COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 30 October 2012 T-PD(2012)12_en

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

(T-PD)

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

INDEX

DRAFT RECOMMENDATION CM/REC(2012)… 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 … 2012
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 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 with regard to the processing of their 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 (hereunder referred to as "Convention 108") and of its Additional Protocol regarding Supervisory Authorities and Transborder Data Flows of 8 November 2001, and the desirability of translating their principles 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;

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;

Recalling the European Social Charter (CETS No.: 163), as revised on 3 May 1996, 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 (89)2, are reflected in the application of domestic legislation on data protection to the employment sector,

- 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

[Part I – General principles]

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.

Non-automated processing of personal data should not be used by employers in order to jeopardise the principles contained in this recommendation.

1.2. Unless provisions of domestic law provides otherwise, 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.

1.3. For the purposes of this recommendation:

- 'Personal data' means any information relating to an identified or identifiable individual ("data subject");

- 'Data processing' means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of data, or the carrying out of logical and/or arithmetical operations on data; where no automated processing is used, data processing means the operations carried out within a structured set established according to any criteria which allows search of personal data;

- ‘Controller’ means the natural or legal person, public authority, agency or any other body which alone or jointly with others has the decision-making power with respect to data processing;

- ‘Recipient’ means a natural or legal person, public authority, service or any other body to whom data are disclosed or made available, including when a transfer of data abroad is made through a service provider;

- ‘Sensitive data’ means personal data relating to racial origin, political opinions, trade-union membership, religious or other beliefs, biometric information, as well as genetic data, data related to health or sexual life, data related to criminal offences or convictions, or security measures [and other data defined as sensitive by domestic law], whose processing presents a serious risk to the interests, rights and fundamental freedoms of the data subject;

- ‘Information systems’ means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purpose of their operation, use, protection or maintenance;

- ‘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;

- ‘Employer’ means any natural or legal person who has an employment relationship with the worker and has the responsibility for the undertaking and/or establishment;

- ‘Employee’ means any person employed by the employer according to an employment relationship;

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

Respect for the protection of personal data, contributing to the respect of human dignity as well as rights and fundamental freedoms, and in particular the right to privacy, 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. By using information systems and technologies for the collection and processing of personal data in the framework of employment purposes, the employer shall be encouraged to monitor the implementation of security principles so as to prevent or at least minimise the risk of interference with the rights and fundamental freedoms of the persons concerned. The fundamental principles of Convention 108 are fully applicable to the processing of personal data using information systems and technologies. These fundamental principles include the quality of data (Article 5), the prohibition of the processing of sensitive data (Article 6), data security (Article 7) and the safeguards afforded to data subjects (Article 8).The same applies when they are used and implemented in the working environment.

3.2. The employer should be invited to 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. *Collection of data*

4.1. Employers should be encouraged in principle to collect personal data 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.

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

[In the course of recruitment, personal data should be obtained solely from the individual concerned.] An employer should not persuade the person concerned to grant access to private information or to enable access to any medical information held by third parties.

In any event, the employer is invited to take appropriate measures 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. Moreover, the data subject concerned should be informed, and, as the case may be, their consent may be required.

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 principles 4, and from principle 14 to 20 and if the storage is intended to serve employment purposes. Where this is not the case, the employer should refrain from using or from collecting or/and using such data.

5.2. The same applies in respect of social data, which shall be collected only for specified purposes and be accessible for specific persons only.

5.3. According to the Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling adopted on 23 November 2010, whose principles are fully applicable here, personal data used in the context of profiling should only be stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are collected and processed. The collection and processing of personal data in the context of profiling of persons who cannot express on their own behalf their free, specific and informed consent should be forbidden, except when this is

in the legitimate interest of the data subject or if there is an overriding public interest, on the conditions that appropriate safeguards are provided for by law.

5.4. Where judgmental data are stored relating to the performance or potential of individual employees, such data should only be based on the purpose of assessing professional skills. These data should be based on fair and honest evaluations and should be relevant, adequate and non-excessive. The collection of data and information relating to the privacy of employees should be therefore prohibited.

6. *Internal use of data*

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

6.2. Where data are to be processed or interconnected for employment purposes other than the one for which they were originally collected, the employer should be encouraged to take adequate measures 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.

6.3. Without prejudice to principle 8, 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.

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

7.1. 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.

