5062/01/EN/Final
WP 48

Opinion 8/2001

on the processing of personal data in the employment context

Adopted on 13 September2001

ARTICLE 29 WORKING PARTY OPINION[1] ON THE PROCESSING OF PERSONAL DATA IN THE EMPLOYMENT CONTEXT

DRAFT EXECUTIVE SUMMARY

The processing of personal data in the employment context is the subject of debate at both the Community and the national levels. Governments and Data Protection Authorities in the Member States have produced or are in the process of producing legislation, codes, or recommendations addressing several data protection issues in the employment context. The European Commission, in the framework of the Social Policy Agenda, has launched a consultation with social partners on data protection in the employment context.

In order to contribute to the uniform application of the national measures adopted under the Data Protection Directive 95/46/EC[2], the Working Party has set up a subgroup to examine this question[3] and has adopted an **extensive document** which can be found on the Internet in the following address[4]:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

Employers and workers must be aware that **many activities performed routinely in the employment context entail the processing of personal data of workers**, sometimes of very sensitive information.[5]. Any collection, use or storage of information about workers by electronic means will almost certainly fall within the scope of the data protection legislation. This is also the case of the monitoring of workers' email or Internet access by the employer. **The monitoring of email necessary involves the processing of personal**

---

[1] The Article 29 Working Party is an advisory group composed by representatives of the data protection authorities of the Member States, which acts independently and has the task, inter alia, of examining any question covering the application of the national measures adopted under the Data Protection Directive in order to contribute to the uniform application of such measures;

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data. OJ L 281, 23.11..95, p. 31

[3] The following supervisory authorities have contributed to the work of this subgroup: AT, BE, DE, EL, ES, FR, IR, IT, NL, UK.

[4] The document includes a catalogue of the most relevant data protection legislation in the Member States with some impact in the employment context.

[5] Examples of employment records usually involving the processing of personal data covered by Directive 95/46/EC. Application forms and work references, Payroll and tax information-tax and social benefits information, Sickness records, Annual leave records, Unpaid leave/special leave records, Annual appraisal/assessment records, Records relating to promoting, transfer, Training, disciplinary matters, Records relating to accident at work, etc.

data. The processing of sound and image data in the employment context falls within the scope of the data protection legislation and video surveillance of workers is covered by the provisions of the Directive and the national laws transposing it.

When processing workers' personal data, employers should always bear in mind **FUNDAMENTAL DATA PROTECTION PRINCIPLES SUCH AS THE FOLLOWING**:

- **FINALITY**: Data must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes.
- **TRANSPARENCY:** As a very minimum, workers need to know which data is the employer collecting about them (directly or from other sources), which are the purposes of processing operations envisaged or carried out with these data presently or in the future. Transparency is also assured by granting the data subject the right to access to his/her personal data and with the data controllers' obligation of notifying supervisory authorities as provided in national law.
- **LEGITIMACY:** The processing of workers' personal data must be legitimate. Article 7 of the Directive lists the criteria making the processing legitimate.
- **PROPORTIONALITY:** The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Assuming that workers have been informed about the processing operation and assuming that such processing activity is legitimate and proportionate, such a processing still needs to be fair with the worker.
- **ACCURACY AND RETENTION OF THE DATA:** Employment records must be accurate and, where necessary, kept up to date. The employer must take every reasonable step to ensure that data inaccurate or incomplete, having regard to the purposes for which they were collected or further processed, are erased or rectified.
- **SECURITY:** The employer must implement appropriate technical and organisational measures at the workplace to guarantee that the personal data of his workers is kept secured. Particular protection should be granted as regards unauthorised disclosure or access.
- **AWARENESS OF THE STAFF:** Staff in charge or with responsibilities in the processing of personal data of other workers need to know about data protection and receive proper training. Without an adequate training of the staff handling personal data, there could never be appropriate respect for the privacy of workers in the workplace.

CONSENT. The Article 29 Working Party has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.

WORKERS ARE DATA SUBJECTS who benefit from the rights conferred by the Data Protection Directive. The most important of these rights is the right of access provided for in Article 12 of the Directive.[6]

INTERACTION BETWEEN LABOUR LAW AND DATA PROTECTION LAW. The Working Party would like to point out that data protection law does not operate in isolation from labour law and practice, and labour law and practice does not operate in isolation from data protection law. This interaction is necessary and valuable and should assist the development of solutions that properly protect workers' interests.

SURVEILLANCE AND MONITORING. Data protection requirements apply to the monitoring and surveillance of workers whether in terms of email use, Internet access, video cameras or location data. **Any monitoring must be a proportionate** response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers. **Any personal data** held or used in the course of monitoring must be **adequate, relevant and not excessive for the purpose for which the monitoring is justified**. Any monitoring must be carried out in the least intrusive way possible.

TRANSFER OF WORKERS' DATA TO THIRD COUNTRIES. Article 25 of the Directive establishes that transfers of personal data to a third country outside the EU can only take place where the third country ensures an adequate level of protection for the data. It must be remembered that whatever the basis of the transfer under Articles 25 and 26 processing involved in the transfer must still satisfy Article 6 to 8 and all the other provisions of the Directive.

The Working Party believes that **it is preferable to rely on** adequate protection in the **country of** destination **rather** than relying on **the derogations listed in Article 26, for example the workers' consent.** Where consent is relied on, it must be unambiguous and freely given. Employers would be ill-advised to rely **solely** on consent other than in cases where, if consent is subsequently withdrawn, this will not cause problems.

FURTHER GUIDANCE. The Working Party is considering further guidance on the issues where the application of general principles of data protection raises particular problems relevant to the employment context, such as the surveillance and monitoring at the working place, employee evaluation data and others.

