COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Ministers' Deputies
CM Documents

CM(2015)32 addfinal 1 April 2015[1]

1224 Meeting, 1 April 2015

5 Media

5.1 Steering Committee on Media and Information Society (CDMSI)

a. Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment – Explanatory Memorandum

EXPLANATORY MEMORANDUM

to Recommendation CM/Rec(2015)5
of the Committee of Ministers to member States
on the processing of personal data in the context of employment

(Adopted by the Committee of Ministers on 1 April 2015
at the 1224th meeting of the Ministers' Deputies)

Introduction

1. Recommendation No. R (89) 2 of the Committee of Ministers to member States on the protection of personal data used for employment purposes was the sixth such instrument adopted by the Committee of Ministers within the framework of the "sectoral approach" to data protection issues.

2. Twenty-five years have passed since the recommendation was adopted. Work per se has changed a lot (in terms of subject matter, form, duration and intermediaries), as have the places where it is performed and the way in which it is organised. Employers, employees and their needs have changed, and due to the increasing use of new technologies, the spectrum of personal data that is handled has become broader (IP addresses, log files and location data, for example). The need to review the recommendation thus became clear.

3. The Consultative Committee of Convention 108 mandated an expert in 2011 to carry out a study on Recommendation No. R (89) 2 and to suggest proposals for its revision (document T-PD-BUR(2010)1FIN – "Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes – proposals for the revision of the above-mentioned Recommendation" by Giovanni Buttarelli).

4. On the basis of the study, the consultative committee worked on the revision of the recommendation and approved the draft text during its 31st Plenary meeting (2-4 June 2014). It subsequently transmitted the draft revised recommendation to the Steering Committee on Media and Information Society (CDMSI) for examination and approval, which ensured parallel consultation of the European Committee on Legal Co-operation (CDCJ).

5. With regard to the development of context as compared to 1989, the following elements were taken into consideration:

- the growing use of information technologies in the context of employment and the need to protect employee's dignity and fundamental rights against the monitoring of their activities;
- the tendency of employers to collect data on employees outside the strict perimeter of work, as for example on search engines and social networking sites;

[1] This document has been classified restricted until examination by the Committee of Ministers.

- the introduction of particular forms of processing carrying specific risks to individuals, involving for instance biometric or location data.

6. The draft recommendation was approved by the CDMSI at its 7th meeting (18-21 November 2014).

7. The Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment was adopted by the Committee of Ministers of the Council of Europe on 1 April 2015.

Preamble

8. The preamble sets out the reasons that have led the Committee of Ministers to present the recommendation to governments of member States.

9. The work of the Council of Europe in the field of data protection has always supported the position that information systems and technologies (ICTs) bring undoubted benefits to society. The main concern of the Organisation in this area has been to set standards allowing technological progress to be accompanied by a clear recognition of the need to safeguard the interests of the individual, in particular in respect of data processing.

10. The employment sector, private and public – to which the principles contained in this recommendation are directed – reflects this preoccupation: how to strike a balance between the undoubted advantages offered by technology to enterprises on the one hand and on the other, the rights and freedoms of employees in a work environment where ICTs are part of the employees' daily activities. The benefits which result for them in better organisation of work, a reduction in routine tasks and so on, must be evaluated in the light of the possible impact on the privacy of the individual employee, and of the workforce of an entity as a whole, which technology may possibly produce. The preamble also recognises that other rights and freedoms may possibly be put at risk through the introduction of ICTs in the workplace – for example, freedom of association or freedom of expression as guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, more commonly known as the European Convention on Human Rights and hereinafter "ECHR"), as well as the rights guaranteed by the European Social Charter which are of direct concern to the relationship between employers and employees.

11. The first paragraph of Article 8 of the ECHR provides that "Everyone has the right to respect for his private and family life, his home and his correspondence". The European Court of Human Rights (hereinafter "the Court") has also developed case law under which Article 8 may also give rise to positive obligations that are inherent to the effective "respect" for private life. In light of those positive obligations, the State must take the necessary measures, including legislative ones, to ensure in practice effective compliance with the rights deriving from Article 8 of the ECHR.

12. At the outset, the point is made that privacy is not simply to be interpreted in terms of the right of the employee to be free from unjustified intrusion into his or her workaday life, although the recommendation's principles on monitoring and surveillance of employees are closely related to this traditional meaning of the concept of privacy. Rather, the principles set out reflect the concern spelt out in the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) of 28 January 1981 (hereinafter referred to as "Convention 108") to protect the data subject through the regulation of the processing (collection, use, storage, etc.) of personal information.

13. The recommendation is, accordingly, structured in such a way as to make Convention 108's broad principles meaningful to the employment context by offering principles designed to regulate the relevant activities of the employer. In other words, by adapting the convention's basic principles relating to fair and lawful processing, intended purposes, proportionality, data minimisation and access to data, the guidelines set out in the recommendation provide responses to questions such as: how should data be collected by employers? For what purposes? What use can be made of the data stored? What are the rights of the employee in regard to the data processed by the employer?

14. Given that the recommendation constitutes a sectoral approach to data protection, it is necessary to take into account all the elements distinguishing the sector in question and which influence the way in which Convention 108's basic principles are to be adapted. Accordingly, the text seeks to reflect the typical legitimate information needs of the employer as well as the legitimate privacy/data protection needs of the employee. However, and as the preamble points out, it is also a feature of the employment sector that both group interests and individual interests are at stake. A valid sectoral approach must also seek to tailor Convention 108's broad principles to the reality of the collective interest. It is for this reason that, at various stages in the text, the principles set out in the recommendation accept the possibility of employee

representatives defending the data protection interests of the individual employee and employees as a whole within an entity.

15. As regards the implementation of the recommendation's principles, governments of member States should ensure that the principles contained in the appendix of the recommendation are reflected in the application of domestic legislation on data protection in the employment sector, as well as in other branches of the law which have a bearing on the use of personal data for employment purposes.

16. The purview of the recommendation allows for a number of ways in which these principles can be implemented. In the first instance, it is possible for the data protection authorities established pursuant to the national data protection legislation to avail themselves of the principles when they are confronted by problems of data protection in the context of employer-employee relations. The governments of the member States should, accordingly, ensure that such authorities are aware of the existence of the recommendation and of its value to dispute resolution in this sector. Convention 108, to which the domestic norms conform, makes no exception for the employment sector. Accordingly, national data protection authorities responsible for the application of the domestic norms can usefully avail themselves of the provisions of the recommendation to help them discharge their tasks in giving effect to data protection norms in the employment sector. By way of example, the principles could be used by them in specific cases or as a basis for proposed codes of conduct in the employment field. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, which lays down rules regulating the processing of personal data in profiling techniques, can be of particular relevance in the context of employment.

17. Beyond these considerations, it is felt that social partners themselves can negotiate acceptance and respect for the principles, either as a complement to the existing legal regulations or as an alternative to it. The preamble takes into account the different national approaches to government involvement in labour relations, which may range from varying degrees of regulation to free collective bargaining - free from State intervention - between the social partners on issues relating to employer-employee relations. Accordingly, in the absence of legislative initiatives designed to give effect to the principles of the recommendation, governments should ensure that the representative bodies of employers and employees are adequately informed of the value of the recommendation's approach to data protection issues.

Appendix to Recommendation CM/Rec(2015)5

Part I - General principles

1. Scope

18. Consistent with the scope of Convention 108, the principles contained in the recommendation apply to the processing of personal data in public and private sector employment. As will be seen hereafter, "employment purposes" is to be understood as covering a range of processing activities relating to recruitment, performance of the contract of employment, discharge of obligations laid down by law or laid down in collective agreements, the management planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of termination of the employment relationship.

19. Principle 1.2 of the recommendation brings the activities of employment agencies or "head-hunting agencies" in the public and private sectors within the scope of some of its provisions ("unless domestic law provides otherwise"). It may be the case that a number of member States consider public sector employment agencies in a different context to the employment field and regulate them outside the scope of labour law – for example by social security law. While such countries may decide not to apply the principles of the recommendation to their activities, it will nevertheless be the case that general data protection legislation of the countries in question will apply to their data processing activities.

