Strasbourg, 28 May/mai 2014

T-PD(2014)03

CONSULTATIVE COMMITTE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD)

LE COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL (T-PD)

COMPILATION OF COMMENTS ON THE DRAFT REVISED RECOMMENDATION ON THE PROTECTION OF PERSONAL DATA USED FOR EMPLOYMENT PURPOSES

* * *

COMPILATION DES COMMENTAIRES RELATIFS AU PROJET DE RECOMMANDATION REVISEE SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL UTILISEES A DES FINS D'EMPLOI

Directorate General Human Rights and Rule of Law /
Direction Générale Droits de l'homme et Etat de droit

TABLE OF CONTENTS / TABLE DES MATIERES

AUSTRIA / AUTRICHE 3

CZECH REPUBLIC / REPUBLIQUE TCHEQUE 16

ITALY / ITALIE 29

SWEDEN / SUEDE 44

SWITZERLAND / SUISSE 58

AUSTRIA / AUTRICHE

INDEX

Preamble

Appendix:

Part I – General principles

1. Scope
1bis. Definitions
2. Respect for human rights, dignity and fundamental freedoms
3. Application of data protection principles
4. Collection of data
5. Storage of data
6. Internal use of data
7. Communication of data to employee's representatives, including the use of information systems and technologies
8. External communication of data
9. Processing of sensitive data
10. Transparency of processing
11. Right of access, rectification and to object
12. Security of data
13. Preservation of data

Part II - Particular forms of processing

14. Information systems and technologies for the monitoring of employees, including video surveillance
15. Internal reporting mechanism
16. Use of Internet and e-mails in the workplace
17. Equipment revealing employees' whereabouts
18. Biometric data
19. Psychological tests, analyses and similar procedures
20. Other processing posing specific risks to employees' rights
21. Additional safeguards

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, , 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.

3.3 When using ICTs for the processing of personal data for employment purposes, employers shall ensure adequate data security safeguards.

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 for employment purposes is permissible only if the data have been collected in accordance with the requirements outlined in principles 4, 9 and 14 to 20. 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. Employers 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 such data are 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 should only be accessible to and processed by personnel who are bound by medical confidentiality or other rules of professional secrecy or confidentiality. Such data must:

Comment [SM1]: Are there any health data that are not covered by medical confidentiality?

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 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, 11.2, 11.4 and 11.5 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 duly 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, including the additional safeguards provided for in principle 21. 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 the latter, uses professional devices outside the company or institution premises, enabling the employer to 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, including the additional safeguards provided for in principle 21.

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.

Comment [SM2]: What is the meaning/additional value of this sentence?

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, including the additional safeguards provided for in principle 21. 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. Principles 11.1. and 11.2. apply correspondingly.

Comment [SM3]: It should be made clear that an individual has the right to access to the results.

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, in particular, 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.

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

INDEX

Preamble

Appendix:

Part I – General principles

1. Scope
1bis. Definitions
2. Respect for human rights, dignity and fundamental freedoms
3. Application of data protection principles
4. Collection of data
5. Storage of data
6. Internal use of data
7. Communication of data to employee's representatives, including the use of information systems and technologies
8. External communication of data
9. Processing of sensitive data
10. Transparency of processing
11. Right of access, rectification and to object
12. Security of data
13. Preservation of data

Part II - Particular forms of processing

14. Information systems and technologies for the monitoring of employees, including video surveillance
15. Internal reporting mechanism
16. Use of Internet and e-mails in the workplace
17. Equipment revealing employees' whereabouts
18. Biometric data
19. Psychological tests, analyses and similar procedures
20. Other processing posing specific risks to employees' rights
21. Additional safeguards

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.

Comment [N4]: Mention the specific, weaker, position of (prospective) employee, the question of freedom of will and the need to protect the weaker party?

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.

Comment [N5]: Data of whom? Other employers, clients? Will be better to clarify.

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 for employment purposes is permissible only if the data have been collected in accordance with the requirements outlined in principles 4, 9 and 14 to 20 and only for necessary time period. 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~~ Every substantive changes in the processing ~~occur,~~should be communicated to 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 such data are 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 in advance; 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

Comment [N6]: The original purpose of collecting data is to perform the contract. What other employment purpose is possible and this paragraph deals with?

Comment [N7]: Chance of the data controller is always substantive change. So I suggest this change.

Comment [N8]: Because of a little bit vague conditions in this part, I would be more strict.

Comment [N9]: So the consent is not the condition sine qua non but only some additional security measure? It might be understood as a degradation of consent and it may have some consequences, for example in situation when employee will not give or withdraw the consent.

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 allowed by domestic law and 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 expressly 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 or confidentiality. 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 and the conditions of the processing. 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, blocked 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~~ processed 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 and of the need to maintain confidentiality about the measures as well.

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 in any situation.

14.3 In the event of dispute or legal proceedings, employees should be able to obtain copies of the recording made with respect to protection of other employees' privacy.

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 duly 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 about the possibility of use employer's ICT equipments for private purposes and about monitoring of it´s use. 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 otherwise 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, including the additional safeguards provided for in principle 21. 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 the latter, uses professional devices outside the company or institution premises,

enabling the employer to 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, including the additional safeguards provided for in principle 21.

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, including the additional safeguards provided for in principle 21. 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, in particular, 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.

ITALY / ITALIE

INDEX

PREAMBLE

APPENDIX :

Part I – General principles

1. Scope

1bis. Definitions

2. Respect for human rights, dignity and fundamental freedoms

3. Application of data protection principles

4. Collection of data

5. Storage of data

6. Internal use of data

7. Communication of data to employee's representatives, including the use of information systems and technologies

8. External communication of data

9. Processing of sensitive data

10. Transparency of processing

11. Right of access, rectification and to object

12. Security of data

13. Preservation of data

Part II - Particular forms of processing

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

15. Internal reporting mechanism

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

17. Equipment revealing employees' whereabouts

18. Biometric data

19. Psychological tests, analyses and similar procedures
20. Other processing posing specific risks to employees' rights
21. Additional safeguards

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

Comment [IT10]: General comment. In some cases the long process of revision we have been working on has led to an excessively complex wording, sometimes amending the original version when it was probably not really needed. In those cases we have suggested to compare the original and the current texts in order to re-assess the relevance and appropriateness of the proposed amendments, possibly deleting those which are not entirely motivated and going back to the initial text where more clear and balanced.