---

[6] Every data subject is entitled to obtain from the controller (the employer in this case):
a) without constraint at reasonable intervals and without excessive delay or expense:
- Confirmation as to whether or not data relating to the worker are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipient or categories of recipients to whom the data are disclosed,
- Communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- Knowledge of the logic involved in any automatic processing of data concerning him at least in the case of automated decisions

b) as appropriate the rectification, erasure or blocking of data the provisions of which does not comply with data protection law, in particular because of the incomplete or inaccurate nature of the data;
c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with the previous obligation, unless this proves impossible or involves a disproportionate effort.

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[7],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT OPINION:

1. Introduction

The processing of personal data in the employment context is the subject of debate at both the Community and the national levels.

Governments and Data Protection Authorities in the Member States have produced or are in the process of producing legislation, codes, studies and recommendations addressing several data protection issues in the employment context.

Current Work and Recent Initiatives:

BELGIUM	*Opinion 10/2000 of the Commission for the Protection of Privacy "Opinion regarding the monitoring by the employer of the use of computer systems at the workplace"*[8]
FRANCE	*CNIL public consultation based on the report "La cybersurveillance des salariés dans l'entreprise"*[9]
GREECE	*Draft recommendation on the Protection of Employees' Data*[10]
GERMANY	*Following suggestions from the German Supervisory Authority, the Parliament has repeatedly asked the Government to present a bill on data protection in the labour relations.*
NETHERLANDS	*Report of the Registratiekamer "Working Well in Networks"*[11]
SPAIN	*Study published by the Spanish Data Protection Agency related to "Use and Control of automated employment data"*[12].
UNITED KINGDOM	*Draft Code of Practice from the Information Commissioner "The Use of Personal Data in Employer/Employee Relationships"*[13]

[7] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

[8] www.privacy.fgov.be

[9] www.cnil.fr/thematic/indextd2.htm

[10] www.dpa.gr (only in Greek language)

[11] www.cbpweb.nl

[12] not available on the Web; please contact: Agencia de Protección de Datos. C/Sagasta 22, 28004, Madrid

[13] wood.ccta.gov.uk/dpr/dpdoc.nsf

Supervisory authorities have regularly dealt with a range of data protection issues in employment. These include:

- accuracy of employee data
- monitoring of personal telephone use
- access to medical information
- use of information on trade union membership
- processing in the course of business mergers or acquisitions

Data Protection laws in the EU confer individual rights to any person concerned by the processing of personal data (e.g.: right of access, right to rectify). As a general rule, these rights apply fully to the employee-employer relationship, and the only possible exceptions are those allowed by Directive 95/46/EC. However, as the provisions of the Directive are rather general, some guidance will be helpful to clarify certain aspects of the application of the above provisions in the employment context.

The European Commission, in the framework of the Social Policy Agenda, has launched a consultation with social partners on data protection in the employment context.

In order to contribute to the uniform application of the national measures adopted under Directive 95/46/EC, the Working Party has set up a subgroup to examine this question[14] and has adopted this opinion.

The subgroup is currently working on a specific opinion which will focus on the application of Directive 95/46/EC to the surveillance and monitoring of electronic communications in the workplace .

2. Processing of personal data at the workplace

Employers and workers, both in the public and the private sector, must be aware that many activities performed routinely in the employment context entail the processing of personal data of workers, sometimes of sensitive information.

In fact, employers are collecting personal data from their workers for many different purposes since the very beginning of the employment relationship or even before. During the recruitment process, individuals applying for a job have to provide personal information to their potential employer who, at the same time, usually processes this personal information in order to asses the merits of the candidates.

The collection and further processing of personal data of workers continues during the whole employment relationship. These processing activities concern in normal circumstances all personal information the employer has requested and/or obtained from his workers.

All employers collect payroll and tax information of their workers. The processing of this personal data is necessary for the performance of the employment relationship or for

[14] The following supervisory authorities have contributed to the work of this subgroup: AT, BE, DE, EL, ES, FR, IR, IT, NL, UK.

compliance with legal obligations (social security, payment of taxes), to which the employer is subject. In some Member States, employers collect and process medical information that they store in sickness records; in other Member States, this information is limited to absence data because of illness.

Employers, indeed, assess their workers' performance by collecting personal information directly from the individuals or by other means, including surveillance and monitoring carried out electronically.

Finally, although the collection of personal data of a given worker normally finishes at the end of his/her employment relationship, the processing of his personal information by the former employer may continue. Employers usually keep employment records for a certain period of time, in many cases for mere compliance with a legal obligation of storing employment records for a prescribed period of time.

Examples of employment records usually involving the processing of personal data covered by Directive 95/46/EC
Application forms and work references
Payroll and tax information-tax and social benefits information
Sickness records
Annual leave records
Unpaid leave/special leave records
Annual appraisal/assessment records
Records relating to promoting, transfer, Training, disciplinary matters.-
Records relating to promoting, transfer, Training, disciplinary matters
Records relating to accident at work
Information generated by computer systems
Attendance records
Family members[15]
Reimbursement of expenses, e.g. travel

As the European Court of Human Rights has pointed out in the case Niemitz v. Germany:

"Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of private life should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lifes that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not."[16]

[15] Data processed in order to facilitate access to certain services such as nursery schools, studies, transport/travel, etc

[16] ECHR, 23 November 1992, Series A No. 251/B, para. 29.

3. Most relevant international instruments

3.1. European Community

- Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data[17].
- Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector[18]
- Article 286 EC Treaty
- Regulation (EC) No. 45/2001 of the EP and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[19]
- Charter of Fundamental Rights of the European Union[20].

