COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

RECOMMENDATION No. R (89) 2

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES
ON THE PROTECTION OF PERSONAL DATA
USED FOR EMPLOYMENT PURPOSES

(Adopted by the Committee of Ministers on 18 January 1989
at the 423rd meeting of the Ministers’ Deputies)

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,
Considering that the aim of the Council of Europe is to achieve a greater unity among its members;
Aware of the increasing use of automatic data processing in the relations between employers and employees, and the corresponding advantages thereof;
Believing, however, that the use of automatic data processing methods by employers should be guided by principles which are designed to minimise any risks which such methods could possibly pose for the rights and fundamental freedoms of employees, in particular their right to privacy;
Bearing in mind in this regard the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and the desirability of adapting them to the particular requirements of the employment sector;
Recognising also that the interests to be borne in mind when elaborating principles for the employment sector are of an individual as well as collective nature;
Aware of the different traditions which exist in the member states in regard to regulation of different aspects of employer-employee relations, regulation by law being only one method of regulation;
Recalling in this context Article 6 of the European Social Charter of 18 October 1961,

1. When this recommendation was adopted, the Representative of Ireland, in application of Article 10.2.c of the Rules of Procedure for the meetings of the Ministers’ Deputies, reserved the right of his Government to restrict the scope of the recommendation solely to automated data, and to exclude from its scope household employment and family businesses where employment is confined to members of the family.
Recommends that the governments of member states:

- ensure that the principles contained in the recommendation are reflected in the application of domestic legislation on data protection to the employment sector, as well as in other branches of the law bearing on the use of personal data for employment purposes;
- for this purpose, ensure that the recommendation is brought to the attention of the authorities established under domestic data protection legislation which are competent to supervise implementation of such legislation;
- promote acceptance and implementation of the principles contained in the recommendation by ensuring its wide circulation among representative bodies of both employers and employees.

1. Scope and definitions

1.1. The principles set out in this recommendation apply to the collection and use of personal data for employment purposes in both the public and private sectors.

These principles apply to automatically processed data as well as to other data on employees which are held by employers, in so far as such information is necessary to make automatically processed data intelligible.

Manual processing of data should not be used by employers in order to avoid the principles contained in this recommendation.

1.2. Notwithstanding the principle laid down in paragraph 1.1, second sub-paragraph, a member state may extend the principles of this recommendation to manual processing in general.

1.3. For the purposes of this recommendation:

The expression “personal data” covers any information relating to an identified or identifiable individual. An individual shall not be regarded as “identifiable” if identification requires an unreasonable amount of time, cost and manpower.

The expression “employment purposes” concerns the relations between employers and employees which relate to recruitment of employees, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, as well as planning and organisation of work.

1.4. Unless provisions of domestic law exist to the contrary, the principles of this recommendation apply, where appropriate, to the activities of employment agencies, whether in the public or private sector, which collect and use personal data so as to enable a contract of employment to be established between the persons registered with them and prospective employers.

1.5. This recommendation does not, to the extent necessary for the protection of state security, public safety and the suppression of criminal offences, apply to confidential information collected or held by employers for employment purposes on persons recruited for posts or who work in jobs closely related to these matters.

2. Respect for privacy and human dignity of employees

Respect for the privacy and human dignity, in particular the possibility of exercising social and individual relations at the place of work, of the employee should be safeguarded in the collection and use of personal data for employment purposes.

3. Information and consultation of employees

3.1. 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 the representatives of the latter about the introduction or adaptation of automated systems for the collection and use of personal data of employees.

This principle also applies to the introduction or adaptation of technical devices designed to monitor the movements or productivity of employees.
3.2. The agreement of employees or their representatives should be sought before the introduction or adaptation of such systems or devices where the consultation procedure referred to in paragraph 3.1 reveals a possibility of infringement of employees' right to respect for privacy and human dignity unless domestic law or practice provides other appropriate safeguards.

4. Collection of data

4.1. Personal data should in principle be obtained from the individual employee. The individual concerned should be informed when it is appropriate to consult sources outside the employment relationship.

4.2. Personal data collected by employers for employment purposes should be relevant and not excessive, bearing in mind the type of employment as well as the evolving information needs of the employer.

4.3. In the course of a recruitment procedure, the data collected should be limited to such as are necessary to evaluate the suitability of prospective candidates and their career potential.

In the course of such a procedure, personal data should be obtained solely from the individual concerned. Subject to provisions of domestic law, sources other than the individual may only be consulted with his consent or if he has been informed in advance of this possibility.

4.4. Recourse to tests, analyses and similar procedures designed to assess the character or personality of the individual should not take place without his consent or unless domestic law provides other appropriate safeguards. If he so wishes, he should be informed of the results of these tests.

5. Storage of data

5.1. The storage of personal data is permissible only if the data have been collected in accordance with the rules outlined in paragraph 4 and if the storage is intended to serve employment purposes.

5.2. The data stored should be accurate, where necessary kept up to date, and represent faithfully the situation of the employee. They should not be stored or coded in a way that would infringe an employee's rights by allowing him to be characterised or profiled without his knowledge.

5.3. Where judgmental data are stored relating to the performance or potential of individual employees, such data should be based on fair and honest evaluations and must not be insulting in the way they are formulated.

6. Internal use of data

6.1. Personal data collected for employment purposes should only be used by employers for such purposes.

6.2. Where data are to be used for employment purposes other than the one for which they were originally collected, adequate measures should be taken to avoid misinterpretation of the data in the different context and to ensure that they are not used in a manner incompatible with the original purpose. Where important decisions affecting the employee are to be taken, based on data so used, he should be informed.

6.3. The interconnection of files containing personal data collected and stored for employment purposes is subject to the provisions of paragraph 6.2.

7. Communication of data to employees' representatives

In accordance with domestic law and practice or the terms of collective agreements, personal data may be communicated to employees' representatives in so far as such data are necessary to allow them to represent the interests of the employees.

8. External communication of data

8.1. Personal data collected for employment purposes should be communicated to public bodies for the purposes of their official functions only within the limits of employers' legal obligations or in accordance with other provisions of domestic law.
8.2. The communication of personal data to public bodies for purposes other than the exercise of their official functions or to parties other than public bodies, including enterprises in the same group, should only take place:

   a. where the communication is necessary for employment purposes which are not incompatible with the purposes for which the data were originally collected and where employees or their representatives are informed of this; or

   b. with the express and informed consent of the individual employee; or

   c. if the communication is authorised by domestic law.

