally in the **Netherlands** (with rather low union density).

The most common lawful processing of trade union membership data by an employer would normally be data relating to the deduction from wages of trade union subscriptions (in many Member States employers often provide the facility of deducting subscriptions from wages and passing them on to the trade union). This relates to the so-called check-off clause, which under normal employment regulations implies the express individual consent. It may also be that employers need union related data in order to refund union dues (like is the case in **Belgium**).

1. Under the **Austrian** Data Protection Act, data regarding trade union follow the general regime of other sensitive data. Under labour law, the principle of relevancy leads often to the conclusion that the employer can inquire on trade union affiliation data in the case of "*Tendenzbetriebe*". In Austria, the leading opinion is that an employer's question about a prospective employee's membership in a trade union or a political party is not allowed[218], but only in so called "Tendenzbetrieben", aiming at political acting (trade unions, chambers, confederation of employers, political parties, newspapers published by a political party etc) as the employer should have the right to recruit employees going along with the goals and aims of the undertaking. In businesses where an employee's membership would not be controversial to the undertaking's aims or interests such questions are not allowed. Once the employment contract is concluded, questions about the membership may be asked in any company as trade union fees are often withdrawn from the employee's salary.

2. As far as **Belgium** is concerned, it has been indicated that the Data Protection Act takes a very restrictive approach with regard to sensitive data processing in the employment context. In Belgium, article 27 of the Royal Decree of 13 February 2001 stipulates that if the processing of personal data relates to sensitive or health-related data and is only made lawful on the basis of the consent of the data subject, this processing is still prohibited if the controller of the processing is the current or potential employer of the data subject. This prohibition is lifted in case the data processing has the purpose of providing an advantage to the data subject.[219] The official preparatory documents of the Royal Decree give the example of the payment of trade union allowances.[220]

Under the Belgian Data Protection Act it remains however possible to process sensitive data, including trade union data, in light of the rights and obligations under employment law. Yet, under Belgian labour law, it may be questioned whether employers would have a legitimate interest in knowing the trade union affiliation of employees. This certainly becomes an issue

[218] *Mayer-Maly*, Grundsätzliches und Aktuelles zum Tendenzbetrieb, BB 1973, 769; *Egger*, Rechtsprobleme bei der Anbahnung von Arbeitsverhältnissen, DRdA 1982, 93ff.
[219] Article 27 Royal Decree 13 February 2001.
[220] Report to the King, Preparatory Works, *B.S.* 13 March 2001, 7859.

at the port of entry, in the recruitment and selection stage, but also later during employment. There is a risk that employers will use this information in their decisions regarding selection, promotion, rewarding, and dismissal. In this respect, Collective Bargaining Agreement (CBA) n° 38 provides that (prospective) employers may not make selection decisions on the basis of the trade union affiliation of a job applicant.[221] The employer may only inquire with regard to such affiliation in case he is able to show that this is relevant for the job (e.g. it is argued that in case of a job with a trade union (or trade union related) organisation, the employer may take trade union membership of the applicant into account, e.g. to verify whether the applicant has not committed himself already to another trade union. In some case however, the knowledge by the employer of an employee's trade union affiliation becomes inevitable, certainly during the employment stage, e.g. when the employee is acting on behalf of a trade union at the employer's premises, when employees are candidate for 'social elections'[222], and so on. However, apart from CBA nr. 38, there are no other specific laws in this respect.

3. In **Denmark**, the Personal Data Act prohibits the processing of data regarding trade union membership status. However, with regard to data on trade union membership status, it is provided that the processing of such information is permitted under certain specific conditions: if the data subject has given his express consent, or if the data subject himself has made the information public, or if processing of the information is necessary for the employer to fulfil his obligations under labour law or collective agreement.

4. In **Finland**, during the last decades, the knowledge about trade union membership has not appeared to be a dramatic issue. Through collective agreements it has been a common pattern that the union member consents in writing to a procedure where the employer deduces his union fee from the salary. The employer then sends the money to the union. In the Finnish Data Protection Act, trade union membership is listed as sensitive data in accordance with the directive (Section 11, pt 2). As a derogation from this prohibition, a clause exists permitting "the processing of data on trade-union membership in the operations of a trade union or a federation of trade unions, where the data relate to the members of the union or federation or to persons connected to the union or federation on a regular basis and in the context of the stated purposes of the union or federation, and where the data is not disclosed to a third party without the consent of the data subject" (Section 12, 1, pt 8). Processing of data on trade-union membership is also permitted when it is necessary for the observation of the special rights and duties of the controller in the field of labour law. (Section 12, 1, pt 9).

5. In **France** the new Bill of Law on data protection, treats trade union membership data as sensitive data. Only on the basis of individual consent, such data may be processed. Also French Labour law would consider as automatically unlawful any collection, storage or processing of data if unrelated to the workers' ability to perform his work. Insofar as these data do not present a direct and necessary link with the evaluation of the workers' activity, any collection of these data would violate article L.121-6 of the French labour code. Employers, therefore, do not have right to collect data concerning employees' trade union

[221] Article 2bis CBA nr.38.
[222] These elections are held every four years to elect the workers' representatives for the company's works council and health and safety committee.

activities if such data is irrelevant to the evaluation of the workers' professional abilities. Furthermore any employer who process data concerning trade union membership may be found liable for discriminatory treatment. The only fact to process these data infringes article L.122-45 of the Labour code which prohibit any discriminatory treatment based on trade union membership.

6. Under the **German** Data Protection Act, data regarding trade union membership is regarded as sensitive data and the processing thereof is, therefore, in principle prohibited. Still, exception is provided for individual consent. As indicated above, no general exception is made for labour or employment law purposes in the act.

7. Under the **Hellenic** Data Protection Act, the processing of trade union membership data are expressly prohibited, without authorisation, either in combination with the consent of the individual concerned[223] or when processing is carried out exclusively for purposes relating directly to an employment or project relationship and is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the aforementioned relationships, and upon prior notification of the data subject.[224]

The Data Protection Authority's code of conduct does not specify the conditions of lawful access to such data. One should consider that any employer's request of such data from job applicants would be disproportionate with the purposes of the employment contract. Under Greek labour law, it is very questionable whether employers would have a legitimate interest in knowing the trade union affiliation of employees or job applicants, seen the risk of employment discrimination.

8. The **Irish** Data Protection (Amendment) Bill 2002 provides, with regard to sensitive data, including trade union membership data, an exception to the prohibition of processing relating to the rights and obligations under employment law. However, in **Ireland**, the only trade union membership data that an employer would normally lawfully process would be data relating to the deduction from wages of trade union subscriptions. In a significant ruling, the **Irish** Data Protection Commissioner has decided that such data could not be used for any other purpose. The particular case involved the Department of Education which had used data about trade union subscriptions to identify teachers who were members of a trade union. These data were used to withhold pay from teachers who had been on strike. The Commissioner found that this breached the principles of fair obtaining, purpose specification and compatible use.

9. According to Article 8 of the **Italian** Workers' Statute it shall be unlawful for an employer, for recruitment purposes or during the course of the employment relationship, to make enquiry or have enquiry made into political, religious or trade union opinion of a worker. It is argued that an employee's opinions about trade unions are irrelevant in evaluating professional competency.[225] The only exception to this broad prohibition is found in connection with employers engaged in activities that are ideologically oriented, for example,

[223] Article 7 Hellenic Data Protection Act.
[224] Article 7 Hellenic Data Protection Act
[225] Cf. M .Grandi & G. Pera, *Commentario Breve Alle Leggi sul Lavoro*, CEDAM EDITORE 484 (1996).

political parties, trade unions themselves or religious foundations and associations.[226] Even in this case, a restrictive interpretation has been suggested: the ban on investigations would be lifted only for employees performing tasks that are directly linked to the employer's ideological stance.[227] For employees performing non-ideological functions, employer's investigations would continue to be illegal.

With regard to sensitive data, as indicated above, the Data Protection Authority has granted some bona fide authorisations *ex officio* either to individual controllers (i.e. employers) or, by means of a general provision, in respect of specific categories of controllers or processing operations. It has done so, for a large range of employment purposes, with regard to data disclosing political opinions, membership of parties, trade unions, associations or organizations with a political or trade-union aim, as well as any data relating to trade-union activities or offices and the deduction of fees due for trade-union services.

10. Under the **Luxembourg** Draft Bill on data protection, trade union membership data are considered as sensitive data, and follow the same regime of protection. As indicated above, an exception to the prohibition of processing exists with regard to specific obligations under employment laws (see above).

11. In **Portugal**, as the processing of data concerning the affiliation to trade unions has been considered a part of salary administration, its processing by the employer has been admitted by the Portuguese Data Protection Authority, as under Portuguese law[228] employers may process directly the fee to deliver the trade union.[229]

12. In **Spain**, the Data Protection Act provides that files created for the sole purpose of storing personal data which reveal the ideology, trade union membership, religion, beliefs, racial or ethnic origin or sex life remain prohibited.[230] But it is accepted that data regarding union membership may be used for specific legal purposes, such as the deduction of union dues.

13. In **Sweden**, the provision in section 13 of the Data Protection Act prohibits the processing or registration of personal data of trade union membership and other sensitive data. These data may nevertheless be processed when the data subject has given his consent or when he has manifestly made the data public.

14. In the **Netherlands**, the processing of data by an employer concerning membership of his employees with a trade union is prohibited on the basis of the Data Protection Act. Processing of this information can only be done on the basis of consent or by the 'trade union concerned or the trade union federation to which this trade union belongs, provided that this is necessary to the aims of the trade union or trade union federation'. In practice, employers

226 F. SANTONI, LE ORGANIZZAZIONI DI TENDENZA E I RAPPORTI DI LAVORO GIUFFRÉ. (1983)
227 *Id.*
228 Trade Union Act (215-B/75) published on the official bulletin Diário *da República* of 30th April 1975.
229 Portuguese Data Protection Authority' Decision 15/95.
230 Article 7, paragraph 4 Data Protection Act.

appear not to be so much interested whether (certain) employees are members of a (certain) trade union.

15. There were also long-standing concerns in the **U.K.** about the use of personal data on trade union membership and activities: a minority of employers consulted 'blacklists' of union activists and members before recruiting new employees. Legislation in the 1990s created certain limits upon this practice[231], but it would seem that the Data Protection Act has now made the operation of such lists unlawful in almost all circumstances. Information about an individual's membership of a trade union is sensitive personal data (as is data about that individual's political beliefs, which might cover the unlikely case where a trade union activist is not actually a member of a union); and the only possible condition which could legitimise the processing of such data would seem to be the consent of the data subject. It is perhaps to be imagined that this consent will rarely be forthcoming; and although, as in the other cases, there may be little that a job candidate can do to prevent an employer from consulting such a blacklist, it would seem quite within the capabilities of the Information Commissioner and of the courts to prevent the activities of the organizations which maintain such lists.

So in the U.K., employers may wish to use personal data on trade union membership for perfectly legitimate reasons – such as the deduction from wages of trade union subscriptions – but they will need the employee's express permission for this, and they must not then use the information for any other purposes. Where there is a legal obligation to keep such records – as for example would seem to be the case where a union official is to be disciplined (because special legal protection applies to such workers) – then the legal necessity would legitimise the processing, so consent would not be required, but all of the other Data Protection Principles would have to be respected.

Closing remarks

1. All Member States protect, in general, the right to privacy. The concrete form given to such protection may however differ and is self evidently influenced by the respective national legal and political traditions. Some Member States have an express constitutional provision regarding the right to privacy or one of its aspects, other primarily rely on civil laws or international conventions (of which the European Convention on Human Rights (1950) is the most important) that are applied in their legal system. Most labour and employment laws only refer to privacy in a general way, and often indirectly, not mentioning the concept as such but using other general principles (like 'good faith' or 'trust and confidence').

Although there are some (more or less academic) discussions with regard to the horizontal effect ('*Drittwirkung*') of constitutional (privacy) rights, it may be concluded that all Member States, either through constitutional concepts or through civil law concepts, protect privacy in the employment context in general and abstract terms. Due to the respect that the Member States have to provide in light of their international obligations, a sufficient abstract level of privacy protection is ultimately granted under article 8 of the European Convention on Human Rights.

[231] See the *Trade Union and Labour Relations (Consolidation) Act 1992*, section 137; and the *Employment Relations Act 1998*, section 3.

2. With regard to the law on workers' data protection, the basic point of reference is Directive 95/46/EC of 24 October 1995 on data protection as well as the Member States' labour and employment law traditions.

Directive 95/46 applies to the employment relationship. As Member States have either implemented or are in the processing of implementing Directive 95/46, employees enjoy (or will be enjoying soon) the protection that it offers. In their scope of application, national data protection laws make no exception for the employment situation (upon fulfilment of all other conditions of applicability of the relevant data protection legislation). When processing workers' personal data, employers should therefore be aware of the general data protection principles laid down in the Directive 95/46 (and the corresponding national legislation), such as *legitimacy* (personal data may only be processed for limited purposes), *finality* (personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes), *transparency* (information to the data subject is required regarding data processing relating to him or her), *proportionality* (personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed), *confidentiality and security* (technical and organisational measures to be taken), and *control* (supervision by data protection authorities).

3. As far as labour and employment law traditions in the Member States are concerned, a common feature is the concept of subordination, implying that an employment relationship, i.e. the individual relationship between employer and employee, is a subordinate relationship. On this basis it is accepted that, in view of the specific context of the employment relationship, the employee's perspectives of exercising fundamental rights including the right to privacy, are relatively affected. Still, it is commonly accepted that the employment relationship does not imply a waiver by an employee of his fundamental rights.

Apart from some exceptions, referred to above, labour and employment laws do not typically address the issue of workers' privacy. However, some concepts have been developed in reconciling employer and employee interests in this respect. The '*relevancy principle*' can be found in practically all Member States' systems, often derived from labour and employment laws and general legal principles. The relevancy-test implies that the employer may only exercise his right to information – or his right to collect and process personal data of workers – in so far as this is relevant for the employment situation. The principle is therefore primarily concerned with the need for justification in data collection and further processing and with the requirements of data quality. The principle of relevancy receives many forms and formulations in the Member States. It generally remains rather abstract and vague, although some Member States' laws have used the principle in more concrete employment situations.

A specific concept that has developed over the years, more or less as a specific form of application of the above mentioned relevancy-principle, is the notion of '*Tendenzbetrieb*' or, literally translated as '*Tendency company*'. With this term, companies are indicated which are biased or show a certain social, ideological, political, religious, … affinity. Examples are religious organisations, political parties, or various non-profit organisations. With regard to such organisations, the employer's interest in collecting specific personal, including sensitive,

data of workers may increase in relation to the specific biased (but legitimate) business purposes.

Under some Member States' labour and employment laws a role is foreseen for the workers' representatives (mostly the works council) with regard to personal data protection. In general terms, this role is rather of a procedural nature and where consent of the works council is required, it cannot replace individual employee consent. This role is often implied (on the basis of existing collective labour law provisions), rather than express.

4. As far as workers' data protection is concerned, there is a strong interaction of privacy and labour laws. This also implies that the application of the general data protection principles, as laid down in Directive 95/46, to the employment context, needs to take account of Member States' labour laws. As labour laws are strongly inter-linked with the Member States' own traditions, this may, at least partly, explain differences in approach and different solutions given to certain issues.