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;

Comment [DPA11]: We wonder whether it is appropriate to state definitions that are not specific of the employment sector and that are still under discussion within the CAHDATA. Moreover, what would be the value of a definition in a Recommendation that may be not in line with the future Convention 108?

- 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.

Comment [IT12]: We would suggest to simply say that "Employers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned" for two main reasons.
Firstly, we are not sure we understand here the expression" where relevant in line with additional conditions and safeguards set out in domestic law". Moreover, we may not want to give the impression that pseudonymisation can be put on the same level as anonymisation as part of the minimisation principle. As stated in the WP29 Opinion 5/2014 pseudonymisation is not a method of anonymisation. It merely reduces the linkability of a dataset with the original identity of a data subject, and is accordingly a useful security measure.

Comment [DPA13]: We think that we have lost the idea of simplification which was at the basis of the original proposal, namely that simplified solutions should be found for small scale working environments.

Comment [DPA14]: This is probably too heavy. Was it that necessary to amend the original text of Rec (89)2?
"Personal data should in principle be obtained from the individual employee. The individual concerned should be informed when it is appropriate to consult sources outside the employment relationship"

Comment [DPA15]: The sentence is not clear, in this case too we may consider the possibility to go back to the original version of Rec (89)2 which appeared more balanced.
"Personal data collected for employment purposes should be relevant and not excessive, bearing in mind the type of the employment as well as the evolving information needs of the employer"

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 for employment purposes is permissible only if the data have been collected in accordance with the requirements outlined in principles 4, 9 and 14 to 20. 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 in compliance with the principles of this Recommendation.

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 such data are necessary for the fulfilment and supervision of obligations laid down in collective agreements.

Comment [IT16]: The sentence has some ambiguities. We assume that this principle refers to social networking. The practice carried out by employers to ask the employees/prospective employees the credentials for accessing their profiles on social networking has been banned by some national legislations with a specific prohibition. Can we imagine a similar principle in this Recommendation? (Something as: "Employers should refrain from asking employees/prospective employees for access to information stored on social media or other online site").

Comment [IT17]: Compared to the original version the following sentence was deleted: "Where important decisions affecting the employee are to be taken, based on the processed data, he/she should be informed". Is this appropriate?

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 and informed consent of the individual employee; or

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

Comment [IT18]: Is this necessary? (It was not in the original version).

Comment [IT19]: It was in the original text, why should we delete this?

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, 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 within the limits laid down by domestic law and in accordance with 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.

Comment [DPA20]: See the comment regarding Article 1 bis.

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.

Comment [DPA21]: The original version was probably clearer. " Health data [and genetic data"]) may not be collected from sources other than the employee concerned except with his/her express and informed consent or in accordance with domestic law"

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

Comment [DPA22]: Should we extend this principle also to genetic data (where the processing is lawful) as in para 9.3?

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.

Comment [DPA23]: Do these three hypothesis (a,b,c) cover all the processing of health data indispensable for the specific employment recruitment or to fulfil legal obligations related to the employment contract of employment?
Aren't the principles stated in the first and second paragraph of this Article sufficient to ensure that the processing does not go beyond the legitimate purpose?

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.

Comment [IT24]: Is this paragraph necessary? Isn't it unlikely/paternalistic that the employer can be requested to judge the seriousness of the harm to the employee?

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.

Comment [DPA25]: The way it is drafted now seems to refer to the right to access (which is covered by Article 11) rather than the duty for the controller to give notice regarding the processing. The original version was more appropriate. "Information concerning personal data held by the employer should be made available either to the employee concerned directly or through the intermediary of his representatives or brought to his notice through other appropriate means".

Comment [IT26]: This wording is not very clear. We may want to put this provision in line with the text of the modernised Convention.

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.

Comment [IT27]: See article 7 of the modernised Convention

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 employment purposes outlined in Principle 1 bis 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

14.2. The introduction and use of systems for the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted where it leads to the 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.

Internal investigations should not be carried out on the sole basis of an anonymous report, except where it is duly circumstantiated and relates to serious domestic law infringements.

Comment [IT28]: Both the adjective "deliberate" and "systematic" are unclear and susceptible to neutralise the rights of the employee.

Comment [IT29]: We have lost the reference to consultation of employee's representatives

Comment [IT30]: This is more in line with Article 29 Opinion 1/2006 which considers that whistleblowing schemes may lead to anonymous reports being filed through the scheme and acted upon, but as an exception to the rule and under specific conditions.

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. 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, including the additional safeguards provided for in principle 21. 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 the latter, uses professional devices outside the company or institution premises, enabling the employer to 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.

Comment [IT31]: If we are not mistaken concerns were raised by some delegations in respect of this provision. Shouldn't we say that with regard to this very delicate processing appropriate agreements should be made in order to ensure that employees' right to respect for private life?

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, including the additional safeguards provided for in principle 21.

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. ..

Comment [IT32]: The wording of this sentence is not technical. Moreover, this principle should be valid for any data processing not only for biometrics.

19. Psychological tests, analysis and similar procedures

19.1 Recourse to tests, analysis and similar procedures 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, including the additional safeguards provided for in principle 21. 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.

Comment [IT33]: We would suggest to go back to the original text of Rec (89)2 which appears much simpler and clearer. "4.4 Recourses to [these] tests, analyses and similar procedures […] should not take place without his[/her] consent or unless domestic law provides other appropriate safeguards. If he/she so wishes, he/she should be informed of the results of the tests"

20. Other processing posing specific risks to employees' rights

20.1 Employers 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.

Comment [IT34]: In principle 14 there is no longer a reference to the consultation procedure.

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, in particular, 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 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.

SWEDEN / SUEDE

INDEX

Preamble

Appendix:

Part I – General principles

1. Scope
1bis. Definitions
2. Respect for human rights, dignity and fundamental freedoms
3. Application of data protection principles
4. Collection of data
5. Storage of data
6. Internal use of data
7. Communication of data to employee's representatives, including the use of information systems and technologies
8. External communication of data
9. Processing of sensitive data
10. Transparency of processing
11. Right of access, rectification and to object
12. Security of data
13. Preservation of data

Part II - Particular forms of processing

14. Information systems and technologies for the monitoring of employees, including video surveillance
15. Internal reporting mechanism
16. Use of Internet and e-mails in the workplace
17. Equipment revealing employees' whereabouts
18. Biometric data
19. Psychological tests, analyses and similar procedures
20. Other processing posing specific risks to employees' rights
21. Additional safeguards

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 for employment purposes is permissible only if the data have been collected in accordance with the requirements outlined in principles 4, 9 and 14 to 20. 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 such data are 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 or confidentiality. 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.