9. Transborder data flows

Transborder transfers of personal data collected and stored for employment purposes should be subject to the principles stated in paragraphs 6 and 8.

10. Particular categories of data

10.1. Personal data relating to racial origin, political opinions, religious or other beliefs, sexual life or criminal convictions, referred to in Article 6 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, should only be collected and stored in particular cases within the limits laid down by domestic law and in accordance with appropriate safeguards provided therein. In the absence of such safeguards, such data should only be collected and stored with the express and informed consent of the employees.

10.2. An employee or job applicant may only be asked questions concerning his state of health and be medically examined in order:

   a. to determine the suitability of an employee or job applicant for his present or future employment;

   b. to fulfil the requirements of preventive medicine; or

   c. to allow social benefits to be granted.

10.3. Health data may not be collected from sources other than the employee concerned except with his express and informed consent or in accordance with provisions of domestic law.

10.4. Health data covered by medical secrecy should only be stored by personnel who are bound by rules on medical secrecy. The information should only be communicated to other members of the personnel administration if it is indispensable for decision-making by the latter and in accordance with provisions of domestic law.

10.5. Health data covered by medical secrecy should be stored separate from other categories of personal data held by the employer. Security measures should be taken to prevent persons outside the medical service having access to the data.

10.6. The data subject's right of access to his health data should not be restricted unless access to such data could cause serious harm to the data subject, in which case the data may be communicated to him through a doctor of his choice.

11. Publicity in regard to personal data

11.1. Information concerning personal data held by the employer should be made available either to the employee concerned directly or through the intermediary of his representatives, or brought to his notice through other appropriate means.

   This information should specify the main purposes of storing the data, the sort of data stored, the categories of persons or bodies to whom the data are regularly communicated and the purposes and legal basis of such communication.

11.2. The information should also refer to the rights of the employee in regard to his data, as provided for in paragraph 12 of this recommendation, as well as the ways and means of exercising the right of access.
12. Right of access and rectification

12.1. Each employee should, on request, be enabled to have access to all personal data held by his employer which concern him and, as the case may be, to have such data rectified or erased where they are held contrary to the principles set out in this recommendation. In the case of judgmental data, each employee should have the right, in accordance with domestic law, to contest the judgment.

12.2. Exercise of the rights referred to in paragraph 12.1 may, in the case of an internal investigation conducted by the employer, be deferred until the close of the investigation if the result of the investigation would be otherwise threatened.

12.3. When an employee is faced with a decision based on automatic processing of data held by an employer, he should have the right to satisfy himself that the data have been lawfully processed.

12.4. Except where provisions of domestic law exist to the contrary, an employee should be entitled to designate a person of his choice to assist him in the exercise of the right of access or to exercise the right on his behalf.

12.5. If access to data is refused or if a request for rectification or erasure of any of the data is denied, domestic law should provide a remedy.

13. Security of data

13.1. Employers or firms which may process data on their behalf should implement adequate technical and organisational measures designed to ensure the security and confidentiality of personal data stored for employment purposes against unauthorised access, use, communication or alteration.

13.2. The personnel administration, as well as any other person engaged in processing the data, should be kept informed of such measures and of the need to respect them.

14. Conservation of data

14.1. Personal data should not be stored by an employer for a period longer than is justified by the purposes outlined in paragraph 1.3 or is required in the interests of a present or former employee.

14.2. Personal data submitted in furtherance of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made.

14.3. Where such data are stored with a view to a further job application, the data should be deleted if the candidate concerned so requests.

Where it is necessary to store data submitted in furtherance of a job application for the purpose of defending legal actions, the data should only be stored for a reasonable period.
COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

EXPLANATORY MEMORANDUM

to Recommendation No. R (89) 2
of the Committee of Ministers to member states
on the protection of personal data used for employment purposes

(Adopted by the Committee of Ministers on 18 January 1989
at the 423rd meeting of the Ministers' Deputies)

Introduction

1. Recommendation No. R (89) 2 on the protection of personal data used for employment purposes is the sixth such instrument adopted by the Committee of Ministers within the framework of the so-called "sectoral approach" to data protection problems. The value of adapting the broad principles laid down in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981[1] to the specific needs of particular sectors is now well accepted. Hitherto, the Committee of Ministers has adopted the following sectoral recommendations:

- Recommendation No. R (81) 1 on regulations for automated medical data banks (23 January 1981);

- Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983);

- Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing (25 October 1985);

- Recommendation No. R (86) 1 on the protection of personal data used for social security purposes (23 January 1986);

https://rm.coe.int/168050195b
- Recommendation No. R (87) 15 regulating the use of personal data in the police sector (17 September 1987).

2. The employment sector is an appropriate context for the elaboration of specific guidelines. In the first place, the vast majority of the population will either permanently or at various times find itself in an employment relationship in the public or private sector. Secondly, the employment sector gives rise to both individual and collective interests. The data processing activities of employers may have an impact on the workforce as a whole and accordingly guidelines on data protection must also address the collective interest. Thirdly, more and more employers are having recourse to technology as an aid to management and organisation of work. While the undoubted benefits of technology in the workplace cannot be denied, it is important to ensure that its introduction and application do not adversely affect the privacy interests of either individual employees or of the workforce as a whole.

3. With these concerns in mind, the intergovernmental Committee of experts on data protection mandated a working party "to identify and study the problems connected with the distribution and protection of personal information in the field of employment and to present concrete proposals for their solution". Under the chairmanship of Mr V. Librando (Italy) the working party, composed of specialists in the field of employment law and data protection law, met on four occasions between February 1985 and December 1986. The draft recommendation which emerged from its deliberations, along with the draft explanatory memorandum prepared by the Secretariat, was presented for final examination and approval at the 16th meeting (13-16 September 1988) of the Committee of experts on data protection (CJ-PD).

4. The committee of experts approved both texts and subsequently forwarded them to the European Committee on Legal Co-operation for examination and approval.

5. The draft recommendation and explanatory memorandum were approved by the European Committee on Legal Co-operation (on 2 December 1988) at its 50th meeting from 28 November to 2 December 1988.