The interplay of data protection law and labour law can be noticed, for example, in applying the principle of legitimacy of data processing in the employment context. Directive 95/46 and Member States' data protection laws, provide that data processing is legitimate if necessary for the purposes of the legitimate interests pursued by the controller, after a balance-test is made with the rights and interests of the data subject (cf. article 7, (f) Directive 95/46). Opinion 8/2001 of 13 September 2001 the Data Protection Working Party affirms that this criterion requires a balance to be struck between the interests of the employer and the interests of workers.[232] Such balance is actually referring to the relevancy-test, used in the sphere of Member States' employment laws. It also requires to make an evaluation of the specific rights – and the extent of such rights – of the employer which are provided under national employment law, including the understanding of managerial prerogative and freedom of enterprise, or of liabilities and responsibilities of business.

If the issue of the processing of sensitive data is taken, it also becomes clear that it is strongly related with the issue of discrimination in employment. As Directive 95/46 makes an exception from the prohibition of processing sensitive data when necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law (cf. article 8, 2, (b) Directive 95/46), it is likely that the actual level of protection of the employee's privacy will depend on the content of national employment laws. For example, to the extent that employment laws prohibit discrimination on certain grounds (or by use of sensitive data) will determine (for example limit) the employer's possibilities to justify the processing of workers' sensitive data.

The issue of individual consent, as a basis for legitimate data processing, shows that in regulating workers' data protection, it becomes almost inevitable to touch upon labour law issues. In labour law, the issue of 'free' consent of employees (or job applicants) is highly discussed. Taking this into account, Belgian data protection law provides that if the processing of personal data relates to sensitive or health-related data and is only made lawful

[232] Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, Adopted on 13 September 2001, 5062/01/EN/Final, 15.

on the basis of the consent of the data subject, this processing remains prohibited if the controller of the processing is the current or potential employer of the data subject. This prohibition is only lifted in case the data processing has the purpose of providing an advantage to the data subject. There is no precedent of such provision under Belgian labour law and it is not unlikely that the concerned data protection provision may influence labour law doctrine.

The interplay between data protection law and employment law has also become clear in countries that have regulated employment privacy in specific legislation, like e.g. France or Finland. Both the Finnish Employment Privacy Act as well as the French labour code provide rules that apply data protection principles to the employment context.

5. The general data protection principles that are laid down in the European Directive 95/46, and the Member States' implementation measures thereof, appear to be quite clear in their abstract meaning. Nevertheless, it is felt that specific guidance with regard to the employment situation is desirable. To this end, some Member States have drafted clarifications or codes of conduct, or even specific laws, in order to make the data protection principles more specific or concrete with regard to the employment context. The respective approaches in the Member States in this respect are quite different.

In the first place, as suggested above, it is not unusual that the application of general principles, such as the data protection principles laid down in Directive 95/46, to the employment context, gives rise to interpretation and different solutions.

A difference in approach with regard to the protection of sensitive data may be noticed. Some countries provide for a system of prior authorisation by the national data protection authority or some exclude individual consent. It may also be noted that many Member States have not used the same wording of the employment law -exception mentioned in article 8, 2, (b) of Directive 95/46 ("processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law") which may have more restrictive results.

In some cases, Member States have not addressed certain issues of data protection in the employment context. This is the case, in general with the issue of drug and alcohol at the workplace. While it is considered as an issue in all Member States, the legal regulation of drug and alcohol data processing by the employer concerning employees, is not always clear. In some countries, where the issue has been specifically addressed, it is not done so in a comprehensive way. It is therefore primarily on case law that Member States rely, although few cases in the field are available. Mostly, lawfulness of drug and alcohol testing will be considered on the basis of the general data principles and the relevancy-test and on the condition that sufficient guarantees for the individuals concerned are put in place.

As far as genetic data are considered, there is no evidence that such data are used by employers. The experts have noticed an increased attention of genetic tests within the framework of work-related insurance schemes. However, there is little guidance in the Member States' law with regard to this issue. No rules were found addressing the relationship

between employers and insurance companies and the personal data regarding workers that can be exchanged.

Little attention is also given in the Member States to psychological testing, although it is considered to be an issue. A main question here is whether data revealed through psychological tests can be considered as health data as understood in the Directive 95/46 and whether psychological testing of workers should follow the same regime as medical testing. It seems that according to most Member States' laws psychological testing would come under the concept of health or medical data, although this is a matter of opinion and few case law guidance is available. Furthermore, in practice, the collection and processing of data obtained from personality, aptitude or psychological tests do not always follow the medical regime. It would appear that mostly the employer himself would determine the necessity of a particular psychological or aptitude test on the basis of the relevancy principle.

It is not clear whether violations of the employee's right to privacy are *de facto* efficiently sanctioned. Most sanctions would arise from specific laws addressing specific issues of privacy or data protection. Many data protection laws are enforced through criminal sanctions and/or administrative fines, so there is a cause of action. Furthermore, in most countries employees will also be able to undertake legal actions against employers for privacy violations, on the basis of existing rules of civil or employment law. While data protection authorities and labour inspectorates have sometimes wide investigation competencies, efficient investigation of private actor violations does not always seem to be quite evident in practice. Practical problems may also exist with regard to the production of evidence of unlawful data processing (e.g. in cases where employees are not aware of data collection or use of certain data). The issue of workers' data protection seems to give rise to so-called 'silent violations', i.e. employees, their representatives or official bodies are not always aware of the existence of a violation of data protection principles or, generally, of privacy.

6. As mentioned above, there seems to be a clear understanding regarding the abstract principles that should be in place. But it is not always predictable and clear on beforehand what results these principles would have in their practical application. This may be an inherent feature of the general data protection principles and of abstract employment law principles (such as 'relevancy'). It may also leave wide scope of appreciation of judges in the Member States. There are diverging opinions on whether or not such result is desirable, although in many cases, it is seen as problematic. Furthermore, it is felt that some issues of workers' data protection, more in particular in the field of medical and psychological testing, may deserve additional guidance.

Where the opinion is that more clarity or additional guidance is desired in the field of employment, there is no uniform attitude among the experts whether such clarity should come from further abstract regulation or from case law.

It is argued that, within a few years, there might be enough cases addressing the issue of workers' personal data, clarifying how the general data protection principles have to be applied in the field of employment. In this respect, clarification would be a matter of time. Dealing with the issue on a case by case approach would probably also offer a degree of

flexibility, for example to adapt a data protection principle to the specific elements of a case or to anticipate new circumstances, like the evolution of technology. But it is not excluded that further abstract regulation might offer a similar degree of flexibility. It is also argued that, while it may be possible to give some examples of the application of abstract data protection principles, it would be difficult to formulate new abstract rules, adapted to the employment situation, which go further (in terms of clarity) than the principles of Directive 95/46. This argument may well be sustained if reference is made to the principle of legitimacy, or the principle data quality (including relevancy, proportionality, adequacy, …). Nevertheless, it still seems that some issues of workers' data protection could be further addressed, for example in the field of the processing of sensitive data. It is questioned whether particular guarantees or clarifications with regard to drug and alcohol testing, Hiv/Aids-testing, genetic testing and psychological testing, to which the general data protection principles apply, should be left to case law (e.g. conditions of lawful testing, individual guarantees, collective guarantees, professionalism, role of employer, use of testing results, …). Furthermore, the ILO Code on workers' data protection is an example that shows that abstract clarifying rules are possible and could be useful.

Whether or not there is a case for an initiative on European (EU) level, should be addressed. One angle of approach is the free movement of information and another the free movement of workers. Having regard to the different approaches and the application of principles in the Member States with regard to workers' data protection, the risks to the free movement of data within the internal market resulting from such differences, may be evaluated. Transnational disclosure or the circulation within the EU of employee data may, for example, not be hindered because of a lack of clarity or different approaches with regard to the legal treatment of such data in other countries. It could be argued that the fact that employee personal data are subject to different restrictions in one country than another, or lack of clarity in protection in certain countries, may pose potential obstacles to the functioning of the internal market. This would involve a European Directive as a method to address the issue. The third preamble of Directive 95/46 makes reference to (former) articles 7a an 100A (internal market) of the EC Treaty, and provides that the establishment and functioning of an internal market in which the free movement of goods, persons, services and capital is ensured, require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded. It is also provided, in the ninth preamble, that "Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners"; and "within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community". In view of the fact that the employment (or labour relations) sector is a major field in which data processing takes place within the Community, and taking into account that employment privacy, including workers' data protection, is increasingly becoming an issue in the Member States and the Community, a situation whereby lack of clarity or lack of protection, or disparities within Member States would remain or increase, may be considered to be problematic. Therefore, there is a potential case for a European initiative in order to remove obstacles to intra-Community trade and the functioning of the internal market,

although further study may be needed with regard to the actual and practical impact of the lack of clarity or lack of protection, or disparities on the free movement of data.

As indicated above, the second 'freedom' to be addressed is the free movement of workers (article 39 EC Treaty). It may be that in the Member States measures exist that, while not discriminatory either in law or in fact, nevertheless impede access to the market of one Member State or more Member States. According to the case law of the European Court of Justice, national measures may breach article 43 of the EC Treaty – arguably, *mutatis mutandis*, article 39, paragraph 1 EC Treaty – which are liable to hinder or, make less attractive, the exercise of the fundamental freedoms guaranteed by the Treaty.[233] The question is whether a situation whereby there is a lack of clarity with regard to the application of data protection principles to the employment situation, or a lack of protection with regard to some issues of workers' data protection, or where disparities within Member States would remain or increase in this field, may run contrary to the principle of freedom of movement of workers as provided in article 39 EC Treaty. There seems to be less believe that such obstacle(s) would exist in the case at hand. It may be argued that the effect of the situation in the Member states in hindering the freedom of movement of workers is not overall certain and still quite indirect in order to be likely to hinder such free movement. It seems to be in accordance with the case law of the European Court of Justice to conclude that there is no strong case under article 39 EC Treaty for a European Directive, as the study did not show evidence of direct hindrance of access of workers to the labour market of one or more Member States.[234]

There is a strong belief among the experts that alternative routes of initiative on European level should be further examined. Instead of taking a relatively strong regulatory viewpoint, a valuable contribution may arise from promotional or supporting acts. A first alternative would be the drafting of a European code of practice in the field of workers' data protection. This would suit the concept of regulation implied in Directive 95/46 which provides the possibility of (draft) Community Codes, in contributing to the proper implementation of both national and community provisions, taking into account the specific features of the various sectors (article 27 Directive 95/46). It may be interrogated whether a European initiative would add value to already existing codes, such as the one drafted on workers' data protection within the framework of the International Labour Organisation. However, both in its structure and content, a European code could meet the specific requirements of adapting and applying the general data protection principles of Directive 95/46 in the employment context, and take into account the specific labour law traditions of the Member States. It may also show to be valuable in contributing to the free movement of information within the Community and the operation of the internal market, and serve as an alternative for a (binding) European Directive. It would also be able to give guidance on the uniform application of European Community law in this matter.

An alternative route for abstract binding or non-binding regulation may be the formulation of a set of clarifications. Such clarifications may serve as concrete examples or cases of good practice, or of how the general data protection principles may be applied in the employment

[233] Case C-55/94, *E.C.R.* 1995, I-4165.
[234] Cf. Case C-190/98, All ER (EC) 170.

context, in conformity with Directive 95/46 and taking into account the Member States' labour law traditions. This rather proactive method may meet the requirements of flexibility which is often referred to in arguing for a case-by-case approach, while anticipating the fact that there is no case law providing for sufficient clarification. Although it would not concern case law delivered by a court, and although clarifications would be of a non-binding nature, it might be proposed to issue clarifications on a more permanent basis, in order to cope with new developments, both in law as well as in fact.

It is considered necessary to involve the social partners in the process of developing any of the above mentioned European initiatives.

*

Protection of workers' personal data in the EU: surveillance and monitoring at work.

Professor Frank Hendrickx
University of Leuven
University of Tilburg

With the collaboration of:

Catarina Castro
Xosé Carril Vásquez
Michele Colucci
Michael Forde
Armin Höland
Taufan Homan
Annamaria Johansson
Leonidas Kanellos
Jens Kristiansen
Nora Melzer
Gillian Morris
Sophie Nerbonne
Anders von Koskull

Manuscript completed in October 2001

I. Introduction

This paper contains the report on the outcome of the project “Protection of workers’ personal data: the case of surveillance and monitoring”. This project has been financed by the European Commission, DG Employment and Social Affairs.

A. Subject of the study

The main purpose of the project was to undertake a European comparative study on the issue of **“**Protection of workers’ personal data in the European Union: the case of surveillance and monitoring”. The study has focused on the situation in the various Member States of the European Union and will carry out to determine, among other things:

- the extent of the present Member State laws and guidelines on this subject (how is it regulated, under what conditions may an employer monitor, how and to what extent are workers informed and give their consent, etc.);
- whether the current laws and guidelines adequately protect the worker, while balancing the worker's right to privacy against the legitimate business interests of the employer;
- the types of surveillance and monitoring currently in use by employers, or future types;
- suggestions or recommendations on appropriate guidelines and/or laws which would ensure suitable protection for the worker in relation to his/her monitoring and surveillance by the employer, addressing general principles or the extent to which workers should be informed.

B. Methodology

The project has been realised on the basis of European wide research. The research has been undertaken under the supervision of the contractor with the co-operation of a group of experts, specialised in the field of employment privacy. Each expert has prepared a country study regarding the situation in the relevant Member State. The national research activities have resulted in a general discussion at a closed expert meeting on 4 and 5 October 2001, organised at the Law Faculty of the University of Leuven (Belgium). During this seminar, country surveys were further explained and discussed and policy options or suggestions regarding European initiatives have been looked upon in the examined field of study.

The group of experts is composed as follows:

AUSTRIA
Dr. Nora Melzer
University of Graz
Institut für Arbeidsrecht und Sozialrecht

BELGIUM
Prof. Frank Hendrickx
University of Leuven

DENMARK
Prof. Jens Kristiansen
University of Copenhagen

FINLAND
Prof. Anders von Koskull
Swedisch School of Economics and Business Administration

FRANCE
Mrs. Sophie Nerbonne
Chef de la division des affaires économiques
Commission Nationale de l'Informatique et des Libertés

GERMANY

Prof. Armin Höland
Martin-Luther-Universität Halle-Wittenberg

GREECE
Prof. Leonidas Kanellos
University of the Aegean

IRELAND
Prof. Michael Forde
Law Society of Ireland

ITALY
Dr. Michele Colucci
University of Salerno

LUXEMBOURG
Prof. Frank Hendrickx
University of Leuven

PORTUGAL
Mrs. Catarina Castro
University of Coimbra
Comissão Nacional de Protecção de Dados

SPAIN
Prof. Xosé M. Carril Vásquez
University of Coruña

SWEDEN
Dr. Annamaria Johansson
University of Lund

THE NETHERLANDS
Prof. Taufan C.B. Homan
University of Tilburg

UNITED KINGDOM
Prof. Gillian Morris
Brunel University

The general report departs from the horizontal approach of comparativism. This means that it integrates all relevant information regarding Member States horizontally, throughout the general theme and its appropriate sub themes.

C. Background and general context of the study/project

Before providing an overview of the results of the study, an introduction will be provided with background regarding the subject of employee data protection and the case of surveillance and monitoring. This is done from a general European perspective with some general comments and thoughts with regard to the subject. This background information constitutes the general context of the study undertaken.

1. General problem of workers' data protection and surveillance and monitoring

1. The growth of information technology not only has drawn the attention of a number of scholars examining the implications for personal privacy. Also business practice is confronted with several new policy questions in this regard. In terms of the workplace, human resources management has received new concerns as regards workers' data protection and particularly in the case of surveillance and monitoring.

