Strasbourg, 15 April 2014 T-PD(2013)05rev_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(2013)… 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 … 2014 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 designed to minimise any risks that such methods might pose to employees' rights and fundamental freedoms, in particular their right to privacy;

Bearing in mind 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 articulating the application to the employment sector;

Recognising also that there are other interests (individual or collective, private or public) to be borne in mind when articulating principles for the employment;

Considering that personal data in official documents held by a public authority or a public body may be disclosed by the authority or body in accordance with domestic law to which the public authority or body is subject, in order to reconcile access to such official documents with the right to the protection of personal data pursuant to this Recommendation;

Aware of the different traditions which exist in member states with respect to the regulation of different aspects of employer-employee relations, and noting that law is only one of the means to regulate such relations;

Aware of the changes which have occurred internationally in the employment sector and related activities; notably due to the increased use of information and communication technologies (ICTs) and the globalisation of employment and services;

Considering that, in light of such changes Recommendation No. 89 (2) on the protection of personal data used for employment purposes should be revised so that it continues to provide an adequate level of protection for individuals in the employment sector;

Recalling that Article 8 of the European Convention on Human Rights protects the right to private life, including activities of a professional or business nature, as interpreted by the European Court of Human Rights;

Recalling the applicability of the existing principles set out in other relevant recommendations of the Council of Europe, in particular 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, Recommendation R(97)5 on

the protection of medical data and Recommendation R(92)3 on genetic testing and screening for health care purposes;

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 especially relevant;

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;

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, 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 of this Recommendation by means of complementary instruments such as, codes of conducts, to ensure that the principles are well known, understood and applied by all employment sector participants, including representative bodies of both employers and employees, and taken into account in the design, deployment and use of ICTs in the employment sector.

## Appendix to the Recommendation

## Part I – General principles

### *1. Scope*

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

1.2. Unless domestic law provides otherwise, the principles of this recommendation also apply to the activities of employment agencies, whether in the public or private sector, which process personal data so as to enable one or more concurrent contracts of employment, including part-time contracts, to be established between individuals concerned and prospective employers, or to help employers discharge their duties relating to those contracts.

### *1bis. Definitions*

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, interconnection, 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; where no automated processing is used, data processing means the operations carried out within a structured set established according to any criteria which allow to search for personal data ;

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

- ‘Processor’ means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller;

- ‘Recipient’ means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

- ‘sensitive data’ covers genetic data, personal data concerning offences, criminal convictions and related security measures, biometric data uniquely identifying a person, as well as personal data for the information they reveal relating to racial origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life;

- ‘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’ concern the relations between employers and employees which relate to recruitment and end of employees’ labour affiliation, 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. The consequences of the contractual relationship may extend beyond the term of the contract of employment;

- Employer’ means any natural or legal person, public authority or agency who has an employment relationship with an employee or a prospective employee and has the legal responsibility for the undertaking and/or establishment;

- ‘Employee’ or ‘prospective employee’ means any person concerned engaged by an employer under an employment relationship.

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

Respect for human dignity, privacy and the protection of personal data should be safeguarded in the processing of personal data for employment purposes, notably to allow free development of employees’ personality and to foster possibilities of individual and social relationship on the workplace.

### *3. Application of data processing principles*

[3.1. Employers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned and should anonymise data where relevant in line with additional conditions and safeguards set out in domestic law, or pseudonymise data where anonymisation is not possible.]

3.2. Employers should develop appropriate measures, to ensure that they respect in practice the principles and obligations relating to data processing for employment purposes. At the request of the supervisory authority, employers should also be able to demonstrate their compliance with such principles and obligations. These measures should be adapted to the volume and nature of the data processed, the type of the activities being undertaken, and should also take into account possible implications on employees' fundamental rights and freedoms of the data subjects.

### *4. Collection of data*

4.1. Employers should collect personal data directly from the data subject concerned. When it is necessary, lawful, fair and appropriate to process data collected from third parties, for example to obtain professional references, the data subject should be duly informed.

4.2. Personal data collected for employment purposes should be relevant and not excessive, having regard to the nature of the employment as well as the legitimate needs of the employer in connection with its activities and where relevant, in line with additional conditions and safeguards set out in domestic law.

4.3. Employers should not have access to personal data that the employee shares with others where these data are not necessary for the assessment of the employ's ability to carry out his/ her duties.

4.4. Employers should take appropriate measures to ensure that, in particular for online data publicly available, only relevant, accurate and up-to-date data are processed, thus avoiding data to be used in a different context for which they were originally disclosed.

4.5. Health data may only be collected for the purposes set out in principle 9.2 of this Recommendation.

### *[5. Storage of data*

5.1. The storage of personal data is permissible only if the data have been collected in accordance with the requirements outlined in principles 4, 9, 14 to 20 and if the storage is intended to serve employment purposes. Such data should be relevant, adequate, accurate and necessary.