6. Recommendation No. R (89) 2 on the protection of personal data used for employment purposes was adopted by the Committee of Ministers of the Council of Europe on 18 January 1989.

Preamble

7. The work of the Council of Europe in the field of data protection has always proceeded on the basis that automation brings undoubted benefits to society. The main concern of the Organisation in this area has been to place its introduction and use on a principled basis which allows technological progress to be accompanied by clear recognition of the need to safeguard the interests of the individual from the possible misuse of technology in particular data processing.
8. The employment sector - to which the principles contained in this Recommendation are directed - reflects this preoccupation: how is a balance to be struck between the undoubted advantages offered by technology to the running of enterprises, on the one hand, and, on the other, the rights and freedoms of employees in an automated work environment. 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 costs to the privacy of the individual employee, and of the workforce of an enterprise as a whole, which technology may possibly produce. And not only costs to privacy, although this is the primary concern of the principles set out in this Recommendation. The preamble also recognises that other rights and freedoms may possibly be put at risk through automation in the workplace - for example freedom of association or freedom of expression as guaranteed by the European Convention on Human Rights and which are of importance at the workplace, as well as the rights guaranteed by the European Social Charter which are of direct concern to the relationship between employers and employees, for example the right to organise and the right to bargain collectively.

9. 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 workday 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 of 28 January 1981 to protect the private life of the data subject from misuse of technology by regulating the collection, use, processing, storage etc. of personal information.

10. The Recommendation is, accordingly, structured in such a way as to make the Convention's broad principles meaningful to the employment context by offering principles designed to regulate the personal information activities of the employer. In other words, by adapting the Convention's basic principles relating to fair and lawful collection, purpose specification, finality, subject access, 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 his data stored by his employer?

11. Given that the Recommendation constitutes a sectoral approach to data protection, it is necessary to take account of all the elements characterising the sector in question which influence the way in which the Convention'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 group interests as well as individual interests are at issue. A valid sectoral approach must also seek to tailor the Convention'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 enterprise. Moreover, the inclusion of collective interests in the text is also justified by the fact that employees within an enterprise may be considered as a sort of "captive population" in regard to the use of data processing techniques, and the possible misuse of such techniques can affect the personnel within an enterprise as a whole as well as individual employees.

12. As regards implementation of the Recommendation's principles, the operative part of the preamble accepts that there exists a number of ways which are capable of ensuring that effect is
given to them. In the first instance, it is possible for the data protection authorities established pursuant to 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. Domestic data protection legislation under which the data protection authorities operate will of course apply to data processing in public and private sector employment. The Data Protection Convention, 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 concrete cases or as a basis for proposed codes of conduct for the employment field.

13. In addition, governments themselves should, where appropriate, strive to give recognition to the principles within the framework of other areas of the law which have a bearing on the employment sector. By way of example, social security legislation, tax legislation and, above all, labour legislation could usefully incorporate certain of the Recommendation’s principles in so far as such laws have a bearing on the personal information activities of employers.

14. Beyond these considerations, it is felt that the social partners themselves can negotiate acceptance and respect for the principles, either as a complement to legal regulation or as an alternative to it. The preamble takes account of the different national attitudes 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, governments should ensure, by means of publicity, that the representative bodies of employers and employees are adequately informed of the value of the Recommendation’s approach to data protection issues. The reference in the preamble to Article 6 of the European Social Charter emphasises the fact that the right to bargain collectively is an appropriate mechanism for ensuring acceptance and implementation of the principles through their incorporation in collective agreements.

1. **Scope and definitions**

15. Consistent with the scope of the Data Protection Convention, the principles contained in the Recommendation apply to the collection and use of personal data in public and private sector employment. Accordingly, the frequent references to "enterprises" in this commentary on the principles should not be interpreted as meaning that employees working in government departments, public institutions, etc. are not included within the scheme of protection. As will be seen from later provisions, "use" is to be understood as covering a range of processing activities including storage, communication and conservation of personal data.

16. While it is felt desirable that the principles should extend to automatically as well as manually processed data, since similar data protection problems may arise irrespective of the processing medium used, the Recommendation is essentially directed at personal data undergoing automatic processing. However, the drafters of the instrument felt that personal data not undergoing automatic processing should not entirely escape the reach of the Recommendation. Accordingly, while accepting that member states may extend the principles to both types of processing - and this is already the practice of some countries - (Principle 1.2), it was thought that the Recommendation should also apply to other personal data which are held
17. Furthermore, in addition to this justification for a limited inclusion of manual files, the Recommendation also makes it clear that the general exclusion of manual files from the scope of the Recommendation, subject of course to Principle 1.2, should not be seen as offering a way to escape the principles. The Recommendation is not to be undermined by deliberate attempts to opt for manual processing rather than automatic processing, which defeat its protective spirit by creating manual data havens.

18. The definition of "personal data" has acquired acceptance over the years through its use in other legal instruments of the Council of Europe in the field of data protection. This said, as technology evolves, so also should the breadth of the concept. Accordingly, it should be interpreted in such a way as to allow it to respond to the new problems posed by digitalisation of images, expert systems and other techniques.

19. The principle of finality or purpose specification is of crucial importance, serving as it does to define and limit the personal information activities of the employer. The finality identified for this sector - "employment purposes" - seeks to balance the interests of the employer with those of his 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 pursuant to tax or social security or industrial safety legislation ("the discharge of obligations laid down by law"). It is felt that the various elements (or subfinalities) expressed in the second sub-paragraph of Principle 1.3 which go to make up the notion of "employment purposes" are representative of the information needs of employers and are a valid reflection in this sector of Article 5.b of the Convention, under which data should be "stored for specified and legitimate purposes and not used in a way incompatible with those purposes".

20. Principle 1.4 of the Recommendation brings the activities of employment agencies or "head-hunting bureaux" in the public and private sectors within the scope of certain of its provisions ("where appropriate"). It may be the case that certain countries treat public sector employment agencies as distinct from the employment field and regulate them outside the context 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, where such exists, will apply to their data processing activities.