3.2. Council of Europe

- European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Art. 8
- Council of Europe's Convention (108) for the Protection of Individuals with regard to Automatic Processing of Personal Data.[21]
- Council of Europe's Recommendation (89) 2 on the Protection of Personal Data used for Employment Purposes[22]
- Council of Europe's Recommendation (97) 5 on the Protection of Medical Data[23]

---

[17] OJ L 281, 23.11.1995, p. 31. http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

[18] OJ L 24, 30.01.98, p. 1.
http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf

[19] http://europa.eu.int/eur-lex/en/search/search_lif.html

[20] http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf
Article 8. Protection of personal data.
Everyone has the right to the protection of personal data concerning him or her.
Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.
Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
Compliance with these rules shall be subject to control by an independent authority

[21] http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=108&CM=8&DF=

[22] http://cm.coe.int/ta/rec/1989/89r2.htm

[23] http://cm.coe.int/ta/rec/1997/97r5.html

- Council of Europe's Recommendation (86) 1 on the Protection of personal data used for social security purposes[24]

3.3. International Labour Office (ILO)

- The International Labour Office Code of Practice on protection of workers' personal data (1997)

4. National data protection legislation applying to the employment context

a) Member States of the EU

Austria

- General legislation: Federal Law on the protection of personal data[25]
- Explicit provision concerning the use of sensitive data in the workplace[26]
- Information and consent procedures before introducing control measures at the workplace (Labour Councils)[27]
- Specific prohibition for employers to have workers or candidates genetically tested[28]

Belgium

- General Law : Law of 8 December 1992 on the protection of privacy of individuals[29]
- Specific regulation concerning the handling of medical data in connection with medical examinations of workers
- Decree at regional level concerning the handling of sensitive data in outplacement, recruitment and selection agencies
- Two collective agreements (No. 13 and 68) containing provisions as regards information and consultation procedures with the employees.

Denmark

- General Law: The Act on Processing of Personal Data (Act No. 429 of 31 May 2000)[30]
- Specific legislation concerning the handling of medical data in connection with medical examinations of workers:
- Specific legislation for public servants

[24] http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R(86)1E.htm

[25] http://www.bka.gv.at/datenschutz/indexe.htm

[26] Sect 9, subparagraph 11

[27] Constitutional Act on Labour No. 22/1974, Art. 96.

[28] Genetic Engineering Act No. 510/1994, Sect. 67.

[29] http://www.privacy.fgov.be/loi98coordi.htm

[30] http://www.datatilsynet.dk/eng/index.html

Finland

- General Law: Personal Data Act (523/1999) [31]
- Specific legislation on the protection of privacy in the working life (Act adopted by the Finnish Parliament in May 2001, scheduled to come into force in Autumn 2001).[32]

France

- General Law: Law Nr. 78-17 of 6 January 1978 on the protection of privacy of individuals[33]
- Specific rules on the protection of workers' data in the Labour Code[34]

Germany

- General Law: FederalData Protection Act (BDSG)[35]
- Detailed data protection regulations for civil servants (Framework Civil Service Act - BRRG- , 56 to 56 f and Federal Civil Service Act -BBG- 90 to 90 g, both enacted in 1997).

Implementation of technical installations which can be used for the monitoring of the performance of the behaviour only with agreement of workers' council according to legal regulations of collective labour law (private and public sectors).

Greece

- General Law 2472/97 on the protection of individuals with respect to the processing of personal data [36]

Ireland

- General Law: Data Protection Act of 1988[37]

---

[31] http://www.tietosuoja.fi/uploads/hopxtvf.HTM

[32] This is the first legislation in the Community dealing specifically with data protection at the workplace. This Act addresses most of the issues mentioned in this paper as well as particularised issues such as tests assessing the suitability of employees (Section 5), medical examinations and other testing (Section 6), Genetic tests (Section 7), Data on the employee's state of health (Section 8) or procedures related to technical surveillance and arrangement of the use of information networks (Section 9).

[33] http://www.cnil.fr/textes/index.htm

[34] http://www.legifrance.gouv.fr/html/frame_codes1.htm

[35] http://www.bfd.bund.de/information/BDSG_neu.pdf

[36] http://www.dpa.gr/2472.htm

[37] http://www.dataprivacy.ie/6ai.htm

Italy

- General Law: Protection of individuals and other subjects with regard to the processing of personal data Act no. 675 of 31 December 1996[38]
- Law n. 135 of 11 May 1999 on sensitive data processed by Public Administrations
- Law n. 300/1970 (Workers Statute)
- Specific provisions restricting surveillance and monitoring of workers
- Authorisation n. 2/2000 of the Italian Supervisory Authority

Luxembourg

- General Law on the use of data in electronic transfer (law of 31 March 1979).
- New law project presented in October 2000, first reading scheduled Autumn 2001.

The Netherlands

- General Law: Data Protection Act of 6 July 2000[39] (entering into force on the 1st of September 2001).
- Labour law provisions on information and consent procedures with the Works Councils.[40]
- Law concerning sickness records and payment of employees (January 2001)[41]
- Law concerning the registration of the ethnical origin of employees (April 1998).

Identification Act (December 1993) and the Personal identification number Act (January 2001).[42]

[38] http://astra.garanteprivacy.it/garante/frontdoor/1,1003,,00.html?LANG=2

[39] http://www.registratiekamer.nl/bis/top_2_6.html

[40] Working Conditions Acts (November 1998), Arts. 5.1.-5.3, Works Council Law (October 1999), General Labour regulations for governmental staff (December 2000)

[41] Article 29. The Unions should be informed, be heard and in some cases have to agree when there is a collective agreement.

[42] Only in some cases necessary for the fulfilment of a legal obligation, the employer is authorised to use the personal identification number.

