COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 30 August 2011 T-PD-BUR(2011)07prov2 EN

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

(T-PD-BUR)

Draft Recommendation on the protection of personal data used for employment purposes[1]

[1] Changes proposed to the existing text of Recommendation (89)2 are highlighted.

DRAFT RECOMMENDATION CM/REC(2011)… 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 … 2011
at the … 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 new technologies and means of electronic communication in the relations between employers and employees, and the corresponding advantages thereof;

Believing, however, that the use of data processing methods, in particular automatic processing, 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 rights to privacy and protection of personal data;

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 of its Additional Protocol regarding Supervisory Authorities and Transborder Data Flows of 8 November 2001, 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;

Aware of the changes which have occurred internationally in the working world and related production processes; notably due to the use of information and communication technologies and of the globalisation of activities and services;
[EM[2]: private and public employment]

Considering that such changes impose a revision of Recommendation No. 89 (2) on the protection of personal data used for employment purposes in order to continue providing an adequate protection of individuals;

Recalling 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, referred to in Resolution 1604 (2008) of the Parliamentary Assembly of the Council of Europe, which are fully topical and relevant and thus deeming it unnecessary to incorporate into a new recommendation further specific principles governing the use of video surveillance;

[2] EM stands for Explanatory Memorandum and indicates that additional details on a specific point will be given in the explanatory memorandum to the Recommendation.

Recalling the European Social Charter of 18 October 1961, in particular its Articles 1.2 and 6, and the International Labour Office's 1997 Code of Practice on the Protection of Workers' Personal Data;

Recalling the European Convention on Human Rights, which protects in its Article 8 the right to private life, encompassing activities of a professional or business nature as interpreted by the relevant case law of the European Court of Human Rights;

Recommends that governments of member states:

- ensure that the principles contained in the present recommendation and its Appendix, which replace the above-mentioned Recommendation Rec(89)2, 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 present 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 appendix to this recommendation also by means of complementary instruments such as codes of conducts, ensuring its wide circulation among representative bodies of both employers and employees**,** as well as by involving designers and suppliers of technologies in the implementation processes of certain principles.

Appendix to the Recommendation

1. *Scope and definitions*

1.1. The principles set out in this recommendation apply to any collection and processing 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, or used in any way to take decisions having a significant effect on the rights of the data subject concerned (EM: by analogy, they apply, where appropriate, to any personal data relating to individuals outside the workplace which are processed for work safety purposes, and also to trade union organisations.)

The manual processing of personal 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:

'Personal data' means any information relating to an identified or identifiable individual ("data subject"). An individual is not considered "identifiable" if identification requires unreasonable time or effort. [EM: by analogy : professional associations]

- ‘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. [EM: also relates to data processed after termination of the employment contract]

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 process, also through online information systems, personal data so as to enable one or more contracts of employment, including simultaneous or part-time contracts, to be established between the persons registered with them and prospective employers, or to help discharge the duties relating to those contracts. [EM: Information systems and technologies, genetic data, sensitive data]

2. *Respect* for human rights, dignity and fundamental freedoms

Respect for human rights, dignity and fundamental freedoms, including the right to private life, the right to the protection of personal data, the right to non-discrimination should be safeguarded in the processing of personal data for employment purposes, notably to allow to employees the free development of their personality and to foster possibilities of individual and social relationship on the workplace.

3. *Necessity, development of other principles and simplifications*

3.1. Information systems and technologies used for the collection and processing of personal data for employment purposes should be configured, and as the case may be certified, so as to minimise the use and storage of personal data, as well as to limit the use of directly identifying data to only that necessary for the aims pursued in the individual cases concerned. The same applies when they are used and implemented in the working environment. [EM: specify that tools and devices are covered by the notion of information systems and technologies – ref 3.3]

3.2. The employer should develop appropriate measures, including organisational ones, to ensure that they respect in practice the principles relating to data processing for employment purposes, and to enable this to be demonstrated adequately at the request of the supervisory authority.

3.3. Measures should be adopted according to the size of the concerned entity and the nature of the activities undertaken, taking also into account the possible consequences for data subjects.