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

SE suggestion: The article should be in the first hand deleted as the use of monitoring devices, including video surveillance, is already regulated in the recommendation, why article 14.3 seems surplus. If the article is not deleted we would like to suggest the following modification

14.3 In the event of dispute or legal proceedings, employees should be able to obtain copies of the recording made in accordance with domestic law / where appropriate .The storage of the recordings made should be limited in time in accordance with domestic law.

Rationale: Recordings from for example surveillance cameras might contain trade secrets or other confidential information It is therefore not reasonable that employees should at any time have the right to obtain copies hence there is a risk that such recordings can be used outside the company/workplace. Conflict between trade secrets or confidential information and the duty of disclosure, are usually regulated by member state law. At least there should be a proportionality between the interest of a disclosure and the interest of trade secrets or other

confidential information (For instance this balance is in Sweden made by the court in accordance with the principle of proportionality).

Moreover, it is not reasonable that employers should have to keep the recordings (storage of data) for an unlimited period of time (there is no time limit in the article). The storage of the recordings made should be limited in time in accordance with domestic law. This should be clarified in the recommendation.

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 duly 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, including the additional safeguards provided for in principle 21. 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 the latter, uses professional devices outside the company or institution premises, enabling the employer to 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, including the additional safeguards provided for in principle 21.

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, including the additional safeguards provided for in principle 21. 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, in particular, 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.

SWITZERLAND / SUISSE

INDEX

PREAMBULE

ANNEXE :

Partie I – Principes généraux

1. Champ d'application

1bis. Définitions

2. Respect des droits de l'homme, de la dignité et des libertés fondamentales

3. Application des principes de traitement

4. Collecte de données

5. Enregistrement des données

6. Utilisation interne des données

7. Communication des données aux représentants des employés, y compris l'utilisation de systèmes et technologies d'information

8. Communication externe

9. Traitement de données sensibles

10. Transparence du traitement

11. Droit d'accès, de rectification et d'objection

12. Sécurité des données

13. Conservation des données

Partie II – Formes particulières de traitement

14. Systèmes et technologies d'information pour le contrôle des employés, incluant la vidéosurveillance

15. Mécanismes internes de signalement

16. Utilisation de l'Internet et des messages électroniques sur le lieu de travail

17. Appareils permettant de géolocaliser les employés

18. Données biométriques

19. Tests psychologiques, analyses et procédures analogues

20. Autres traitements de nature à présenter des risques spécifiques au regard des droits des employés

21. Garanties Complémentaires

PROJET DE RECOMMENDATION CM/REC(2013)… DU COMITE DES MINISTRES AUX

ETATS MEMBRES SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL UTILISEES A DES FINS D'EMPLOI.

(Adoptée le … 2014 par le Comité des Ministres lors de la … réunion des Ministres délégués)

Le Comité des Ministres, en vertu de l'article 15.b du Statut du Conseil de l'Europe,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Conscient de l'utilisation croissante des nouvelles technologies et des instruments de communication électronique dans les relations entre employeur et employés et des avantages qui en découlent ;

Estimant, toutefois, que l'utilisation de méthodes de traitement des données, par l' employeur devrait être gouvernée par des principes destinés à réduire au minimum les risques que de telles méthodes pourraient éventuellement présenter pour les droits et les libertés fondamentales des employés, notamment leur droit à la vie privée ;

Ayant à l'esprit les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (ci-après la Convention 108), ainsi que celles de son Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données du 8 novembre 2001, et compte tenu de l'intérêt de convertir l'application de ces principes au secteur de l'emploi ;

Reconnaissant également que, lors de l'élaboration de principes dans le secteur de l'emploi, il doit être tenu compte aussi bien des autres intérêts (individuels, ou collectifs, privés et publiques);

Considérant que les données à caractère personnel dans les documents officiels détenus par une autorité publique ou un organisme public peuvent être divulguées par l'autorité ou l'organisme conformément à la législation nationale à laquelle l'autorité ou organisme public est soumis, afin de concilier le droit d'accès à ces documents officiels avec le droit à la protection des données à caractère personnel conformément à la présente Recommandation;

Conscient des traditions différentes existant dans les Etats membres en ce qui concerne la réglementation des divers aspects des relations employeur-employé, et constatant que la réglementation par voie législative ne constitue qu'une des méthodes utilisées ;

Conscient des changements intervenus à l'échelle internationale dans le monde du travail et activités qui y sont liés, du fait notamment du recours accru aux technologies de l'information et de la communication (TICs) et de la mondialisation de l'emploi et des services ;

Considérant que ces changements appellent à une révision de la Recommandation N° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi en vue de continuer à assurer un niveau de protection adéquat des personnes dans le secteur de l'emploi ;

Rappelant l'article 8 de la Convention européenne des droits de l'Homme, qui protège le droit à la vie privée, comprenant, tel qu'interprété par la Cour européenne des droits de l'homme, les activités de nature professionnelle et/ou commerciale;

Rappelant l'application des principes établis par d'autres recommandations pertinentes du Conseil de l'Europe, en particulier la Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, la Recommandation R(97)5 relative à la protection des données médicales et la Recommandation R(92)3 sur les tests et le dépistage génétiques à des fins médicales ;

Rappelant les «Principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance » adoptés par le Comité Européen de Coopération juridique (CDCJ) du Conseil de l'Europe en mai 2003 et mentionnés dans la Résolution 1604 (2008) de l'Assemblée parlementaire du Conseil de l'Europe qui sont particulièrement pertinents ;

Rappelant la Charte sociale européenne (STCE n° 163), dans sa version révisée du 3 mai 1996, ainsi que le Code de conduite du Bureau international du travail de 1997 sur la protection des données à caractère personnel des travailleurs ;

Recommande aux gouvernements des Etats membres :

- d'assurer que les principes contenus dans la présente recommandation et son annexe, qui remplace la Recommandation R N° (89)2 susmentionnée, soient reflétés dans la mise en œuvre des législations nationales relatives à la protection des données dans le secteur de l'emploi, ainsi que dans d'autres branches de toute loi portant sur l'utilisation des données à caractère personnel à des fins d'emploi;

- d'assurer, à cette fin, que la présente recommandation soit portée à l'attention des autorités établies conformément à la législation nationale en matière de protection des données et chargées de contrôler l'application de cette législation ;

- et de promouvoir par ailleurs l'acceptation et l'application des principes contenus dans l'annexe de la présente Recommandation, au moyen d'instruments complémentaires tels que des codes de conduite, en s'assurant que ces principes soient bien assimilés/ admis et mis en application par tous les intervenants du secteur de l'emploi, incluant les organes représentatifs

de l'employeur et des employés et pris en compte dans la conception, le déploiement et l'utilisation des TICs dans ce secteur.