Portugal

- General legislation: Law 67/98 of 26 October 1998[43]
- Sectoral legislation:
  - Constitutional Law of the Portuguese Republic[44]
  - Law on the protection of privacy in the telecommunications sector – Law n° 69/98 of 28 October[45]
  - Legislation setting up the obligation for the employer to inform the employee on conditions applicable to the labour contract – Decree n° 5/94 of 11 January[46]
  - Law on the system of collection of union contributions – Law n° 81/2001 of 5 August[47]
  - Modalities of organisation and functioning of services for safety, hygiene and health on the workplace – Decree n° 26/94 of 1 February[48]

Spain

- General Law: Organic Law 15/99 of 13 December on the Protection of personal Data[49]
- Royal Decree 994/1999 on the mandatory security measures for the computer files which contain personal data[50]
- Royal Decree 1/1995 on the consolidated text of the Law of the Statute of Workers[51]
- Organic Law 11/1985 on Freedom of Trade Union[52]

Labour Hazards Prevention Law 31/1995[53]

Sweden

- General Law: Personal Data Act of 24 October 1998 (1998:204)[54]
- Specific provisions as regards consultation with workers' representatives when introducing camera surveillance. Regulation stating that monitoring of workers' performance is not allowed without his or her knowledge and trade union representatives are to be heard prior to introducing control mechanisms.[55]

---

[43] http://www.cnpd.pt/Leis/leis.htm

[44] Art. 32(8) – Any proof obtained through abusive intrusion in private life, domicile, correspondence and telecommunications is unacceptable; Art. 34(1) – The privacy of correspondence and other means of private communication is inviolable.

[45] Art. 5 – Confidentiality of communications (http://www.cnpd.pt/Leis/leis.htm)

[46] Art. 3(2) and 4

[47] Art. 3 and 4

[48] Art. 16, 17 and 18

[49] http://www.agenciaprotecciondatos.org/datd1.htm

[50] http://www.agenciaprotecciondatos.org/datd8.htm

[51] http://www.ccoo.es/legislacion/ley11_8S.htm

[52] http://www.ccoo.es/legislacion

[53] http://www.websindical.com/legis/prl.htm

[54] http://www.datainspektionen.se/in_english/

[55] Article 11 Lag (1976:580), Articles 1 and 3 Lag (1998: 150)

United Kingdom

- General Law: Data Protection Act 1998[56]

b) EEA Member States

Norway

- General Law: Personal Data Protection Act[57]
- Specific provisions in the main collective agreement regulate the matter of monitoring the workplace, with consultation and information procedures with Trade Union representatives.

Iceland

- General Law: Act on Protection of Individuals with regard to the Processing of Personal Data No. 77/2000[58]

5. Scope and implementation of the Directive

Directive 95/46/EC applies 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 relevant filing system or are intended to form part of a filing system. "Personal data" means any information relating to an identified or identifiable natural person. Processing is very widely defined. Thus any collection, use or storage of information about workers by electronic means will almost certainly fall within the scope of the Directive.

The monitoring of workers' email or Internet access by the employer falls within the Directive's scope. The monitoring of email necessarily involves the processing of personal data. The monitoring of Internet access, unless conducted as such a high level, that access to particular sites or patterns of access cannot be linked to specific individuals, and only aggregated information is produced necessarily involves the processing of personal data about the worker gaining access. The processing of sound and image data in the employment context falls within the scope of the Directive and video surveillance of workers is covered by its provisions.

Not all manual records necessarily fall within the Directive's scope. They only do so if they form part of a 'personal data filing system'. This is defined as any structured set of personal data, which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. Most employment records are likely to fall within this definition. However, in some countries, the implementing measures may exclude some hand-written notes retained outside any form of filing system but given the necessarily structured nature of employment records will include most information kept about workers whether centrally or by line managers.

[56] http://wood.ccta.gov.uk/dpr/dpdoc.nsf

[57] http://www.datatilsynet.no/

[58] http://www.personuvernd.is/tolvunefnd.nsf/pages/1E685B166D04084D00256922004744AF

In addition to the general Data Protection Directive (95/46/EC) the Telecommunications Data Protection Directive (97/66/EC) might also be relevant. This particularises and complements Directive 95/46/EC with respect to the processing of personal data in the telecommunications sector. As well as falling within the scope of Directive 95/46/EC monitoring of electronic communications by employers, including email and Internet access, might also fall within the scope of Directive 97/66/EC, which is being revised in the context of the review of community legal framework on telecommunications.

The Working Party would like to point out that data protection law does not operate in isolation from labour law and practice, and labour law and practice does not operate in isolation from data protection law. There is necessarily an interaction between the two. The precise nature of this interaction varies between Member States, but it is generally the case that:

- the developing use of information and communications technology in employment increases the extent of this interaction because employment practices rely more and more on the processing of personal data to which general data protection principles apply;

- not all problems that arise in the employment context and involve the processing of personal data are exclusively data protection ones;

- the interaction is necessary and valuable and should assist the development of solutions that properly protect workers' interests.

6. Lawfulness of the processing of personal data

Any processing of personal data, including in the employment context, must meet the requirements of Section II of Directive 95/46/EC to be lawful. In any case, it is necessary to establish a lawful basis for processing under Articles 6, 7 and 8 of the Directive (this last Article in the case of sensitive data).

The data controller must also observe other requirements which include:

FURTHER REQUIREMENTS IN ADDITION TO ARTICLES 6, 7 AND 8
INFORMATION TO BE GIVEN TO THE DATA SUBJECTS (ARTICLES 10 AND 11)
THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA (ARTICLE 12)
THE DATA SUBJECT'S RIGHT TO OBJECT TO PROCESSING (ARTICLES 14 AND 15)
CONFIDENTIALITY AND SECURITY OF PROCESSING (ARTICLES 16 AND 17)
NOTIFICATION TO THE SUPERVISORY AUTHORITY (ARTICLES 18,19,20,21

The Directive allows some limited exemptions from some of the above requirements but not from Article 7 or 8 (Articles 9 and 13).

7. Criteria for making data processing legitimate. Article 7.

At least one of the criteria set out in Article 7 must be satisfied if personal data are to be processed in the employment context. Each of these criteria requires that in any case, in which it is relied on the processing that takes place is actually "necessary for" the achievement of the objective in question rather then merely incidental to its achievement.

Those most likely to be relevant are:

PROCESSING IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY…
(ARTICLE 7.1.B)

Employment relationships are very often based on a contract of employment between the employer and worker. To meet its obligations under the contract to, for example, pay the worker, the employer must process some personal data.