20. According to Principle 1.2, employment agencies shall use the data in their capacity either as data controllers or as processors, in compliance with the principles of this recommendation and only for the purposes for which the data were initially collected. In some cases, employment agencies shall use the data of candidates to help employers discharge their duties relating to the contracts of employment.

2. Definitions

21. The definition of "personal data" is consistent with that of Convention 108. It is a long-lasting established definition which has been reaffirmed over the years through a variety of legal instruments of the

Council of Europe. The term “personal data” is defined broadly and should be interpreted in such a way as to allow it to also respond to the increasing use of new technologies and means of electronic communication in the relations between employers and employees. Personal data may include an employee’s name, age, home address, marital status, education, log files, etc. It may also include an employer’s appraisal or opinion of an employee and a digitised image of the employee.

22. The definition of “personal data” refers to any information relating to an identified or an identifiable person. “Identifiable individual” means a person who can be directly or indirectly identified. An individual is not considered “identifiable” if his or her identification would require unreasonable time, effort or means. The determination of what constitutes “unreasonable time, effort or means” should be assessed on a case-by-case basis, in the light of the purpose of the data processing and taking into account objective criteria such as the cost, in relation to the benefits, of such an identification, the technology used and available at the time of the processing, technological developments, etc.

23. Data that appears to be anonymous because it is not accompanied by any obvious identifiers may nevertheless, in particular cases, permit the identification of the individual concerned. This is the case where, for example, alone or through the combination of physical, physiological, genetic, mental, economic, cultural or social data (such as age, sex, occupation, geolocation, family status, etc.), it is possible for the controller, or any legitimate or illegitimate actor (in particular when the data was made publicly available) to identify the person concerned. Where this is the case, the data may not be considered to be anonymous and must therefore be treated as personal data.

24. “Data processing” covers an open-ended general notion capable of flexible interpretation which starts from the collection or creation of personal data and covers all automated operations, whether partially or totally automated. Data processing also occurs where no automated operation is performed but data are organised in a structure which allows a search, combination or correlation of the data related to a specific employee or potential employee.

25. “Information systems” refers to any kind of devices such as computers, cameras, video equipment, sound devices, telephones and other communication equipment, as well as various methods of establishing identity and location, or any method of surveillance. The terms “tools” and “devices” are covered by the notion of “information systems” and information technologies, whose definitions are outlined in the recommendation.

26. As regards the notion of “employment purposes”, it should be emphasised that the principle of purpose or purpose specification is of crucial importance, serving as it does to define and limit the personal information activities of the employer. As provided for in Convention 108, personal data undergoing processing should be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes. The purpose identified for this sector – "employment purposes" – seeks to balance the interests of the employer with those of the employees while, at the same time, accepting that the employer may act as intermediary between the State and the employee for the purpose of collecting and storing personal data for subsequent transmission to the State; for example, when it is pursuant to tax or social security or industrial safety legislation ("the discharge of obligations laid down by law").

27. “Employment purposes” shall also cover the disciplinary framework (e.g. internal investigations and sanctions), as well as data processed after the termination of employment. It should be clarified that when the data are stored after the termination of employment, the processing should be in line with Principle 13 and with the principle of intended purpose. The term “contract of employment” should be understood as an oral or written, expressed or implied, agreement, specifying terms and conditions under which a person consents to perform certain duties as directed and controlled by an employer, usually but not always in return for a previously agreed wage or salary. It was understood that for the drafters of the recommendation the term “contract of employment” would also refer to non-remunerated employment such as volunteering jobs, internships and training courses. The principles of the recommendation thus also apply to individuals who are in an employment relationship with such status. Furthermore, the employment relationship in the public sector should be covered, even if it is not necessarily based on a contract of employment. The employment terms, conditions and duties are usually specified under the relevant regulations of administrative law.

28. The “employer” is a legal entity that controls and directs an employee in the context of an employment relationship, which generally exists when a person performs work or services under certain conditions in return for remuneration. It is through the employment relationship that reciprocal rights and obligations are created between the employee and the employer. It has been, and continues to be, the main vehicle through which workers gain access to the rights and benefits associated with employment in the areas of labour law and social security.[2]

[2] Source ILO: www.ilo.org/ifpdial/areas-of-work/labour-law/WCMS_CON_TXT_IFPDIAL_EMPREL_EN/lang--en/index.htm.

29. An "employee" is a person who is hired to perform work for an employer within an employment relationship. The terms of "worker" or "staff member" also refer to the definition of "employee". Special attention should be given to the concept of employee and, in this regard, to the ruling of the Court of Justice of the European Union (CJEU) in the Case C-94/07 – *Andrea Raccanelli v. Max-Planck-Gesellschaft zur Förderung der Wissenschaften eV*. The CJEU ruled that the concept of the "worker" within the meaning of Article 35 of the Treaty on the Functioning of the European Union (TFEU) has a specific meaning in EU law and must not be interpreted narrowly. Any person who pursues activities which are real and genuine, to the exclusion of activities of such a small scale as to be regarded as purely marginal and ancillary, must be regarded as a "worker". The essential feature of an employment relationship is that, according to this case law, for a certain period of time a person performs services for and under the direction of another person in return for which he or she typically receives remuneration.

30. Prospective employees should benefit from the same protection and rights as employees, even if their candidature does not lead to a contract of employment. Similarly, it should be underlined that the principles of this recommendation also apply to former employees.

3. Respect for human rights, human dignity and fundamental freedoms

31. Principle 3 constitutes a general statement which informs the approach taken in the rest of the recommendation to the issue of personal data processing in the employment field. Privacy is to be seen in terms of data protection and as imposing limits on the processing of personal information by employers. In this sense, it is also to be seen as conferring positive rights on employees to allow them to make sure, through the rights specified in Principle 11, that employers have respected the requirements of data protection.

32. The reference to "human dignity" in the text takes account of the fact that technology should not be used in a way which inhibits social interaction among employees. These concerns are reflected later in the text.

33. The approach taken is consistent with the position adopted by the European Court of Human Rights, which has stated repeatedly that it is difficult to completely separate matters of private and professional life. In *Niemietz v. Germany*,[3] which concerned the search by a government authority of the complainant's office, the Court held that Article 8 afforded protection against the search of someone's office by stating: "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 lives 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".

34. Moreover, in the case of *Halford v. the United Kingdom*,[4] the Court decided that interception of workers' phone calls at work constituted a violation of Article 8 of the Convention, ruling that "telephone calls made from business premises as well as from the home may be covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8 paragraph 1 (…)".

35. In *Copland v. the United Kingdom*,[5] the Court reaffirmed this position in respect of the monitoring of an employee's use of telephone, e-mail and the Internet. The Court considered that the collection and storage of personal information relating to Ms Copland through her use of the telephone, e-mail and Internet interfered with her right to respect for her private life and correspondence, and that that interference was not "in accordance with the law", there having been no domestic law at the relevant time to regulate monitoring. While the Court accepted that it might sometimes have been legitimate for an employer to monitor and control an employee's use of telephone and Internet, in this case it was not required to determine whether that interference was "necessary in a democratic society".

4. Application of personal data protection principles

36. Information systems and technologies used for the processing of personal data in the context of employment should be used in such a way as to minimise the processing of personal data, as well as to limit

[3] *Niemietz v. Germany*, Application No. 13710/88, 16 December 1992.
[4] *Halford v. the United Kingdom*, Application No. 20605/92, 25 June 1997.
[5] *Copland v. the United Kingdom*, Application No. 62617/00, 3 April 2007.

the use of data identifying or allowing the identification of individuals to only that necessary for the aims pursued in the individual cases concerned.

37. Principle 4.2 states that employers should develop appropriate measures to ensure that they respect in practice the principles and obligations relating to data processing for employment purposes and that they should furthermore be in a position to demonstrate their compliance with such principles to the relevant supervisory authority. According to this principle, employers are obliged to put in place measures aimed at guaranteeing that data protection rules are adhered to in the context of processing operations and to maintain records of categories of personal data processing activities under their responsibility, in order to prove to employees and to supervisory authorities that measures have been taken to achieve compliance with the data protection rules.