5.2. When evaluation data are stored relating to the performance or potential of employees, such data should only be based on the purpose of assessing professional skills. ]

### *6. Internal use of data*

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

6.2. Employer should adopt data protection policies, rules and/or other instruments on internal use of personal data.

6.3. Where data are to be processed for employment purposes other than the purpose for which they were originally collected, the employer should take adequate measures to avoid misuse of the data in a different context and inform the employee.

6.4. Without prejudice to principle 8, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principles of proportionality and 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 to employee's representatives, including the use of information systems and technologies*

7.1. In accordance with domestic law and practice, or the terms of collective agreements, personal data may be communicated to employees' representatives, but only to the extent that such data are necessary to allow those representatives to properly represent the interests of the employees concerned or if necessary for the fulfilment and supervision of obligations laid down in collective agreements.

7.2. In accordance with domestic law and practice, the use of information systems and technologies for the communication of data to employees' representatives should be subject to appropriate agreements that set out, in advance, transparent rules prescribing their use and safeguards to protect confidential communications.

### *8. External communication of data*

8.1. Personal data collected for employment purposes should only be communicated to public bodies acting in their official functions, and for the purposes of carrying them out, and only within the limits of employer's legal obligations or in accordance with other provisions of domestic law.

8.2. The communication of personal data to public bodies for other purposes or to other parties, including entities in the same group, should only take place:

a. where in line with additional conditions and safeguards set out in domestic law, the communication is necessary for employment purpose, the purposes are not incompatible with the purposes for which the data was originally collected and the employees concerned or their representatives, as the case may be, are informed of this; or

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

c. if the communication is provided for by domestic law.

8.3. The communication of personal data among a group of companies is lawful only if it is necessary for the purpose of discharging legal obligations or collective agreements and where additional conditions and safeguards are provided for by domestic law. The consent of the employee may also be required in appropriate cases as additional safeguard.

8.4. With regard to the public sector, for the provisions governing the disclosure of personal data to ensure government and other public authority/ body transparency and/or to monitor the correct use of public resources and funds should provide appropriate safeguards for individuals' right to privacy and protection of personal data.

### *9. Processing of sensitive data*

9.1 The processing of sensitive data referred to in Principle 1bis of this Recommendation is only permitted in particular cases, where it is indispensable for the specific employment recruitment or to fulfil legal obligations related to the employment contract of employment. The processing is also conditional on the applicable law providing additional appropriate safeguards, complementing those set out in Convention 108 and in this Recommendation. Appropriate safeguards shall aim at preventing the risks that the processing of such sensitive data may present to the interests, rights and fundamental freedoms of the employee concerned, notably a risk of discrimination. Processing of biometric data is possible under conditions provided in Principle 18 of this Recommendation.

9.2. In accordance with domestic law, an employee or job applicant may only be asked questions concerning his or her state of health and/or be medically examined:

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

b. to fulfil the requirements of preventive medicine;

c. to guarantee an appropriate rehabilitation or in any other way comply with work environment requirements;

d. to safeguard vital interests of the data subject or other employees and individuals;

e. to allow social benefits to be granted; or

f. to satisfy judicial procedures.

The processing of genetic data, to determine for instance the professional suitability of employees or job applicants, is prohibited even with the consent of the person concerned.
Processing of genetic data may exceptionally be provided if it is provided by domestic law and subject to appropriate safeguards, in particular to avoid any serious prejudice to the health of the data subject or third parties.

9.3. Health data and - where their processing is lawful - genetic data should only be collected from the employee concerned except if otherwise determined by law, with appropriate safeguards.

9.4. Health data covered by the obligation of medical confidentiality should only be accessible to and processed by personnel who are bound by medical confidentiality or other rules of professional secrecy. Such data must:

a. relate directly to the ability of the employee concerned to exercise his or her duties, or
b. be necessary in support of measures to protect the employee's health or
c. be necessary to prevent risks to others.

Where such data are communicated to the employer, this processing should be performed by a person duly authorised, such as personnel entitled with administration, health and safety at work and the information should only be communicated if it is indispensable for decision making by the personnel administration and in accordance with provisions of domestic law.

9.5. Health data covered by medical confidentiality and - where their processing is lawful - genetic data, where appropriate should be stored separately from other categories of personal data held by the employer. Technical and organisational security measures should

be taken to prevent persons outside the authorised medical service having access to the data.

9.6. The employee'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 employee. Any such restriction must be in accordance with domestic law. The data may thus be communicated to the employee through a medical practitioner of his or her choice.