21. It will be noted that Principle 1.5, which makes provision for exclusion of certain types of personal data from the Recommendation's scope, is based on a proportionality test ("to the extent necessary"). The types of employment (private as well as public sector) envisaged in this paragraph are linked to certain of the interests set out in paragraph 2 of Article 9 of the Data Protection Convention, which can be invoked to justify a derogation from the Convention's basic principles. It will also be noted that the employment in question must be "closely related" to these interests. Accordingly, there is no open-ended exclusion for such types of employment from the principles of the Recommendation.
22. In conclusion, the Recommendation does not make a distinction between small or medium-sized enterprises and large enterprises for the purpose of application of the Recommendation's principles. It is felt that the size of the enterprise 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 employers, including small family businesses, with a minimum of bureaucracy. As recalled earlier, national data protection legislation, in conformity with the Convention, should apply to data processing in public and private sector employment, irrespective of the size of particular enterprises or government departments. Such legislation should, of course, be sensitive to the need not to impose unnecessary bureaucratic requirements on small employers.

23. It may be the case that a member state, at the time of signature or ratification of the Data Protection Convention, has excluded certain categories of personal data files in the employment field (for example, files containing payroll or accounting data), in application of Article 3, paragraph 2.a, of the Convention. Should this be the case, the principles of the Recommendation will not apply to such files, should that be the wish of the member state in question.

2. Respect for privacy and human dignity of employees

24. Principle 2.1 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. As stated earlier, privacy is to be seen in terms of data protection and as imposing limits on the personal information activities of employers. In this sense, it is also to be seen as conferring positive rights on employees to allow them to control, through the rights specified in Principle 12, that employers have respected the requirements of data protection.

25. The reference to "human dignity" in the text takes account of the fact that it may be all too easy for employees to become a "captive population" under constant surveillance by technological devices if it is not recalled that employees are first and foremost individuals with human needs for social contact with fellow employees at the place of work. Technology should not be used in a way which inhibits social interaction among employees. In another sense, respect for human dignity relates to the need to avoid statistical dehumanisation by undermining the identity of employees through data processing techniques which allow for profiling of employees or the taking of decisions based on automatic processing which concern them. These concerns are reflected at later stages of the text.

3. Information and consultation of employees

26. Whereas Principle 4 discusses in detail the procedures which should be respected by the employer when collecting data from, or on, an individual at the time of recruitment or in the course of his subsequent employment with the employer, Principle 3 deals with the more general, but equally important, issue of what should constitute a fair and lawful collection of data when the employer has recourse to automated systems or technical devices which allow data to be collected and processed in regard to employees as a whole at the place of work. Bearing in mind what was said in the preamble to the effect that the regulation of data processing within the employment sector must take account of collective as well as individual interests, Principle 3 of the Recommendation addresses the need to ensure transparency, for the benefit of the personnel
or workforce, in regard to any proposed introduction of automated systems or technical devices which allow data concerning them to be collected and stored. As stated previously (see paragraph 11), such data can be subsequently used for the taking of decisions affecting the employees as a whole (a wholesale restructuring), on a selective basis (selective redundancy), or individually (a dismissal).

27. Principle 3, accordingly, emphasises the need for such automated systems or technical devices to be introduced only after the personnel or workforce has been fully apprised of, or consulted about, the consequences attendant on the introduction of these techniques. They may range from telephone accounting systems, keyboard depression monitoring and the issuance of electronic tracking cards, perhaps with multifunctional uses, to fully-blown automated personnel systems. The reference to “technical devices” may be taken to include the proposed installation of video cameras at the place of work which are intended to monitor employee output.

28. It is important to stress in the context of Principle 3 that the provisions regarding information or consultation of employees are not solely applicable to techniques designed to monitor directly the output of employees - as may be the case with the proposed installation of video cameras. The provisions of Principle 3.1 will also apply to indirect surveillance of productivity or attitude to work - for example, a telephone logging system, primarily designed for billing purposes but which incidentally allows the employer to condemn a particular employee’s attitude to his work on the basis that he makes an exaggerated number of personal calls in the course of his working day.

29. It is believed that the approaches proposed in Principles 3.1 and 3.2 are sufficiently flexible to embrace the varying legal traditions which exist in member states in regard to the regulation of employer-employee relations (“in accordance with domestic law and practice”). In some countries, employees are informed to a limited extent only, even in regard to the processing of their personal data. In other countries, the collection and processing of personal data are subject to the procedure of information and consultation between the social partners. Obviously, the Recommendation does not advocate any particular solution. However, a minimum set of rights for employees in the context of data processing seems necessary.

30. The Recommendation suggests that these rights are to be protected by the information and consultation process. Employees should know of all the consequences which accompany the introduction of technology. They should be made fully aware of any possible threat to their privacy or human dignity which technology at the place of work may pose. Whenever the consultation process leads to the conclusion that the privacy and human dignity of the individual might be affected, the employer should be expected to seek - and if possible win - the consent of his employees. However, the employees’ consent as such is not the minimum requirement envisaged in the Recommendation. This said, the authors of the Recommendation felt that collective agreements negotiated between the social partners are a useful vehicle for reflecting the principle of information and consultation. While they may in some countries be used to compensate for the absence of statutory provision in this regard, they should also be viewed as capable of supplementing such regulations. For example, if domestic law is silent on the issue of provision of independent expert assistance to the personnel during the information and consultation procedure, such a clause could be negotiated into a collective agreements. Again, unless already provided for in domestic law, a referral of the sort of issues discussed in Principle 3 to an independent arbiter could also be envisaged in the collective agreement in the event of a failure to win the consent of the employees.
31. In conclusion, Principle 3 should not be seen as applying solely to unionised employees, where elected or nominated representatives speak on behalf of the personnel or workforce. The information and consultation principle as well as the agreement principle are equally applicable to situations of non-unionised labour. Accordingly, the fact that a non-unionised labour force or personnel exists within a small enterprise should not defeat respect for the principle. The employees themselves can still be collectively informed or consulted, or their agreement sought, as the case may be.

4. Collection of data

32. Principle 4 seeks to adapt certain of the protective provisions of Article 5 of the Data Protection Convention to the collection of data concerning individuals by their employers or potential 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 who may not be offered employment. It is felt desirable to provide guidelines relating to collection at the recruitment stage also.

33. Principle 4.1 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 4.1 accepts that it may be necessary at times to bypass the individual employee so as to obtain data on him, for example by means of consultation with his superiors or by having recourse to his employment record.