4. *Information and consultation of employees*

4.1. The introduction and use of information systems and technologies for the direct and principal purpose of remotely monitoring employees’ activity, behaviour or localisation should not [in principle] be permitted when leading to a permanent monitoring of employees [except where no alternative means which are less intrusive are available and where appropriate safeguards exist].

[EM: complementary to 4.1 – without prejudice of measures relating to well founded defence proceedings. The use of information systems and technologies, such as video surveillance on the workplace or geolocalisation systems, should be limited only to organisational and/or production necessities, or for security purposes on the workplace. Such systems should only

be allowed if legitimate, necessary and regulated. They should not aim at permanently monitoring the quality and quantity of the individual work on the workplace, nor aim at remotely monitoring employees' behaviour or localisation.]

4.2. In case of the introduction, adaptation and operation of information systems and technologies for the collection and processing of personal data necessary for requirements relating to production or safety or work organisation, employees or their representatives, in accordance with domestic law or practice and, where appropriate, in accordance with the relevant collective agreements, should, in advance, be fully informed or consulted**.** [EM: tools also covered by information systems and technologies]

4.3. The employer should take appropriate measures to assess the impact of any data processing which poses specific risks to the right to privacy, human dignity and protection of personal data, and to process such data in the least invasive manner possible. The agreement of employees' representatives should be sought before the introduction or adaptation of such information systems and technologies where the information or consultation procedure referred to in principle 4.2 reveals such risks unless domestic law or practice provides other appropriate safeguards.
[EM: for small enterprises, representatives refers to employees as such.]

5. ***Collection of data and particular forms of processing or of information***

5.1. Personal data should in principle be collected from the data subject concerned. When it is appropriate to process data external to the employment relationship or consult third parties, for example concerning professional references, the data subject should be informed.

5.2. 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.

5.3. In the course of a recruitment or promotion procedure, the data collected should be limited to such as are necessary to evaluate the suitability of the persons concerned and their career potential.

In the course of a recruitment, personal data should be obtained solely from the individual concerned. Subject to provisions of domestic law, external sources, including those from consultancies or social networks for the development of professional relationships, may only be consulted with the consent of the individual concerned or if he or she has been informed in advance of this possibility. Profiling of the person concerned based on the secret collection of data from search engines should [in principle] be prohibited. An employer should not persuade the person concerned to provide or to enable access to any medical information held by third parties. [EM: added value of this Recommendation concerning electronic medical data / Ref recommendation (97)5 – explain profiling]

In any event, appropriate measures should be taken so that also in the case of data readily accessible in electronic communications networks available to the public, only relevant, accurate and up-to-date data are used, thus also avoiding misinterpretation or unfair processing of that data viewed in the light of the context of its origin.

5.4. Recourse to tests, analyses and similar procedures designed to assess the character or personality of the individual should not take place without his or her consent or unless domestic law provides other appropriate safeguards. If the individual so wishes, he or she should be informed in advance of the use that will be made of the results of these tests**,** analyses or similar procedures and, subsequently, the content thereof. [EM: no decision

producing legal effects can be taken on the sole basis of such tests, analysis and similar procedures. The individual's profile should be based on objective data an in no circumstances reveal health related information. Such tests must be relevant and based on scientifically recognised methods. Regarding information on the content, possibility to delay in the provision of this information when protecting legitimate interests, including the ones of the employer]

5.5 The processing of biometric data to identify or authenticate individuals should in principle only be permitted where it is necessary to protect the legitimate interests of the employer, employees or third parties and should be based on scientifically recognised methods which appropriately ensure security. [EM: definition of legitimate interests]

5.6. With regard to possible processing of personal data relating to Internet or Intranet pages viewed by the employee, preference should be given to the adoption of preventative measures, such as:

- the configuration of systems or use of filters which prevent particular operations, as the case may be; [EM: such as uploading and downloading of particular content]

- the identification of sites which are or are not deemed to relate to the work carried out;

- the grading of possible monitoring on personal data, providing first for non-individual random checks on data which are anonymous or in some way aggregated. [EM: for example, by production unit].