2. Automated and computer supported information systems may be seen as new and better ways of organising work and doing business. However, computers and software seem to have a bigger impact on the personal and working life of people than manual filing systems. Indeed, with the introduction of modern information and communication technologies, the issue of privacy has moved at the forefront. These new technologies have lead to tremendous changes in the working environment. The importance of information and information resources gave rise to information management and the introduction of systems of data processing, inclusive personal data. The employers' needs of employee information have been translated into 'personnel information systems'. They are used as a tool within the general framework of human resources management, which goes beyond mere salary administration. Another example of increasing data processing is the use of 'personnel surveillance systems'. These techniques allow employers to monitor workers' presence at work, their whereabouts, their activities, performances, use of time, etc. Examples are: electronic recording, video-surveillance, time registration, black boxes, badges, data logging and, finally, the use of software for the monitoring of e-mail and internet use.

3. Internet and e-mail are one of the most striking problem creators in the workplace and is therefore, at the moment, the most well known problem as regards monitoring. The growth in employee use of e-mail has been accompanied by employee use of employer equipment (as well as "company time") for non-employment related activities. This has often led to misuse of such equipment. This prospect has been accompanied by employer efforts to monitor employee use. Occasionally, such monitoring goes beyond the workplace, whereby employers screen employee home pages and demand the removal of references to the company, or, whereby employees are discharged because of the content or nature of there web visits. Employers are concerned about employees devoting their working time to personal business – considered to be a problem – such as trading on the world wide web, surfing for private purposes, playing and gambling, etc. Attention is also given to company liability for employee action, such as for contractual liability, infringement of property rights, and so on. Similar concerns do exist with regard to conduct such as harassment of co-workers, especially when predicated on sex, race or other statutorily protected category, or when amounting to (criminally sanctioned forms of) stalking. The use of cameras at the workplace is another issue, which is quite under debate at the moment.

4. The above may lead to the conclusions that privacy, more specifically workers' privacy, is under pressure. However, it should nevertheless be clear, when studying employee privacy, that specific attention must be drawn to the particularities of the employment environment. Indeed, an employment relationship implies, as a general rule, a subordinate relationship. This means that the employer is contractually allowed to exercise authority over the employee. Still, the individual is only subject to the authority of the employer in so far as this is embodied in the specific employment relationship, in other words, in so far as this is relevant for the employment contract. Furthermore, the existence of an employment relationship does not take away the respect of the right to privacy and human dignity. More in particular, monitoring issues will need to take the employee's right to privacy and the protection of his/her personal data into account.

2. EU policies

1. The study has taken into account the **policy background** in light of which the study of employee data protection should be conducted.

One of the main objectives outlined in the **Social Policy Agenda** of the Commission (COM2000/379final, 28.6.2000) is to ensure the development and respect of fundamental social rights as a key component of an equitable society and of respect for human dignity, including the protection of personal data of individuals in the employment relationship. With a view to reach these goals, the Social Policy Agenda defines as a major road of action the launching of a consultation of the social partners – on the basis of Article 138 of the Treaty of Rome – with regard to data protection.

The issue of 'electronic monitoring', which includes forms of surveillance and monitoring such as internet and e-mail monitoring, the use of cameras, recording devices, dataveillance etc., indeed received an increased attention among the Member States of the European Union. It

has been widely discussed amongst the media, governments, data protection authorities, academic institutions and business.

2. Still, it would appear that there is a **certain lack of clarity and transparency with regard to the rules** that should be applied **in the area of (electronic) surveillance and monitoring of workers**.

It seems to be that such lack of clarity and transparency comes from the specific nature of the subject. Indeed, the juridical assessment or regulation of surveillance and monitoring may be the outcome of the application / implementation of different sets of rules and principles.

a. In the first place, there are basic Community instruments such as **Directive 95/46/EC of 24 October 1995 on data protection** (*O.J.* 23 November 1995, L281/31). It is common knowledge that the impact of this Directive has been paramount, as it caused a dynamic of amending/modifying of the Member States' data protection legislation along the lines of the general rules and principles, laid down in said Directive. Such rules and principles to be found could be labelled as, e.g., *legitimacy* (personal data may only be processed for limited purposes), *finality* (personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes), *transparency* (information to the data subject is required regarding data processing relating to him or her), *proportionality* (personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed), *confidentiality and security* (technical and organisational measures to be taken), and *control* (supervision by data protection authorities). The case of monitoring of workers has given rise to discussion with regard to the interpretation of the principles and their application in the employment context.

b. Secondly, **Directive 97/66/EC of 15 December 1997** (*O.J.* 13 January 1998, L24) concerning the processing of personal data and protection of privacy in the telecommunications sector has in its turn required further consideration with regard to employee monitoring, e.g. as far as the scope of the permissible exceptions to the principles of privacy and confidentiality are concerned (cf. Article 5 of this Directive).

Furthermore, it should be stressed that workers' data protection, including surveillance and monitoring, should be evaluated along the lines of **social policy and labour law principles and traditions**. In this respect, labour policy is confronted with new challenges and must adapt to new issues rising up in the information society, e.g. as far as information to the workers or managerial prerogative is concerned. Indeed, labour lawyers and social policy makers within the Member States are realising that labour law principles must play a role in respect of fundamental rights and human dignity. Furthermore, some techniques of human resources management seek to tie the employee to ever-tighter bonds of loyalty to the employer and so to heighten employer controls of employee behaviour and attitude. Some controls may be connected to employer concern for liability (e.g. sexual harassment, vicarious liability, …), other may be driven by employer concern for its business image in the community, or may arise out of the felt need to display the exercise of power over the workforce.

c. The aforementioned general rules and principles, applying to all forms of personal data processing, have been / are being adapted to the specific employment context, including specifically monitoring and surveillance, by some Member States (such as, e.g., the United Kingdom, the Netherlands, Belgium, Finland). Other Member States are still in the process of recognising that there may be a need for regulation in some way.

3. In light of the above, and in particular taking into account the objectives and actions laid down in the Social Policy Agenda (see above), the Proposed Study will examine **the content and the extent** of workers' data protection as presently to be found in the laws and principles of the Member States. As it may be that the various Member State initiatives and approaches appear diversified, uncoordinated or even incompatible in some way, suggestions will be made with regard to appropriate guidelines/regulation in relation to monitoring and surveillance by the employer. In this respect, the framework of reference will not only relate to

existing guidance to be found at Member State level, but also to possible direction or instruction coming from international standards, with strong emphasis on the European level.

II. Legal framework in the Member States

A. General

An examination of the legal framework of the Member States learns that there is no consistent and uniform approach of employment privacy issues. The privacy protection of employees is dealt with through a combination of constitutional laws, general privacy laws and employment laws. As a general rule, privacy laws are not specifically written for the employment relationship and often do not take into account specific principles or categories of employment and labour laws. On the other hand, most employment laws have not addressed the issue of employee privacy. Furthermore, some Member States have general constitutional provisions on privacy, where others do not have a constitutional concept of 'the right to privacy', while still others may not really recognise a generic concept of 'constitutional rights'.

If Member States are compared, the approach of regulating privacy may also be different. Most Member States have complied with the European Directive 95/46/EC on data protection. Still, the national implementation of this directive has not given rise to a specific regulation or manner of regulation of the issue of monitoring and surveillance. As already indicated, it often concerns an interdependency of data protection laws, criminal provisions, employment law principles, civil law provisions, codes of practices, etc.

B. The situation in the Member States

1. Constitutional right to privacy

In all of the Member States, the right to privacy is guaranteed to an employee vis-à-vis his employer in some way. However, the manner in which this is done, may differ strongly.

A primary issue is the constitutional guarantee of the right to privacy. Some countries do have a clear constitutional provision on this right, like is for example the case in **Belgium**, **Finland** or **Spain**, but it in most countries it remains difficult to invoke the constitution directly vis-à-vis a private employer. Furthermore, it must be noted that some countries do not know a general constitutional right to privacy (like e.g. **Austria**, **Denmark**, **Ireland**) or even do not know a generic concept of privacy (like e.g. **Italy**). But, even these countries, still adhere to some form of fundamental privacy protection, e.g. by protecting specific issues, like telecommunications or correspondence, or the integrity of the home, and so on.

It must also be noted that the **U.K**. has a different constitutional tradition than the continent. It does not have a written constitution, nor, until recently, could it be said to recognise a generic concept of `constitutional rights'. However, the Human Rights Act 1998, which came fully into force on 2 October 2000, brings the UK closer to recognising a generic concept of `constitutional rights' by giving further effect in domestic law to rights and freedoms guaranteed by the European Convention on Human Rights. Still, the principle of parliamentary sovereignty remains. Nevertheless the principle of parliamentary sovereignty remains in that a `Convention right' does not override legislation of the UK Parliament that cannot be interpreted compatibly with it'.

The right to privacy generally covers information privacy, medical privacy, integrity, protection of communication and/or correspondence and personal autonomy or self-determination.

Greek law, jurisprudence and legal theory traditionally accept that the right to privacy is a derivative of a broader right to personality. The latter is an absolute, autonomous, non transferable "composite" or "framework right" since it also includes several particular dependent rights such as right to respect of honour, reputation, personal integrity and

professional image[235]. Any unlawful act of any third natural person, legal entity, public or private authority may violate the right to personality. The provisions on privacy protection described below equally apply on personality. However, although the term "privacy" is used in many statutes, there is no legal definition of it. In practice, this concept has mainly been specified by case law and legal literature. According to legal writers, privacy may be defined as the person's "right to be left alone"[236]. The private sphere is the minimum space which is necessary to the individual if he is to exercise his personal, professional and social activities without interference by curious third parties. Private life includes but is not limited to sensitive personal information about family life, health, sex, religion, friendship, profession, property, political beliefs, ideas and other data characterising a person that this person wants to keep secret or outside the reach of publicity, even in workplace. The Hellenic Constitution of 1975, as revised on 18 April 2001[237]**,** contains a set of fundamental rules covering privacy and the broader right to personality.

In **Germany**, the constitutional doctrine on personality rights, privacy and data protection is essentially anchored in four articles forming part of the so-called basic rights part of the Constitution. Pursuant to article 1 (1), manifestly drawing historical lessons from national socialism, human dignity is inviolable. To respect and protect it is the duty of all state authorities. Article 2 (1) of the Constitution guarantees everyone the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or against morality. Article 10 (1) guarantees the privacy of letters as well as the secrecy of post and telecommunication as inviolable. Article 13 (1) is of classically succinct wording: “The home is inviolable.”

At present, various scholars debate regarding the manner in which the constitutional right to privacy should be protected in private labour relationships. The discussion relates to the doctrine of horizontal effect (“Drittwirkung”). Indeed, while most people would still agree that a worker enjoys privacy protection, it remains unclear whether he or she may directly invoke the constitution or, alternatively, should rather rely on existing provisions of civil law or employment law, referring to concepts such as ‘fairness’, ‘reasonableness’ or ‘good faith’.

The Portuguese constitution may be regarded as quite modernistic in this respect. **Portugal** has a specific constitutional provision on data protection (article 35 ‘Use of computerised data’), and some other constitutional provisions connected with privacy. These provisions are part of the Portuguese constitutional framework since 1976 (Constituição da República Portuguesa de 1976). These constitutionally guaranteed rights have to be respected both by public and private actors, meaning that they also have to be protected in private labour relationships. The so-called horizontal effect or ‘Drittwirkung’, is provided in article 18 which expressly states that constitutional provisions on rights, freedoms and guarantees are directly applicable to, and binding on, both public and private bodies.

In the **Netherlands**, article 10 of the Dutch Constitution states that everyone has the right to respect of his privacy. Also here, it is still unclear whether this article may be applied in the relationship between employer and employee. The Dutch constitution primarily covers the relationship between State and citizens. It is certain, though, that article 10 would have an indirect effect on other legal rules so that one could argue that article 10 is indirectly applicable to employment relationships.

Apart from the theoretical discussions, it must be observed that some judges apply the constitution in employment cases, either directly or indirectly. In a recent case regarding video surveillance, the *Cour de Cassation* (Belgian Supreme Court, 27 February 2001) has directly applied article 22 of the **Belgian** constitution (right to privacy). Sanctions however, must be based on other legal provisions (civil law, employment law, criminal law, …).

---

[235] Dr Leonidas Kanellos, Greek Report, pages 189-200, in: *International Privacy, Publicity and Personality laws*, edited by Michael Henry, Butterworths, Reed Elsevier, London 2001.

[236] Sourlas, *Commentary on articles 57-60 of Civil Code*, see also Dagtoglou, *Press and Constitution,* 1989.

[237] The Hellenic Constitution was recently revised by resolution of the Parliament dated 6 April 2001, which was published in the Official Gazette on 18.4.2001.

It is a matter of fact that the legal systems in the Member States must be in conformity with the European Convention on Human Rights (4 November 1950). Therefore, article 8 of the European Convention on Human Rights plays an important role in guaranteeing the right to privacy. Reference may also be made to other articles of this Convention, for example to article 3, which provides that no one shall be subjected inhuman or degrading treatment. In **Denmark**, compared to the national constitutional framework, a more general and probably more effective protection of the right to privacy follows from article 8 of the European Convention of Human Rights.

2. Civil law

In most Member States, the relationship between an employer and an employee is governed by civil law (in so far as labour law does not provide specific derogations).

It is therefore no surprise that privacy issues come up under civil law concepts or tort laws (e.g. **Austria**, **Portugal**), under rubrics as 'good faith', (e.g. **Belgium**), 'loyalty' (**Finland**) or 'trust and confidence' (**U.K.**). For decades already, **German** case law has brought the general personality right under the scope of the basic tort law provision of section 823 (1) of the **German** Civil Code (*Bürgerliches Gesetzbuch*). The right of personality which is guaranteed by Articles 1 and 2 of the **German** Constitution has significance also for the employment relationship and the rights and duties which are the result of it.[238] Any violation of the right of personality of an employee by the employer is equivalent with a violation of contract obligations. In the case of an objectively illegal encroachment upon his personality right the employee has a right, based on an analogous application of sections 12, 862 and 1004 German Civil Code, to apply for an injunction.

In **Greece**, privacy violations of employees by the employer and vice versa are sanctioned by articles 57- 60 of the Civil Code which define the general rules for protection of personality. According to article 57 a person who has suffered an unlawful offence on his personality has the right to claim the cessation of such offence as well as the non-recurrence thereof in the future. The above provisions may also be invoked by the employer against any employee who is liable for the damage caused to the employer through privacy violations which resulted from fraud or negligence.

3. Employment law

An employment relationship, i.e. the individual relationship between employer and employee, is a subordinate relationship. Indeed, leaving aside the details, **all** labour laws in the Member States define the employment contract as a contract whereby the employee agrees to perform the work, for a certain wage, under the authority of the employer. The main labour law principle implies that subordination by the employee to the employer is not an 'economic' subordination, but a legal subordination. Furthermore, this subordination may be considered as the general rule in the employment context.

However, the fact that an individual concludes an employment contract with an employer, and therefore agrees to work in a subordinate relationship, does not necessarily imply that he waives his fundamental rights.

Still, it must be recognised, that the employment contract **limits the individual's freedom** and the exercise of his fundamental rights. In other words, the employment relationship has a significant impact on the employee's fundamental rights and the exercise of his right to privacy.

Most employment laws do not directly refer to the issue of privacy. But there are a few exceptions. For example, **Finland** is currently preparing an "Act on Protection of Privacy in Working Life". The supervision of the Act on Protection of Privacy in Working Life is to be divided between the Data protection agencies and the authorities for protection of working

[238] *Bundesarbeitsgericht* BAGE 64, 308, 312; cf. BAGE (GS) 48, 122, 136, 139.

environment. This clearly shows that the issue of employment privacy goes further than data protection and involves the broad range of employment and labour laws and principles.

Another example is **Spain**, where the Employees´ Statute of 1995 dedicates some of its articles to the topic of the protection of the privacy and dignity of the worker, but it does not seem to offer a complete and coherent treatment in the protection of the worker's intimacy.