38. It must also be stressed that data protection principles should also be respected in both the development and the use of technologies and that the principles of Convention 108 are fully applicable in this regard (notably those relating to the quality of data, sensitive data, data security and the rights of the data subjects). Experience has shown that in the context of employment, the employer will seek to efficiently manage his business and optimise the use of new technologies and thus benefit from their potential. Hence, these new technologies, such as video surveillance, biometrics or geolocation, give the employer the opportunity to monitor all activities of employees, if the law does not regulate or prohibit such monitoring. The manner in which the data protection principles should be respected and how to strike a balance between the employees' rights and any legitimate interest of the employer will be developed later in the text.

39. Moreover, according to Principle 4.2, the measures should be adapted to the volume and nature of data processed, as well as the scope, context and purpose of the processing and, in respect of this, appropriate simplified solutions should be adopted in small-scale working environments. The recommendation does not make a distinction between small or medium-sized and large working environments for the purpose of the application of the recommendation's principles. It is felt that the size of the working environment is not a decisive factor for data protection since problems may arise regardless of the number of people employed by an employer. The principles can be readily applied by small working environments, including small family businesses, with a minimum of requirements. However, legislation should be sensitive to the need not to impose unnecessary legal requirements on small working environments which process small volumes of non-sensitive data.

5. Collection and storage of data

40. Principle 5 seeks to adapt some of the protective provisions within Article 5 of Convention 108 to the collection of data concerning individuals by their employers. The principle is not restricted solely to data collection on employees within the course of their employment. It also addresses the data protection needs of job applicants, even if no employment offer has been made to them. It is felt desirable to also provide guidelines relating to data collection at the recruitment stage.

41. Principle 5.1 emphasises the need to make the individual employee the primary source of information. In other words, if the employer requires information on a named employee, then such information should be sought directly from the employee. This is not an absolute rule. The text of Principle 5.1 accepts that it may be necessary at times to bypass the individual employee so as to obtain data on him or her, for example, to check the accuracy of information supplied by a prospective employee in the course of a hiring or promotion procedure, on condition that the employee, or prospective employee, has been duly informed before the data is collected from third parties.

42. It is important to stress in the context of Principle 5 that many aspects of the processing of employees' data do not require specific consent, as they have another legitimate basis prescribed by law. There are limitations as to how far consent can be relied upon in the employment context to justify the processing of personal data. To be valid, consent must be informed, "freely given" and limited to cases where the employee has a genuinely free choice and is subsequently able to refuse or withdraw consent without detriment. In general, all data processing within the context of employment should be provided for by domestic law.

43. It emerges from Principle 5.2 that the amount of personal information which can be legitimately collected on employees depends on the job in question. Employers should review their data collection practices – for example, the type of data required on application forms – so as to ensure that they are not storing more personal information than necessary in view of the nature of the employment or the needs of the moment. The text accepts that, at certain periods in the life of an entity, it may be necessary for the employer to obtain more data than normal – for example, for the purposes of a proposed merger or wholesale restructuring, it may be appropriate to seek the personal views of the employees. Here it may be noted that in

addition to the requirements of relevancy and accuracy, the collection procedure must also respect the principle of proportionality and transparent and fair processing.

44. Using search engines for instance to assemble data (including sounds, pictures or videos) can have a significant impact on a person's private and social life, especially if personal data derived from a search is incomplete, excessive, incorrect or not relevant any more. A preventive approach inspired by a rationale of privacy by design could reduce implementing problems, by encouraging the distribution of privacy-oriented products which are more focused, from a technical and organisational viewpoint, on the principles of necessity, data minimisation and proportionality.

45. Principle 5.3 refers to the concept of "social networking". A social networking service is a platform which enables the building of social relations among people who share interests, activities, backgrounds or real-life connections. It is a web-based service that allows individuals to create a profile, to establish a list of users with whom to share views and to develop contacts within the system. Controllers of social networking services are themselves bound to the principles of data protection and to the correspondent obligations, especially in terms of information, violations of terms of service and proportionality. However, employers should refrain from collecting data relating to job applicants or employees without their knowledge through an intermediary, under another name or using a pseudonym.

46. When an employee's or prospective employee's access to social networking accounts is restricted, employers do not have the right to ask for access to such accounts, for instance by requiring that employees/prospective employees provide them with their login credentials.

47. Although the collection and processing of health data is dealt with under Principle 9, the drafters of the recommendation considered it to be important to recall this rule in Principle 5.4, given that health data are sensitive data and their processing in the employment context can only occur where appropriate safeguards are put in place and specific conditions met.

48. The storage of personal data referred to in Principle 5.5 is linked to the collection of data. Employers should have a legitimate grounds for storing the personal data of employees that have been collected for employment purposes, and the length of the storage period will depend on the need for and the purpose of the processing. To this end, data collected on job applications and interview records of candidates that have not been accepted should be stored for a very short period (see also paragraphs 107-108).

6. Internal use of data

49. Principle 6 deals solely with the situation where personal data are used internally by the employer. Principle 6.1 underlines the need to respect the purposes specification. Personal data collected and stored for employment purposes should only be used for those purposes. It is important to identify clearly the various circumstances in which personal data can be legitimately used for "employment purposes" and to provide the necessary specifications and safeguards. However, it should be borne in mind that the expression "employment purposes" covers a range of sub-purposes for which data can be processed. For example, personal data may be processed for the purpose of administering an employee training scheme, or a company loan or pension scheme, or the data may relate to candidates who have put themselves forward for promotion, or they may be processed for salary purposes. It is important to consider the context for which the data were collected, since random use of data, although for an employment purpose, may distort the purpose for which data were originally collected.

50. With due regard to the principles of relevance and accuracy, and with regard in particular to large-scale or territorially extensive working environments, certain personal data, for example e-mail addresses or pictures, could be made easily accessible in internal communication networks in order to speed up the performance of the work carried out and to facilitate interaction with other employees. In such cases employees concerned should be duly informed about the internal communication of their data.

51. Principle 6.2 encourages employers to adopt internal privacy policies/rules and to inform employees about them. Such rules should take account of the data protection principles outlined in the recommendation and, more specifically:

- the principle of fair processing: data collection directly from the employee concerned, information provided to the employees, the exercise of the employee's rights;
- the purpose of the processing: data should be collected for explicit, legitimate and specified purposes and should not be used for other purposes;
- the communication of data: only for the purposes provided above;

- data security: appropriate security measures should be provided to prevent unauthorised access to, or alteration, disclosure or destruction of, the data and to prevent their accidental loss or destruction;
- measures on how to keep data accurate and up to date: in order to prevent taking decisions or actions based on inaccurate data;
- the limitations on data storage: this requirement places a responsibility on employer to be clear about the length of time for which data will be kept and the reason for retaining the information;
- the rights of employees;
- the obligations of the employer.

52. Employers are further encouraged to adopt binding internal procedures and/or policies defined prior to the introduction of new data processing operations; for example, how to provide adequate information to employees or how to give them adequate replies in the event that they exercise their rights or complain.

53. Principle 6.3 recommends the taking of adequate measures so as to guarantee that the new context in which data are redeployed reflects faithfully the original contextual meaning assigned to the data as well as continuing respect for the specific purpose for which the data were collected and stored. For example, when an employer is considering whether or not an employee's wages should be reduced for repeated absence or irregular attendance, care should be taken to analyse attendance data to ensure that the employee is not absent because of his or her attendance on an authorised training scheme. Alternatively, the fact that an employee's file reveals that his or her repayments of a company loan are in arrears should not be taken into consideration in the context of disciplinary proceedings.

54. Moreover, irrespective of different national approaches to the issue of "incompatibility", it may also be the case that an employer's undertaking that he or she will not use data collected for certain purposes for other purposes within the employment relationship may effectively restrict subsequent use of the data. Sometimes the very nature of the original purpose for which personal data were collected – for example statistics or research relating to industrial diseases – will preclude the subsequent use of the data collected for another unrelated employment purpose. Whether or not subsequent use of personal data is to be considered "incompatible" with the original purpose for which the data were collected is to be assessed on a case-by-case basis.

55. Informing the employee of any proposed use of data drawn from different contexts in order to take decisions which affect his or her interests is seen as a safeguard for the employee against the sort of prejudice illustrated above. This is a fundamental requirement of the principle of fair processing and of transparency which governs the employment relationship.