34. In addition, Principle 4.1 states the desirability of the individual being told of the possibility that recourse may be had to third parties outside the employment relationship so as to obtain data on him. As regards when such a collection procedure is deemed appropriate, it may be the case that an employer will need to check the accuracy of information supplied by an employee in the course of a promotion procedure, or if he has submitted a misleading claim for expenses.

35. It emerges from Principle 4.2 that the amount of personal information which can be legitimately collected on employees will of course depend on the job in question. Employers should review their data collection practices - for example the sending of detailed questionnaires to their employees - so as to ensure that they are not storing too much personal information, and which is out of proportion either to the nature of the employment or the needs of the moment. The text accepts that, at certain periods in the life of an enterprise, it may be necessary for the employer to obtain more data than normal - for example, for the purposes of a proposed merger or wholesale restructuration, it may be appropriate to seek the personal views of the employees.

36. It will be noted that, in addition to the requirements of relevancy and adequacy, the collection procedure is also linked to respect for finality ("for employment purposes"). (As regards the collection of particular categories of data, see the commentary on Principle 10, and in particular paragraphs 68 et seq.)
37. Principle 4.3 relates to data collected in furtherance of a job application. It places limits on the sort of questions which can be asked of candidates during job interviews or, prior to interview, in application forms. In brief, the sort of data which can be legitimately collected should be limited to information thought necessary to determine whether a given candidate is the right person for the job. Once again, the type of employment in question will influence the amount of information which can be sought, bearing in mind also that certain types of employment may require the prospective employer to obtain additional data relating to candidates' ability in the long term to move up in the hierarchy, to assume more responsibility with the passage of time, etc.

38. Although Principle 4.3 stresses again the need to regard the individual as the primary source of information, it also accepts the need for prospective employers to consult other parties to obtain data, for example, referees named in candidates' application forms or other unnamed sources capable of verifying the accuracy of the information submitted by the candidate for a post. However, unless provisions of domestic law prevent this - and this may be the case for security-risk employment - the individual should be able to influence to a greater ("with his consent") or lesser ("informed in advance of this possibility") extent the decision to consult third parties. In other words, a secret collection of data is to be avoided.

39. Even where domestic law would allow information to be collected on a job applicant without his knowledge, it should be the case that the legal provision authorising a secret collection of data should satisfy the requirements of paragraph 2 of Article 8 of the European Convention on Human Rights.

40. Principle 4.4 refers to certain techniques, for example handwriting tests, which are designed to enable employers to draw conclusions concerning the psychological make-up of employees or job applicants. Quite apart from the issue of whether or not such techniques provide accurate results, it is felt that they pose privacy problems. It is for this reason that they should only be used on the individual with his consent or if domestic law circumscribes their use by requiring other appropriate safeguards to be observed. Moreover, account should be taken of the fact that use of certain techniques (lie detectors, brainwave screening) may be incompatible with Principle 2 as well as with the requirement that data should be collected lawfully. At any rate, member states should give careful consideration to the need to place the use of such tests, analyses or procedures on a legal basis accompanied by safeguards. As regards genetic screening techniques which allow health predictions to be made on the basis of a genetic map supplied by job applicants or employees, regard should be had to Principle 10.

5. Storage of data

41. The personal data stored by employers must have been obtained as a consequence of a fair and lawful collection procedure as interpreted in the preceding principle and in conformity with the principle of finality (Principle 5.1).

42. Principle 5.2 subjects the data stored to the data quality requirements of Article 5.c of the Data Protection Convention. The reference to the need for the data to "represent faithfully the situation of the employee" reflects the desirability for the information to be complete in the sense that its interpretation should not convey only half the story - for example, that an employee has been frequently absent from work with no accompanying reference to the fact that
the absence was due to periods of hospitalisation. Although the text does not require employers to update personal data on a daily basis, since this would in many cases oblige employers to collect much more data which in turn might have adverse effects on the interests of the employee, it should nevertheless be the rule that updating takes place when important decisions affecting an employee are to be taken on the basis of the data.

43. Principle 5.2 also takes up the human dignity issue expressed in Principle 2. It will be recalled that employees should not lose their individual identity by being seen in solely statistical terms or as coded numbers in an automated system.

44. The second sentence of Principle 5.2 is intended to guarantee that the employee is in a position to understand the data stored on him. It should be prohibited to store data which are coded in such a way as to be unintelligible to anyone except the initiated. In addition, a system of data storage which is unintelligible to the employee presents a severe obstacle to the exercise of the rights laid down in Principle 12. Finally, the storage of personal data in expert systems should also comply with this requirement.

45. The opinions referred to in Principle 5.3 are of a subjective nature and it is for this reason that it is felt desirable that they should conform to the requirements laid down therein. The importance of the issue of respect for human dignity is reflected in the prohibition on storing insulting comments on members of the personnel or workforce.

46. It will be seen from the situations identified in Principles 6 to 9 that, with the exception of the use of personal data within the enterprise, public body, etc. where the employee is engaged, all other types of use are referred to as communications.

6. Internal use of data

47. It is important to identify clearly the various circumstances in which personal data can be legitimately used and to provide for the necessary safeguards in the event of use going beyond the notion of finality on which the Recommendation is based - "employment purposes". However, it should be borne in mind that the expression "employment purposes" covers a range of sub-finalities for which data can be collected, stored and used. For example, personal data may be collected and stored on a file 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 stored for salary purposes. It is felt important to bear in mind the context for which the data were collected, since random use of data, although for an employment purpose, may distort the meaning originally reserved for a particular category of data.

48. Principle 6 deals solely with the situation where personal data are used internally by the employer. Principle 6.1 is a general statement requiring respect for finality. Personal data collected and stored for employment purposes should only be used for employment purposes.
49. For the reasons stated in paragraph 47, Principle 6.9 cautions against the free use of personal data relating to specific employment purposes so as to enrich a particular data file or to produce an entirely new context.

Principle 6.2 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, care should be taken to show that the repeated absence of an employee is attributable to his being on an authorised training scheme when it is sought to use such information in deciding whether or not his wages should be docked for irregular attendance at work. Alternatively, the fact that an employee's file reveals that his repayments of a company loan are in arrears should not be taken into consideration in the context of disciplinary proceedings.