4. Data protection law

Practically all Member States, with some exceptions (like **France** or **Luxembourg** who are preparing new laws) have transposed European Directive 95/46 of 24 October 1995 ("the Directive") into national legislation. This law is commonly considered as a quite technical and detailed law and, what more is, it does not appear to be specifically designed for the employment situation, while it nevertheless remains applicable to it.

In some Member States, Data Protection Authorities have formulated opinions or codes of practice or made studies regarding the applicability of some of the principles laid down in the data protection legislation to the employment relationship, often specifically involving the issue of electronic monitoring in the workplace, like e.g. **Belgium, France, The Netherlands** or the **U.K.** and **Portugal** (both in preparation).

5. Sanctioning privacy violations

It must be noted that most of the Member States do not provide for special designed **sanctions** as far as privacy violations by the employer is concerned.

Therefore, as far as the sanctioning of privacy violations is concerned, it always remains necessary to invoke other legal provisions which may be applicable in the case *in concreto*. This shows that both impact and protection of the constitutional right are mostly indirect. In Member State practice, most sanctions would take the form of the nullity of a contractual clause, or would be translated in the unlawfulness of a dismissal (upon which the payment of a severance indemnity may become due) or a disciplinary action by the employer. It should be noted that most countries enforce privacy through specific criminal acts. In these cases however, only specific violations are sanctioned and it does not provide for the protection of a general right to privacy.

Furthermore, it may be pointed out that it is very likely that most privacy disputes arise in situations where the employment relationship has already come to an end or where it is difficult for employer and employee, due to the circumstances or the nature of the dispute, to continue the employment relationship.

It must be noted that the level of protection is far from uniform among the Member States. It must also be pointed out that some countries are actually lacking sufficient protection mechanisms. For example, the protection of employees' privacy is largely unexplored territory in **Irish** law. There is no legislation that protects the right to privacy generally nor in the employment context. In 1988, the Data Protection Act was passed but it does not apply to all employment-related data and goes no further than what is required by the Council of Europe Convention of 1981 on the subject. In other Member States the general rule regarding privacy violations appears to be that they are translated in the payment of an amount of money (for incurred or punitive damages) or through criminal sanctions. There are no sufficient elements to conclude whether this manner of protection would be adequate.

C. Interplay between the data protection Directive and the telecommunications data protection Directive.

This is a specific issue which may imply particular consideration. In many Member States questions arise with regard to the interplay between the Data Protection Directive and the Telecommunications Data Protection Directive 97/66/EC of 15 December 1997 (OJ, L24, 13 January 1998).

Most Member States appear to have difficulties in dealing with the double application of the two Directives. While the Data Protection Directive is, besides few exceptions, generally clearly implemented into national law, it seems not always to be clear how and to what extent the Telecommunications Directive fits into general data protection principles or into existing labour and employment laws.

Article 5(1) of the Telecommunications Data Protection Directive requires Member States to ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular they are obliged to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14 (1).

The Directive permits two exceptions to this principle, firstly article 5(2) provides that Article 5(1) shall not affect any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication; secondly article 14(1) allows Member States to adopt legislative measures to restrict the scope of the obligations and rights provided for in Article 5 when such restriction constitutes a necessary measure to safeguard, *inter alia*, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system.

In the **U.K**., where the two directives have been implemented by different statutes, the Data Protection Directive by the Data Protection Act ('DPA') 1998 and the Telecommunications Directive by the Regulation of Investigatory Powers Act ('RIPA') 2000, the relationship between these two provisions has caused considerable difficulty. The DPA 1998 imposes restrictions on monitoring and surveillance which are not present in RIPA or in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 made under the authority of RIPA. A more integrated approach to this area would undoubtedly be welcome.

Similar problems occur under **Belgian** law. In Belgium, there is not much discussion with regard to the interplay between the Data Protection Directive 95/46/EC of 24 October 1995 and the Telecommunications Data Protection Directive 97/66/EC of 15 December 1997. The Data Protection Directive 95/46 has been implemented in Belgian law by the law of 11 December 1998 which amended the existing Law of 8 December 1992 with regard to data protection. The Telecommunications Data Protection Directive 97/66/EC has not been implemented by one single measure. As far as the protection of telecommunication is concerned, the implementation of Directive 97/66 can be found in Article 314bis of the Criminal Code and Article 109terD and 109terE of the Law of 21 March 1991. However, the content of these articles, except for some minor elements, already existed before the entering into force of the European Directive. Furthermore, it remains unclear what link there would exist between the two sets of rules. If the idea would be that Directive 97/66 should constitutes a specification of the principles of Directive 95/46, there is no express link in Belgium between the national laws which implement both Directives. If any link can be made between the implementing measures of both Directives in Belgium, such link would rather appear to be contradictory. Indeed, the Law on Data Protection (8 December 1992) sets a frame of general principles for the monitoring of telecommunications of workers by their employer, but the specific criminal laws on telecommunication strongly deviate from these principles, in the sense that they depart from a more strict prohibition of electronic monitoring.

Problems also occur in **Germany**. Directive 97/66/EC has been transposed into German law by three different legislations. The confidentiality rule of Article 5 of the Directive has become legislatively broken down in the Telecommunications Act, especially in the sections 85 (telecommunications secrecy) and section 89 (data protection), and in section 3 (principles) of the Telecommunications Data Protection Ordinance (TDSV) which has become issued under Section 89(1) of the Telecommunications Act. The problem now is that there is a differentiated and explicit legislation on secrecy and data protection for the private use situation which complements the employment relationship by an offer-demand-relationship and transforms the employer into a "service provider". By contrast, no legal secrecy rule

applies to telecommunication for business purposes. This does not mean that there is no legal protection concerning contents and circumstances of workplace telecommunication. For these situations the established principles of the case law of the Federal Court of Labour on employees' privacy within the organisation remain in force. The situation remains unsatisfactory.

In **Denmark**, there is no discussion with regard to the interplay between the Data Protection directive 95/46/EC of 24 October 1995 and the Telecommunications Data Protection Directive of 15 December 1997. The Data Protection Directive has been implemented through the Processing of Personal Data Act of 2000. The Telecommunications Data Protection Directive is implemented through Act no. 418 of 31 may 2000 on Competition- and Consumer conditions on the Telemarket. The Telemarket Act does not regulate personal data protection as such, and can hardly be seen as a more specified legislation as far as the main principles in the general Data Protection Act concerns.

III. Monitoring and surveillance

A. General comments

The importance of information and information resources has given rise to new tools in the sphere of human resources management, such as ‘personnel information systems’ and ‘personnel surveillance systems’. New techniques allow employers to monitor workers’ presence at work, their whereabouts, their activities, performances, use of time, etc. The most common examples are the monitoring of telephone communications, the monitoring of internet and e-mail and camera surveillance. However, other forms like time registration, black boxes, badges, data logging and so on, may also be introduced in the workplace, but the main discussion still regards internet, e-mail and cameras. These features have often common characteristics, purposes or problems so that it can be assumed that common legal principles may be applied to such different forms of monitoring.

1. No uniform law

What is striking is that, in most Member States, there is no single and uniform rule or law on the legal assessment of electronic monitoring of workers. In most of the cases, the assessment takes into account various existing employment laws and principles, as well as data protection laws. Involving labour law seems obvious, as electronic monitoring at work directly relates to rights and obligations arising from the employment relationship. However, the relevance of data protection legislation should also be stressed. Indeed, electronic monitoring will trigger the applicability of these particular laws in the Member States, providing for guarantees with regard to the employee’s privacy in case the monitoring would involve the processing of personal data, which is most often the case. Furthermore, a legal assessment of monitoring often takes account of specific monitoring laws, which are often enforced through criminal sanctions.

The labour law principles are often used as point of departure. Put in general and abstract terms, employers have the contractually based right to determine work tasks and to control the contract fulfilment by the employees. This includes the surveillance of the proper use by employees of employers' property and the control of company premises, the compliance with work-related rules and quality requirements and, to a restricted extent, with professional and organisational behaviour standards. At the same time, the employer also has certain responsibilities, e.g. in term of workplace health and safety, so that it is generally recognised that employers may (or must) look after or monitor the employees’ health and safety.

In some countries, there exists partly regulation of specific aspects of monitoring of workers. For example, under **Belgian** law, although the assessment involves the application of different sets of rules, a specific monitoring regulation is laid down in Collective Bargaining Agreement n° 68 of 16 June 1998. Still, it is only confined to the issue of camera surveillance in the workplace and its scope of application remains limited.

The approach of each Member State may also differ according to its specific legal practice. In **Denmark**, for example, monitoring and surveillance in the workplace is - in a labour law perspective - mainly a topic for collective agreements and especially the so-called basic agreements. The main principle in this area laid down in the basic agreements is the principle of the employers' prerogatives. As a central part of these prerogatives, the employer is empowered to monitor the work in the workplace. Questions about monitoring and surveillance are usually seen from the employer's viewpoint, but attention should self-evidently also be paid to the position of workers.

While a general right to monitor - and to monitor electronically – is accepted under the employment contract doctrines in the Member States, limitations are also accepted. Due to the overall absence of specific monitoring regulations, except for a few cases (see above) the laws of the Member States rely in the first place on general principles to indicate the limitations of the employer's monitoring rights. Self-evidently, one of the main difficulties in the laws of the Member States lies in the drawing of consistent demarcation lines between legitimate control interests of the employer and legitimate interests of the employee's privacy, translated as a right *not* to be controlled or to have control over personal information.

In **Denmark**, case law has subjected the employers to carry out their rights under the prerogatives in a responsible manner without any kind of abuse. This means that the monitoring or surveillance activity in question has to be carried out for legitimate purposes, without any discrimination among the employees, with respect of the principle of proportionality and in respect of the privacy and dignity of the employees in the workplace. According to Danish case law, these general guidelines do not set very intensive limitations to the use of monitoring and surveillance in the workplace. Their aim is first of all to oblige the employer to respect some fundamental principles of fairness preventing abuse of the rights. This approach is seen in a lot of Member States.

In the **United Kingdom**, it may be possible to argue that some forms of monitoring and surveillance constitute a breach of the employment contract because they violate the implied duty of trust and confidence that employers are deemed to owe their employees.[239] Furthermore, the Health and Safety (Display Screen Equipment) Regulations 1992 implement EC Directive 90/270 on the minimum safety and health requirements for work with display screen equipment. They provide that in designing, selecting, commissioning and modifying software, and in designing tasks using display screen equipment, the employer must take into account the principle that no quantitative or qualitative checking facility may be used without the knowledge of the operator or users. Employers must ensure that operators and users at work in the undertaking are provided with adequate information about such measures taken by it in compliance with its duties as relate to them and their work.

In **Greece**, the constitutional principles concerning privacy have been transferred to civil law, which governs, in parallel with specific labour laws, the employer-employee relationship. Under articles 648-680 of the Civil Code, the employment contract requires the employee to perform services of a certain kind for pay at a place, time, manner and other conditions fixed by the employer[240]. As a subordinate relationship, the employment contract requires the employee to follow the instructions and orders given by the employer who has the right to manage company assets, control cost and monitor his work performance.

2. Role of collective labour law

In general terms, the laws of the Member States do not uniformly address the role of collective labour law with regard to data protection issues. In many countries, the general provisions with regard to workers' representatives (works councils or health and safety committees) or trade unions imply forms of collective worker involvement in electronic monitoring issues. It must nevertheless be noted that in places where the works council or unions receive a role in electronic monitoring issues, it is mostly limited to procedural rights, rather than substantial rights.

[239] *Malik* v *BCCI SA* [1997] IRLR 462.
[240] *Greek Civil Code*, English translation by C. Taliadoros, Athens, 1982.

In the case of **Belgium**, existing provisions of collective labour law may be applied to electronic monitoring. They imply that the employer is obliged to inform and consult (consultation means an exchange of view) the works council with regard to (electronic) monitoring practices. The law also implies that the work regulations have to be amended in case of electronic monitoring (involving the consent of the works council). Nevertheless, the existing labour law provisions are often neglected in daily practice. The main reason is that there is no clear and specific rule or provisions regarding electronic monitoring and the existing labour law provisions leave too much scope for discussion as regards their applicability to electronic monitoring.

In **Denmark**, the employer is obliged to inform and consult the works council in the workplace. In Danish labour law, the works council is not regulated in legislation, but in specific co-operations agreements. Following these co-operation agreements, the employer is obliged to inform the works council on a monitoring activity. The information must enable the works council and especially its employee members to discuss the activity in a serious manner. According to an annex of 24th April 2001 to the Basic Agreement between the Danish Confederations of Employers and the Danish Confederation of Trade Unions the employer is obliged to inform the employees in the workplace with a notice of two weeks in advance of the enforcement of the specific monitoring activity. It is likely that this rule also will be adopted in other basic agreements.

In **Austria**, the role of the works council seems to go a step further than merely procedural. If the employer is willing to carry out surveillance for purposes of controlling employees – no matter if technical (e.g. cameras) or human resources (e.g. superiors) reasons apply – and the control measures affect a person's dignity, the works council's approval must be obtained. Otherwise the employer may not take the concerned measures. The required consent cannot be replaced by individual agreement (e.g. in the employment contract). Such a works agreement dealing with the surveillance can be a fixed-term one or concluded for an indefinite term.

In **Finland**, the **"Co-operation Act"** deals with the right of information and of consultation of employees and the employer's duties in this respect. But the aim of the legislation is rather to establish a dialogue, which could influence the employer's decision. The new **Act on privacy protection in working life** also involves the procedure of co-operation. The aim of the new provisions (both in the Act on Privacy Protection in Working Life and in the Act on Co-operation within enterprises) is to assure a basis for a dialogue. The objective of the dialogue is the aim of monitoring and the methods to be used in technical monitoring and surveillance. The statutes deal explicitly with the question of the employer's activity directed towards the employees – an activity based on the employer's right to supervise and monitor the work. This entity will now be brought under the scope of application of the "Co-operation law". For the (small) companies that are not covered by that law an elementary procedure of dialogue of the same kind is established. The new provisions and the preamble explaining them seem to depart from the point that the duty of information and negotiation is triggered only when the employer is about to make a decision on the issues mentioned. This would mean that there is no legal obligation to bring the existing practices to the procedure.

In the **United Kingdom**, there are no statutory provisions requiring consultation with workers and or worker representatives about monitoring and surveillance other than those requiring consultation with safety representatives appointed by a recognised trade union (or, in their absence, employees themselves or elected `representatives of employee safety') about the health and safety consequences of the introduction of new technologies into the workplace. The Draft Code of Practice on the Use of Personal Data in Employer/Employee Relationships recommends that employers should assess the impact of proposed monitoring in consultation with trade unions or other employee representatives, but (at the time of writing) it remains to be seen whether it will remain in the final version of the Code. Even if it does remain, it falls short of a legal duty to consult, although it is possible that measures introduced with the agreement of unions or other employee representatives are more likely to be regarded as `fair' for the purposes of the first of the data protection principles (cf. legitimacy of the monitoring). At its 2000 Congress, the Trade Union Congress passed a motion calling on

employers and unions to reach workplace agreements on the use of new technologies and employee surveillance. The UK government has indicated that it encourages businesses to agree with employees appropriate levels of recording or monitoring if they wish, but does not want to oblige them to engage in collective bargaining in this area.