56. In the event of the transfer of undertakings or businesses, it may be acceptable that certain categories of employees' personal data be communicated to third parties (e.g. to other companies of the same group or to the new employer in the event of acquisitions or mergers, transfer of contracts, etc.). The amount of personal information on employees which can be legitimately communicated to third parties will of course depend on the job in question and, in addition to the requirements of relevancy and proportionality, the communication will also be linked to respect for the purposes specification ("for employment purposes"). Where substantive changes in the processing occur, the persons concerned should also be informed in due respect of applicable law and as may be found appropriate by data protection authorities. Where the transfers of undertakings or businesses result in a transfer of employees' data to third countries, those can only take place where the third country ensures an adequate level of protection for the data or appropriate safeguards.

57. The text of Principle 6 says nothing about the issue of the processing of personal data for research or statistical purposes by employers. Planning and organisation of work may require this to be carried out at times. Should this be the case, the principles laid down in Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics should be respected.

7. Communication of data and use of ICTs for the purpose of employee representation

58. The meaning to be assigned to the term "employee's representatives" will be determined by national law and practice in the field of labour relations. These representatives may include works councils, trade union representatives or other associations to which the employee is affiliated. The names and addresses of employees may in some cases need to be communicated to the representative organ so as to allow literature relating to proposed union elections to be circulated. The communication of personal data relating to employees who are not affiliate to a representative body should be done with their consent. However, if the purpose is to verify compliance with a collective agreement or other terms of employment and this is made through employee's representatives, which may be the case for some member States, transfer of personal data relating to employees who are not members of the representative body can be done if necessary to verify such compliance.

59. The term “collective agreement” should be understood as an agreement between an employers’ organisation or an employer, on the one hand, and a trade union on the other. The agreement should be in writing and should normally detail the conditions of employment and the relationship between the employer and the employee.

60. Furthermore, for the purposes of this recommendation, the term “communication” provided for in Principles 7 and 8 should include the disclosure, transmission and transfer of personal data.

61. The quantity of personal information which can be communicated should satisfy the principle of proportionality – only that that is "necessary to allow them [the representatives] to represent the interests of the employees". The particular national context will obviously influence the amount of data which can be communicated to representative bodies, in particular the existence of statutory regulations on the relations between employers and representative bodies. For example, national law may authorise the communication of personal data relating to a candidate for promotion so as to allow a works council to be consulted before any decision is taken. The obligations provided in collective agreements, stated in the Principle 7.1, usually concern both employers and employees and may refer for instance to pay agreements, employment conditions and joint dispute resolution procedures.

62. Information systems referred to in Principle 7.2 are those defined in Principle 2. New technologies, such as e-mails or intranet, may be used for the communication of employees’ data to their representatives. This communication should be done in accordance with domestic law and practice. The agreements setting the procedures for the secure use of the data and the confidentiality of the communications should also be provided for in domestic law or determined by the data protection authorities.

63. Reference could be made here to electronic voting, often online, which has been increasingly developed during recent years, particularly for employees’ representatives elections within companies. Electronic voting operations may pose risks to employees, notably the risk of disclosure of sensitive data such as trade union membership or political opinions. The processing of personal data necessary for elections should seek to ensure the protection of the privacy of employees. The implementation of effective security measures is essential for a successful vote operation, such as the use of cryptographic methods, sealing and encryption.

64. The data processed by representative bodies in these circumstances are naturally subject to the general principles of data protection, particularly so in the case of electronic voting referred to above.

8. External communication of data

65. It has been noted that the employer may act as an intermediary between the State and the employee for the purpose of supplying data to State agencies, such as those referred to in Principle 8.1. It may for instance be tax or social security authorities or health and safety inspectorates. The nature and amount of personal data which can be communicated to such public bodies or State agencies will be determined by the level of fulfilment of the statutory duties. "Legal obligations" should be understood in this sense.

66. Public bodies may require the processing of personal data to enable them to exercise their official functions – for example, government research in the field of job-related injuries and diseases or the analysis of employment patterns in deprived areas. It is accepted that the expression “in accordance with other provisions of domestic law” may oblige communication of employee data in those circumstances (for the definition of “communication” see paragraph 56 above) and will depend on the national context. In addition, domestic law, in compliance with the ECHR, may at various times require the communication of personal data to the police, courts and other public bodies discharging official functions. It will be noted that, in these cases, personal data are not being communicated for employment purposes. For example, divorce proceedings involving an employee and his/her spouse may require the communication of data relating to his/her salary by the employer to the court so as to enable it to assess the amount of maintenance which should be paid on the dissolution of their marriage. Regarding the communication of personal data to the police – which may be required by domestic law as applied in conformity with Convention 108 – reference should also be made to the provisions of Recommendation No. R (87) 15 of the Committee of Ministers to member States regulating the use of personal data in the police sector.

67. Principle 8.2 addresses the situation where personal data are to be communicated outside the place of employment to public bodies not exercising official functions – for example a government agency acting as employer in the labour market – and to private parties, including entities within the same group.

68. Principle 8.2.*a* deals with the communication of personal data for employment purposes to the type of bodies referred to above. For example, an employer may engage an auditor to run the company accounts, pay wages, deal with personal tax liability of employees, etc. Or an employee may be on a temporary assignment with another employer. Both examples will require the disclosure of personal data. The text accepts that communication in such circumstances is legitimate since the sort of matters referred to fall within the scope of the expression "employment purposes". It should be noted that the legitimacy of communication in those circumstances is made subject to ensuring respect for purposes specification ("which are not incompatible with the purposes for which the data were originally collected") and the considerations discussed under Principle 6.3 are equally valid for the interpretation of Principle 8.2.*a*. Principle 8.2.*a* also makes communication of the data conditional on prior information being given to the employee concerned or his/her representatives. Once again, the text of the recommendation recognises the value of data protection operating in conjunction with transparency.

69. As regards Principle 8.2.*b*, the personal data to be communicated may not be intended for use for employment purposes – for example, a request made by a direct marketing firm or a political party to have lists of employees' names and addresses. In situations such as these, the safeguards are increased: the express, freely given, specific and informed consent of the individual employee must be obtained.

70. It may also be the case that domestic law authorises the communication of personal data to private bodies or public bodies not discharging official functions. National legislation on statistics may be such a case. More often, the communication referred to in Principle 8.2.*c* is provided for the purpose of discharging legal obligations, relating for example to social security and the welfare of employees, or to optimise the allocation of human resources or, where necessary, for judicial purposes, including the exercise of the right to remedy.

71. Principles 8.3 and 8.4 were introduced in the light of other legislation that aims to enhance the transparency of public administrative activities and to facilitate access to public records by introducing various obligations for public administrative bodies to publish and disseminate records, documents and information on their organisation and activities. Communication of data relating to a public authority's staff can cover a wide range of topics, including the names of employees, organisation charts and internal directories, as well as other data where individual employees can be identified, such as information on salaries and pensions, severance payments and compromise agreements, sickness statistics and training records.

72. There are a number of factors that could indicate whether communication would be fair, including whether it is necessary and proportional to the fulfilment of the public interest, if it is sensitive personal data, the consequences of disclosure and the balance between the employees' rights and any legitimate public interest in disclosure. In principle, the information should relate to their public role rather than their private life. When it comes to sensitive personal data, full respect of Article 6 of Convention 108 should be ensured. These data are likely to relate to the most personal aspects of employees' lives, for example their health or sexual life, rather than their working life.

73. Additional safeguards may be considered for the fair processing and publication of employees' data, such as the determination of proportionate time limits for their publication as well as taking measures for restricting the availability of such information on external search engines.

9. Processing of sensitive data

74. As with Convention 108 and other recommendations in the field of data protection, a separate principle is devoted to the issue of sensitive data. It will be noted however that Principle 9 also lays down special guidelines for the processing of health data, given that such data are a more common feature of the employment sector than the other types of data referred to in Principle 9.1. For this reason, health data require more extensive consideration. Due attention should also be paid to Recommendation No. R (97) 5 of the Committee of Ministers to member States on the protection of medical data.