9.7. In any circumstances health data related to third parties will not be processed unless full unambiguous informed consent is given, such collection is authorised by a data protection supervisory authority, or the collection is mandatory according to domestic law.

### *10. Transparency of processing*

10.1. Employees should be able to obtain information concerning their personal data held by the employer. This information can be provided directly or via their representative.

Except in relation to employees' name and habitual residence or establishment, employers should provide employees with the following information:

- a full list of the personal data to be processed and a description of the purposes of processing
- the recipients, or categories of recipients of the personal data
- the means the employees have of exercising the rights set out in in paragraph 11 of this recommendation, without prejudice to more favourable ones provided by domestic law or in their legal system
- any other information necessary to ensure fair and lawful processing.

In this context, a particularly clear and complete description must be provided of the type of personal data that can be collected by ICTs, including video-surveillance and their possible use. This principle also applies to the particular forms of processing provided for by Part II of this recommendation.

10.2 The information should be provided in an accessible format and kept up to date. In any event, such information should be provided before an 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, rectification and to object*

11.1. Employees should be able to obtain, upon request, at reasonable intervals and without excessive delay, confirmation of the processing of personal data relating to him or her. The communication should be in an intelligible form, include all information on the origin of the data, as well as any other information that the controller is required to provide to ensure the transparency of processing, notably information provided in principle 10.

11.2. Employees should be entitled to have personal data rectified or erased, if they are inaccurate and/or if the data have been processed contrary to the law or the principles set out in this recommendation. They should also be entitled to object at any time to the processing of personal data concerning him/her unless the processing is necessary for employment purposes or otherwise provided by law.

11.3. The right of access should also be guaranteed in respect of evaluation data, including where such data relate to assessments of the performance, productivity or capability of the employee, at least when the assessment process has been completed, without prejudice to

the right of defence of employers or third parties involved. Although such data cannot be directly corrected by the employee, purely subjective assessments should be open to challenge in the manner laid down in domestic law.

11.4. Employees should not 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.

11.5. An employee should also be able to obtain, upon request, knowledge of the reasoning underlying the data processing, the results of which are applied to him/her.

11.6. Derogations to the rights referred to in paragraph 10, 11.1, 11.3 and 11.4 are permitted when they are provided for by law and constitute a necessary measure in a democratic society, to protect State security, public safety, important economic and financial interests of the State or the prevention and suppression of criminal offences, the protection of the data subject or the rights and freedoms of others.

11.7. Furthermore, the exercise of these rights may, in the case of an internal investigation conducted by the employer, be deferred until the closing of the investigation if the exercise of those rights would undermine/threaten the investigation.

11.8. Unless provisions of domestic law provide otherwise, an employee should be entitled to choose and designate a person to assist him or her in the exercise of his or her right of access, rectification and to object or to exercise these rights on his or her behalf.

11.9. Domestic law should provide a remedy where access to data is refused, or requests for rectification or erasure of any of the data is denied.

### *12. Security of data*

12.1. Employers or entities, which may process data on their behalf, should implement adequate technical and organisational measures in response to periodic reviews of the organisation's risk assessment and security policies, updated as appropriate. Such measures should be 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 disclosure of such data.

12.2 Employers shall ensure adequate data security when using ICTs for the processing of employees' personal data for employment purposes.

12.3. 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 retained by an employer for a period longer than is justified by the purposes outlined in Principle 1.3 or is required by 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.

Where such data are stored with a view to a further job opportunity, the person concerned should be informed in due time and his or her data should be deleted if requested by the person.

Where it is required to store data submitted for a job application for the purpose of bringing or defending legal actions or any other legitimate purpose, the data should be stored only for the period necessary for the fulfilment of the purpose.

13.3 Personal data processed for the purpose of an internal investigation carried out by an employer which has not led to the adoption of negative measures in relation to any employee should be deleted after a reasonable period, without prejudice to the employee's 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 monitoring of employees, including video surveillance*

14.1 The introduction and use of ICTs for monitoring employees should be done with respect of the principles of legitimacy, relevance and proportionality, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards. Employers should strike a fair balance, between the employees' right to respect for private life and the employer's interest in the protection of his property rights.

14.2. The use of such systems for the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted where it leads to the deliberate and systematic surveillance of a specific employee, or a specific group of employees. Exceptions may be considered, with due safeguards, when monitoring is not the main purpose pursued by the employer but is just an indirect consequence of a surveillance needed to protect production, health, safety or work organisations. The use of video surveillance for monitoring occurrences at locations that are part of the most personal area of life of an employee is not permitted.