However, whether or not subsequent use of personal data is to be adjudged "incompatible" with the original purpose for which the data were collected is to be determined by national law. It will be recalled that the Data Protection Convention tolerates different applications of the notion of compatibility. For example, it may be the case that domestic law may prohibit the use of personal data collected for a particular employment purpose and for which the data could not have been lawfully collected in the first place. For example, if domestic law prevents the collection of health data without the consent of the employee it would be unlawful to use data relating to the type of canteen meals consumed by an employee to determine whether he suffered from, for example, diabetes.

Moreover, irrespective of different national approaches to the issue of "incompatibility", it may also be the case that an employer's undertaking that he will not use data collected for certain purposes for other purposes within the employment relationship may effectively restrict subsequent use of the data. Moreover, 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 subsequent use of the data collected for another unrelated employment purpose (see also paragraph 50).

50. The text of Principle 6 is silent on the issue of the collection and storage 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 of the Committee of Ministers should be respected.

51. Informing the employee of any proposed use of data drawn from different contexts so as to take decisions which affect his interests is seen as a safeguard for the employee against the sort of prejudice illustrated above. It is not simply a fair employment practice, it is also fair data protection practice.

52. As Principle 6.3 suggests, the interconnection of different employment files is an illustration of the latter practice - for example, the new context may be an employee profile developed through interlinkage of data relating to punctuality, discipline, age, discharge of a company loan, absence from work, use of employee sports facilities, etc. If such data produce an overall negative picture of the employee, adverse decisions could be taken which affect his
interests - for example, a refusal of promotion, a deduction from wages, a denial of a company loan, or transfer to another post.

7. Communication of data to employees' representatives

53. The meaning to be assigned to the term "employees representatives" will, as stated earlier, be determined by national law and practice in the field of labour relations. They may include works councils, trade union representatives or other associations to which the employee is affiliated. It may be that 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. As a rule, the transfer of personal data relating to employees who are not members of the representative body should only be done so with their consent.

The quantity of personal information which can be transferred is subject to a proportionality test - only such as is "necessary to allow them 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 regulation of 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 text also refers to the possibility of the social partners themselves agreeing through the mechanism of the collective agreement on the quantity and categories of personal data which can be communicated. However, the safeguards identified in Principle 7 must still be observed:

a. are such data necessary for b. representing the interests of the employees?

54. It goes without saying that the data collected and stored by representative organs in these circumstances are subject to the general principles of data protection.

8. External communication of data

55. 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. The various public bodies referred to in Principle 8.1 may be tax or social security authorities, health and safety inspectorates, and so on. The nature and amount of personal data which can be communicated to such public bodies will be determined in accordance with the scope of the statutory duty imposed on the employer. "Legal obligations" should be understood in this sense. It does not extend to contractual commitments undertaken by an employer vis-à-vis a public sector enterprise which needs lists of names and addresses for the sending out of promotional literature in pursuance of a proposed privatisation scheme.

56. Statutory bodies may require personal data to enable them to exercise their official functions - for example, government research in the field of occupational injuries and diseases, or the analysis of employment patterns in depressed areas. It is felt that the expression "or in accordance with other provisions of domestic law" may oblige communication of employee data in
those circumstances. It depends on the national context. In addition, domestic law may at
various times require the communication of personal data to the police, courts, as well as 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 spouse may require the communication of data relating to his 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 his marriage. As regards the communication of personal data to the
police - which may be required by domestic law - reference should also be made to the provisions
of Recommendation No. R (87) 15 of 17 September 1987 regulating the use of personal data in
the police sector.

57. 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 in the capacity of an employer in the market place - as well as to
private parties, including enterprises within the same group. The circumstances envisaged in
Principle 8.2 may cover communication for employment purposes as well as for non-employment
purposes. Not surprisingly, the safeguards laid down vary in accordance with the circumstances.

58. 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 a bookkeeper 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 transfer 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 will be noted that the legitimacy of communication in those
circumstances is made subject to ensuring respect for finality. Accordingly, the considerations
discussed under Principle 6.2 are equally valid for the interpretation of Principle 8.2.a ("which are
not incompatible with the purposes for which the data were originally collected"). Principle 8.2
also makes communication of the data conditional on prior information being given to the
workforce or its representatives. Once again, the text of the Recommendation recognises the
value of data protection operating in conjunction with transparency. If the information referred to
in Principle 8.2.a is not provided for in domestic law or practice, it could, like so many other
aspects of this Recommendation, be the subject of a collective agreement, or alternatively be
introduced by the employer himself as a matter of fair employment practice.

59. As regards Principle 8.2.b, the personal data to be communicated may not be intended to
be used 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 and informed consent of the individual employee must be
obtained.

60. It may also be the case that domestic law will authorise a communication of personal
data to private bodies or public bodies not discharging official functions, and for other than
employment purposes. Principle 8.2c provides for such a possibility. National legislation on
statistics may be one such case.

9. Transborder data flows
61. The text of the Recommendation takes account of the reality of the multinational enterprise with subsidiaries situated in various states or even continents. From the point of view of data protection, problems may arise if a head office, situated in the territory of a state where there is no legislation on data protection, requests its subsidiary, situated in a country where personal data are protected by law, to send employee data to it.

62. As regards transfers between enterprises which are established in the territory of states which have ratified the Data Protection Convention, problems should not arise in practice even if the problems of private international law which transborder data flows could pose are not to be underestimated. However, given the fact that this Recommendation is designed to adapt the broad principles contained in the Data Protection Convention, including Article 12 which is devoted to transborder data flows, it is felt that the criteria set out in Principle 9 constitute a desirable way of implementing Article 12 in the context of transborder communication of data relating to employees.

63. As with Article 19 of the Convention, the text of the Recommendation is silent on the question of transborder data flows between a firm situated on the territory of a Contracting Party and a firm established in a country which has no legislation in the field of data protection. In these cases, consideration should be given to the possibility of contractually obliging the person who is to receive the data to respect the principles laid down in this Recommendation. At any rate, transborder data flows are expressly stated to be subject to the safeguards set out in Principles 6 to 8.

64. Although the commentary places emphasis on transborder data flows between enterprises in the same group, it should also be borne in mind that there may be other situations which raise the same issues for example litigation in one state which requires personal data to be communicated by an employer established in another state, or the transfer of employee data for an international research project. The policies advocated earlier are equally applicable to these situations of transborder flow.

10. Particular categories of data

65. As with the Data Protection Convention 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 10 also lays down special guidelines for the collection and storage 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 10.1. It is felt that for this reason health data require more extensive consideration.