7.2. Employers should be invited to consider the use of information systems and technologies for trade union communications as a subject-matter of appropriate agreements designed to lay down in advance transparent rules permitting correct use and to identify safeguards to protect any confidential communications.

8. *External communication and dissemination 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 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.

8.3. 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.

8.4. With regard to the public sector, domestic legislation providing for disclosure of personal data in order to ensure transparency or monitoring of the correct use of public resources and funds should provide for appropriate safeguards for individuals' right to privacy and protection of personal data, in particular by ensuring full respect for the principle of purpose specification and avoiding the disclosure of irrelevant personal data. The law should also reconcile the right to privacy and the protection of personal data with the requirements relating to the security of State, the fight against crime, namely corruption and other public interests protected by law.

9. *Sensitive data*

9.1 Personal data referred to in Article 6 of Convention 108 whose processing shall in principle be prohibited, may nevertheless be processed, as in particular cases, where it is indispensable for the recruitment or to fulfil legal obligations related to the contract of employment, under the condition that the applicable law provides additional appropriate safeguards.

9.2. 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

d. to satisfy judicial procedures.

In principle, the processing of genetic data, in particular to determine the professional suitability of employees or job applicants, even with the consent of the person concerned, is prohibited. Provision may be made for exceptions only where applicable law provides for additional 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, or to third parties' health and safety or working conditions.

9.3. 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.

9.4. 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.

9.5. 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.

9.6. 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.

9.7. 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.

10. *Transparency of processing*

10.1. Employees should be provided with information concerning his or her personal data held by the employer, directly or through the intermediary of his or her representatives.

Apart from information concerning at least his or her identity and habitual residence or establishment, this information should specify the purposes of the processing of data carried out by the data controller, that is to say the employer, the data processed, the recipients or categories of recipients of the personal data and the means of exercising the rights set out in Article 8 of Convention 108, as well as any other information necessary to ensure fair and lawful data processing.

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. Specific and clear information should be provided with regard to the particular forms of processing of employee's personal data provided for by Part II of this Appendix.

10.2. The information should also refer to the rights of the employee in regard to his or her data, as provided for in principle 11 of this recommendation, as well as the ways and means of exercising his or her rights.

10.3 The information 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.

11. *Right of access and rectification*

11.1. Each employee shall be entitled not to be subject to a decision significantly affecting him or her, based solely on an automatic processing of data without having his or her views taken into consideration.

11.2. Moreover, he or she should obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all information on

their origin as well as any other information that the controller is required to provide to ensure the transparency of processing. Each employee should also obtain, on request, knowledge of the reasoning underlying the data processing, the results of which are applied to him or her and, as the case may be, rectification or erasure of such data if they have been processed contrary to the law or the principles set out in this recommendation, in particular where it is incorrect.

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.

11.3. 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.

11.4. Derogations to the rights referred to in paragraph 11.1 and 11.2 can occur when they are provided for by an accessible and foreseeable law and constitutes a necessary measure in a democratic society, as referred to in Article 9 of Convention 108, to protect State security, public safety, important economic and financial interests of the State or the prevention and suppression of criminal offences, the data subject or the rights and freedoms of others, notably freedom of expression. In this respect, according to the Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling adopted on 23 November 2010, "where it is necessary in a democratic society for reasons of state security, public safety, the monetary interests of the state or the prevention and suppression of criminal offences, or protecting the data subject or the rights and freedoms of others, member states need to apply the provisions set out in Sections 3, 4 and 5 (conditions for the processing of personal data in the context of profiling, information and rights of data subjects) of the present recommendation, where this is provided for in law".

11.5. Furthermore, the exercise of these rights 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.

11.6. Unless provisions of domestic law provide otherwise, 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.

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

12. *Security of data*

12.1. Employers or firms which may process data on their behalf should be invited to 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 accidental or unauthorised modification, loss or

destruction of personal data, as well as against unauthorised access, dissemination or divulgation of such data.

12.2. 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.

13. *Preservation of data*

13.1. 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.

13.2. 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.

13.3. 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 the shortest possible period.

13.4 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 must in principle be deleted in due time, without prejudice to the right of access up to the time at which they are deleted.