14.3 In the event of dispute or legal proceedings, employees should be able to obtain copies of the recording made.

### *15. Internal reporting mechanism*

Where employers are obliged by law or internal rules to implement internal reporting mechanisms, such as hotlines, employers should secure protection of personal data of all parties involved. In particular, employers should ensure the confidentiality of the employee who reports on illegal or unethical conduct (e.g. a whistleblower). Personal data of the parties involved should be used solely for the purpose of appropriate internal procedures relating to the report, law or judicial order.

Where applicable, employers should enable anonymous reporting. However, internal investigations should not be carried out on the sole basis of an anonymous report, except where it is circumstantiated and relates to serious domestic law infringements.

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

16.1 The employer should avoid unjustifiable and unreasonable interferences with employee's right to private life. This principle extends to all technical devices and ICTs used by an employee. The persons concerned should be properly and periodically informed,

through a clear privacy policy, in accordance with principle 10 of the recommendation. The information provided should be kept up to date and should include the purpose of the processing, the preservation or back-up period of traffic data and the archiving of electronic messages.

16.2 In particular, in respect of the possible processing of personal data relating to Internet or Intranet pages accessed 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.

16.3 Access to professional emails of employees who have been informed in advance of the existence of that possibility can only occur [in accordance with the law and] where necessary for security or other lawful reason. In case of absent employees, the employer should take the necessary measures and foresee the appropriate procedures aimed at enabling, access to professional emails only when such access is of professional necessity. Further access must be undertaken in the least intrusive way possible and only after having informed the employees concerned.

16.4 In any case, the content, sending and receiving of private emails at work shall not be monitored.

16.5 When an employee leaves the organisation, the employer should take the necessary organisational and technical measures to automatically deactivate the employee's account upon his or her departure. If the employer needs to recover the contents of the employee's account for the efficient running of the company, he shall do so before the departure of the employee and when feasible, at his or her presence.

### *17. Equipment revealing employees' whereabouts*

17.1 While devices revealing the location of employees 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 or excessive monitoring of employees. Given the potential to violate the rights and freedoms of persons presented by the use of these devices, employers should ensure all necessary safeguards for the employee's right to privacy and protection of personal data. Employers shall in particular pay special attention to the purpose for which such devices are used. Notably, monitoring should not be the main purpose, but only an indirect consequence of action needed to protect production, safety or work organisations.

17.2 When an employee, following his or her employer's instructions or with the knowledge and approval of his or her employer, uses professional devices outside the company or institution premises, and by virtue of that use the employer acquire knowledge of the employee's location, the collection and further processing of that personal data must be exclusively limited to the strict verification of the fulfilment of professional duties or organisational aspects.

17.3 Employers shall apply appropriate internal procedures relating to the processing of these data and shall notify it to the persons concerned in advance.

### *18. Biometric data*

18.1 The collection and further processing of biometric data should only be undertaken when it is necessary to protect the legitimate interests of the employer, employees or third parties, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards.

18.2 The processing of biometric data should be based on scientifically recognised methods and shall be subject to the requirements of strict security and proportionality. The employee should be in control of the processing of his/ her biometric data.

### *19. Psychological tests, analysis and similar procedures*

19.1 Recourse to tests, analysis and similar procedures performed by specialised professionals, subject to professional confidentiality that are designed to assess the character or personality of an employee or job applicant should only be allowed if legitimate and necessary for the type of activity performed in the job.

19.2 These tests, analysis and similar procedures should not take place without the employees or job applicants consent, and domestic law should provide appropriate safeguards. The employee's consent should be free, informed and without any financial or other compensation foreseen. The employee or job applicant 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.

### *20. Other processing posing specific risks to employees' rights*

20.1 Employer or where applicable processors, should carry out a risk analysis of the potential impact of the intended data processing on the employee's rights and fundamental freedoms and design data processing operations in such a way as to prevent or at least minimise the risk of interference with those rights and fundamental freedoms.

20.2 Unless domestic law or practice provides other appropriate safeguards, the agreement of employees' representatives should be sought before the introduction or adaptation of ICTs where the information or consultation procedure referred to in principle 14 reveals such risks.

### *21. Additional safeguards*

For all particular forms of processing, set out in Part II of this Recommendation, the employer should ensure that appropriate measures are taken to secure the respect of the following safeguards:

- Inform the employees before the use of any surveillance/ monitoring system. The information provided should be kept up to date and should be undertaken taking into account principle 10 of the Recommendation. The information should include the purpose of the operation, the preservation or back-up period, as well as the existence or not of the rights of access and rectification and how those rights may be exercised.

- Take appropriate internal procedures relating to the processing of that data and notify employees in advance.

- Before any monitoring can occur, or in circumstances where such monitoring may change, employees' representatives should be consulted in accordance with domestic law or practice. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, the agreement of employees' representatives should be sought.

- Consult, in accordance with domestic law the national supervisory authorities on the processing of personal data.