In **Germany**, connected with surveillance and monitoring is the discussion regarding the scope of the co-determination right of the works council pursuant to section 87 (1) no. 6 Works Constitution Act. This provision gives works councils a compulsory right of co-determination concerning the introduction and use of technical devices designed to monitor the behaviour or performance of employees.[241] A technical device in the sense of section 87 (1) no. 6 Works Constitution Act is designed to monitor the behaviour or performance of employees, when the device is objectively and immediately suited for monitoring, regardless of the employer's intention to use it for this purpose and of the evaluation of the data gained by the surveillance.[242] A telephone system in an establishment which automatically registers incoming and outgoing phone calls and phone numbers, the time duration, the call charge and other parameters is a technical device in the sense of section 87 (1) no. 6 Works Constitution Act. Its installation and operation is therefore subject to the right of co-determination.[243]

According to article 27 of the **Dutch** Law on Works Councils, the employer needs the consent of the works council when he wants to implement, modify or withdraw rules concerning the processing of personal data. This provision gives the works council a firm position. In general, any form of registration or monitoring will come under the scope of the aforementioned obligation.

The **Portuguese** Constitution gives workers' committees, trade unions and workers themselves relevant rights to enforce their privacy against non-justified monitoring. Article 54 gives workers' committees the right to receive necessary information for the carrying out of their activities. So they must be given the accurate information to monitor the management of enterprises, but also on the changes in working conditions. The introduction of new monitoring technology must be considered as a change in the working conditions. Workers' committees must be consulted before significant changes are introduced in the workplace, so they can have an important role in determining the fairness of employees' data processing. Workers' committees also have the constitutional right to participate in the preparation of labour legislation. This means that they should be called to discuss specific rules on workers data protection. Law also gives them the right to be informed about work organisation, and they should be called to give advice about it [244]. Trade Unions also have the right to participate in companies restructuring, particularly when there is a change in working conditions (Article 56.2.e). Furthermore, they have the right to participate in the preparation of labour legislation (Article 56.2.a). This general consulting obligation could also follow from a specific legal provision on safety, health and hygiene, which provides that workers and their representatives should be informed about the introduction of a new technology[245].

Notwithstanding the constitutional provisions[246] and specific labour laws guaranteeing freedom of association[247], the **Greek** law expressly recognises the competence of work

[241] There are corresponding rules in the personnel representation acts of the Länder for employees in the public services.
[242] *Bundesarbeitsgericht* 9/11/1975 BAGE 27, 256 = Der Betrieb 1975, 2233; cf. Däubler, Internet und Arbeitsrecht, p. 128 et seq.
[243] *Bundesarbeitsgericht* 6/12/1983 BAGE 44, 285 = AP Nr. 7 zu § 87 BetrVG 1972 Überwachung; 23/4/1985 AP Nr. 12 zu § 87 BetrVG 1972 Überwachung; 27/5/1986 BAGE 52, 88 = Der Betrieb 1986, 2080.
[244] See also Workers' Committees Act (Law 46/79, published on the official bulletin *Diário da República* the 12th September 1979).
[245] Act 441 (DL 441/91), published on the 14 of November 1991, on the portuguese official bulletin *Diário da República*.
[246] Articles 22 and 23 of the Constitution.
[247] Law 1264/1982 as subsequently amended.

councils with regard to the introduction of new technologies and the alteration of working methods. More specifically, Law 1767/1988, which ratified the 135th International Work Treaty, as amended by Law 2224/1994, grants work councils wide ranging powers to jointly decide with the employer on various issues such as wages, working hours, duties of supervising personnel, including electronic surveillance at workplace through cameras and modern audio-visual media[248]. Any disputes between the parties on the authority or the validity of the terms of a collective agreement can be settled through a mediation procedure[249] or by civil courts since it is a private agreement. Based on the above statute, the data protection legislation, and on good employership standards, one should conclude that before introducing any surveillance measures, the employer should in principle consult with work councils and individually inform data subjects.

3. The right to private access

According to various principles arising from labour laws, it is easy to defend the employer's right to limit access to internet and e-mail facilities. The employer, indeed, has the right to manage the workplace and to exercise authority over the workers. The employer therefore, in principle, has the right to impose restrictions on the use of computers, internet and ICT at the workplace, knowing that these instruments are introduced to reach the company's goals and purposes. Furthermore, the employer is considered to be the "owner" of the available ICT in the company. At least, the company bears the costs of the use thereof. The fact that these instruments 'belong' to the employer would also imply that the employer has the right to prohibit any use or any abuse of equipment or any use for other than the defined purposes.

However, this principle remains open for interpretation, and it is still possible for workers to claim certain rights to the use of company facilities for private purposes.

In the first place, it is possible that the employer allows the use of facilities for non work-related purposes. It happens, for example, that internet policies stipulate that private use of the company's internet is only allowed in limited circumstances, e.g. during lunch breaks. Still, it may happen to be that the employer allows private use less restrictively. Under some laws, this may create a legal entitlement of the employee to the private use of the internet, based upon the construction of the 'unilateral obligation' of the employer, or on the basis of an implicit policy of toleration, which may be qualified as corporate custom (regarded in many countries as a source of rights and obligations).

More difficult is the issue of private facilities arising from the employee's constitutional right to privacy, understood as a 'right to communication'. There is little guidance for the moment in the Member States on this issue.[250]

Among the Member States, legal scholars argue that some form of personal access by the employee should be provided for. Also the case law seems to make a start of following this line of reasoning. In **Italy**, a judge has allowed the use of a telephone if the workplace lacks a public telephone point and if the employee does not abuse it.[251]

A general exception to the prohibition to use ICT for private purposes may also be found in written (or also oral) permission given by the employer. An **Italian** judge has held that, in the case in which the use without limitations (of telephone) by the employees constitutes a deeply rooted practice known by the employer, such practice has to be considered as a permission *per facta concludentia*.[252]

---

[248] Article 12 para. 4 of Law 1767/1988 as amended by article 8 of Law 2224/1994.
[249] This mediation procedure is provided for in articles 15 and 16 of Law 1876/1990.
[250] But there is guidance from the European Court in Strasbourg, cf. *Niemietz v. Germany*, Judgment of 16 December 1992 Hudoc, REF00000472.
[251] Nogler, Il lavoro a domicilio, Giuffre',2000, 577.
[252] V. Ferrante, Privacy in the Workplace, Remote Control and Data Protection: An Overview of the Italian Legal Regulation, manuscript unpublished in file with Bulletin of Labour Law and Industrial Relations, Kluwer Law International.

In **Austria**, the prevailing opinion derives form the wide employer's duty of care, a right to telephone on private matters to avoid social deprivation and isolation.[253] A similar legal situation may be stated for e-mail or website visiting. However, it is still considered to be an exception and depending on specific circumstances.

In **France**, the data protection authority ('CNIL') has found out that past case law has accepted limited private access with regard to telephones or minitel and is of the opinion that there should not be a different approach with regard to new forms of communication, such as e-mail.

In the **Netherlands**, much case law exists with regard to the use of internet for private purposes, mostly with regard to information of a pornographic nature. The outcome of the judgements varies, according to the circumstances. It would appear that much policy lies with the judge in order to assess the case and make a decision taking into account all factual elements. General conclusions are often difficult to draw. Still, it appears that one may assume from an employee that he is aware of his limited privacy expectations in a work environment.

The problem of the private use of email and internet was already in 1999 on the agenda of the largest Dutch trade-union, the FNV Bondgenoten. FNV published in that year a model-protocol, titled 'privacy in the use of internet and e-mail'.[254] It provides, for example, that employees are authorized to use the e-mail system for non-commercial transactions in order to send and receive personal e-mail messages, both internally and externally, provided that this does not interfere with their day-to-day work commitments. The following conditions apply to the employee's right to send and receive personal e-mail messages: the e-mail must contain a disclaimer and it is not permitted to send threatening, sexual or racist oriented messages. The employer is not allowed to read the content of either personal or commercial e-mail messages. Neither shall personal data with regard to the number of e-mails, e-mail addresses or other relevant data be registered and/or checked. But this does not affect the employer's right to carry out occasional checks based upon compelling reasons in the interest of the company. Such checks shall be reported to the works council.

According to the FNV guidelines, employees are also authorized to use the internet system for non-commercial transactions, provided that this does not interfere with their day-to-day work commitments. However, employees shall not be permitted to deliberately consult websites that contain pornographic or racist matters. The employer should not register and/or check on personal data concerning the use of the internet, such as the time spent browsing or the sites that are visited. This does not affect his right to carry out occasional (see above), reported to the works council.

B. Telecommunications (internet, e-mail and telephone)

The use of the telephone at work gives probably rise to one of the oldest forms of 'electronic monitoring'. It may be assumed that workers are supposed to use their employers' phone for professional purposes. At the same time, however, it would appear that such general assumption may not exclude that an employee would be able to claim that his/her right to privacy is violated, or that specific laws in this respect (e.g. criminal provisions) have been contravened, in case the use of the telephone is monitored by the employer.

Telephone conversations clearly come under the concept of telecommunication. Another application is electronic mail, which is equally problematic in terms of workplace policy. Indeed, there are many million employees using e-mail over the world, but not all of these e-mail concern private matters. Indeed, workers are supposed to correspond professionally, with a view to spend their time and effort to the performance of their employment contract. Still, it is often argued that, when using company e-mail equipment, workers will be able to claim for protection under the general right to privacy, or under specific laws in this respect.

---

[253] *Adamovic,* ZAS 1992, 196; *Reischauer,* Persönlichkeitsrecht auf Achtung des Fernsprechgeheimnisses (§ 16 ABGB) und seine Bedeutung für das Dienstverhältnis, DRdA 1973, 217.
[254] See http://www.fnv.nl, the complete text of the protocol can be found in addendum A.

The same counts for surfing on the web. However, while often the use of e-mail and internet are treated in similar terms or through the same laws, it remains unclear in some Member States whether or not surfing on the world wide web may be regarded as a form of communication.

It would appear that some specific rules may be found for the monitoring of telephone conversations, e-mail and internet use.

This is also why, often, fine distinctions need to be made and particular attention should be given to the reasons of monitoring and the concrete business context. Therefore, the use of e-mail and the use of internet are often distinguished. Furthermore, logging is distinguished from monitoring the content of e-mail. Moreover, it would appear that the legal assessment may vary according to the circumstances, such as the availability of alternative private facilities or access to communication technology at the workplace. Human dignity may also come up, often to the extent where privacy as such is not considered to be an issue.

1. Protection by the right to privacy

In **Germany**, case law has developed the question whether the "right of one's own word" applies also to workplace communication. The jurisprudence of the Federal Constitutional Court has acknowledged this right as a manifestation of the constitutional protection of personality.[255] In the definition given by the Federal Constitutional Court this basic right comprises the freedom of man to determine himself whether his/her words shall be accessible to the person only, to whom he/she talked, to a certain circle of persons or to the public.[256] In a decision of 1991 the Federal Constitutional Court has extended this protection area to telephone communication at the workplace. Overruling the Higher Labour Court (*Landesarbeitsgericht*) which had exempted telephone calls operated by an employee at the workplace from the protection of the general right to privacy the Federal Constitutional Court saw this as a violation of Articles 2 (1) and 1 (1) of the German Constitution protecting the privacy of the spoken word. [257] The business character of a phone call as such does not suppress the freedom to choose the addressees. Unnoticed eavesdropping of employees' phone calls by the employer has, according to this judgement, in principle to be qualified as an infringement on the general personality right of employees. It is up to the individual (employee) to decide on who shall have the right to access to spoken communication. Any knowledge obtained by unnoticed eavesdropping must not be used in judicial proceedings.[258] The Federal Court of Labour, however, in a decision of 1996, has accepted that there may be outweighing interests of the employer to control the uniform service quality of the enterprise by eavesdropping of service communication of new recruited employees during the probationary period.[259]

The **German** situation seems to be in line with the protection offered at the level of the Council of Europe, where workplace communication may be protected by the right to privacy. It still remains unclear, however, whether or not specific conditions have to be fulfilled in order to have such privacy protection. It is not quite clear what the role of the concept of 'privacy expectation' would be in such case and how or to what extent the parties themselves (employer and employee) may influence (e.g. by agreement) the degree of privacy expectation in the workplace, or with regard to communication.

A recent judgement of the **French** Cour de Cassation of 2 October 2001 shows how far privacy protection may go with regard to workplace communication. The Court held that a

[255] *Bundesverfassungsgericht* BVerfGE 34, 238, 245; 54, 148, 154.
[256] *Bundesverfassungsgericht* BVerfGE 54, 148, 155.
[257] *Bundesverfassungsgericht* 19/12/1991 Der Betrieb 1992, 786; cf. Beckschulze/Henkel, Der Einfluss des Internets auf das Arbeitsrecht, Der Betrieb 2000, 1491, 1493; Däubler, Internet und Arbeitsrecht, 2001, no. 245, 246.
[258] *Bundesarbeitsgericht* 10/12/1998 – 8 AZR 366/97.
[259] *Bundesarbeitsgericht* NZA 1996, 218; Der Betrieb 1998, 371.

worker has the right to respect for his intimacy and privacy, even during working hours and at the workplace, which also covers the secrecy of correspondence. According to the Court, this implies that the employer cannot have access to the content of personal messages, either sent or received by the employee, through an information system made available to the employee for his job, even if the employer would have prohibited non-professional use.

In **Portugal** Courts have already decided that it is illegal for a superior to listen to a telephone conversation between two of his employees if consent is not given. The privacy right and the secrecy of the communications were considered of a greater importance than the obedience duty[260].

2. Prohibition of monitoring

As far as the monitoring of communications are concerned, many countries have specific laws, often enforced through criminal sanctions, which regulate the protection of telecommunication, like telephone communications, e-mail communications and the use of internet or intranet, also if the communications take place in a work related context.

It must nevertheless be noted that these laws are not always specifically focused on employment situations and often provide for a general **prohibition** of interception of telecommunication without the consent of the parties involved. Exceptions to such prohibition are often not designed for employers.

Still, it must be noted that the prohibition is only important in cases where only few or very restrictive exceptions are allowed. In **Belgium**, the prohibition of intercepting telecommunication is regarded to be very strict in the sense that there are only few exceptions on which the employer may rely (leaving aside consent). Also in **Italy**, the prohibition is very severe. Furthermore, the specific telecommunication laws do not solve the problem of third party involvement in monitoring by the employer. For example, the **UK'**s *Regulation of Investigatory Powers Act 2000 (`RIPA')* provides that the sender or recipient of a communication could seek an injunction against, or seek damages for any loss incurred from, an employer who intercepted a communication to or from its system, but only provided that it was done 'without lawful authority'. In the context of employment the scope of "lawful authority" is widely defined (see below).

In this respect, the legal framework in **France**, namely the law of 10 July 1991 may be mentioned. This law is enforced through criminal sanctions and prohibits the mere fact of monitoring telecommunications with 'bad intent' ('mauvaise foi') or installing equipment for that purpose. It is irrelevant whether it concerns telephone communication for private or for professional purposes. The only exception would be an interception or monitoring with 'good faith' ('bonne foi'). The question remains whether this exception of 'good faith'-monitoring would apply to surveillance by the employer, in case he has informed the employees thereof on beforehand. In an official statement, the French Minister of Justice has expressed the opinion that merely informing the employees of a monitoring practice, would not be sufficient to make the practice lawful. Therefore, in an attempt to clarify the law, the French data protection authority ('CNIL') has formulated some principles that would support the lawfulness of interceptions of telecommunications (see below).

The **exceptions** to the prohibition of interception often vary from one Member State to another.

3. Consent

In most legal systems, a common exception to the prohibition of interception or monitoring is, as already indicated, **consent**. The **Belgian** criminal provisions on the protection of telecommunication protection provide for example that it is unlawful to intercept communication without the consent of all participants to the communication.

[260] Ac. Rel. Lisboa of 10th December 1991, *Colectânea de Jurisprudência*, Ano XVI, Tomo V, p. 153.