PROCESSING IS NECESSARY FOR COMPLIANCE WITH A LEGAL OBLIGATION…
(ARTICLE 7.1.C)

Employment law may impose legal obligations on the employer, which necessarily require the processing of personal data. The employer may be under a legal obligation to make certain disclosures of personal data, for example, to the tax authorities or to process data or in connection with social security payments.

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 …
(Article 7.1.F).

This criterion requires a balance to be struck between the interests of the employer and the interests of workers. Some supervisory authorities have issued guidance on how the balance between the interests of the data controller and the interests of the data subject should be struck. It is important to remember that if this criterion is relied on the worker retains the right to object to the processing on compelling legitimate grounds (Article 14).

Other criteria that are less likely to be relevant in the employment context are:

- **PROCESSING IS NECESSARY IN ORDER TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT.**
  (Article 7.1.D)

  This may be relevant in the context of the protection of safety.

- **PROCESSING IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST….**

(Article 7.1.E).

The circumstances, in which this criterion is relevant in the employment context, are likely to be very limited.

If none of the criteria are applicable to the processing of a worker's data by an employer, the employer can, alternatively, obtain the worker's unambiguous consent to the processing. The meaning of "consent" is discussed further in Section 11.

8. The processing of sensitive data. Article 8.

The Directive identifies special categories of data, which are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and those concerning health or sex life. The Directive also affords special protection to data relating to offences, criminal convictions or security measures. Member States do not have freedom to add to this list nor to reduce it. They can of course establish special safeguards for certain categories of data, such as genetic data.

Article 8 starts from the proposition that the processing of data in the special categories ("sensitive data") is prohibited. There are then several exceptions, which set out particular circumstances in which the prohibition does not apply. The national laws of some Member States may limit the extent to which employers can take advantage of these exceptions. Thus Members States make more or less extensive use of these exceptions. The Directive allows Member States to lay down additional exceptions for reasons of substantial public interest.

If none of the other exceptions apply an employer can rely on the explicit consent of the data subject for processing sensitive data unless the law of its member state provides that the prohibition on processing sensitive data may not be lifted by the data subject's consent as it is the case, under certain circumstances, for example in Belgium. The extent to which consent can be used in the employment relationship is however limited, as is outlined in section 11.

Example:
Circumstances in which the processing of sensitive data by an employer is limited by national law even though it might fall within one of the exceptions in Article 8 are the processing of data on a worker's medical condition in France and of genetic data in Austria. An example of additional exceptions laid down by Member States is the processing of sensitive data as to racial or ethnic origin for the purpose of ensuring equality of treatment. Several Member States make specific provision for this.

As additional examples, in the employment context the sensitive data most likely to be held by employers, if permitted by national law and provided the purpose limitation principle is respected, include

•	Trade union membership	-	for example to enable the employer to deduct trade union subscriptions from salary on behalf of the trade union
•	Health	-	for example in connection with pay during sickness, meeting health and safety requirements, providing an occupational health scheme, providing insurance or pension benefits
•	Criminal offences	-	for example in connection with the investigation of fraud by workers, ensuring workers with convictions for dishonesty are not put in a position of trust.

The Article 8 exceptions are much narrower than the Article 7 criteria.

Those most likely to be relevant in the employment context are:

PROCESSING IS NECESSARY FOR THE PURPOSES OF CARRYING OUT THE OBLIGATIONS AND SPECIFIC RIGHTS OF THE CONTROLLER IN THE FIELD OF EMPLOYMENT LAW INSOFAR AS IT IS AUTHORISED BY NATIONAL LAW PROVIDING FOR APPROPRIATE SAFEGUARDS.
(ARTICLE 8.2.B)

This is clearly directed at the employment context and can have wide effect. Much depends on the extent to which in each Member State the obligations and rights of an employer are set out in employment law or simply a matter of custom and practice.

PROCESSING IS NECESSARY FOR THE ESTABLISHMENT, EXERCISE OR DEFENCE OF LEGAL CLAIMS.
(ARTICLE 8.2.E)

This has some relevance in the employment context particularly in relation to claims made by workers against their employer perhaps on the grounds of unfair dismissal, e.g. transfer of workers' data to lawyers and courts. It is however limited to actual and really prospective claims. It would not justify the processing of sensitive data of all workers on the basis that one day one of them or a third party might make a legal claim.

PROCESSING IS REQUIRED FOR MEDICAL PURPOSES AND THE DATA ARE PROCESSED BY A HEALTH PROFESSIONAL SUBJECT TO AN OBLIGATION OF PROFESSIONAL SECRECY OR SOMEONE ELSE SUBJECT TO A SIMILAR OBLIGATION.
(ARTICLE 8.3)

This will be relevant in the context of occupational health schemes.

Moreover, Article 20 of the Directive lays down additional safeguards by stipulating that the processing operations likely to present specific risks to the rights and freedoms of data subjects are subject to prior checking by the supervisory authorities.

9. Principles relating to data quality. Article 6.

A data controller must meet the requirements of its national law implementing Article 6 of the Directive as well as satisfying an Article 7 criteria and in the case of sensitive data an Article 8 exception. Article 6 establishes that personal data must be:

(a) processing fairly and lawfully
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes
(c) adequate, relevant and not excessive
(d) accurate and, where necessary, kept up-to-date
(e) kept in a form, which permits identification of data subjects for no longer than is necessary.

These principles apply to the processing of personal data in an employment context as they do elsewhere. They take account of the circumstances in which personal data are processed, including where they are processed by an external subcontractor.

Example:
A record held by a bank that includes a customer's social insurance number may be excessive but if an employer's record does not include this information about workers it may not be sufficient for its purpose. Several supervisory authorities have taken the view that the collection of social insurance numbers from all applicants for jobs is likely to be excessive and thereby breach data protection requirements. It is only the successful applicant who should be required to supply these details.