Annexe à la Recommandation

Partie I – Principes généraux

1. Champ d'application

1.1. Les principes de la présente recommandation s'appliquent au traitement de données à caractère personnel à des fins d'emploi dans les secteurs public et privé.

Comment [SN35]: En Suisse il y a des différence entre les traitement des données du secteur public et privé. Par exemple des données sensibles ne peuvent être traité qu' avec une base légal. A voir paragraphe 9

1.2. Sauf législations nationales contraires, les principes de la présente recommandation s'appliquent aussi aux activités des agences pour l'emploi, dans les secteurs public et privé, qui traitent des données à caractère personnel afin de permettre l'établissement d'un ou de plusieurs contrats de travail simultanés, y compris de contrats à temps partiel, entre les personnes concernées qui figurent sur leurs listes et d'éventuels employeurs, ou afin de faciliter les démarches pour les employeurs dérivant desdits contrats.

1bis. Définitions

Aux fins de la présente recommandation :

– «données à caractère personnel» signifie toute information concernant une personne physique identifiée ou identifiable (« personne concernée »).

– « traitement» s'entend de toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, et notamment la collecte, l'enregistrement, la conservation, la modification, l'extraction, l'interconnexion, la communication, la mise à disposition, l'effacement, la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques aux données ; lorsqu'aucun procédé automatisé n'est utilisé, le traitement de données s'entend des opérations effectuées au sein d'un ensemble structuré établi selon tout critère qui permet de rechercher des données à caractère personnel ;

– « responsable du traitement » signifie la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données ;

– « sous-traitant » signifie la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

– « destinataire » signifie la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui reçoit communication de données ou à qui des données sont rendues accessibles ;

– « les données sensibles » couvrent les données génétiques ou les données concernant des infractions, condamnations pénales et mesures de sûreté connexes, les données

biométriques identifiant un individu de façon unique ainsi que les données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle ;

– « systèmes d'information » signifie tout dispositif isolé ou groupe de dispositifs interconnectés ou liés entre eux, qui assurent - ou dont un ou plusieurs éléments assure(nt)-, conformément à un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ces derniers en vue de leur fonctionnement, utilisation, protection et maintenance ;

– « à des fins d'emploi» concerne les rapports entre employés et employeurs relatifs au recrutement des employés, à l'exécution du contrat de travail et à son encadrement, y compris à l'exécution des obligations découlant de la loi ou de conventions collectives, ainsi qu'à la planification et l'organisation du travail ou la fin des rapports de travail. Les conséquences de la relation contractuelle peuvent s'étendre au-delà du terme du contrat de travail.

– « employeur » signifie toute personne physique ou morale, l'autorité publique ou l'agence engagée dans un lien d'emploi avec l'employé ou un candidat à un emploi et détenant la responsabilité légale de l'entreprise ou de l'établissement ;

– « employé » ou « candidat à l'emploi » signifie toute personne concernée engagée dans une relation de travail avec un employeur ;

2. Respect des droits de l'homme, de la dignité humaine et des libertés fondamentales

Le respect de la dignité humaine, de la vie privée et de la protection des données à caractère personnel devrait être garanti lors du traitement des données à des fins d'emploi, notamment pour permettre aux employés le développement libre de leur personnalité et afin de préserver la possibilité de relations sociales et individuelles sur leur lieu de travail.

3. Application des principes de traitement

[3.1. Les employeurs devraient veiller à ce que le traitement des données à caractère personnel ne porte que sur les données strictement nécessaires pour atteindre l'objectif déterminé dans les cas individuels concernés et le cas échéant procéder à l'anonymisation des données moyennant le respect des conditions et garanties additionnelles prévues par le droit interne ou procéder à la pseudonymisation des données lorsque l'anonymisation n'est pas possible.]

3.2. Les employeurs devraient développer des mesures appropriées, visant à respecter en pratique les principes et obligations en matière de traitement des données aux fins d'emploi. A la demande des autorités de contrôle, l'employeur devrait être en mesure de démontrer qu'il est en conformité avec des tels principes et obligations. Ces mesures devraient être adaptées au volume et à la nature des données traitées et aux activités entreprises ; elles tiendront également compte des conséquences possibles pour les droits et les libertés fondamentales des personnes concernées.

Comment [SN36]: Pas suffisamment concret : →à développer dans l'exposé des motifs.

4. Collecte des données

4.1. L'employeur devrait collecter les données à caractère personnel directement auprès de la personne concernée. Lorsqu'il est nécessaire, licite, loyal et approprié de traiter des données collectées auprès des tiers, par exemple pour obtenir des références professionnelles, la personne concernée devrait en être dûment informée.

4.2. Les données à caractère personnel collectées à des fins d'emploi devraient être pertinentes et non excessives, eu égard à la nature de l'emploi ainsi qu'aux besoins légitimes de l'employeur en lien direct avec ses activités et le cas échéant moyennant le respect des conditions et garanties additionnelles prévues par le droit interne.

4.3. L'employeur doit s'abstenir de chercher à accéder à des données à caractère personnel que l'employé partage et qui ne sont pas liées à l'évaluation des capacités du dit employé à remplir ses fonctions.

4.4. L'employeur doit prendre les mesures appropriées pour veiller à ce que les données à caractère personnel mises en ligne (sur le site de l'entreprise par exemple) et accessibles au public, soient pertinentes, exactes et à jour. L'employeur doit veiller à ce que ces données ne soient pas traitées dans un contexte autre que celui dans lequel elles ont été publiées.

4.5. Les données relatives à la santé ne peuvent être collectées qu'aux fins prévues au principe 9.2 de la présente Recommandation.

[5. Enregistrement des données

5.1. L'enregistrement de données à caractère personnel à des fins d'emploi n'est possible que si les données ont été collectées conformément aux règles définies aux principes 4, 9 et 14 à 20 de la présente Recommandation. Ces données devraient être pertinentes, adéquates et non-excessives.

5.2. Lorsque des données d'évaluation relatives à la productivité ou à la capacité des employés sont enregistrées, de telles données ne devraient servir qu'à évaluer les compétences professionnelles.]