75. Particular attention should be paid to medical technologies which make it possible to uncover the most intimate information on the state of an employee's health. Given the rights to respect for privacy and to human dignity, such techniques should be used with care, only if provided for by specific domestic legislation and accompanied by appropriate safeguards. Reference may be made to the Recommendation No. R (94) 11 of the Committee of Ministers to member States on screening as a tool of preventive medicine. In addition, employers, both in the public and private sectors, should be made aware of the provisions of Recommendation No. R (87) 25 of the Committee of Ministers to member States concerning a common European public health policy to fight the acquired immuno-deficiency syndrome (AIDS). In that recommendation, the Committee of Ministers discourages the use of compulsory screening for the entire population or for particular groups. It is

felt desirable that employers should follow this approach in the employment sector by not obliging job applicants to undergo AIDS screening against their will.

76. The principles laid down earlier in the recommendation in regard to the processing of personal data must be read in the light of the provisions relating to sensitive data set out in Article 6 of Convention 108. These principles seek to adapt this article to the requirements of the employment sector for which there should be no exception other than the one referred to in domestic law, for instance when processing is necessary for the purpose of pension systems or sickness insurance schemes negotiated by employers and trade unions, on condition that appropriate safeguards are provided. The additional safeguards should mainly ensure the security and lawful processing of the data. As regards to cases not covered by this exception, the prohibition on the processing of sensitive data remains the rule; derogation from this rule is only possible if domestic law lays down appropriate safeguards. Moreover, the attention of employers should be drawn to the strict prohibition of collecting sensitive data that are irrelevant to the nature of employment and could lead to discrimination towards specific employees; for instance, rejecting candidates for employment due to their religious or political beliefs or isolating or dismissing an employee owing to his or her sexual preferences.

77. On the other hand, certain types of sensitive data could be processed lawfully when the very nature of the employment requires sensitive data to be obtained: for example, political organisations which seek to influence public opinion may require information on the political views of candidates for posts with such organisations; and religious institutions may require candidates for employment with them to state their religious convictions at the time of recruitment. However this processing is only lawful when specific and additional appropriate safeguards are provided for by domestic law.

78. Principle 9.2 sets out the situations where health data are likely to be processed in the employment context. They relate to both physical and mental health. Principles 9.2 and following are structured in such a way as to limit the processing of health data while emphasising the need for security. As regards to the collection, Principle 9.2 places restrictions on the sort of health data which may be collected. It will be noted that health data concerning prospective employees as well as employees are covered.

79. Principle 9.2.*a* deals with the suitability of the employee to exercise his or her duties. According to this principle, health data can only be obtained if needed to determine whether the employee is fit for a particular position, for example a scientist participating in an expedition. The need to process health-related data has to be evaluated against the purpose for each specific case. The reference to “the requirements of preventive medicine” in Principle 9.2.*b*, covers periodic check-ups, for example to ensure that employees who are exposed to toxic substances in their work environment do not develop any disease. Principle 9.2.*c* allows health data to be collected in order to enable an employee to work under appropriate conditions in line with his/her illness or disability. Processing of health data carried out on the grounds of safeguarding the vital interest of the data subject or other employees, as stated in Principle 9.2.*d*, is usually related to an emergency context, which will be evaluated on a case-by-case basis. Principle 9.2.*e* allows health data to be collected so as to allow “social benefits” to be granted to an employee. For example, an employee injured in the workplace who makes a claim under a company insurance scheme may need to be medically examined to determine the nature and extent of the disability. Moreover, industrial injuries schemes or employees’ compensation schemes administered by the State may require data to be collected on the state of the health of an employee with a view to settling a claim made by the employee or with a view to assessing the likelihood of future claims against the State fund.

80. The nature of the employment will of course influence the sort of questions which may be asked of an employee or applicant, and thus the amount of data which can be collected. It will also influence the nature of the physical examination. For example, an applicant for a job in a nuclear power plant may, in addition to a rigorous medical test, be required to supply information regarding the incidence of cancer or other diseases in his or her family history. Applicants for jobs in the liberal professions would not be expected to do so.

81. Principle 9.3 recalls that respect for rights and fundamental freedoms should be safeguarded during the collection of data. In this regard, it prohibits the processing of genetic data of employees by the employer, as it can lead to discrimination when it comes to any aspect of employment. The processing of genetic data can only be allowed under very exceptional circumstances, regulated by provisions of domestic law. According to Recommendation No. R (97) 5, such processing can only be permitted for health reasons and in particular to avoid any serious prejudice to the health of the data subject or third parties. Processing of genetic information may be acquired for example through a genetic monitoring programme that monitors the biological effects of toxic substances in the workplace, where the monitoring is required by law or, under carefully defined conditions, where the programme is voluntary.

82. Reference should be made to Recommendation No. R (92) 3 of the Committee of Ministers to member States on genetic testing and screening for health care purposes, and in particular to Principle 6 of

the recommendation which provides that "(…) admission to, or the continued exercise of certain activities, especially employment, should not be made dependent on the undergoing of genetics tests or screening". Principle 6 further sets out that "exceptions to this principle must be justified by reasons of direct protection of the person concerned or of a third party and be directly related to the specific conditions of the activity".

83. Principle 9.4 stipulates that an employer can only obtain the data from the employee concerned and is not allowed to collect health data directly from other sources, for example by contacting a former employer. The individual should be the primary source of information for the purposes of supplying health information – primarily through his or her physical examination and answers to the questions put to him or her to determine their suitability for employment, on condition that such processing is lawful.

84. Principle 9.5 relates to situations where personnel bound by "medical confidentiality" may have access to confidential health data for medical reasons. These situations should only be related to the suitability of the employee to exercise his or her duties or to when the processing of health data by the employer is necessary to impose measures to protect the employee's health or to prevent risks for others. It should be noted that, in Principles 9.5 and 9.6, the drafters of the recommendation made a deliberate distinction between health data in general and health data covered by medical confidentiality. It goes without saying that the latter require particular protection.

85. Subject to the rules on the collection of personal data governed by medical confidentiality, referred to in Principles 9.5 and 9.6, and unlike the other categories of sensitive data referred to in Principle 9.1, the processing of data relating to the health of employees or prospective employees is not subject to a requirement of "particular cases". It is accepted that the processing of such data is a generalised and necessary practice in the employment sector. Domestic law will determine the sort of data which are covered by medical confidentiality.

86. Where a company or organisation employs its own medical staff to conduct medical examinations on employees or job applicants, it is essential that they maintain confidentiality at all levels and even before the employer. Employers should not receive medical information, but only conclusions relevant to the employment decision. The categories of persons, other than doctors, who are bound by rules on medical confidentiality, should be determined in accordance with national law and practice. Principle 9.5 places severe limitations on the communication of medical data *sensu stricto* to administrative personnel, it being understood that general indications on the state of health of an employee or prospective employee can be given (X has passed his medical examination; the results of the medical examination reveal that Y is no longer sufficiently fit to continue employment, etc.). Where it is the case that health data have to be communicated to the personnel administration, the data so communicated may only be subsequently stored within the personnel administration in strict compliance with Principles 5 and 6 of this recommendation.

87. The confidentiality of health data is threatened when they are added to an employment record containing various other categories of data. Physical separation also allows for increased data security. Consideration should be given to the use of passwords for selective access to the data stored so as to ensure that only members of the medical service can access the data. Other technical means can be used to prevent unauthorised access.

88. It is recognised that the processing of health data may require the co-operation of persons outside the medical service, who are not subject to the same codes of ethics or requirements of medical confidentiality – for example information technology (IT) staff. It is of the utmost importance that their attention is drawn to the sensitivity of the information being processed and to the need to respect its confidential nature.

89. As regards to the processing of any health data relating to third parties (see Principle 9.7), reference could be made to family members of the employee in order to grant them specific benefits.

10. Transparency of processing

90. Principle 10 proposes a number of ways in which employees can be informed of both their rights and the data processing activities of the employer. A particularly clear and complete description must be provided of the type of personal data which can be collected by means of information systems and technologies which enable them to be monitored by the employer, and of their possible use. A general policy should explain, moreover, how covert surveillance could happen.

91. A similar description should be provided of the use of biometric and of Radio Frequency Identification (RFID) technology, the possible use of personal identification codes and also the role of IT staff (such as system administrators) in relation to data processing.