The **U.K**. Act specifies a range of circumstances where the requisite 'lawful authority' to intercept telecommunication is deemed to exist. One situation is where the communication is one which, or which the person intercepting has reasonable grounds for believing, is both sent by a person who has consented to the interception and a communication the intended recipient of which has so consented.[261] Employers could almost certainly prove the requisite consent if a worker's contract specifically permitted interception.

In practice, consent does not always work in cases where all communicating parties need to give their consent. Indeed, it may be difficult to obtain consent from parties who are not employees of the employer. On the other hand, consent may become more useful if it concerns communication between employees of the same company.

4. Lawful business purposes

Another exception may be found in so-called **lawful business purposes**. In the **U.K**. for example, employers are likely to rely upon a set of exceptions, contained in *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*,[262] made under the authority of the Regulation of Investigatory Powers Act, (`the Lawful Business Practice Regulations') which do not require the consent of either party.

The Lawful Business Practice Regulations allow interceptions effected by or with the consent of a 'system controller'[263] for the purpose of monitoring or keeping a record of communications for a range of purposes. Monitoring is, for example, allowed:

- to ascertain compliance with regulatory or self-regulatory practices or procedures;
- to ascertain or demonstrate standards that are or ought to be achieved by persons using the telecommunications system in the course of their duties;
- to prevent or detect crime;
- to investigate or detect unauthorised use of that or any other telecommunication system;
- to secure effective system operation (an exception intended to permit activities such as traffic routing or virus checks).

In **Germany**, there is a right for the employer to control the compliance of employees using telecommunication at the workplace with business purposes. This right to control, however, has to be balanced with the opposed right to privacy and protection of personality rights of the employees. The mitigating legal balancing technique is the application of the principle of proportionality. This principle limits monitoring and control normally to the external criterions of telecommunication (addresses, target numbers, length or duration of telecommunication). Only under very exceptional circumstances will the employer be authorised to read contents.

In **Denmark**, the monitoring of telecommunications is in general contradictory to section 263, subsection 1, no. 3, in the Criminal Code. The protection under this rule does not depend on whether the communication is private or work related. It is also of no importance with whom the employees communicate, e.g. colleagues or clients. Telephone communications are protected under the Criminal Code. Monitoring of private e-mails - but not private internet use - may also be in conflict with section of the Criminal Code, but it is still unclear whether an e-mail can be considered a "closed" message.

In **Portugal** a Court has already decided that a worker that refuses to explain to his employer the content of a telephone conversation concerning work related issues would damage trust, and violates the duty of loyalty.[264]

In **Spain**, monitoring by the employer is allowed in order to verify whether or not the employees use the available internet access or their e-mail facilities for work related purposes.

---

[261] RIPA 2000, s 3(1).
[262] SI 2000 No. 2699.
[263] A person with a right to control the operation or use of the system in question.
[264] Ac Rel. Porto of 11th October 1999, www.dgsi.pt .

Prevention or detection of crime or serious wrongdoings by the employee, is also an issue in **Italy**. In this country, a violation of employer property rights by the employee does not allow the former to monitor the communications of the latter, as the Italian criminal law on correspondence prevents the employer from every form of control. However, it does not mean that the violation of the duty of loyalty by the employee would remain without consequence. Still, it is difficult to say whether a different solution could be given if the employee commits a criminal offence in using electronic devices (for instance: if he downloads pornographic photos of children, or if he uses telephone to menace someone). In these cases, dismissal can be lawful if the employer knows the facts without any specific enquiry (from the police or founding some photos), but it is uncertain if the employer can carry on an enquiry on his own. A similar discussion exists in **Belgium**, where it remains unclear to what extent a private employer may involve in criminal investigations in his own workplace. Indeed, article 227 of the Belgian criminal code makes private police activities by employers illegal. 1

5. Evidence of transactions

In the **U.K.**, employers may monitor (but not record) communications to determine whether they are communications by means of which a transaction is entered into in the course of the business or which otherwise relate to the business.[265] This is designed to enable, *inter alia*, staff e-mail to be accessed in their absence so that communications relating to the business can be dealt with, and was said by the government to 'achieve a balance between giving businesses free access to their own communications and protecting the privacy of non-business communications where these are permitted'.[266] However it creates the difficulty that in establishing whether communications do relate to the business there is an inevitable risk of intercepting those which do not.

In **Belgium**, telephone communications – both content as well as external information – may be used as evidence in court, as long as the conversations are recorded lawfully.

The **Portuguese** Telecommunication Act admits the registering of telephone communications when commercial practices take place. On these situations, workers are necessarily informed about the taping procedures.[267]

6. Specific guidance on telephone calls

In **Germany**, for the intensity of control the jurisprudence of the Federal Court of Labour distinguishes between business calls, private calls caused by business circumstances (e. g. unexpected long team conference) and private calls. The first category of (pure) business calls justifies the complete collection of telephone data, i.e. above all the time and the duration of the call and the full target number.[268] The Federal Court of Labour holds the employee contractually obliged to reveal to his employer whether and how he or she fulfils his or her employment contract obligations. The disclosure of business calls informs the employer on the work performance, not on private affairs. The employee has to tolerate the unavoidable restriction of personality rights. The same is true for private calls caused by business purposes. The reasoning of the Federal Court of Labour in its seminal decision of 1986 acknowledges the interest of the employer to learn whether and to which extent this double-sided type of calls has been operated by employees. The information interest of the employer covers the collection of target numbers. The situation is different for pure private calls. The employer makes his telecommunication devices available for the employees who, normally, are obliged to pay for these calls. Nevertheless, the employer has a legitimate interest in learning about the number, the time and the duration of private telephone calls in order to

[265] `Business' includes activities of a government department or any public authority or statutory office-holder.

[266] DTI, *Lawful Business Practice Regulations Response to Consultation*, 2000, www.dti.gov.uk/cii/lbpresponse.htm, para 15.

[267] Article 5.3 of Telecommunication Act (69/98). Phone banking or phone stock transactions are examples of these situations.

[268] *Bundesarbeitsgericht* BAGE 52, 88 = Der Betrieb 1986, 2080.

check the consumption of working time. The target numbers of purely private calls, however, will not or only in a truncated form be registered.[269]

In **France**, the national data protection authority ('CNIL') has formulated some principles with regard to the monitoring of telephone communications.

- a specific and lawful purpose is necessary for the monitoring of telephone correspondence; the general monitoring of all telephone communications may not be regarded as lawful;
- as lawful purposes may be regarded: the verification of orders by intermediaries working for clients on the stock exchange; training of employees who primarily use the telephone for the performance of their job (e.g. call centres); security companies or security services linked with the security of users or clients (motorways, elevators, emergency centres, …);
- the employees concerned must be informed before putting a monitoring system in operation; information must concern the existence of a system of monitoring, the individual consequences which may arise therefrom, the periods during which monitoring would take place;
- telephone lines should remain disconnected from monitoring systems if they are not directly linked with the purposes of the monitoring;
- the employees should have access to the results of the monitoring and should be able to give their comments;
- the other parties to the telephone conversations (either professional parties or private parties) must also be informed of the monitoring of their communication.

More specific rules about monitoring the telephone use of employees are given by the **Dutch** Data Protection Authority in 1996, which published a report on the monitoring of telephone-calls at work. The report gives some situations in which monitoring is allowed and provides for general principles. Although this report was based on the old Privacy act, it still provides the basic rules concerning monitoring of telephone calls at the workplace. The Dutch Data Protection Authority makes several distinctions. A first distinction is being made between real time eavesdropping and taping. The second distinction is between training and guidance situations as well as cases of individual approval or the so-called personal reviews. In the end, there are no big differences in the various conditions, so these distinctions only have a marginal effect. In general terms one may state that employees must be aware of the possibility that the employer can listen in or tape a conversation. Furthermore, the gathered information may not be used for other purposes. If an employer envisages the monitoring of telephone calls for cost control purposes or in order to discourage private telephone calls, he is only allowed to check outgoing calls, not incoming or internal calls. In case of protection of company secrets the measure of control must be accurate, and should not be applied as a general form of monitoring.

7. Specific guidance on e-mails / internet use

In **Denmark**, some test cases before the Data Protection Authority have show that a distinction is made between general monitoring and specific monitoring. The supervisory authority accepts that employers may generally monitor e-mails and internet use if it is for purposes of a legitimate character, like the smooth operation of the IT-system, security in the workplace, monitoring compliance with the general guidelines for the use of the computers. It is accepted that the monitoring can be imposed for several of the mentioned purposes. Monitoring of the *content* of *specific* e-mails or the use of the internet by a *specific* employee is, however, subject to a more restricted view. The supervisory authority has stated that an employer is only entitled to monitor the content of an e-mail, if a specific employee is suspected of having done something contradictory to the rules, e.g. abuse of the equipment for banned purposes for internet use. No distinction between incoming and outgoing e-mails has yet been made.

[269] *Bundesarbeitsgericht* ibidem.

The Danish Data Protection Authority is of the opinion that the employer is in no circumstances entitled to monitor the content of an e-mail if it appears to be of a private character (not workplace-related). This is also the case even if the employer has made a ban on private e-mails.

In respect of monitoring of e-mail and internet use, specific attention should be paid to an Opinion of the **Belgian** Privacy Commission, regarding internet and e-mail monitoring, of 3 April 2000.[270] In light of the proportionality principle, the Belgian Privacy Commission is of the opinion that systematic registration of all telecommunication details *a priori*, cannot be allowed. As far as the monitoring of e-mail is concerned, the Belgian Privacy Commission is of the opinion that gaining access to the content of e-mail messages is excessive and thus not in compliance with the law on data protection. According to the Commission, there are several solutions to solve abuses by employees in this respect, such as installing computer software indicating chain messages, or identifying messages which take up too much space on the network, such as music or video attachments. Therefore, e-mail must be monitored on the basis of a list of e-mail traffic and not on the basis of the content of e-mails.
As far as the monitoring of websites is concerned (surfing), the Belgian Privacy Commission is of the opinion that the monitoring must be based on limited objective information and not on an *a priori* systematic control of the content of all dataflow regarding every employee. In this respect, the Commission also indicates that an employer could make up a list of visited websites, without identifying every single employee. On the basis of such list, an assessment of possible problems could be made. Should an acute problem occur, the Commission continues, the employer could at that time undertake individualised action.

In the **U.K**., the Information Commissioner is empowered by the data protection law to prepare codes of practice for guidance as to good practice after consulting trade associations and data subjects or their representative bodies. At the time of writing the Commissioner is consulting on the terms of a Draft Code of Practice on the Use of Personal Data in Employer/Employee Relationships. The provisions of the Draft Code dealing with the interception of communications are considerably more restrictive than the Lawful Business Practice Regulations discussed above. On **internet** access, it states that sites visited or content viewed should not be monitored unless it is clear that the business purpose for which the monitoring is undertaken cannot be achieved by simply recording the time spent on the internet; if the purpose of monitoring is to detect the downloading of pornography (whose meaning should be defined), the employer should have evidence that the activity is taking or is likely to take place and would pose a significant risk to the employer in terms of distressing or offending other staff.[271] In relation to **e-mail**, it emphasises that content should be monitored only if neither a record of traffic, or traffic combined with subject, achieves the business purpose, and that the privacy of senders, as well as recipients, is material in this context. E-mails that are clearly personal should not be opened, and there should be a means for employees effectively to expunge from the system e-mails they receive or send.[272] Importantly, it emphasises that `routine monitoring of the content of all communications sent and received at work is in many cases likely to go too far', even if confined to business communications, given that employees may wish to impart information relating to the business to intended recipients only, such as personal reasons for wanting to postpone a meeting.[273]

In **France**, the national data protection authority ('CNIL') has drafted some principles with regard to cyber surveillance.

- transparency and loyalty: if a copy of messages is made, the duration of conservation should be communicated to the employees; if fire-walls are created, employees should be aware of the significance of the information collected and the duration of conservation thereof; employees should be informed of the specific hierarchical authorities in the company which can perform specific measures of surveillance;

[270] Opinion n°10/2000 of 3 April 2000.
[271] Para 6.3.3.
[272] Para 6.3.2.
[273] Para 6.3.

- website visiting for private purposes must be allowed: monitoring *a posteriori* is lawful; surf control must be performed without individual analysis of consulted websites or of the content thereof; in any case, employees should be made aware of the fact that they are subject to monitoring;
- a prohibition to use e-mail for non-professional purposes is unrealistic and disproportionate: monitoring of such use is, however, acceptable; but it may not concern the content of messages; as far as incoming messages are concerned (from outside the company), every indication of a private nature of the message should render monitoring by the employer illegitimate;
- trust through negotiation: the use of internet for non-professional purposes and the introduction of monitoring systems should be the subject of negotiations between employer and workers, both on sectoral as well as on enterprise level; at the level of the enterprise, discussions must take place through existing appropriate channels, such as the works council or the health and safety committee).

In the **Netherlands**, at the end of 2000, the Dutch Data Protection Authority published a report with an extensive survey of the problems than may occur if an employer monitors the online behaviour of its employees.[274] In this survey the Dutch Data Protection Authority publishes relevant guidelines that an employer should take in account. With these guidelines it looks like much (but not all) uncertainty among employers is taken away. A summary of the most important guidelines:

- Treat problems online the same as offline;
- Use transparent rules with the consent of the works council;
- Make sure that rules or a policy are easy accessible for the employees;
- Make clear in what way private use is allowed;
- Pay extra attention to the position and integrity of the system-administrator;
- If a problem occurs, discuss this as soon as possible with the employee in question;
- Give employees the opportunity to check the gathered information from time to time;
- Use the gathered information not for other purposes;
- Do not keep gathered information longer then necessary;
- Be alert with checking e-mail of privileged persons, like members of works council.

8. Guarantees

A whole set of **guarantees** exist. In general, in all Member States the guarantees of the **data protection laws** apply to electronic monitoring, as they follow from the European Data Protection Directive 95/46/EC. The principles arising from these data protection laws seem to be important in employee privacy protection. It must be noted that these principles, for the time being and in most cases, are not narrowed down specifically towards employment monitoring cases.

Besides the protection offered in the data protection laws, two elements may seem rather important. In the first place, information to the individual with regard to monitoring is essential. Furthermore, there is the role of collective labour law provisions (already indicated above).

Interceptions are authorised under the **U.K**. Regulations only if the employer has made all reasonable efforts to inform every person who may use the telecommunication system in question that communications transmitted by means thereof may be intercepted. It thus requires staff (but not third parties) to be informed that interceptions may take place.[275] Interceptions must be solely for the purpose of monitoring or, where appropriate, recording communications 'relevant to' the system controller's business, a concept which extends to those taking place in the course of the carrying on of the business as well as those relating to it.[276] In **Denmark**, it is also in general a condition for monitoring that the employees' have been informed about the employers' policy on monitoring of e-mails and internet use. The

[274] Dutch Data protection Autority, 'Goed werken in netwerken, Regels voor controle op e-mail en internetgebruik van werknemers', 2000, online available at :http://www.cbpweb.nl

[275] This reflects the DTI view of the scope of this requirement.

[276] The Regulations provide that conduct falling within this provision is authorised only to the extent that Article 5 of the Telecommunications Data Protection Directive so permits.

employer does not satisfy this obligation as such if he has informed and discussed the monitoring in the works council. The employer should provide for more general information channels, e.g. on the intranet of the company.

C. Camera surveillance

Cameras identify, make images, and provide information with regard to the activities of individuals. This information may be rather accurate. Cameras make it possible to give a good representation of the reality: besides general information regarding whether or not a person is present in a given place, these tools may provide information concerning how he or she communicates with customers, how often he/she smiles or looks depressed, etc. Therefore, the use of cameras at work is often associate with the idea of 'big brother' at the workplace.