6. Utilisation interne des données

6.1. Les données à caractère personnel collectées à des fins d'emploi ne devraient être traitées par l'employeur qu'à de telles fins.

6.2. L'employeur devrait adopter des politiques de protection des données, des règles et/ou d'autres instruments relatifs à l'usage interne des données à caractère personnel.

Comment [SN37]: Consentement obligatoire pour obtenir des références.

Comment [SN38]: C'est à dire quel cas? En général l'employeur ne peut traiter les données qu'en lien direct aves ses activités.

Comment [SN39]: Qu'en est-il des candidats à l'emploi? Comment faire avec les réseaux sociaux? Comment empêcher une telle collecte? Quelles sont les conséquences?

Comment [SN40]: Quel rapport avec la collecte? ce paragraphe est important mais se trouve au mauvais endroit (pourrait être déplacé au principe 8, car la mise en ligne est une forme de communication) Comment l'employeur peut veiller à ce que ces données ne soient pas traitées dans un contexte autre?

Comment [SN41]: Est-ce que c'est vraiment nécessaire de différencier entre collecte et enregistrement ?

Comment [SN42]: Préciser dans l'exposé des motifs ce qu'on entend par usage interne

6.3. Lorsque des données doivent être traitées à des fins d'emploi mais pour des finalités autres que celles pour lesquelles elles ont été initialement collectées, l'employeur devrait prendre des mesures appropriées pour éviter que ces données ne soient mal interprétées dans un contexte différent et en informer l'employé.

Comment [SN43]: Principe de finalité? Le but de la collecte et du traitement des données devrait être le même. Voir aussi 6.1.

6.4. Sans préjudice des dispositions du principe 8, lors de changements au sein de l'entreprise, de fusions et d'acquisitions, il convient de veiller au respect des principes de proportionnalité et de finalité dans l'utilisation ultérieure des données. Lorsque des modifications substantielles du traitement interviennent, la personne concernée doit en être informée.

7. Communication de données aux représentants des employés, y compris l'utilisation de systèmes et technologies d'information

7.1. Conformément aux législations et pratiques nationales et aux conventions collectives, des données à caractère personnel peuvent être communiquées aux représentants des employés, uniquement si de telles données sont nécessaires pour permettre à ces derniers de représenter de façon appropriée les intérêts des employés concernés ou si elles sont nécessaires afin de garantir l'exécution et la supervision des obligations prévues par les conventions collectives.

7.2. Conformément aux législations et pratiques nationales l'utilisation de systèmes et technologies d'information pour la communication des données aux représentants des employés devrait faire l'objet d'accords spécifiques avec l'employeur, visant à définir au préalable des règles transparentes stipulant leur utilisation et garantissant la protection des communications confidentielles.

8. Communication externe

8.1. Les données à caractère personnel collectées à des fins d'emploi devraient être communiquées à des organismes publics uniquement pour l'accomplissement de leur mission officielle et dans les limites des obligations légales de l'employeur ou conformément à d'autres dispositions du droit interne.

Comment [SN44]: Donner des exemples dans l'EM : sécurité sociale, statistiques, etc

8.2. La communication de données à caractère personnel à des organismes publics à d'autres fins ou à d'autres parties, y compris les entreprises du même groupe, ne devrait s'effectuer que :

a. moyennant le respect des conditions et garanties additionnelles prévues par le droit interne, lorsque la communication est nécessaire à des fins d'emploi qui ne seraient pas incompatibles avec les finalités pour lesquelles les données ont été collectées à l'origine et si les employés concernés ou leurs représentants, selon le cas, en sont informés ; ou

b. avec le consentement exprès de l'employé ; ou

c. si la communication est prévue par le droit interne.

8.3. La communication de données à caractère personnel au sein d'un groupe d'entreprises n'est licite que si elle est nécessaire à l'exécution des obligations légales ou des conventions collectives, moyennant le respect des conditions et garanties additionnelles prévues par le droit interne. Le consentement de l'employé peut aussi être requis.

Comment [SN45]: Qui décide de demander le consentement et dans quels cas ?

8.4 En ce qui concerne le secteur public, les dispositions relatives à la divulgation de données à caractère personnel afin d'assurer la transparence du gouvernement et de toute autre autorité publique ou organisme et / ou de surveiller l'utilisation correcte des fonds et ressources publiques, devraient également prévoir des garanties appropriées eu égard au droit au respect de la vie privée et à la protection des données à caractère personnel des employés.

9. Traitement de données sensibles

9.1. Le traitement des données sensibles au sens du principe 1bis de la présente Recommandation, est permis uniquement dans des cas particuliers, lorsque cela est indispensable pour un recrutement spécifique ou à l'exécution d'obligations légales dérivant du contrat de travail. Le traitement est également subordonné à la loi applicable prévoyant des garanties appropriées additionnelles, venant compléter celles de la Convention 108 et de la présente Recommandation. Les garanties appropriées doivent être de nature à prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, droits et libertés fondamentales des employés concernés, notamment le risque de discrimination. Le traitement des données biométriques est sujet aux dispositions du principe 18 de cette Recommandation.

9.2. Conformément au droit interne un employé ou un candidat à un emploi peut être interrogé sur son état de santé et/ou faire l'objet d'un examen médical uniquement aux fins de :

a. déterminer son aptitude à un emploi actuel ou futur ;

b. couvrir les besoins de la médecine préventive ;

c. garantir sa réadaptation appropriée au poste de travail ou en tout état de cause afin de s'adapter aux exigences de l'environnement professionnel ;

d. sauvegarder les intérêts vitaux de la personne concernée ou des autres employés ou d'autres personnes ;

e. octroyer des prestations sociales ; ou

f. répondre à une procédure judiciaire.

Le traitement de données génétiques, pour déterminer par exemple l'aptitude professionnelle des employés ou des candidats est interdit, même avec le consentement de l'intéressé.

Le traitement de données génétiques peut exceptionnellement être prévu par le droit interne et moyennant des garanties appropriées, en particulier pour éviter toute atteinte grave à la santé de la personne concernée ou de tiers.

9.3. Les données de santé et - lorsque leur traitement est licite - les données génétiques, ne devraient être collectées qu'auprès de l'employé concerné sauf dispositions contraires prévues par la loi, moyennant des garanties appropriées.

9.4. Les données de santé couvertes par le secret médical ne devraient être accessibles et traitées que par du personnel lié par le secret médical ou par d'autres règles régissant le secret professionnel et les obligations de confidentialité. Ces données devraient :

a. se rapporter directement à l'aptitude de l'employé à exercer ses fonctions, ou
b. être nécessaires pour prendre des mesures en faveur de la santé de l'employé ou
c. être nécessaires pour prévenir un risque pour d'autres personnes.