66. The principles laid down earlier in the Recommendation in regard to the collection and storage of personal data must be read in the light of the provisions relating to sensitive data set out in Article 6 of the Data Protection Convention. The principles seek to adapt this article to the requirements of the employment sector in regard to which no exception other than the one referred to in Principle 1.5 of the Recommendation (see paragraph 15) can be made. As regards employment 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. Accordingly, the fact that domestic law requires certain information to be obtained by the employer is simply not sufficient to make automatic processing of such information
compatible with the Convention. It is also necessary for any possible processing of the data to be circumscribed by appropriate guarantees which must also be laid down by domestic law. Where necessary, the legislation should also envisage providing for at least the express and informed consent of employees in accordance with the last sentence of Principle 10.1. Moreover, the attention of employers should be drawn to the need not to use automatic processing of sensitive data for daily management purposes and also to the fact that, in practice, it will more often than not be possible to find ways of avoiding having recourse to automatic processing of such data.

67. In the light of those considerations, the Recommendation should apply to cases where, for example, domestic law requires the collection and storage of data relating to the religious beliefs of its employees so as to enable church taxes to be levied on their salaries. And, similarly, national legislation aimed at preventing racial or religious discrimination in employment may require data relating to these factors to be obtained by employers so as to enable bodies which monitor the implementation of such laws to assess whether religious and ethnic minorities are fairly represented numerically within the workforce.

68. The approach should be the same when the very nature of the employment requires certain types of sensitive data to be obtained: political organisations which seek to influence public opinion will require information to be obtained on the political views of candidates for posts with such organisations; religious institutions will require candidates for employment with them to state their religious convictions at the time of recruitment. Beyond the nature of specific types of employment, other particular cases may exist, for example, obtaining data relating to the religious beliefs of certain employees for the purposes of ensuring that certain types of meals are served in a works' canteen.

69. Trade union membership warrants a separate comment. Although Article 6 of the Data Protection Convention does not refer to it expressly, it is understood that certain countries may regard such membership as sensitive data and prohibit or limit collection accordingly. Member states, in accordance with their domestic law and practice, may take additional safeguards to increase the protection to be accorded to personal data relating to trade union activities or beliefs - for example along the lines advocated in Principle 10.1 - and especially because they are linked to political opinions.

70. Subject to the rules on the collection of personal data governed by medical secrecy referred to in Principles 10.4 and 10.5, and unlike the other categories of sensitive data referred to in Principle 10.1, the collection and storage of data relating to the health of employees or job applicants are not subject to a requirement of "particular cases". It is accepted that the collection and storage of such data are a generalised and necessary practice in the employment sector. It is this very fact, coupled with the sensitivity of health data, which calls for particular vigilance so as to make the collection of such data acceptable.

71. It will be noted that, in Principles 10.4 to 10.6, the drafters of the Recommendation made a deliberate distinction between health data in general and medical data covered by medical secrecy. It goes without saying that medical data governed by medical secrecy require particular protection. With this in mind, Principles 10.4 to 10.6 establish a special legal framework aimed at guaranteeing the confidentiality of these data.
72. Principles 10.2 et seq. are structured in such a way as to limit the collection, storage and use of health data (Principles 10.2, 10.3 and 10.4) while emphasising the need for security (Principle 10.5) and access rights for the data subject (Principle 10.6). It should also be borne in mind that the Committee of Ministers of the Council of Europe has already adopted a recommendation on regulations for automated medical data banks (Recommendation No. R (81)1). The principles contained in that Recommendation could also be usefully referred to in this context.

73. As regards collection, Principle 10.2 places restrictions on the sort of health data which may be collected. It will be noted that health data concerning job applicants as well as employees are covered.

74. 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 examination, be required to supply information regarding the incidence of cancer or other diseases in his family history. Applicants for jobs in the liberal professions would not be expected to do so.

75. Particular attention should be paid to modern medical techniques which make it possible to uncover the most intimate information on the employee's health potential. Given the principles on respect for privacy and 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 work on genetic screening techniques carried out by the ad hoc Committee of experts on bioethics (CAHBI). 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 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 in respect of 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 reference to "the requirements of preventive medicine" in Principle 10.2.b covers periodic check-ups, for example to ensure that employees who are exposed to toxic substances in their work environment do not contract illness. Principle 10.2.c allows health data to be collected so as to allow "social benefits" to be granted to an employee. For example, an employee injured at his place of work who makes a claim under a company insurance scheme may need to be medically examined so as to determine the nature and extent of his disability. Moreover, industrial injuries schemes or workmen's 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 his making future claims against the state fund.

77. Principle 10.3 concerns the collection of health data. Domestic law will determine the sort of data which are covered by medical secrecy rules. They relate to both physical and mental health. The individual should be the primary source of information for the purposes of supplying such information - primarily through his physical examination and answers to the questions put to him to determine his fitness for employment. Where an employer seeks to obtain medical data relating to an employee from another source, for example by contacting a former employer, he
must first obtain the express and informed consent of the employee or do so in accordance with provisions of domestic law which take account of the requirements of medical confidentiality. As regards health data relating to the general state of health or general physical condition of an employee or job applicant, the Recommendation accepts that such broad enquiries can be directed to previous employers, referees, an employee’s superiors, etc. In addition, the finalities specified in Principle 10.2 also apply to Principle 10.3.

78. Where a company or organisation employs its own medical staff to conduct medical examinations on employees or job applicants, it is essential that the members of it enjoy ethical independence from their employer. The categories of persons, other than doctors, who are bound by rules on medical secrecy should be determined in accordance with national law and practice. Principle 10.4 places severe limitations on the communication of medical data stricto sensu to administrative personnel, it being understood that general indications on the state of health of an employee or job applicant 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.

79. Principle 10.5 reflects the concern expressed in Recommendation No. R (81) 1 that medical data should be stored in special data banks and not integrated into general data banks. 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 utilised so as to prevent unauthorised access.

80. 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 secrecy - for example computer 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.

81. In conclusion, consideration could also be given to the need to avoid automating health data, so as to avoid the possibility of unauthorised access which networks offer.

82. The limitation contained in Principle 10.6 on the exercise of the right of access is taken over from Article 9.2.b of the Data Protection Convention ("protecting the data subject") and is consistent with paragraph 6.1.b of the appendix to Recommendation No. R (81) 1.