1. General

In many Member States, there are no express legal provisions concerning camera surveillance in the workplace.

Camera surveillance in the workplace has given rise to a lot of debate in **Denmark** in the last years. This is partly due to an unsatisfactory act in this area, namely the Consolidated Act no 76 of 1 February 2000 on Prohibition against Camera Surveillance. The act dates back to 1982 but the specific provisions on camera surveillance in the workplace received amendments in 1998 and 1999. The amendments took place after the employers' organizations had refused to make collective bargaining on these issues. The background for the unions call for guidelines in collective agreements was - among other things - a decision from an industrial court in 1992, which upheld a secret camera surveillance in an enterprise in order to verify a sincere suspicion of serious misconduct.

In **Denmark**, the Camera Surveillance Act obliges the employer to inform the employees about the camera surveillance in a distinct way, e.g. by displaying a sign. This is the case for both private and public workplaces. Breach of the information obligation is punished by a fine. The obligation is indispensable. The employer has to make a contact to the police if secret cameras are necessary in order to verify serious misconduct in the workplace. It is quiet unclear how far this information obligation reaches in practice. It is, for instance, uncertain whether an employer has to mark every camera position, every location or just the entrance to the workplace in a distinct way. Up to the union's minds, there is a widespread feeling among employees that they are subjected to secret camera surveillance in the workplace. This is due to the fact that employers often post very few signs in the workplace and the employees accordingly don't know of the cameras' exact positions.

Furthermore, it is unclear whether the employer is entitled to monitor all kinds of locations in the workplace. The employer is not entitled to monitor single rooms and such monitoring probably constitutes a breach of section 264a in the Criminal Code. However, it is very uncertain to which degree the employer is entitled to monitor general rooms, e.g. a lunchroom. The Camera Surveillance Act has no answer to this question.

It is a reasonable assumption that the employer has to fulfil the complete set of obligations laid down in the Processing of Personal Data Act of 2000, including the information obligations. These obligations should in the future introduce more restrictions than is the case in the present situation. It is first of all clear that the employer has to fulfil the principle in section 5, subsection 2, that personal data must only be collected for explicit and legitimate purposes and must not subsequently be used in ways which are incompatible with such purposes.

2. Lawful uses

In **Belgium**, camera surveillance at the workplace is regulated by a specific collective bargaining agreement, namely C.B.A. n° 68 of 16 June 1998. It is applicable to the entire private sector and explicitly states that it must be seen as completing the law on data protection on the issue of camera monitoring at work.

The lawful **purposes** of camera surveillance are enumerated in a limitative way. Allowed are one or more of the following uses of cameras:

- the protection of health and safety;
- the protection of the employer's property;
- the monitoring of the production process;
- the monitoring of the work performance of the employees.

Thus, in theory, C.B.A. n° 68 does not constitute an obstacle for electronic monitoring, as various uses of cameras may be justified on these grounds.

Similar provisions can be found in the draft data protection law of **Luxembourg**.

In **Denmark**, the Camera Surveillance Act does not contain any provisions on the employer's legitimate purposes with the surveillance or use of data, which means that this question largely depends general labour law and data protection principles. This gives both employers and employees the assumably wrong impression that the employer has a wide entitlement to impose camera surveillance.

In **Austria** if permanent video monitoring is carried out, the works councils' approval is needed in the form of a works agreement. The ground for participation may be found in the fact that the works council is able to demand compensating measures to ease the employee's disagreeable work situation (for examples longer breaks; job rotation between colleagues under surveillance and those without). Jurisdiction also made clear that the representative's consent is not needed, when only parts of the workplace or services are monitored by video systems[277].

In **Sweden**, the Act on Public Camera Surveillance (1998:150)[278] is also applicable at the workplace. The Act has different constructions for different situations but does not specifically mention the cases of lawful use. For example, in the non-public workplaces, the use of cameras may be considered as a breach of good labour market practice. Furthermore, the employer is obliged to negotiate with the trade unions before making a decision to introduce camera surveillance.[279]

In the case of **Portugal**, besides the Data Protection Law, employment law and criminal law, the Private Security Act also applies to camera surveillance in the workplace. In most of the cases, cameras have been installed for security reasons of persons and goods in places like banks, shops, public buildings, etc. The purpose is not monitoring workers, but assuring security in general. It must also be noted that workers have the constitutional right to safe and healthy working conditions (Article 59). Sometimes these conditions may be more efficiently provided when camera surveillance is being used. Courts have already decided about the use of cameras in the work relationship: they have admitted as admissible evidence the unregistered use of camera surveillance images taped by casinos surveillance's systems[280].

3. Secret cameras

In **Germany**, the case law of labour courts on this matter is restrictive. Under normal working conditions camera surveillance of employees at their workplaces will legally not be acceptable. The Federal Labour Court sees, for instance, the hidden use of video cameras by the employer in order to survey employed sellers as an inadmissible impingement on the personality rights of these employees, if there are no outweighing interests of the employer which merit protection.[281]

---

[277] EA Wien 24.4.1986, RdW 1986, 281.

[278] See the Parliamentary Commission Report SOU 1996:88, Government Bill prop. 1997/98:64, and Judicial Committee Report 1997/98: JuU 14.

[279] See Government Bill prop. 1997/98:64, p. 47.

[280] Ac. Rel. Porto, 20th September 1999; Ac. Rel. Porto, 27th September 1999, http://www.dgsi.pt .

[281] Cf. *Bundesgerichtshof* 25/4/1995 AP Nr. 25 zu § 611 BGB Persönlichkeitsrecht; *Bundesarbeitsgericht* 7/10/1987 AP Nr. 15 op.cit.; *Bundesverfassungsgericht* 19/12/1991 Neue Juristische Wochenschrift 1992 p. 815; Landesarbeitsgericht Köln 26/2/1999, 11 Sa 795/98.

A prevalence of employer's interest could, for instance, be accepted if such an approach is the only choice to identify the person which is responsible for considerable losses of goods in the establishment. The installation of a hidden camera would, however, have to be the only way to identify the offender; this means: the employer must be sure that the operating of an overt video camera as a less intruding and more mild means of investigation would not work.[282] A more recent judgement of the *Landesarbeitsgericht Baden-Württemberg* follows the same lines of reasoning according to which video camera surveillance of the cashier in a retail business encroaches upon the general right of personality if there is only a general suspicion towards the whole staff but no substantial and individualised suspicion of intentional grave breach of contract or of a criminal offence committed by the concerned person.[283] Any information obtained by illegal measures of surveillance is by the courts hold for "fruits of the forbidden tree" and must not be used in legal proceedings.[284]

Quite recently, the **Belgian** *Cour de Cassation* had a chance to give its opinion on secret cameras in a case where shop attendants were stealing from their employer. They were caught solely on the basis of the secret camera installed by the employer. In its judgement of 27 February 2001[285] the Court held that Article 8 of the European Convention on Human Rights (right to privacy) does not prevent the employer to install a camera in a shop without the knowledge of the workers in order to verify a sincere suspicion of serious wrongdoing or misconduct. This is considered to be a quite far-reaching case, but it must nevertheless be noted that the *Cour de Cassation* has not verified the use of the secret camera in light of Collective Bargaining Agreement n° 68 of 16 June 1998. This probably would have made the outcome of the case quite different.

In the **U.K**., the Information Commissioner's Draft Code suggests that covert monitoring is likely to be justified only in highly exceptional cases, such as where overt monitoring would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. In addition, covert monitoring is likely to constitute a breach of the implied contractual duty of trust and confidence.

In the **Netherlands**, reference has to be made to the *Koma*-judgement.[286] In this case, the Dutch firm Koma installed 18 cameras to monitor the workfloor. The employer argued that this would give him a better position to more effectively 'give direct guiding and assistance to the employees'. The employer did consult the works council before installing the cameras and the works council agreed. Nevertheless, a certain number of employees did not agree with the way the employer monitored the workplace. The President stated that Koma could not justify the use of the cameras at the workfloor. According to the President, the employer did not act accordingly to what is expected from a 'good employer' as laid down in article 7:611 of the Dutch civil code, as there was no need for the employer to use the cameras. The President stated that an employer is allowed to supervise his employees and that this kind of surveillance is not unlawful when this is physically performed by a designated person. However, a camera could not be used without a justifiable interest.

Quite recently, the Dutch Supreme Court decided that an employer, who is confronted with theft, may install a camera to solve the problem and use the evidence in court.[287]

The Dutch Data Protection Authority made a checklist in 1998 with some conditions under which camera-surveillance is allowed.[288] The most important guideline that an employer has

[282] *Bundesarbeitsgericht* 7/10/1987 AP Nr. 15 zu § 611 BGB Persönlichkeitsrecht; cf. *Sozialgericht München* 15/5/.1990 CR 1991, 417-418.
[283] *Landesarbeitsgericht Baden-Württemberg* 6/5/1999 BB 1999, 1439 = ArbuR 1999, 491.
[284] *Landesarbeitsgericht Baden-Württemberg* ibidem; cf. *Andea Raffler/Peter Hellich*, Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer e-mails zulässig?, Neue Zeitschrift für Arbeitsrecht (NZA) 1997, pp. 862-868 (863).
[285] Judgement of 27 February 2001, n° P.99.0706.N.
[286] President Rechtbank Roermond, 12 September 1985, KG 1985/299, also known as the Koma-case.
[287] Hoge Raad, 27 April 2001, JAR 2001, 95

to follow in using methods of camera surveillance is firstly that the chosen method is proportional with the goal of the surveillance and that the gathered information should not be used for other purposes. In addition, the gathered information should not be kept for a longer period than necessary. Total and structural camera surveillance is not allowed. The employee must always have the opportunity to do personal activities like eating, putting up make-up etc, also at work. This only applies in those situations where employees are monitored totally. A fragmentary use of cameras vis-à-vis employees would be allowed.

4. Guarantees

In most countries, guarantees for workers in case of camera surveillance arise from the principles laid down in the laws on data protection, or from employment or labour laws.

Some countries that have specific regulations regarding cameras provide for specific procedures. The main guarantee consists of information to employees concerned and to the works council (which also would include consultation). For example, the **Belgian** C.B.A. n°. 68 provides for information to be given to the employees concerned (such as number of cameras, the position of the cameras, the purposes thereof). Furthermore, information and consultation (exchange of views) is required with the workers' representatives, or in the absence thereof, with the workers. Furthermore, if the camera surveillance would have an impact on the rights and duties of the supervising personnel or would be used for the determination of the workers' wages, an amendment of the work regulations is required.

In **France**, camera surveillance in the workplace also requires information and consultation with the works council, before the operational decision is taken, to the extent the cameras allow the monitoring of the employees' activities. Furthermore, the Labour Code also provides that in all cases in which employee data are collected, prior information to the employees is necessary.

D. Other forms of monitoring

There are, of course, other forms of monitoring than telecommunications, internet and e-mail monitoring. The use of recording devices, location data, dataveillance, use of badges, black boxes, etc. are a quite widespread practice among the Member States.

The Member States have not addressed these issues specifically or regulated by specific laws (except, to a certain extent, the case of recording devices).

In some countries, single cases have come up. In **Portugal**, a case before the Data Protection Authority concerned time registration[289]. Employers controlled the presence of employees in the company bathrooms. To control the use of time, the company had installed an electronic device that registered the length of work breaks by the use of an electronic card. One of these devices was installed in the bathrooms. The Portuguese Data Protection Authority was informed of this system by the newspapers and initiated an investigation. It came to the conclusion that this company was using a monitoring system that involved aspects of the employees' private lives, and decided to order the end of data processing. The company reacted in court, but court has agreed with the Data Protection Authority[290].

---

[288] Letter of the Dutch Data Protection Authority of 23 July 1998, and also by the Dutch Data Protection Authority: 'In beeld gebracht, privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging'. Althought this report is not about the relationship employer-employee and is based on the WPR 1988, it still provides some useful information. Both are online available at http://www.cbpweb.nl

[289] Decision 31/96.

[290] STA 5 th June 1997; STA, 19th June 1997. Company has argued that privacy was of less importance than the interest of work and productivity, and that monitoring was important to control work breaks' abuses which could be a reason for sanctions. Nevertheless, they didn't notify the data processing to the Data Protection Authority.

IV. Conclusive remarks and discussion

A. Conclusive remarks

From the above, it may be concluded that the issue of electronic monitoring and surveillance is an extremely actual topic in practically every Member State of the European Union. As far as regulation in the Member States is concerned, the following points may be noted:

1. There is no consistent and uniform approach of employment privacy issues in the Member States. The privacy protection of employees is dealt with through a combination of constitutional laws, general privacy laws and employment laws. As a general rule, privacy laws are not specifically written for the employment relationship and often do not take into account specific principles or categories of employment and labour laws. On the other hand, most employment laws have not addressed the issue of employee privacy. Furthermore, some Member States have general constitutional provisions on privacy, others do not have a constitutional concept of 'the right to privacy', while still others may not really recognise a generic concept of 'constitutional rights'.

2. If Member States are compared, the approach of regulating privacy appears to be different. Most Member States have complied with the European Directive 95/46/EC on data protection. Still, the national implementation of this directive has not always given rise to a specific regulation or manner of regulation of the issue of monitoring and surveillance. It often concerns an interdependency of data protection laws, criminal provisions, employment law principles, civil law provisions, codes of practices, etc. Member States are rather comparable in their specific diversity.

3. Most Member States have implemented the Data Protection Directive 95/46/EC of 24 October 1995 into national law. It must be pointed out that, except from marginal cases, Member States have not gone further than taking over the general principles of the Directive. Furthermore, in many Member States questions arise with regard to the interplay between the Data Protection Directive 95/46/EC of 24 October 1995 and the Telecommunications Data Protection Directive 97/66/EC of 15 December 1997. While the Data Protection Directive is, besides few exceptions, generally clearly implemented into national law, its seems not always to be clear how and to what extent the Telecommunications Directive fits into general data protection principles or into existing labour and employment laws. Where implementation of Directive 97/66/EC may be found, it often takes the form of a general prohibition of monitoring of telecommunication (through specific criminal laws), applicable to, but often not designed for, labour relationships.

4. As far as monitoring by the employer is concerned, the general labour law principles are often used as point of departure. Put in general and abstract terms, these principles imply that employers have a contractually based right to control contract fulfilment and to monitor work performance and the proper use by employees of company equipment. This labour law starting point is subject to limitations. However, most Member States do not specifically address those limitations under their labour laws as far as electronic monitoring is concerned.

5. According to various principles of labour law, it is easy to defend the employer's right to limit access to internet and e-mail facilities, or to telephone communications, and to reserve it strictly for professional purposes. The employer, indeed, has the right to manage the workplace and to exercise authority over the workers. However, this principle remains open for interpretation, and it is still possible for workers to claim certain rights to the use of company facilities for private purposes. Nevertheless, it remains rather unclear on which legal basis employees could rely to claim such private access. Furthermore, the line between acceptable and unacceptable use remains vague and undetermined.

6. In evaluating specific rules on electronic monitoring, where they exist, privacy protection would rather come through specific guarantees and procedures, rather than through severely restricting the monitoring powers of the employer. In this respect, however, the role of collective labour law remains rather unclear. Some Member States expressly involve the works council or the trade unions in electronic monitoring issues. In other Member States, this

involvement is under debate, following lack of clarity with regard to the scope of existing labour law provisions. In cases where trade unions or works councils have a role to play, questions arise as to whether or not such role should be substantial or merely procedural.

7. In most Member States, it remains unclear to what extent professional communication is protected by the right to privacy. Furthermore, in some Member States there is discussion whether or not surfing on the internet may be qualified as a form of communication (opposed to the case of telephone conversations and e-mail).