Lorsque ces données sont communiquées à l'employeur, cette communication devrait être faite aux ayants droit comme l'administration du personnel, de la santé et de la sécurité au travail et l'information ne devrait être communiquée que si elle est indispensable pour la prise de décision par l'administration du personnel, conformément au droit interne.

9.5. Les données de santé couvertes par le secret médical et - lorsque leur traitement est licite - les données génétiques, lorsque cela est approprié, devraient être enregistrées séparément des autres catégories de données détenues par l'employeur. Des mesures de sécurité techniques et organisationnelles devraient être prises afin d'éviter que des personnes étrangères au service médical n'aient accès à ces données.

9.6. Le droit d'accès des employés à leurs données de santé ne devrait pas faire l'objet de restrictions, à moins que l'accès à de telles données ne puisse porter une grave atteinte à l'employé. Une telle restriction doit être conforme aux dispositions prévues par le droit interne. Les données pourraient alors être communiquées à l'employé par l'intermédiaire du médecin de son choix.

9.7. En aucun cas les données de santé relatives à des tiers ne feront objet d'un traitement, à moins que la personne concernée n'ait donné au préalable son consentement non-équivoque, et que ce traitement ne soit autorisé par l'autorité de contrôle compétente ou que la collecte des données ne soit indispensable à l'exécution des obligations légales.

Comment [SN46]: Généralement l'employeur ne reçoit que les conclusions des constats médicaux!

Comment [SN47]: Quelles données sont couvertes par le secret médical? Ce sont plutôt les personnes qui sont liées par le secret médical.

Comment [SN48]: Seulement les conclusions des constats médicaux, pas les diagnostics.

Comment [SN49]: Dans l'exposé des motifs, il faudra préciser ce que l'on entend par enregistrées séparément.

Comment [SN50]: Difficile à trouver un cas ou ce traitement serait vraiment nécessaire. En Suisse l'autorité de contrôle n'a pas cette compétence.

10. Transparence du traitement

10.1. L'employé devrait pouvoir être en mesure d'obtenir des informations sur les données à caractère personnel détenues par son employeur. Ces informations pourraient lui être fournies directement ou par l'intermédiaire de ses représentants.

Sauf les informations concernant le nom de l'employé et sa résidence habituelle ou son lieu d'établissement –l'employeur devrait fournir à l'employé les informations suivantes :

- une liste complète des données qui seront traitées et une description des finalités du traitement,
- les destinataires ou catégories de destinataires de ces données,
- les moyens d'exercer les droits énoncés au paragraphe 11 de la présente recommandation, sans pour autant porter préjudice à des moyens plus favorables prévus dans le droit interne ou le système législatif,
- toute autre information nécessaire pour garantir un traitement loyal et licite des données.

Dans ce contexte, devrait être fournie une description particulièrement claire et complète des catégories des données à caractère personnel qui peuvent être collectées au moyen de systèmes et technologies d'information et de communication telle que la vidéosurveillance et de leur utilisation potentielle. Ce principe s'applique pour toutes les formes particulières de traitement des données à caractère personnel prévues à la partie II de la présente Recommandation.

10.2. Les informations devraient être fournies sous une forme accessible et tenues à jour. En tout état de cause, ces informations devraient être fournies avant que l'employé n'exerce effectivement l'activité ou l'action prévue, et être mises à disposition au moyen des systèmes d'information habituellement utilisés par l'employé.

11. Droit d'accès, de rectification et d'objection

11.1 Les employés devraient pouvoir obtenir, à leur demande, à intervalle raisonnable et sans délai excessif, la confirmation d'un traitement de données les concernant. La communication devrait être faite sous une forme intelligible, inclure toutes informations disponibles sur l'origine des données, ainsi que toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements, en particulier les informations prévues au paragraphe 10.

11.2 Les employés devraient avoir le droit d'obtenir la rectification ou l'effacement de leurs données à caractère personnel en cas d'inexactitude et/ou lorsqu'elles sont traitées en violation du droit interne ou des principes énoncés dans cette Recommandation. Ils devraient également être autorisés à s'opposer à tout moment au traitement des données à caractère personnel les concernant, à moins que ce traitement ne soit nécessaire à des fins d'emploi ou ne soit prévu par la loi.

11.3. Le droit d'accès devrait également être garanti s'agissant des données d'évaluation, y compris celles relatives aux appréciations de la performance, de la productivité ou du potentiel de l'employé, au plus tard lorsque le processus d'appréciation est terminé, sans préjudice du droit de défense de l'employeur ou des tiers impliqués. Bien que ces données ne puissent être directement corrigées par l'employé, les évaluations purement subjectives devraient pouvoir être contestées selon les modalités prévues par le droit interne.

11.4. Les employés ne doivent pas être soumis à une décision les affectant de manière significative, qui serait uniquement basée sur un traitement automatisé de données, sans que leur point de vue ne soit pris en compte.

Comment [SN51]: Donner des exemples dans l'exposé des motifs.

11.5. Un employé doit également obtenir, à sa demande, des informations concernant les finalités du traitement des données, les résultats de ce traitement et les moyens par lesquels ces résultats l'affectent.

11.6. Des dérogations aux droits auxquels il est fait référence aux paragraphes 11.1, 11.3 et 11.4 peuvent être admises lorsqu'elles sont prévues par une loi et constituent une mesure nécessaire dans une société démocratique, à la protection de la sûreté de l'Etat, à la sécurité

publique, à des intérêts économiques et financiers importants de l'Etat ou à la prévention et à la répression des infractions pénales, ainsi qu'à la protection de la personne concernée et des droits et libertés d'autrui.

11.7. Par ailleurs, dans le cas d'une enquête interne effectuée par l'employeur, l'exercice de ces droits peut être différé jusqu'à la conclusion de cette enquête, si l'exercice de ces droits peut nuire/mettre en péril l'enquête.

11.8. Sauf dispositions nationales contraires, l'employé devrait pouvoir désigner une personne de son choix pour l'assister lors de l'exercice de son droit d'accès, de rectification ou d'effacement de ses données ou afin d'exercer ces droits en son nom.

11.9. Une voie de recours devrait être prévue par le droit interne lorsqu'un employé se voit refuser l'accès aux données le concernant ou la possibilité de rectifier ou d'effacer certaines de ces données.