The persons concerned should be properly informed, in conformity with principles 4 and 12.

Where an employee uses, with the employer's authorisation, equipment which may reveal whereabouts, in particular outside working hours, appropriate arrangements should be made so that data relating to such whereabouts are not used and are automatically deleted as soon as possible.

Appropriate internal procedures relating to the processing of that data should be established and notified to the persons concerned in advance. (EM: procedure which concerns policy in monitoring – procedure also valid for other types of processing?)

5.7 The employer should take the necessary measures and foresee the appropriate procedures aimed at enabling, in case of absence of the employee, access to professional emails when such access is of absolute professional necessity, and after having informed the employee. Access to personal emails of the employee shall never be permitted.
[EM: structure : surveillance of employees ?
Where possible, preference should be given to assigning employees email addresses which are directly traceable to posts rather than to individuals.
Appropriate instructions should be issued so that where an employee is absent the email system automatically communicates the details of another point of contact, indicating that the employee is temporarily absent.
In order to inform the addressee that the email account is used purely for professional purposes, an appropriate warning should be inserted in emails sent by the employee.]

6. *Storage of data*

6.1. The storage of personal data is permissible only if the data have been collected in accordance with the rules outlined in principles 4.1 and 5 and if the storage is intended to serve employment purposes. Where this is not the case, the employer should refrain from using the stored data.

6.2. 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 or her to be characterised or profiled without his or her knowledge.

Where the use of biometric data is permitted under paragraph 5.5, they should not, as a rule, be stored in a database, and preference should be given, where appropriate, to biometric identification or authentication systems based on media made available solely to the person concerned. [EM: specify when such a storage is permissible].

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

7. *Internal use of data*

7.1. Personal data collected for employment purposes should only be processed by employers for such purposes.

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 could be made easily accessible in internal communication networks in order to speed up the performance of the work carried out and facilitate interaction with other employees. [EM: identification data – large scale context : intranet tools for instance : tel/email/picture only with consent].

7.2. Where data are to be processed 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 processed, he should be informed. [EM: illustrate with concrete examples]

7.3. The interconnection of files containing personal data collected and stored for employment purposes is subject to the provisions of principle 7.2.

7.4. Without prejudice to principle 9, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principle of purpose specification in the subsequent use of the data. Where substantive changes in the processing occur, the persons concerned should be informed. [EM: in the due respect of applicable law and as may be found appropriate by data protection authorities]

8. *Communication of data and use of information systems for the purpose of employee representation*

8.1. 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.

8.2. The use of information systems and technologies for trade union communications should form the subject-matter of appropriate agreements with the employer designed to lay down in advance transparent rules permitting correct use and to identify safeguards to

protect any confidential communications. [EM: the type of agreement is not to be determined by the data protection authorities]

9. *External communication* and dissemination *of data*

9.1. 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.

9.2. 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 consent of the individual employee; or

c. if the communication is authorised by domestic law, in particular where necessary for judicial purposes or to exercise a right before a judge. [EM: give other examples]

9.3. On the basis of adequate safeguards provided by domestic law, personal data can be communicated within a group of enterprises for the purpose of discharging duties provided for by law or collective agreements. The consent of the employee may also be required as safeguard.
[EM: it cannot be excluded that in precise areas, a freely given consent may play a role. Illustrate with examples of situations such as sharing CVs. Duties relating to social security and welfare for employees, or to optimise the allocation of human resources.]

9.4. With regard in particular to the public sector, the law should reconcile the right to privacy and protection of personal data with the requirements relating to transparency or monitoring of the correct use of public resources and funds by identifying professional categories or profiles in respect of which there are requirements relating to the publication of certain information, and also the type of the relevant notices which, for homogeneous classes, can be made public, that is to say by also considering the possibility of identifying them more easily where they can be traced through external search engines.

9.5. When the work tasks entail a constant relationship with the public or where this is necessary to meet the requirements relating to transparency vis-à-vis users, consumers and citizens, appropriate measures and safeguards may be adopted to make the employee concerned directly or indirectly identifiable. [EM: To that end, one may also relate – if appropriate - on an identification code allocated to and displayed by the employee or another personal reference.]