92. The information should also refer to the rights of the employee in regard to his or her data, as provided for in Principle 11 of this recommendation, as well as the ways and means of exercising those rights. The information referred to in Principle 10.1 should be provided and updated in due time and, in any event, before the employee carries out the activity or action concerned, and should also be made readily available through the information systems normally used by the employee.

93. It should be noted here that the term “recipient”, included in the type of information to be provided to employees, should be understood as a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available.

94. In accordance with domestic law or practice and, where appropriate, in accordance with relevant collective agreements, employers should, in advance, fully inform or consult their employees or representatives about the introduction, adaptation and operation of information systems and technologies for the collection and use of personal data necessary for requirements relating to production or safety, or to work organisation.

11. Right of access, rectification and to object

95. Employees should be entitled to know about the personal data processed relating to them. Principle 11.1 advocates that each employee should, on request, be able to access all personal data held by the employer which concern him or her. The employee should also be granted the right to know any available information as to their source, the parties to which the data have been, or could be, communicated and/or the reasoning behind any automated process concerning him or her. To that end, the employer should introduce general procedures to ensure that there is an adequate and prompt response where the right of access, deletion and rectification are exercised, in particular in large-scale entities or entities spread out across the country.

96. The term “controller”, stated in Principle 11.1, refers to the person or body having the decision-making power concerning the processing, whether this power derives from a legal designation or from factual circumstances. In some cases, there may be multiple controllers or co-controllers (jointly responsible for processing and possibly responsible for different aspects of that processing). For the principles set out in this recommendation, the controller is usually the employer. The “processor”, referred to in Principle 20.1, is a separate entity acting on behalf of the controller carrying out the processing in the manner that was requested by the controller and for the needs of the controller. An employee of a controller is not a processor, but a data subject, in respect of the processing of his or her personal data.

97. Under Principle 11.2 each employee should further have the right to request rectification, blockage or erasure of his/her data when they are held contrary to the law or to the principles set out in this recommendation, in particular when they are incorrect. The right to object may be limited by virtue of a law when, for example, the data should be processed pursuant to tax or social security or industrial safety legislation. The right to object may not be applicable when the processing is necessary for employment purposes, such as the execution of a contract of employment.

98. The right of access should also be guaranteed in respect of personal assessment data, referred to in Principle 11.3, including when they relate to assessments of the productivity or capability of the employee (see paragraph 5.5), when the assessment process has been completed at the latest, without prejudice to the right of defence of employers or third parties involved. Principle 11.3 seeks to find a balance between the right of access of the employee, which also extends to evaluation data, with the legitimate need of the employer to express evaluation of the employee. On the other hand, the employee should have a means of appeal for challenging the assessment and defend him/herself against any negative assessment, preferably before the evaluation is finalised. Any deferment for defence purposes shall only be temporary.

99. Principle 11.4 recognises the right of an employee to have his or her views taken into account when subject to a decision solely based on an automated processing of data which has an adverse effect on him or her (for example, a disciplinary measure, a dismissal, a denial of promotion). This could be the case for example when an employee is dismissed for not performing his or her duties on the basis of monitoring carried out via video surveillance, when this monitoring is lawful, and the decision of dismissal is based solely on the images recorded. In addition, the fact that a decision is based on automatic processing cannot deprive the employee of the right to know the reasons on which the decision is based.

100. Principle 11.5 is connected to the previous one, since the implementation of the requirements of Principle 11.4 necessitates the employee being informed of the reasoning on which the automated decision is based, and for this purpose he or she should be entitled to consult and examine the relevant reasoning.

101. Principle 11.6 defines the authorised exceptions to Principles 10, 11.1, 11.2, 11.4 and 11.5. The rights of the employee are not unrestricted and they have to be reconciled with other rights and legitimate interests. They can, in accordance with Convention 108, be limited only where laid down by law and where this constitutes a necessary measure in a democratic society in the interest of legitimate grounds exhaustively listed by Convention 108. For instance, the right to be informed about the reasoning on which processing is based can be limited to protect the rights of others, such as legally protected secrets (e.g. trade secrets). As regards the right to object, the employer may have a compelling legitimate ground for the processing, which overrides the interests or rights and freedoms of the employee. The legitimate interest will, of course, have to be demonstrated on a case-by-case basis in order to pursue such processing. Moreover, there may be practical limitations to an exercise of the right of access. For example, a particular data file may contain data on several employees. In such a case, the employer may extrapolate the personal data referring to the employee concerned and when it is not possible to separate the data of the employee concerned from that of his or colleagues, the employer may be obliged to seek the colleagues' consent before being granted access to the specific data file.

102. The limitation on the exercise of rights expressed in Principle 11.7 applies to, for example, the opening of an investigation by an employer into cases of theft of goods from a factory or from employees. It should be noted that, if the exercise of the right of access has been suspended – and this may only be carried out to an extent necessary for the needs of the investigation – such suspension may not last beyond the end of the inquiry.

103. The person designated by the employee in accordance with the provisions of Principle 11.8 may be a colleague, a lawyer or his or her representative. What is essential is that the employee himself or herself must appoint such a person. Principle 11.8 accepts that domestic law may restrict, or even prohibit, the assistance offered to the employee.

104. Domestic law will further determine the nature of the remedy envisaged in Principle 11.9. Such remedies presuppose the intervention of an independent authority, whether a court or independent body as understood by the Additional Protocol to Convention 108, i.e. one having the power to investigate and to order appropriate sanctions.

12. Security of data

105. Principle 12.1 deals with the technical and organisational steps which should be taken to ensure data security. One way of implementing this recommendation is by legal means; other means might be considered involving the establishment of internal security policies and procedures. Practical precautions also have to be taken by the controller to avoid any accidental or malicious processing incidents. The level of security must be appropriate to the likelihood and severity of risks of the data processing and the nature of personal data, as well as the nature, scope, context and purpose of the processing.

106. Adequate technical and organisational measures, as stated in Principle 12.1, should be adapted according to each situation and should ensure effective data protection. For example:

a. updated processing inventories;
b. privacy impact assessments for high-risk processing operations;
c. the appointment of a data protection officer or a more precise assignment of responsibility to ensure more structured management of data processing; the introduction of internal audit mechanisms or independent inspection of the state of progress in applying legislation;
d. the identification of internal procedures aimed at highlighting security risks or breaches;
e. training activities and certification at various levels, including management.

Furthermore, it should be borne in mind that the minimisation of data provides preventive benefits from the very beginning of the processing. Also where data breaches occur, the employer should implement appropriate technological protection measures to prevent prejudice to employees' rights and should communicate the data breach, without undue delay, to the employees concerned.

107. Principle 12 concerns not only employers, but also third parties, such as employment agencies and IT companies processing the personal data of employees on behalf of employers ("entities which may process data on their behalf"). Reference shall be made in this regard to the obligations of the "processor". The "processor" is a separate entity acting on behalf of the controller carrying out the processing in the manner that was requested by the controller and for the needs of the controller (see also paragraph 90). The rules on security of processing imply an obligation on the controller and the processor to implement

appropriate technical and organisational measures in order to prevent any unauthorised interference with data processing operations [see Directive 95/46/EC].

108. Principle 12.3 sets out the obligations of the personnel administration, as well as other people engaged in the processing of the data, such as webmasters, who, in the exercise of their duties relating to the normal functioning and the security of networks, have access to a certain amount of personal data though mailboxes, login files, temporary files or cookies. This principle provides that the employer should inform the personnel involved in the processing of data about the security measures they should apply, preferably by means of internal policy rules. Another measure would consist of including a clause of confidentiality in their contract and, as the case may be, in the IT charter of the establishment or in the internal regulations.

13. Preservation of data

109. Principle 13.1 provides that the length of time for which personal data can be retained by an employer should be determined by the employment purposes indicated in Principle 2 of the recommendation. For some employment purposes, the length of time that data are to be kept will be longer than for other purposes. The period of preservation will be determined on a case-by-case basis. For example, payment of a company pension scheme will oblige the employer to retain data long after the employee has retired.