12. Sécurité des données

12.1. L'employeur ou les entités, auprès desquelles les données peuvent être sous-traitées, devraient mettre en œuvre des mesures techniques et organisationnelles, qui seront mises à jour si cela s'avère nécessaire, en vue des examens périodiques d'une évaluation des risques et des politiques de sécurité. De telles mesures devraient garantir la sécurité et la confidentialité des données à caractère personnel enregistrées à des fins d'emploi, contre la modification, la perte ou la destruction accidentelles ou non autorisées de données à caractère personnel, ainsi que contre l'accès à ces données, leur diffusion ou leur divulgation non autorisées.

12.2 L'employeur assure de manière adéquate la sécurité des données lors de l'utilisation des TICs pour le traitement de données à caractère personnel à des fins d'emploi.

12.3. Le service du personnel ainsi que toute autre personne intervenant dans le traitement des données devraient être tenus informés de ces mesures et de la nécessité de les respecter.

13. Conservation des données

13.1. Un employeur ne devrait pas traiter des données à caractère personnel pendant une période plus longue que ne le justifient les finalités définies au principe 1.3. ou que ne le nécessite l'intérêt d'un employé en poste ou d'un ancien employé.

Comment [SN52]: Il s'agit probablement de la définition à des fins d'emploi du principe 1bis ?

13.2. Les données à caractère personnel fournies à la suite d'un acte de candidature devraient en principe être effacées dès qu'il devient clair que la candidature ne sera pas retenue.

Comment [SN53]: Les documents fournis par la personne concernée doivent lui être retournés

Lorsque de telles données sont conservées en vue d'une demande d'emploi ultérieure, l'intéressé devrait en être informé en temps utile et les données devraient être effacées à sa demande.

Lorsque pour intenter ou soutenir une action en justice ou pour toute autre finalité légitime, il est indispensable de conserver les données fournies à l'occasion d'une candidature, ces données ne devraient être conservées que pour la période nécessaire à l'action en justice.

Comment [SN54]: Seulement s'il y a un degré élevé de certitude qu'une action aura lieu

13.3. Les données à caractère personnel traitées aux fins d'une enquête interne réalisée par un employeur et qui n'a entraîné l'adoption d'aucune sanction à l'égard des employés devraient être effacées dans un délai raisonnable, sans préjudice de l'exercice du droit d'accès de l'employé jusqu'à ce qu'elles soient effacées.

Partie II – Formes particulières de traitement

14. Systèmes et technologies d'information pour le contrôle des employés, incluant la vidéosurveillance

14.1 L'introduction et l'utilisation des TICs afin de contrôler les employés doivent être faites en respectant les principes de légitimité, de pertinence et de proportionnalité, uniquement lorsqu'il y a impossibilité d'utiliser d'autres méthodes alternatives de traitement qui sont moins intrusives pour la vie privée et lorsqu'ils sont accompagnés de garanties appropriées. Les employeurs devraient établir un juste équilibre entre le droit des employés au respect de la vie privée et l'intérêt de l'employeur de protéger ses droits de propriété.

Comment [SN55]:
Proposition de changement ::

Il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail.

Lorsque des systèmes de surveillance ou de contrôle sont nécessaires pour d'autres raisons, ils doivent notamment être conçus et disposés de façon à ne pas porter atteinte à la santé et à la liberté de mouvement des travailleurs

14.2 L'utilisation des tels systèmes directement et essentiellement afin de contrôler à distance le travail et le comportement des employés, ne doit pas être autorisée lorsqu'elle conduit à une surveillance délibérée et systématique d'un employé en particulier, ou d'un groupe spécifique d'employés. Des exceptions à ce principe pourraient être envisagées, avec des garanties appropriées, lorsque la surveillance n'est pas l'objectif principal poursuivi par l'employeur, mais uniquement une conséquence indirecte d'une surveillance nécessaire aux fins de la production, de la sécurité, de l'organisation du travail de l'établissement ou de la protection de la santé. L'utilisation de tels dispositifs, notamment de vidéosurveillance, dans des endroits qui portent atteinte à la vie intime des employés n'est pas autorisée.

14.3 En cas de litige ou d'action en justice, les employés devraient pouvoir obtenir la copie des enregistrements réalisés.

15. Mécanismes internes de signalement

Lorsque l'employeur est tenu par la loi ou les règles internes de mettre en œuvre des mécanismes internes de signalement, tels que les numéros d'urgence, il doit assurer la protection des données à caractère personnel de toutes les parties concernées. En particulier, l'employeur doit garantir la confidentialité à l'égard de l'employé qui signale les comportements illicites ou contraires à l'éthique (tel qu'un donneur d'alerte). Les données à caractère personnel des parties en cause doivent être utilisées uniquement aux fins des procédures internes appropriées relatives aux dits signalements, à la loi ou à l'ordre judiciaire.

Le cas échéant, l'employeur doit permettre le signalement anonyme. Cependant, un signalement anonyme ne saurait être l'unique origine d'enquêtes internes, sauf si ce signalement est dûment circonstancié et concerne de graves infractions au droit interne.

Comment [SN56]: Le ch. 15, paragraphe 2, va trop loin en ce qu'il impose l'admission de signalements anonymes dans les mécanismes internes de signalement. Il faudrait remplacer « doit » par « peut ».

Il faudrait au moins que la recommandation soit cohérente avec les autres textes traitant du signalement. A cet égard, il est à noter que, au niveau de l'UE, l'avis du 1er février 2006 du Groupe de travail « Article 29 » sur la protection des données s'en tient à la confidentialité et prévoit que le signalement anonyme doit rester exceptionnel. Il faut aussi surtout prendre en compte la recommandation CM/Rec(2014)7 du Comité des Ministres sur la protection des lanceurs d'alerte, adoptée le 30 avril 2014. Cette recommandation (ch. V, par. 18) s'en tient aussi à la confidentialité.

16. Utilisation de l'Internet et des messages électroniques sur le lieu de travail

16.1 L'employeur devrait éviter de porter des atteintes injustifiées et déraisonnables au droit au respect de la vie privée de l'employé. Ce principe s'étend à tous les dispositifs techniques et aux TICs utilisés par un employé. Les personnes concernées devraient être convenablement et périodiquement informées à l'aide d'une déclaration claire en matière de respect de la vie privée conformément au principe 10 de la Recommandation. L'information fournie devrait être mise à jour et inclure la finalité du traitement, la durée de conservation des données collectées ainsi qu'à la sauvegarde des données de connexion et à l'archivage des messages électroniques.