[Part II - Particular forms of processing]

14. *Information systems and technologies for the processing of employees' personal data and the monitoring of employees, including video surveillance*

The introduction and use of information systems and technologies for the direct and principal purpose of remotely monitoring employees' activity, behaviour or localisation relating to the production, the safety or the work organisation of the establishment should not in principle be permitted when leading to a permanent [or should not aim at deliberately and systematically] monitoring [of] a specific employee, or a specific group of employees, except where no alternative means which are less intrusive are available, [and when a prior authorisation from a national supervisory authority has been delivered.] Employees or their representatives, in accordance with domestic law or practice and, where appropriate, with the relevant collective agreements, should be informed or consulted before the introduction or adaptation of a video surveillance system. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, their agreement should be sought. In the event of a lawsuit or counterclaim, employees should be able to ground them on the recording made.

15. Whistleblowing devices

Whistleblowing devices can also have an impact on the rights and fundamental freedoms of the persons concerned. These devices, which can enable employees of an undertaking to alert the public about financial problems, or with regard to corruption or competition, are in

general dealt with specifically. The scope of these devices shall be restricted, shall not be of a general nature and shall not target the respect of all of the legislative or regulatory provisions, or internal rules established by the establishment. When serious facts occur, outside of the restricted scope, the whistleblowing shall immediately be redirected to the responsible person, as the case may be the financial director or the human resources director.

16. Use of Internet and e-mails in the workplace

16.1 With regard to possible processing of personal data relating to the use of Internet or Intranet, employers should be encouraged to prevent unjustifiable interferences with individuals' right to private life and to the protection of personal data should be prevented.

The persons concerned should be properly and periodically informed, in conformity with principle 10, in particular when disciplinary measures are envisaged on the basis of compiled monitoring files. The information given shall cover the purpose of the system [or operation], the preservation or back-up period of connection data. This information shall also cover the archiving of electronic messages.

16.2 In particular, in respect of the possible processing of personal data relating to Internet or Intranet pages viewed by the employee, preference should be given to the adoption of preventive measures, such as the use of filters which prevent particular operations, and to 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. The persons concerned should be periodically informed, in conformity with principle 10 and more generally, employees must have been previously informed of the company or institution's policy of conducting such monitoring activity.

16.3 Access to professional emails of employees who have been informed of the existence of that possibility can only occur where in accordance with the law and strictly necessary for security or operational reasons. The employer should be invited to avoid any kind of unjustified access to e-mails sent or received by the employee. The employer should be encouraged to 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, in the least intrusive way possible and after having informed the employee.

17. Equipment revealing employees' whereabouts

While devices revealing whereabouts can be used in the interests of the employees (for instance to enable the determination of an occupational injury), their use shall not lead to a permanent monitoring of employees. Given the risks of infringement to the rights and freedoms of persons presented by the use of these devices, the employer should be invited to take all the necessary guarantees. He shall in particular pay special attention to the purpose for which such devices are used.

If, in virtue of the characteristics of the professional activity, the employee, by instructions or with the knowledge and approval of the employer, is to use professional equipment outside the company or institution facilities, and in virtue of that use the employer acquire knowledge of the employee's whereabouts, the collection and further processing of personal data resulting from that knowledge must be exclusively limited to the strict verification of the fulfilment of professional duties or organisational aspects.

The employer shall take appropriate internal procedures relating to the processing of that data and shall notify it to the persons concerned in advance. The prior consultation of representative bodies should be ensured.

18. Biometric data

The access to such data shall be subject to requirements of security and proportionality. In this regard, careful consideration should be given to the implications of storage in a central database or alternative systems based on media made available solely to the person concerned.

The collection and further processing of biometric data should only be done when necessary to protect the legitimate interests of the employer, employees or third parties, should be accompanied by appropriate safeguards, in particular with regard to the security of data and should comply with health and hygiene rules. Employees must have been previously informed of the company/institutional policy regarding the collection and further processing of such data.

No collection and further processing of biometric data should be done without previous authorisation of national supervisory authorities.

19. Psychological tests, analyses and similar procedures

Recourse to tests, analyses and similar procedures performed by specialised professionals and designed to assess the character or personality of the individual should only be done when strictly necessary and should not take place without his or her consent, unless domestic law provides other appropriate safeguards. 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. These procedures may be supervised by national supervisory authorities.

20. Other processing posing specific risks to employees' rights

The employer should carry out a risk analysis of the potential impact of the intended data processing on the rights and fundamental freedoms of the persons concerned, and in particular their right to privacy, human dignity and protection of personal data, and to process such data in the less possible intrusive manner. 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 14.2 reveals such risks unless domestic law or practice provides other appropriate safeguards.