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 processed in particular cases**,** where it is indispensable for the recruitment or to fulfil legal obligations related to the contract of employment, 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 processed with the express consent of the employees and provided it is in the employee's interest.
[EM : also covers pension systems / sickness insurance schemes negotiated by employers/ trade unions]

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

a. to determine their suitability for the present or future employment;

b. to fulfil the requirements of preventive medicine;

c. to allow social benefits to be granted**;** or [EM: explain social benefits]

d. to satisfy judicial procedures.

In principle, it should be prohibited to collect and process genetic data, in particular to determine the professional suitability of employees or job applicants, even with the consent of the person concerned. Provision may be made for exceptions only within the limits laid down by domestic law and where there are appropriate safeguards, which should also provide for the prior involvement of the supervisory authorities, for the sole purpose of adopting, at the request of the employee, the measures necessary with regard to his or her health, safety or working conditions.
[EM: according to Recommendation(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]

10.3. Health data and - where their processing is lawful - genetic data, may not be collected from sources other than the employee concerned except with his or her express consent or in accordance with provisions of domestic law.

10.4. Health data covered by medical secrecy and - where their processing is lawful - genetic data, should only be processed by personnel who are bound by 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 and - where their processing is lawful - genetic data, should be stored separately 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 or her health data and genetic 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 through a medical practitioner of his or her choice.

10.7. The employer should process any health data relating to third parties in so far as is necessary to discharge obligations laid down by law or collective agreements, while maintaining the safeguards relating to the health data of employees. [EM : examples of processing health data relating to third parties such as family members of the employee in order to attribute specific benefits to them].

11. *Transparency of processing*

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 or her representatives, or brought to his or her notice through other appropriate means.

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

In this context, 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 indirectly by the employer, and of their possible use. 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 any system administrators in relation to data processing.

11.2. The information should also refer to the rights of the employee in regard to his or her data, as provided for in principle 12 of this recommendation, as well as the ways and means of exercising his or her rights.

11.3 The information referred to in the preceding paragraph should be provided and updated in due time and, in any event, before the employee carries out the activity or action concerned, and made readily available also through the information systems normally used by the employee.
[EM: illustrate possible “activity or action concerned”]

12. *Right of access and rectification*

12.1. Each employee should, on request, be enabled to have access to all personal data held by the employer which concern him or her 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 particular where it is incorrect. Each 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 as to the knowledge of the logic involved in any automated process concerning him or her.

To that end, in particular in large-scale or territorially extensive places of work, the employer should introduce general preventative procedures to ensure that there is an adequate and prompt response where the rights are exercised.
[EM: general policy will explain how covered processing – surveillance could happen.]

12.2 The right of access should also be guaranteed in respect of evaluation data, including where they relate to assessments of the productivity or capability of the employee provided for in principle 5.3, at least when the assessment process has been completed, without prejudice to the right of defence of employers or third parties involved; although they cannot be directly rectified by the employee, purely subjective assessments should be open to challenge in the manner laid down in domestic law. [EM: postponement for defence purpose on temporary basis.]

12.3. 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. However, internal investigations should not be carried out on the basis of an anonymous report, except where it is circumstantiated and relates to serious infringements which should be identified by domestic law or a decision of the supervisory authority. [EM: communication of the results of the

internal investigation to a third party – reference to principle 9.2's requirements to develop the notions of "circumstantiated / serious infringements" and refer to WP 29's opinion 1/2006 on the application of EU data protection rules to internal whistle blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime].

12.4. 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.

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

12.6. 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, which are updated as new technologies are developed, designed to ensure the security and confidentiality of personal data stored for employment purposes against unauthorised access, use, communication or alteration. [EM: employers should be given time to adapt to new technologies / connected to principle 2.3. and possible reference to Article 17.3 Directive 95/46 EC on 'processor']

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 person concerned should be informed in due time and 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.

14.4 Personal data processed for the purpose of an internal investigation carried out by the employer which has not led to the adoption of negative measures in relation to any employee should in principle be deleted in due time, without prejudice to the right of access up to the time at which they are deleted.