110. Principle 13.2 devotes particular attention to the case of personal data submitted by prospective employees. In principle, such data should be deleted when the candidate's application is rejected. In addition, the documents provided by the applicant should either be returned to the applicant or be deleted from the system (online applications for instance). This said, it may sometimes happen that an employer may wish to retain information on a particular candidate who has, for example, failed to meet the requirements of the job description but who could be considered for another post at a later stage and for which he or she is more suited. It may also be in the interests of the rejected prospective employee to have his or her information kept on the employer's databases. Nevertheless, the employer should do so only with the consent of the prospective employee concerned, after he or she has been duly informed.

111. Principle 13.3 also considers the possibility of data submitted in furtherance of a job application being retained by the employer as a precaution against legal action being taken against him by a failed applicant, as well as for other legitimate purposes. For example, the employer may wish to prove to a court that the job applicant was not rejected on grounds of sex, ethnicity, religion, etc., or that correct recruitment and interview procedures were followed. In such cases data should be stored only for the period necessary for the fulfilment of the said purpose, and deleted when the period during which a legal action could have been introduced has expired. The data submitted should also be stored when necessary for other legitimate purposes. For instance, this might be the case when an employer is legally obliged to provide information about circumstances in their activities that are of importance for the supervision of a law, e.g. legislation on non-discrimination. In such cases, the data should be stored as long as necessary.

112. According to Principle 13.4, when an internal investigation is carried out and does not give rise to any charge or negative measure against the employee concerned, the data should be deleted after a reasonable period. There are no rules as to what would constitute a reasonable period. As stated earlier, the length of preservation will be determined on a case-by-case basis. Special attention should be drawn to the right of access of the employee concerned. If the exercise of this right was suspended for the needs of the investigation, personal data processed for the purposes of the investigation should be communicated to the employee concerned before their deletion.

Part II – Particular forms of processing

14. Use of the Internet and electronic communications in the workplace

113. Employers have the right to encourage efficient management and to protect themselves against liabilities and damages which employees' actions may give rise to. Monitoring and surveillance activities in the interests of the employer should however be lawful, transparent, effective and proportionate, and this reasonable approach would also avert possible negative effects on the quality of their professional relationship.

114. To prevent unjustifiable interferences with individuals' rights to private life and to the protection of personal data with regard to the possible processing of personal data relating to Internet or intranet use, employers could be made to formally communicate the information to the persons concerned, outlined in Principle 16.1, in a document such as an IT charter or privacy policy, which should be signed by employees

and periodically updated. The information in the policy on the use of media and on monitoring should be clear, comprehensive, accurate and easily accessible.

115. Principle 14.1 extends to all aspects of an employee's employment, including his or her use of any computer, smartphone or other digital device, either in the framework of the employer's intranet or extranet, or by their direct or indirect use of the Internet provided by the employer. It applies whether the device used by the employee is provided by the employer or by the employee him/herself.[6] Furthermore, it is often the case that information devices in the workplace are used for purposes other than professional ones. Although this should remain appropriate and fair and should not affect either the network's security or the productivity of the establishment, the employer may determine the conditions and restrictions on the use of the Internet that do not constitute a disproportionate infringement of employees' privacy.

116. Principle 14.2 provides for the processing of personal data relating to Internet or intranet pages viewed by the employees. According to this principle the employer may adopt appropriate measures in order to reduce the risk of improper use of the Internet (browsing of non-relevant sites, file or software uploads or downloads, the use of network services for purposes unrelated to work), even by using filters, thus avoiding subsequent processing of employees' personal data which could also involve sensitive data.

117. The employer could, for example, take the following measures:

a. identify and specify a priori the categories of sites which are definitely not related to work;
b. ensure that, when necessary, during screening/check-ups, only data that is anonymous or that does not allow the immediate identification of users is processed through appropriate data aggregation techniques (for example, analysis of log files relating to web traffic of groups of employees only).

118. Principle 14.3 lays down the conditions of lawfulness of access to employees' professional electronic communications. It should be noted that, for the purposes of the recommendation, "professional communications" shall refer particularly to e-mails sent or received during the performance of the employees' duties, or professional information exchanged via Internet messaging services. Access to professional electronic communications may be necessary in order to obtain confirmation or proof of misconduct or in order to detect infringements of employer's intellectual property. When it is professionally necessary to access such communications, employers should demonstrate the security needs or other lawful reasons for that access (such as when the employer is to be held liable for the actions of its employees, has to detect the presence of viruses or guarantee the security of the information system). Employers should take further necessary measures and consider appropriate procedures in order to access an employee's professional electronic communications. For example, if an employee is absent from work unexpectedly and/or for a prolonged period, in view of the possible need for the employer to access the contents of e-mail messages on account of pressing requirements related to work, the employee in question should be allowed to entrust another employee (trusted party) with checking the contents of his/her e-mail messages and forwarding messages that are considered to be professionally relevant to the employer.

119. In addition to providing compelling legitimate grounds for access to professional electronic communications of employees, employers should furthermore inform employees in advance of the existence of this possibility, preferably by means of an explicit internal policy. A proper policy shall therefore clarify the legitimate expectations of employees or third parties to the confidentiality of their communications.

120. It may on some occasions be difficult to distinguish a professional communication from a personal one. In some countries, the content of electronic communications – together with certain data outside of these communications and attached files – is protected by a guarantee of confidentiality of correspondence and communication, sometimes determined at the constitutional level. At least at the beginning, access should in principle be limited to data about the communication (length, recipient, etc.) rather than the content of the communication itself, if this is sufficient to satisfy the employer's needs.

121. Principle 14.4 upholds that private communications at work should not be monitored, including the content, as well as information on sending and receiving.

122. Principle 14.5 sets out the situations where employees leave the organisation. It is stipulated that employers should deactivate former employees' accounts in such a way as to avoid having access to their communication after their departure. If the employers wish to recover the content of an employee's account, they should take the necessary measures to do so before their departure, and preferably in their presence.

[6] See the guidelines on "Bring Your Own Device" (BYOD) issued by the Information Commissioner's Office (ICO) http://ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

123. Principles 14.1 to 14.5 should be interpreted in the sense that all interference with private communications must be in conformity with Article 8 of the ECHR and the corresponding case law of the Court.

15. Information systems and technologies for the monitoring of employees, including video surveillance

124. Principle 15.1 sets strict conditions in respect of the introduction and use of information systems and technologies for monitoring employees' activity and behaviour. Without prejudicing measures relating to well-founded defence proceedings, the use of information systems and technologies, such as video surveillance in the workplace or geolocation systems, should be limited only to organisational and/or production necessities, or for security purposes or the protection of health. Such systems should only be allowed if legitimate, necessary, proportionate, fair, transparent and regulated. They should not aim at permanently monitoring the quality and quantity of the individual work in the workplace, nor aim at remotely monitoring employees' behaviour or location.

Moreover, with regard to video surveillance systems, employers should adopt preventive measures, such as:

- the shortest possible maximum preservation period, to be defined and allowed for by the system;
- only allowing images to be accessed and viewed by duly authorised staff in the exercise of their duties (for example the person responsible for security in the establishment).

125. Principle 15.2 states that the processing of personal data in connection with the use of information systems and technologies must uphold employees' fundamental rights and freedoms and in particular their right to respect for privacy. This approach is consistent with the position adopted by the Court, which has stated repeatedly that increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data. With regard to video surveillance systems, it is clearly stated within Principle 15.2 that placing cameras at locations such as toilets or cloakrooms ("occurrences that are part of the most personal area of life of employees") is strictly prohibited in any situation.

126. While bearing in mind that video surveillance systems are also covered by information systems and technologies, according to the "Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance" adopted by the European Committee on Legal Co-operation (CDCJ) of the Council of Europe in May 2003, "any video surveillance activity should be undertaken by taking such measures as are necessary in order to ensure that this activity complies with personal data protection principles, in particular by only using video surveillance if, depending on the circumstances, the purpose cannot be attained by measures which interfere less with privacy, provided that the alternative measures would not involve disproportionate cost […] and by preventing the data collected from being indexed, matched or kept unnecessarily. When it proves necessary to keep data, these data must be deleted as soon as they are no longer necessary for the determined and specific purpose sought […]."

127. Principle 15.3 stipulates that, in the event of a lawsuit or counterclaim, employees should be able to found it on the recording made. Nonetheless, the application of this principle should not lead to the storage of the recording made for an unlimited and disproportionate period of time and the data protection principles set forth in Principle 3 should apply accordingly.