The requirement that personal data are processed fairly and lawfully provides significant protection. For personal data to be processed lawfully they must be processed in a way that does not bring about a breach of either data protection law or other legal requirements. These may be general legal requirements that are relevant in the employment context, for example a duty of confidence that an employer owes to its workers, or specific legal requirements applying to employment, for example a law prohibiting particular types of discrimination in employment.

For personal data to be processed fairly they must be processed in a way that does not bring about unfairness to the data subject. This is potentially a very wide-ranging requirement. For example worker monitoring, even if it meets the requirements of the Directive in all other respects, must nevertheless be conducted in a way that is "fair" to the workers being monitored. This is an additional proportionality test.

It is important to remember that Articles 6, 7 and 8 have a cumulative effect. The principles set out in Article 6 are a vital element of the protection the Directive gives to workers in relation to the processing of their personal data. Personal data held by an employer may be excessive even if they have been volunteered by an worker who has given consent to their being held. The national laws of some Members States may, in any case, prevent the collection of some data even with consent.

Processing of personal data in the context of worker monitoring may be unfair even if the worker has consented to the monitoring or one of the other Article 7 criteria is met. The fact that consent has been given may be taken into account in determining whether processing satisfies Article 6. How far this is the case varies between members states but the existence of consent is never an overriding consideration.

9.1. Main principles to bear in mind when considering data protection in the employment context

Workers do not leave their right to privacy at the door of their workplace every morning. However, privacy is not an absolute right. It needs to be balanced with other legitimate interests or rights or freedoms. This also applies to the employment context.

Workers, as long as they form part of an organisation, have to accept a certain degree of intrusion in their privacy and they must share certain personal information with the employer. The employer has a legitimate interest in processing personal data of his workers for lawful and legitimate purposes that are necessary for the normal development of the employment relationship and the business operation.

The question, therefore, is never whether data processing at the workplace *per se* are lawful activities or not. The real question is what are the limits that data protection imposes to such activities or, the other way around, which are the reasons that may justify the collection and further processing of personal data of any given worker.

Of course, there are not absolute answers to these questions *a priori.* The level of tolerated privacy's intrusion will very much depend on the nature of the employment as well as on the specific circumstances surrounding and interacting with the employment relationship which may have an influence.

Example:
What amount of personal information about a potential worker should be an employer allowed to collect?

The answer to this question would be very different for a security supervisor of the European Investment Bank than for one of the workers in the cafeteria in the same building.

The Working Party would like to identify certain principles extracted from the Directive 95/46/EC, which must govern all personal data processing activities in the employment context. Supervisory Authorities in the Member States are called to play a fundamental role in the application of these general principles to the concrete case, taking properly into account the peculiarities of national legislation.

BASIC DATA PROTECTION PRINCIPLES GOVERNING THE PROCESSING OF PERSONAL DATA OF WORKERS
FINALITY
TRANSPARENCY
LEGITIMACY
PROPORTIONALITY
ACCURACY AND RETENTION OF THE DATA
SECURITY
AWARENESS OF THE STAFF

FINALITY

Data must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes. The Working Party is presently working to provide some guidance in this regard.

> **Example:**
> 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.

TRANSPARENCY

It should govern everything. Many processing operations in the employment context in the Member States may be in breach of data protection rules not because such processing is *per se* unlawful, but because workers have not been properly informed about them. As a very minimum, workers need to know which data is the employer collecting about them (directly or from other sources), which are the purposes of processing operations envisaged or carried out with these data presently or in the future.

Transparency is also assured by granting the data subject the right to access to his/her personal data and with the data controllers' obligation of notifying supervisory authorities as provided in national law.

> **Example:**
> An employer may have a legitimate interest in checking the performance of his clerks by assessing workers' output (for instance, how many cases has a worker dealt with, how many telephone calls has he answered, etc.). In addition to the application of the principles mentioned below, in particular, the proportionality principle, the employer will only be able to process this kind of data, if the workers have been properly informed. If such a surveillance took place without proper information to the staff, the processing of workers' data would be in contradiction with the provisions of Directive 95/46/EC.

LEGITIMACY

Any processing operation, even carried out with full transparency towards workers, can only take place if it is legitimate. Although we have already analysed in depth this question in a separate chapter, it is however important to remind here that Article 7, letter f) of the Directive[59] does not give employers a blank cheque for any kind of processing with workers' data. Processing not only still needs to pass the test of proportionality , but cannot unjustifiably prejudice the rights and freedoms of the data subjects.

[59] This Article states*: Member States shall provided that personal data may be processed if processing is necessary for the purposes of the legitimate interests pursued by the controller, in this case the employer.*

Example:
An employer has a legitimate interest in assessing the performance of its workers, and it will often be necessary for the employer to process personal data to do so. This criterion will only be satisfied if any performance monitoring does not unjustifiably prejudice the rights and freedoms of the data subject. The way, in which it might do so, for example, with some types of email or Internet access monitoring, is discussed in Section 12.

PROPORTIONALITY

Finally, assuming that workers have been informed and the processing is legitimate, the personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed[60].

Assuming that workers have been informed about the processing operation and assuming that such processing activity is legitimate and proportionate, such a processing still needs to be fair with the worker[61]

This requirement of proportionality is potentially wide-ranging and presents several sides in the employment context. However, the most important of its effects is that employers should always process the personal data in the least-intrusive way. Different elements should be considered when looking for the least intrusive way: the risks at stake, the amount of data involved, the purpose of processing, etc.

Example:
Employers may need to know (for certain posts) if applicants have a car and a driver licence. The potential employer is entitled to request such information, but it would go against this principle to ask for the model or the color of applicants' cars.