8. Specific guidance with regard to electronic monitoring is found in some Member States, through codes of practice or official opinions of data protection authorities. In other Member States, there is much reliance on case law (judge made law). It would therefore appear that the approaches are not all the same, with sometimes different (or even opposite) outcomes as a result. Still, it would appear that on certain topics a common ground may be present *de lege ferenda* (see below).

9. Having regard to the amount of ambiguity and discussion in many Member States and having regard to the different approaches or outcomes in protection, a European blue print containing common ground on issues of electronic monitoring may be regarded as desirable.

B. Report of the discussion held at the Employment Privacy Seminar (Leuven, 4/5 October 2001)

The following contains a summary of the discussion held at the occasion of the Employment Privacy Seminar, organised at the Faculty of Law of the University of Leuven (Belgium) on 4/5 October 2001. This seminar was the result of the project which is reported in the present report and co-financed by the Walter Leën Fund of Social Law. It offered an independent academic platform for discussion and exchange of views regarding various issues which the subject involves. The present report contains comments, remarks, guidance, clarifications, and suggestions with regard to the issue of employee data protection and electronic monitoring and which may be useful in policy making in the European Union.

The seminar took the format of an expert seminar. The group of experts was composed of the following members (hereafter referred to as “the Experts”):

- Catarina Castro, University of Coimbra
- Xosé Carril Vásquez, University of Coruña
- Michele Colucci, University of Salerno
- Michael Forde, Law Society of Ireland
- Frank Hendrickx, University of Leuven and University of Tilburg
- Armin Höland, Martin-Luther-Universität Halle-Wittenberg
- Taufan Homan, University of Tilburg
- Annamaria Johansson, University of Lund
- Leonidas Kanellos, University of the Aegean
- Jens Kristiansen, University of Copenhagen
- Nora Melzer, University of Graz
- Gillian Morris, Brunel University
- Sophie Nerbonne, Commission Nationale de l'Informatique et des Libertés
- Anders von Koskull, Swedisch School of Economics and Business Administration

1. General comments on employee privacy

1.1. The Experts recognise that the right to privacy is a fundamental human right and they are of the opinion that employees should be protected by the right to privacy. The Experts have not reached a uniform and common view on the issue of horizontal effect (“Drittwirkung”) of the right to privacy. Some Experts are of the opinion that there is no (and should be no) horizontal effect in the sense that an employee may directly invoke the relevant constitutional article vis-à-vis his employer. Realising that this matter is still under development among the

Member States, there is nevertheless a growing acceptance of aforementioned direct horizontal effect.

The Experts also acknowledge that the constitutional principles of privacy protection remain necessarily general and vague. It is, therefore, not quite clear what it exactly would mean if an employee could invoke a right to privacy. Still, it is important to have a general common ground of privacy within Europe. For the time being, such ground is provided by the European Convention on Human Rights (1950), more specifically by article 8 of the Convention and the relevant case law of the European Court of Human Rights in Strasbourg. A common (core) concept of privacy, provided either by the European Union or by the Council of Europe, is desirable in order to have a uniform scope of the right to privacy, for example with regard to its content and possible limitations.

The Experts conclude that, as far as employment privacy is concerned, more specific rules are necessary. A specific regulation is desirable.

1.2. As far as the sanctioning of privacy violations by the employer is concerned, there are different approaches among the Member States. In all Member States sanctions come from a combination of various laws, such as for example employment laws, privacy laws, criminal laws, civil laws. This approach would not appear to create intolerable situations and may therefore be defended. Many Experts pointed out that the ultimate redress for the employee in case of a privacy violation by the employer, would be a financial compensation rather than the more effective remedy of injunctive relief. Furthermore, legal practice often shows that it is not always easy for an employee to bring up evidence of a violation of his right to privacy and/or of the damage occurred.

1.3. The Experts point to the dangers of the concept of 'privacy expectations'. An employee cannot waive his right to privacy. There should always remain a core of privacy which cannot be contracted away. Privacy expectations may be explicated, e.g. in the employment contract or in a company policy, but they cannot replace the essential and substantial level of protection.

1.4. The issue of employment privacy involves more than one legal discipline. According to the employment and labour laws and principles in the Member States, an employment relationship implies that the employer is entitled to exercise authority over the employee (subordinate relationship). The Experts recognise that, in the employment context, monitoring is the rule and privacy would rather appear to be the exception, although the right to privacy cannot be lost by entering into an employment relationship. It also implies that the employer has a right, within limits, to make use of forms of electronic monitoring.

2. Comments on electronic monitoring: substantial issues

2.1. The question has come up whether there is a difference between traditional forms of monitoring and electronic monitoring, which would need to be taken into account in regulating electronic monitoring. The Experts have answered this affirmatively. They believe that electronic monitoring may be more intrusive as far as privacy is concerned and also raises the broader issue of human dignity.

By way of example, the Experts indicate the following elements of electronic monitoring that would make a difference with traditional forms of monitoring: electronic monitoring allows total control of the individual and may therefore be humanly degrading; it makes monitoring often easier and assumably more widespread, e.g. in the sense that it is not likely that employers will make only limited use thereof; it creates problems as far as evidence is concerned, to the extent that electronic data leave tracks and may give an artificial impression of the reality rather than representing actual the physical reality; electronic monitoring may give rise to covert situations and/or may make surveillance anonymous.

Yet, the Experts are of the opinion that permanent monitoring may always become degrading and contrary to the respect of privacy and human dignity, whether or not the monitoring is electronically or physically.

2.2. A difficult issue is whether an employee is entitled to private access to ICT (Information and Communication Technologies) at the workplace, or whether an employer has a right to communicate for private purposes. The Experts have approached the question differently depending on whether or not communication would be involved. They conclude that the employee has a right to communicate for private purposes, even if the employer would prohibit private access. It is less clear though whether there would be a right to private access to all technologies at work. Distinguishing CT (communication technology) from IT (information technology) may be a relevant issue in this respect. Indeed, the Experts have not reached a consensus regarding whether or not some forms of ICT use, like surfing on the world wide web for example, may be qualified as communication. It has been made clear, though, that e-mail correspondence and telephone conversations come under the notion of communication.

According to the Experts, the employees' right to communicate would imply that the employer must give an employee a facility to private use of communication technology. However, the Experts believe that it would rather depend on the circumstances how this is implemented in the company. One solution may be to provide the employees with access to a private mailbox (for private use only and with a private e-mail address) separated from the professional mailbox (for professional use only, with a professional e-mail address).

While there is a right to communicate, it is recognised that this right remains limited and may only be exercised in very specific circumstances and according to what is reasonable. It is desirable to clearly condition these exceptional circumstances, e.g. communication for urgent private matters, on beforehand. Furthermore, the employer must have the possibility to elaborate preventive and organisational measures, such as the use of firewalls. The Experts recognise the employer's responsibilities and interests.

2.3. The Experts are of the opinion that the employer has the right to monitor the employees electronically for legitimate interests. The employer must always be able to justify electronic monitoring. The Experts have not examined the question on which level the abstract categories of legitimate interests should be further specified (the law, judge-made law, collective bargaining agreement, national code of practice). Still, it was recognised that a union agreement or works council approval may make the justification by the employer easier. Furthermore, the Experts suggest that the individual consent by the employee may have to be excluded as much as possible, but only for the sake of higher protection. Indeed, union or works council agreement should not prevent the individual employee from opposing a specific measure of electronic monitoring.

2.4. As far as telecommunication is concerned, the Experts have examined the question whether there would be a legally relevant distinction between content monitoring on the one hand and traffic data (logging) on the other. The distinction may appear to become relevant in applying a proportionality-test. The Experts are of the opinion that proportionality should form part of the global assessment in addition to the legitimate purpose-test mentioned above (see also below on guarantees and procedural issues). The Experts conclude that the employer must give priority to measures which are less far-reaching and less intrusive than others, taking into account the employer's legitimate purposes.

3. Comments on electronic monitoring: guarantees and procedural issues

3.1. As far as guarantees are concerned, the Experts are of the opinion that the principles arising of the Data Protection Directive 95/46/EC should always be applied. These principles include, among other things:

- monitoring is only allowed for legitimate purposes;
- transparency of the monitoring is required (including information of the individual employees concerned);

- the measures of monitoring must be proportionate with regard to the purposes pursued by the employer;
- data may only be retained for a limited period of time;
- a decision affecting the employee significantly cannot be taken solely on purely automated data.

3.2. In addition to the data protection principles mentioned in Directive 95/46/EC, the Experts conclude that there should be a role for the works council and the trade unions. However, there is a divided view on what this role should be. Some Experts argue for a mere procedural role (the union or the works council should be informed or consulted) while other Experts are more in favour of a substantial role of trade unions or works councils (approval of the measure of electronic monitoring). This issue appears to be very closely related with the various national labour laws and practices.

The Experts agree that no form of collective guarantees should ever replace individual guarantees.

3.3. The Experts are reluctant with regard to the use of electronic evidence in the courts. They point out that this kind of evidence may lead to false or incomplete conclusions about the physical reality if not properly presented or not correctly brought into relationship with other elements of proof.

4. Comments regarding policy making

4.1. As far as European policy making is concerned, the Experts are of the opinion that employee privacy protection and free movement of information within the community may be improved by the drafting of an instrument containing a European framework with principles and standards on employment privacy. In the Member States a lack of clarity remains regarding most or some of the questions which arise in the field of employee data protection and electronic monitoring.

As the issue is not only a matter of data protection law, but also strongly linked with labour and employment laws, the Experts recommend to involve the European social partners in the formulation of a European instrument. The Experts have not reached an opinion with regard to the legal nature which such European instrument should receive (collective bargaining agreement, code of practice, directive, …).

4.2. It would be desirable that a regulation on European level clarifies the meaning of the provisions in the Telecommunication Privacy Directive 97/66/EC as well as the interplay of these provisions with the Data Protection Directive 95/46/EC.

C. Some notes on possible EU policy

The following will provide some suggestions and ideas for further discussion at EU level on policy in the examined field of study. It further develops some points relevant to the foregoing conclusions in this matter (study VC/2001/0159). It is not exhaustive and expresses the personal academic impressions of the Contractor.

1. General legitimacy of processing workers' personal data

1.1. The most relevant legitimacy criteria in this matter, besides consent, are laid down in Directive 95/46/EC:
- processing is necessary for the performance of a **contract** to which the data subject is party
- processing is necessary for the purposes of the **legitimate interests** pursued by the controller

One another comes down to determining the legitimate purposes of electronic monitoring (internet, e-mail, cameras):

1.2. In the study mentioned above, the main principle under employment law is that the employer has a legitimate interest and is allowed to process personal data and to monitor the workers. The purposes for which monitoring may be considered to be legitimate may vary from one Member State to another, but generally the following lawful purposes may be found:

- health and safety requirements
- protection of equipment and employer's property
- correct use of equipment (employer's standards)
- monitoring production processes
- work performance (including use of working time) and quality control

The aforementioned purposes may be called 'lawful business purposes'.

2. Specific issue: monitoring of telecommunications

2.1. According to the experts mentioned in the study, employees should be entitled to **limited private access** or private facilities with regard to communication technologies (like telephone and e-mail) in the workplace. A complete ban on the private use of the company's communication system ('zero tolerance') by the employer does not seem to have a legitimate character in view of the fundamental right to privacy (including 'communication privacy').

Private access by the employee should remain **limited**. This implies that:

- such entitlement should be limited to exceptional circumstances (e.g. use of communication technologies for urgent personal matters which have either a close connection with the professional activities in the company or which cannot receive delay);
- private access should be employed by the employee outside normal working hours, if possible;
- if used during normal working hours, private access should remain limited in time;
- private access should not imply 'free access';
- there should be no right to private surfing on the internet if unconnected with communication.

2.2. Employers may however **prohibit** the use of the company's *professional* e-mail address. But in such case, a private e-mail address (e.g. a 'hotmail' address) or alternative must be accessible.

2.3. The employer is allowed to monitor the use by the employee of telephone, internet and e-mail. The following 'lawful business purposes' may be found for telephone, internet or e-mail monitoring:

- to monitor work performance and quality control
- to ascertain compliance with (self-)regulatory standards or procedures
- to investigate or detect unauthorised use of the system
- to secure effective system operation
- to prevent or detect crime
- to collect evidence of business transactions

2.4. Apart from the legitimacy argument, there must be a **proportionality**-test. There may be no excessive monitoring.

- **Time** is an important element. In general terms, *permanent* monitoring or *routine* monitoring is considered to be humanly degrading and therefore unlawful. The timing of the monitoring should be related to the legitimate purposes (e.g. suspicion of abuse; quality control of tele-operators), i.e. as long as is strictly necessary for those purposes. There may be no general *a priori* monitoring for all purposes of all data flow on internet, e-mail or telephone.

- There is an important difference between **content** monitoring and **logging**. It is e.g. often stated that websites visited or content viewed should not be monitored unless it is clear that the business purpose for which the monitoring is undertaken cannot be achieved by simply recording the time spent on the internet.

- There is also an important difference between **general** monitoring and **individualised** monitoring. E.g., as far as web control is concerned, individual analysis of consulted websites or the content thereof must be avoided, unless it is required by the legitimate purpose(s) indicated by the employer.

- The employer is not entitled to monitor the content of e-mail if it appears to be of a **private nature**. This is also the case even when private use is prohibited. It may be possible that the employer does not know on beforehand which communication is private and which one is not. In this case it is recommended to define the reasonable privacy expectations regarding communication in the workplace on beforehand (e.g. when is the professional character of e-mail presumed). Within the limits mentioned elsewhere, this should remain within the employer's managerial prerogatives.

- On (pre)defined **professional areas** (e-mail account, intranet, …) the monitoring of communication by the employer may become more legitimate. To a certain extent, professional e-mail may be compared with professional traditional correspondence like letters. But an e-mail may also be regarded as a combination of a letter and an oral conversation.

- It is also important that the **privacy of senders** (e.g. incoming e-mail) remains protected.

3. Specific issue: camera surveillance

3.1. In general terms, camera surveillance should be considered to be lawful.

3.2. The lawful **purposes** of camera surveillance may be enumerated in a limitative way. The following uses of cameras in the workplace may be considered to be lawful:

- the protection of health and safety
- the protection of the employer's property
- the monitoring of the production process
- the monitoring of the work performance

3.3. A proportionality test should be made:

- no permanent monitoring
- no monitoring in private areas (like bathrooms, …)
- secret monitoring in very limited circumstances (e.g. reasonable suspicion of serious misconduct)

4. Guarantees

4.1. As far as guarantees are concerned, reference can be made to the principles of the Data Protection Directive 95/46/EC.

4.2. Essential elements which have to be addressed in the elaboration of policies are a.o.:

- **transparency:** there should be a clear policy or warning in the company with regard to:
    - purposes of monitoring
    - organisation of monitoring (e.g. time, what, how, who, …) (e.g. in case of cameras: number of cameras, the position of the cameras, …)

    - privacy expectations: professional versus private use
    - further use of data

- **information and consultation** with workers or workers' representatives
    - a procedural right
    - prior to introduction of monitoring systems
    - regular assessment of monitoring systems
    - agreement of workers' representatives or negotiated policies may not override individual privacy rights; may not replace individual consent

- **individual rights:**
    - receiving all relevant information (cf. transparency)
    - prior warnings where relevant
    - access to personal file regarding monitoring
    - access to responsible officer or department within the company
    - a decision affecting the employee significantly cannot be taken solely on purely automated data
    - protection of third parties

- **quality of monitoring:**
    - security
    - integrity of system manager(s)
    - not keep information longer than necessary

*** * ***