16. Equipment revealing employees' location

128. Principle 16.1 refers to the use of equipment which may reveal employees' locations and may track their movements. This could be for instance Radio Frequency Identification technologies (commonly known as "RFID technology"), GPS (Global Positioning System) or portable devices, placed inside objects, clothes or uniforms. The considerations discussed under Principle 15.1 are equally valid for the interpretation of Principle 16.1, limiting the use of such equipment only to organisational necessities, or for security and safety purposes, or for the protection of health, in line with the principles of proportionality and legitimacy and on condition that their introduction will not lead to a continuous monitoring of the employees concerned.

129. The use of such equipment may constitute an infringement of the rights and freedoms of employees and should not lead to continuous monitoring of an employee. Preventive measures must be considered, for instance the possibility to suspend the geolocation outside working hours.

130. Furthermore, as far as the implementation of Principle 16.1 is concerned, the use of these devices should not enable the processing of data with regard to certain offences (speeding, for example), nor enable the geolocation of other people.

131. In this context, a particularly clear and complete description must be provided to employees concerned before the use of the equipment which reveals their location. At the very least, the notification should inform employees of the type of personal data which may be collected by means of the equipment, of their possible use and also the role of any system administrators in relation to data processing. Such notification with regard to the policy on monitoring shall also remain valid for other particular forms of processing referred to in Part II of this recommendation.

17. Internal reporting mechanism

132. Internal mechanisms such as hotlines, specific e-mail addresses or online systems may enable employees to report illegal activities. Recommendation CM/Rec(2014)7 of the Committee of Ministers to member States on the protection of whistleblowers, as well as Opinion 1/2006 of the Article 29 Working Party[7] on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime may provide further guidance on this topic. The term "whistleblower" usually refers to a person who reports or discloses misconduct, alleged dishonest or illegal activity occurring in an organisation, in the context of their work-based relationship, whether it is in the public or private sector.

133. Principle 17 underlines the importance of data security and its specific aims. It states that appropriate security measures should be put in place by employers and personal data should be processed for the purpose of internal reporting mechanisms relating to the report, as well as for the purpose of complying with legal obligations deriving from national law or following a legal action brought on the basis of the internal reporting.

134. Those people subject to internal reporting should be duly informed about the use of their data, in order to exercise their rights referred to in paragraph 11.

135. Even if anonymous reporting is possible, other mechanisms should be preferred in order to protect the rights and interests of all parties involved, confidentiality being the rule under all circumstances.

18. Biometric data

136. Principle 18 deals with the processing of biometric data for employment purposes. In information technology, biometrics usually refers to technologies for measuring and analysing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, especially for authentication purposes. The application of biometrics raises important human rights issues, given that the integrity of the human body and human dignity are at stake.[8]

137. As outlined in Principle 18.1, the processing of biometric data to identify or authenticate employees should, in principle, only be permitted where it is necessary to protect the legitimate interests of the employer, employees or third parties, provided that such interests do not override the fundamental rights of employees. Legitimate interests may prevail, for instance, when protecting the vital interests of employees, or when it is necessary to control access to particularly sensitive areas in terms of security, such as a nuclear plant or a military base.

138. Although the use of biometrics is possible under specific circumstances, employers should use less intrusive means, that is to say methods which uphold individuals' fundamental rights and freedoms and in particular their right to respect for privacy and to human dignity.

139. Where the use of biometric data is permitted under Principle 18.1, the access to such data shall be subject to requirements of security and proportionality. Biometric data should not be stored in a centralised database, and preference should be given, where appropriate, to biometric identification or authentication systems based on media available solely to the person concerned, thus enabling employees to keep the data themselves, on a card for example.

19. Psychological tests, analysis and similar procedures

[7] The Article 29 Data Protection Working Party is an advisory body and was set up under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[8] See also Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005), prepared by the Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (T-PD).

140. Psychological tests are used generally to determine, among other things, the ability of an employee to work under stressful conditions and to assess the potential of a prospective employee to handle the job effectively under those conditions.

141. According to Principle 19.1, recourse to psychological tests, analyses and similar procedures should not take place unless they are legitimate and necessary in the employment context and domestic law provides appropriate safeguards. In this regard, decisions based solely on the results of such tests, analysis and similar procedures should be challengeable. Psychological testing should be administered by a professional organisation or a psychologist, subject to codes of ethics or requirements of medical confidentiality. The individual's profile should under no circumstances reveal health-related information.

142. Principle 19.2 further provides that the employee or prospective employee concerned should be informed in advance of the use that will be made of the results of these tests, as well as the content of the results.

20. Other forms of data processing posing specific risks to employees' rights

143. With regard to data processing, cloud computing is one example that presents a specific risk to employees' rights. When public bodies and private enterprises use the services of a cloud provider, data are stored or processed by a cloud provider and/or its subcontractors. In such cases, employees risk losing control over their personal data as well as having insufficient information with regard to how, where and by whom the data is being processed/sub-processed. Similar concerns around employees' data privacy rights may be raised by the use of mobile devices at work. The functioning of such devices, allowing for example device-activity monitoring, tracking and remote lock, necessarily involves access to personal data contained in these devices and the processing of this data by the employer.

144. Principle 20.1 draws inspiration from Principle 12 of the recommendation regarding the security of data. Before carrying out data processing, the employer and, where applicable, the processor will have to perform an analysis of its potential impact on the rights and fundamental freedoms of the data subjects. This analysis will also have to take into account the principle of proportionality, on the basis of the comprehensive overview of the processing (that is the entire documentation and description of the processing, indicating what personal data will be processed and for what purpose, how it will be collected, how it will be used, internal flows, disclosures, security measures, etc.). The assistance of IT systems developers, including security professionals, or designers, together with users and legal experts, in analysing the risks would be an advantage and could reduce the administrative burdens linked to this exercise.

145. In order to minimise the risks, employers could for example train staff in charge of processing personal data, set up appropriate notification procedures (for instance to indicate when data has to be deleted from the system), establish specific contractual provisions where the processing is delegated, as well as set up internal procedures to enable the verification and demonstration of compliance. One possible measure that could be taken by the employer to facilitate such a verification and demonstration of compliance would be the designation of a "data protection officer" entrusted with the means necessary to fulfil his or her mission independently. Such a data protection officer, whose designation should be notified to the supervisory authority, could be internal or external to the controller.

146. Principle 20.2 further provides for the consultation of employees' representatives before the introduction of high-risk processing operations, unless domestic law provides other safeguards.

21. Additional safeguards

147. Principle 21 was introduced in order to outline the obligations of the employers when using particular forms of processing, especially those that could lead to the monitoring of employees.

148. Regarding the obligation to inform employees before the introduction of information systems and technologies enabling the monitoring of their activities, the employer must indicate in a clear and detailed manner how the tools placed at their disposal will be used and whether monitoring will be carried out, and if so, the indicators and methods which will be used.

149. Information on the policy regarding the use of media and on monitoring shall be clear, comprehensive, accurate and easily accessible.

150. The employer should for example specify, where applicable:

a. the internal rules on data and systems security or on the protection of company or professional secrecy, provided for all employees, as well as the role of the systems administrator and any relocation of servers to other countries;
b. any personal use of electronic communication tools which is permitted and invoiced to the party concerned or which is strictly forbidden (for example, the downloading or possession of software or files that are wholly unrelated to work activity), providing an indication also of the possible consequences, preferably graduated according to the seriousness of the offence (also taking into account the possibility of involuntary visits to websites due to unexpected actions by search engines, advertisements or typing errors);
c. any inspection that the employer reserves the right to perform, providing an indication of the legitimate reasons for it and the methods used;
d. the log files, if any are kept, in the form of back-up copies as well, and the people who have access to them.

151. Employees or their representatives should be informed and consulted before the introduction or adaptation of any surveillance system. Where the consultation procedure reveals a possibility of infringing an employee's right to respect for privacy and human dignity, his or her agreement should be sought.

152. In situations where there are no employees' representatives, some other specific entities should be involved in order to ensure that such particular forms of processing are carried out with the appropriate safeguards for the employees.

153. Ensuring that a risk analysis be carried out when the introduction of new processing is being considered could also constitute a welcome additional safeguard.