ACCURACY AND RETENTION OF THE DATA

Employment records must be accurate and, where necessary, kept up to date. The employer must take every reasonable step to ensure that data are not inaccurate or incomplete, having regard to the purposes for which they were collected or further processed, are erased or rectified. Employment records must be kept in a form which permits identification of workers for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

[60] Article 6.1.c) of Directive 95/46/EC

[61] Article 6: *Member States shall provide that personal data must be processed fairly and lawfully.*

Example:
The annual assessment of a worker contains information regarding a concrete date and a given contact. After some years, there is no need in principle to store the information regarding such evaluations. Therefore, the retention period should be limited to two or three years maximum after the evaluation.

Employers can safeguard the accuracy of the workers' personal data, for instance, by providing employees with an annual print-out of their employment record.

SECURITY

The employer must implement appropriate technical and organisational measures at the workplace to guarantee that the personal data of his workers is kept secured. Particular protection should be granted as regards unauthorised disclosure or access. Personal data must remain safe from the curiosity of other workers or third parties. Nowadays, the technology offers reasonable means for preventing such unauthorised access or disclosure, allowing in any case the identification of the staff accessing the files. Where a data processor is used, there must be a contract between the employer and the third party providing security guarantees and ensuring that the processor acts only on the employer's instructions.

Examples of security measures at the workplace:

- Password/identification systems for access to computerised employment records
- Login and tracing of access and disclosures
- Backup copies
- Encryption of messages, in particular when the data is transferred outside the organisation

AWARENESS OF THE STAFF

Staff in charge or with responsibilities in the processing of personal data of other workers need to know about data protection and receive proper training. It would be desirable that employment contracts of this staff include a professional secrecy clause. They need to be alert of the possible consequences of unlawful processing for them, the organisation and, of course, the privacy of other colleagues. Without an adequate training of the staff handling personal data, there could never be appropriate respect for the privacy of workers in the workplace.

10. Consent

It should be clear from the preceding discussion that the processing of personal data in the employment context, particularly if sensitive data are not involved, need not in many cases rely on the consent of the worker. Consent should be a fall back position if no other Article 7 criteria or Article 8 exception is applicable. Even where consent is relied on, it must be valid and the employer must still satisfy other requirements of the Directive including Article 6, and Article 15, which addresses automated decisions. Furthermore the worker must have information on the processing as required by Articles 10 and 11.

The Directive defines consent as "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". In the context of sensitive data consent must, in addition, be explicit. The Article 29 Working Party takes the view that where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent. Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice.

An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid. The situation is even clearer cut where, as is often the case, all employers impose the same or a similar condition of employment.

THE ARTICLE 29 WORKING PARTY TAKES THE VIEW THAT WHERE AS A NECESSARY AND UNAVOIDABLE CONSEQUENCE OF THE EMPLOYMENT RELATIONSHIP AN EMPLOYER HAS TO PROCESS PERSONAL DATA IT IS MISLEADING IF IT SEEKS TO LEGITIMISE THIS PROCESSING THROUGH CONSENT. RELIANCE ON CONSENT SHOULD BE CONFINED TO CASES WHERE THE WORKER HAS A GENUINE FREE CHOICE AND IS SUBSEQUENTLY ABLE TO WITHDRAW THE CONSENT WITHOUT DETRIMENT.

In other cases the worker should also clearly be provided with information (Article 10) and the Article 7 and Article 8 criteria should be sufficiently broad to legitimise the processing on grounds other than consent.

The Working Party is aware that several Member States' laws have conferred on the local workers' representatives the role of contributing to the protection of workers' rights in the field of data protection. E.g., in some Member States companies must have the agreement of work councils before introducing controls at the workplace.

11. Individual Rights with Regard to Data Protection

As Data Subject, workers benefit from the rights provided by Directive 95/46/EC.

The most important of these rights is the right of access provided for in Article 12 of the Directive by virtue of which every data subject - is entitled to obtain from the controller (the employer in this case):

a) without constraint at reasonable intervals and without excessive delay or expense:

- Confirmation as to whether or not data relating to the worker are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipient or categories of recipients to whom the data are disclosed,
- Communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- Knowledge of the logic involved in any automatic processing of data concerning him at least in the case of automated decisions

b) as appropriate the rectification, erasure or blocking of data the provisions of which does not comply with data protection law, in particular because of the incomplete or inaccurate nature of the data;

c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with the previous obligation, unless this proves impossible or involves a disproportionate effort.

Data subjects have also the right to object on compelling legitimate grounds relating to his particular situation to the processing by the employer of data relating to him, save where otherwise provided by national legislation (Article 14 of the Directive) and to receive compensation by damages as a result of unlawful processing operation or of any act incompatible with data protection legislation.

The Working Party has already provided a recommendation on employee evaluation data[62] and may give further guidance in the future.

12. Surveillance and monitoring

Several aspects of the application of both Directives 95/46/EC and 97/66/EC to the surveillance and monitoring of workers have been previously discussed. There should no longer be any doubt that data protection requirements apply to the monitoring and surveillance of workers whether in terms of email use, internet access, video cameras or location data.

[62] See Recommendation 1/2001 on Employee Evaluation Data, adopted by the Working Party on 22 March (WP 42, 5008/01).

The application of the Directive to monitoring and surveillance, and the importance attached to the subject is evidenced by developments in Member States, such as those reports and initiatives mentioned in the Introduction.

It should be also clear that

- **any monitoring**, especially if it is conducted on the basis of Article 7(f) of Directive 95/46/EC and, in any case, to satisfy Article 6 **must be a proportionate** response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers.
- **Any personal data** held or used in the course of monitoring must be **adequate, relevant and not excessive for the purpose for which the monitoring is justified**. Any monitoring must be carried out in the least intrusive way possible. It must be targeted on the area of risk, taking into account that data protection rules and, where applicable, the principle of secrecy of correspondence[63].
- **Monitoring**, including surveillance by camera, **must comply with the transparency requirements of Article 10**. Workers must be informed of the existence of the surveillance, the purposes for which personal data are to be processed and other information necessary to guarantee fair processing. The Directive does not treat less strictly monitoring of an worker's use of an Internet and email system if the monitoring takes place by means of a camera located in the office.