16.2 En ce qui concerne plus particulièrement l'éventuel traitement de données à caractère personnel relatives aux pages Internet ou Intranet consultées par l'employé, il conviendrait d'une part d'adopter des mesures préventives, telles que la configuration de systèmes ou l'utilisation de filtres qui peuvent empêcher certaines opérations, et d'autre part de prévoir éventuellement des contrôles des données à caractère personnel, effectués de manière graduée et utilisant dans un premier temps par sondages non individuels des données anonymes ou agrégées.

16.3 L'accès aux messages électroniques professionnels des employés doit faire l'objet d'une information préalable des employés et ne peut survenir [qu'en conformité avec la législation et] si cela est nécessaire pour des raisons de sécurité, ou pour d'autres raisons légitimes. En cas d'absence d'un employé, l'employeur devrait prendre les mesures nécessaires et prévoir les procédures appropriées visant à permettre l'accès aux messages électroniques professionnels, uniquement lorsqu'un tel accès est nécessaire d'un point de vue professionnel. Par ailleurs, l'accès doit intervenir de la façon la moins intrusive possible et uniquement après avoir informé l'employé ou les employés concernés.

16.4. En aucun cas le contenu, l'envoi et la réception des messages privés dans le cadre du travail ne peuvent faire l'objet d'une surveillance.

16.5. Lorsqu'un employé quitte son emploi, l'employeur doit prendre des mesures techniques et organisationnelles afin que la messagerie électronique de l'employé soit désactivée automatiquement à son départ. Si le contenu de la messagerie doit être récupéré pour la bonne marche de l'entreprise, l'employeur doit prendre des mesures appropriées afin de récupérer son contenu avant le départ de l'employé et si possible en sa présence.

17. Appareils permettant de géolocaliser les employés

17.1 Si les appareils permettant de localiser les employés peuvent être utilisés dans leur intérêt (par exemple pour déterminer un accident du travail), leur utilisation ne doit pas conduire à leur contrôle permanent ou excessif. Considérant les risques d'atteinte aux droits et aux libertés des personnes que présente l'utilisation de ces appareils, l'employeur devrait prendre toutes les garanties nécessaires à la protection des données à caractère personnel et au respect de la vie

privée, y compris les garanties prévues au principe 21. Il doit notamment accorder une attention particulière aux finalités pour lesquelles de tels appareils sont utilisés. En particulier, la surveillance ne doit pas être l'objectif principal poursuivi par l'employeur, mais seulement une conséquence indirecte d'une action nécessaire aux fins de la production, de la sécurité ou de l'organisation du travail de l'établissement.

Comment [SN57]: voir paragraphe 14

17.2 Lorsqu'un employé, soit conformément aux instructions de son employeur soit après s'être assuré que l'employeur connaissait au préalable les modalités de cette utilisation et en accord avec ce dernier, utilise des appareils professionnels en dehors de l'entreprise ou de l'institution permettant à l'employeur de le localiser, la collecte et le traitement de ces données à caractère personnel doit être exclusivement limité à la stricte vérification de l'exécution des tâches professionnelles ou des aspects organisationnels.

17.3 L'employeur doit prendre les mesures internes appropriées concernant le traitement de ces données et les notifier préalablement aux personnes concernées.

18. Données biométriques

18.1 La collecte et le traitement de données biométriques ne devraient être réalisés que lorsqu'ils sont nécessaires à la protection des intérêts légitimes de l'employeur, des employés ou des tiers et uniquement lorsqu'il y a impossibilité d'utiliser d'autres méthodes alternatives de traitement moins intrusives pour la vie privée. Ce traitement doit s'accompagner de garanties appropriées, y compris les garanties prévues au principe 21.

18.2 Le traitement des données biométriques doit être fondé sur des méthodes scientifiquement reconnues et soumis à des exigences strictes de sécurité et de proportionnalité. L'employé devrait avoir le contrôle du traitement de ces données biométriques.

19. Tests psychologiques, analyses et procédures analogues

19.1 Le recours à des tests, à des analyses et à des procédures analogues effectués par des professionnels spécialisés, soumis au secret professionnel et destinés à évaluer le caractère ou la personnalité d'un employé ou d'un candidat à l'emploi ne devraient être permis que s'il est légitime et nécessaire au regard de la catégorie d'activité exercé dans l'emploi.

19.2 Ces tests, analyses et procédures analogues ne devraient pas se faire sans le consentement de l'employé ou du candidat à l'emploi, et en vertu des garanties appropriées prévues par le droit interne, y compris les garanties prévues au principe 21. Le consentement de l'employé doit être libre, éclairé et sans aucune contrepartie, notamment financière. L'employé ou le candidat à l'emploi devraient être informés au préalable des modalités d'utilisation des résultats de ces tests, analyses ou procédures analogues et, par la suite, de leur contenu.

20. Autres traitements de nature à présenter des risques spécifiques au regard des droits des employés

20.1 L'employeur, et lorsque cela est applicable, le sous-traitant, doivent procéder à une analyse de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des employés et concevoir les traitements de données de manière à prévenir ou pour le moins à minimiser les risques d'atteinte à ces droits et libertés fondamentales.

20.2 A moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationale, l'accord des représentants des employés devrait être recherché préalablement à l'introduction ou à la modification des TICs lorsque la procédure de consultation mentionnée au principe 14 révèle des risques d'atteinte au regard des droits des employés.

21. Garanties complémentaires

- Pour toutes formes particulières de traitement, établies dans la Partie II de cette Recommandation, l'employeur est tenu de prendre en particulier les garanties suivantes :

- Informer préalablement les employés de la mise à place de tout dispositif de surveillance. L'information fournie doit être mise à jour, et le droit d'information doit s'effectuer conformément au principe 10 de la Recommandation. Les informations doivent inclure la finalité du dispositif, la durée de conservation, l'existence ou non des droits d'accès et de rectification et la façon dont ces droits peuvent être exercés ;

- Prendre les mesures internes appropriées concernant le traitement de ces données et les notifier préalablement aux employés ;

- Avant l'introduction d'un système de surveillance ou lorsqu'un système existant doit être modifié, les représentants des employés devraient être consultés, conformément aux législations et pratiques nationales. Lorsque la procédure de consultation révèle une possibilité d'atteinte au droit au respect de la vie privée et de la dignité humaine des employés, l'accord des représentants doit être assuré ;

- Consulter, conformément à la législation nationale les autorités nationales de contrôle sur les traitements de données à caractère personnel.