11. Publicity in regard to personal data

83. Principle 11, taken in conjunction with Principle 12, illustrates the necessary connection which the Recommendation frequently makes between the value of transparency and data protection. To enable the data subject to exercise his rights effectively, he should be informed of the existence of such rights as well as the procedure to be followed so as to avail himself of them (Principle 11.2). The information supplied in this regard should be as clear and intelligible as possible, indicating such matters as when and where the rights can be exercised.
84. In addition to information on the rights of the data subject, publicity should also be given to the general data processing policies of the employer. Principle 11.1 advocates the employees also being informed of the various matters outlined therein. An employer is not obliged to describe in every detail the complexity of data processing, since this would not only involve too much red tape but would also require too much detailed knowledge on the part of the employee.

85. Principle 11 proposes a number of ways in which the employee can be informed both of his rights as well as the data processing activities of the employer. For example, these matters could be brought to the attention of employees in their contract of employment, or by means of literature circulated by their representatives, or quite simply by means of information notices displayed at the place of work.

12. Right of access and rectification

86. Subject to the provisions of Principle 12.2, it was felt by the drafters of the Recommendation that there is no reason in principle why an employee should not, on request, enjoy a right of access in regard to all the data concerning him which are stored by his employer. There may of course be practical limitations to an exercise of the right of access. For example, a particular data file may contain data on several employees. If it is not possible to sever the data of the employee seeking access from the data of his colleagues, the employer may be obliged to seek their consent before access can be granted.

87. The position which the drafters of the Recommendation take in regard to opinions and evaluations ("judgmental data") is inspired by the fact that certain countries have experienced no practical difficulties in extending the right of access to such information - for example, evaluations made by an employee's superiors. It will be recalled from Principle 5, that such judgments must be fair and honest and must not be insulting in the way they are formulated. Principle 12.1 stipulates that the employee should have a means of appeal for challenging the assessment.

88. In principle, the right of access should be free of charge. At any rate it should not exceed a reasonable amount and the employee should be entitled to receive a copy of the data requested at a cost, if such is required, which does not exceed the cost of producing the document. Exercise of the right of access enables the employee to check the accuracy of his data, to determine whether irrelevant data have been processed, to discover if they are a faithful representation of his employment circumstances, to ensure that they have been collected and used properly. It is for these reasons that rights of rectification and erasure accompany the grant of the right of access.

89. The limitation on exercise of the right of access expressed in Principle 12.2 contemplates, 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 exercise of the right of access has been suspended, and this may only be carried out to the extent indispensable for the needs of the investigation, such suspension may not last beyond the close of the inquiry. Principle 12.2 supposes that in all cases the employee shall have the possibility of defending himself.
90. Principle 12.2 is silent on the issue of the exercise of the right of access by employees who work in security-risk employment within the meaning of Principle 1.5. It is suggested that any limitation or denial of the right of access in these cases should be based on the provisions of Article 9.2 of the Data Protection Convention.

91. Principle 12.3 is another illustration of a fair employment practice going hand in hand with a data protection policy in the employment sector. Whereas employment law in various member states may recognise the right of an employee to know the reasons on which a decision adverse to him are based (for example, a disciplinary measure, a dismissal, a denial of promotion), Principle 12.3 advocates that the employee should also be able to determine whether the decision is based on information which has been lawfully processed in accordance with the principles contained in this Recommendation - for example, that the data are accurate, up to date and represent faithfully his employment situation. In addition the fact that a decision is based on automatic processing cannot deprive the data subject of the right which may be granted by his domestic law to know the reasons on which the decision is based.

92. Implementation of the requirements of Principle 12.3 necessitates the employee being granted access to the automatic reasoning on which the decision is based, and for this purpose he should be entitled to consult and examine the relevant automatic reasoning.

93. The person designated by the employee in accordance with the provisions of Principle 12.4 may be a colleague, his lawyer or his representative. What is essential is that the employee himself must appoint such a person. The limits to the sort of assistance to be offered by the nominee will be determined by the employee.

94. Principle 12.4 accepts that domestic law may restrict, or even prohibit, the system envisaged by regarding the right of access as something exclusive to the data subject.

95. Domestic law will determine the nature of the remedy envisaged in Principle 12.5 - for example an appeal to a supervisory authority established in accordance with data protection legislation, or a court or tribunal.

13. Security of data

96. The requirement of data security, as stated in Article 7 of the Convention, is given concrete expression in Principle 13 of the Recommendation.

97. The implementation of Principles 13.1 and 13.2 should take account of possible security risks posed by the use of distributed data processing systems, networks, remote access to data via terminals, etc. which is made possible in the work environment as a result of technology.

98. Principle 13.1 not only addresses employers, but also third parties, such as employment agencies and computer bureaux processing the personal data of employees on
behalf of employers.

14. Conservation of data

99. The length of time for which personal data can be stored by an employer should be determined by the factors indicated in Principle 14.1. It goes without saying that the accomplishment of certain employment purposes will necessitate a longer period of conservation than may be the case for the performance of other such purposes. For example, payment of a company pension scheme will oblige the employer to retain data long after the employee has retired. The context will determine the period of conservation which is justified.

100. Principles 14.2 and 14.3 devote particular attention to the case of personal data submitted by a candidate for employment. In principle, such data should be deleted when the candidate's application is rejected.

101. 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 is more suited. It may also be in the interests of the rejected candidate to have his information kept on the employer's books. Nevertheless, it is felt desirable to inform the candidate of the wish to retain his data. Principle 14.3 reserves to the candidate the right to have all the information deleted.

102. Principle 14.3 envisages 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. For example, the employer may wish to prove to a tribunal that the candidate was not rejected on grounds of sex, race or religion, or that correct recruitment and interview procedures were followed. The data should only be stored for a reasonable period. The circumstances will determine the length of the period. It goes without saying that, should legal proceedings not occur, the data are to be deleted.

[1] The Convention entered into force on 1 October 1985. At the date of publication of the explanatory memorandum, the Convention has been ratified by the following states: Austria, France, the Federal Republic of Germany, Luxembourg, Norway, Spain, Sweden and the United Kingdom; it has been signed by Belgium, Cyprus, Denmark, Greece, Iceland, Ireland, Italy, the Netherlands, Portugal and Turkey.