Example:
A specific example which workers may not be aware of is related to **location data**. It is true that the proposed Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector will include protection of location data. This Directive is intended to replace 97/66/EC. Although location data will be specifically mentioned in the new Directive such data **nevertheless fall within the scope of both Directive 95/46/EC and Directive 97/66/EC**. The requirements of proportionality discussed in the previous paragraph apply fully to an employer's processing of location data relating to workers.

The Article 29 Working Party recognises that there is a need for **further guidance on the application of the Directive to the surveillance and monitoring electronic communications of workers (e.g. e-mail, Internet)**. The production of such guidance is challenging and therefore the Working Party has nevertheless asked the sub group that drew up this preliminary opinion to start work on its development.

[63] See also Articles 7 and 8 of the EU Charter of Fundamental Rights, signed and proclaimed in Nice on 7 December 2000.

13. Transfer of workers' data to third countries

Article 25 of the Directive establishes that **transfers of personal data to a third country** outside the EU **can only take place** where the third country ensures an **adequate level of protection for the data**.

It must be remembered that whatever the basis of the transfer under Articles 25 and 26 processing involved in the transfer must still satisfy Article 6 to 8 and all the other provisions of the Directive.

Article 26 sets out **derogations** including where:

- the data subject has given his consent unambiguously to the proposed transfer (the same considerations of chapter 10 remain applicable here), or
- the transfer is necessary for the performance of a contract between the data subject and the controller, or
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims, or
- the transfer is on the basis of contractual solutions as authorised by a member state as providing adequate safeguards, or
- the transfer is on the basis of standard contractual clauses approved by the Commission as providing adequate safeguards.

The Working Party believes that **it is preferable to rely on** adequate protection in the of**country of** destination **rather** than relying on **the derogations listed in Article 26, for example the workers' consent.** Where consent is relied on, it must be unambiguous and freely given. Employers would be ill-advised to rely **solely** on consent other than in cases where, if consent is subsequently withdrawn, this will not cause problems.

If the third country does not ensure an adequate level of protection and none of the derogations apply the employer can, alternatively, obtain the worker's unambiguous consent to the proposed transfer.

The Article 29 Working Party recognises the importance of these provisions in the employment context. It is apparent that a significant proportion of international transfers involves worker data processed by multi-national businesses or groups of businesses. It should be borne in mind that many transfers are from a data controller in the EU to a processor outside. In this case, the employer in the EU remains a data controller required to respond to a request from a worker for access to his/her data and to respect his/her other rights.

The Article 29 Working Party has given a great deal of attention to the subject of international transfers. It has published several opinions on the subject[64].

13.1. The transfer of employment data under the Safe Harbor

The U.S. Safe Harbor system[65] contains specific provisions on the transfer and further processing of European workers' data by U.S. organisations established in the United States[66].

While this is not the place to explain in detail such provisions, it may be however worthwhile pointing out that employment information has received reinforced protection in this system. For instance, it is recognised that *"certain generally applicable conditions for transfer from some Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected"*.

Moreover, European Supervisory Authorities remain competent for the enforcement of data protection violations concerning employment data. By adhering to the Safe Harbor, U.S. organisations commit to co-operate in investigating by and to comply with the advice of competent Community Authorities in such cases.

13.2. The transfer of employment data under the standard contractual clauses

Transfers of worker's data are possible under the Commission decision setting out the standard contractual clauses in those cases where the recipient acts as a data controller and incorporates them into a contract with the Data Exporter established in the Community. [67]

The standard contractual clauses approved by the Commission offer an alternative mechanism for transferring personal data of workers to subsidiaries or affiliates established in third countries where there is not adequate level of data protection in place. Under the standard contractual all categories of data used in the employment context, even of a sensitive nature, can be transferred. The safeguards put in place by the contract are enforceable by workers vis-à-vis their employer or vis-à-vis the data controller established in the third country[68].

---

[64] See Opinion 5/99 on the level of protection of personal data in Switzerland (WP 22, 5054/99, adopted on 7 June 1999) and Opinion 6/99 concerning the level of personal data protection in Hungary (WP 24, 5071/99, adopted on 7 September 1999) and the Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP 12, 5025/98, adopted on 24 July 1998)

.

[65] Safe Harbor, OJ L 215 dd. 25 August 2000

[66] See FAQ 9 "Human Resources Data"

[67] See Commission decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, OJ reference OJ L 181, 04.07.01; where necessary other formalities under national law may have to be complied with.

[68] http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2faq.htm

14. Conclusions

Directive 95/46/EC applies fully and comprehensively to personal data about workers. Although the Directive gives each Member State a certain margin of manoeuvre to particularise the conditions of such processing operations, the application of the principles contained in this opinion is common and generally recognised. This opinion is aimed at contributing to the uniform application of the national measures adopted under Directive 95/46/EC.

There is a necessary and welcome interaction between data protection law and labour law and practice. Not all problems that involve the processing of personal data are exclusively data protection ones but this interaction is important in ensuring solutions that properly protect the interest of workers.

The legitimate interests of the employer justify certain limitations to the privacy of individuals at the workplace. Sometimes it is the law or the interests of others which impose these limitations. However, no business interest may ever prevail on the principles of transparency, lawful processing, legitimisation, proportionality, necessity and others contained in Directive 95/46/EC. Workers can always object to the processing when it is susceptible of unjustifiably overriding his/her fundamental rights and freedoms.

Given the specificity of the employment relationship, consent will not normally be a way to legitimise the processing in the employment context. Where it is relied on, consent must always be freely given, specific and informed.

The Working Party is considering further guidance on the surveillance and monitoring at the working place, but all the principles described in this opinion fully apply to these activities.

Done at Brussels, 13 September 2001

For the Working Party

The Chairman

Stefano RODOTA