Strasbourg, 9 October/octobre 2013

T-PD(2013)09MosRev

**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)**

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

* * *

PROJET DE RECOMMANDATION SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL UTILISEES A DES FINS D'EMPLOI

Note: This latest version was updated in order to include additional proposals from Sweden regarding some of the articles and make visible the changes proposed by Austria and Switzerland/

Cette dernière version a été mise à jour afin d'inclure des propositions supplémentaires de la Suède concernant certains articles et rendre visibles les propositions de modification de l'Autriche et de la Suisse

DG I – Human Rights and Rule of Law /

Droits de l'Homme et Etat de droit

TABLE OF CONTENTS / TABLE DES MATIERES

ALBANIA / ALBANIE

PROPOSALS FOR THE RESOLUTION ON THE PROTECTION OF PERSONAL DATA USED FOR EMPLOYMENT PURPOSES:

In the point 9 of the resolution "Processing of sensitive data" to add the following points:

1. When the employer must report to the bodies designated by law for accidents at work and professional diseases of the employees, even that the recognition of the diagnosis is legitimate for him, he must communicate to the designated body only health information concerning the reported pathology and not also the data on health that are verified during the employment relationship, as this action would be redundant and not within the purpose.

2. The employer processes health data that informs him on the health of the employees, the latter seeking to participate in rehabilitation or treatment programs while maintaining the job, and when forced to submit (according to the legislative provisions) the specific medical documents .

3. The employer must provide the data on the health of employees to the public authorities to fulfill specific obligations (which come from the law, the norms, rules, from contractual provisions), limited to the necessary information alone, for the purpose for which these data are required.

In the point 14, "Information systems and technologies for monitoring the employees, including video surveillance" to add the following points:

1. The employer may operate surveillance camera in a particular workplace in which employees are at work, if this surveillance is essential:

a) To prevent a significant threat of violence related to the employees performance, a significant damage, a danger to the safety of employees or to their health;

b) Protection of the rights and interests of workers when a surveillance camera is based on the request of the employee who's subject to supervision and the issue is agreed between the employer and the employee.

In the point 18 "Biometric data" to add the following points:

1. Every employee who's biometric data were collected, is entitled, without charge, upon written request, to receive from the employer information on processing of the fingerprints and the purpose of their processing.

2. The place and the processing forms of the biometric data must be adequate and sufficient to have effective systems of biometric data verification, based on the reading of digital traces.

Data collected are stored on devices exclusively available to employees (smart card or analog slide) which exclude the use of identities being sufficient to give to every employee a personal code.

3. In case that the use of biometric data is not regulated by law, the employer must first notify the Authority for Personal Data Protection on the purpose and criteria of collecting and using such data.

4. The access to biometric data should be permissible only for particular employees while implementing security measures, only for the purpose of verification and storing of such data.

5. Every employee, in cases where he claims that the collection and processing of fingerprints is against the legal framework for the protection of personal data, is entitled to submit a complaint to the Authority for Personal Data Protection.

AUSTRIA / AUTRICHE

1) The Republic of Austria is of the opinion that the proposed Recommendation should – just like Recommendation No. R (89) 2 – follow a general approach and stay technically neutral, thus avoiding going too much into details.

2) Preamble:

The first recommendation should read (just like in R (89) 2):

- *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.***

This amendment is necessary in order to cover not only the employment sector but also other branches of the law dealing with the use of personal data for employment purposes.

DRAFT RECOMMENDATION	AMENDING PROPOSALS
Part I – General principles **1. *Scope and definitions*** 1.1. The principles set out in this recommendation apply to any collection and processing of personal data for employment purposes in both the public and private sectors. 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 the duties relating to those contracts. 1.3. For the purposes of this recommendation: - 'Personal data' means any information relating to an identified or identifiable individual ("data subject"); - 'Data processing' means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, ~~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 ;~~	Comment: (word interconnection) The Republic of Austria is of the opinion that the definitions used in the present proposal should not differ from the ones in Convention 108, respectively in the latest proposals for the modernisation of Convention 108.
- '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	**COMMENT 2:** The term 'processor' is used in Principle 20.1.

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, ~~including when a transfer of data abroad is made through a service provider~~; - 'processing of sensitive data' covers the processing of genetic data, personal data concerning offences, criminal convictions and related security measures, the processing of biometric data uniquely identifying a person, as well as the processing of 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 of employees, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, as well as planning and organisation of work. The consequences of the contractual relationship may extend beyond the term of the contract of employment.	**COMMENT 3:** The Republic of Austria is of the opinion that the definitions used in the present proposal should not differ from the ones in Convention 108, respectively in the latest proposals for the modernisation of Convention 108.
- 'Employer' means any natural or legal person, public authority or agency who engages physical persons to perform required tasks in exchange of a salary and has the legal responsibility for the undertaking and/or establishment; - 'Employee' means any person engaged by an employer under a subordination relationship.	**COMMENT4:** The definition of employer should be amended in order to cover public authorities and agencies as well which could act as employers.
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, also to allow the free development of employees' personality and to foster possibilities of individual and social relationship on the workplace.	
3. *Application of data processing principles: minimisation, accountability, simplification and data security* 3.1. Employers should minimise the collection and use of ~~directly identifying~~personal data to only the data that necessary to the aim pursued in the individual cases concerned and should anonymise data when possible. 3.2. Employers should develop appropriate measures, including organisational ones, to ensure that they respect in practice the principles and obligations relating to data processing for employment purposes. At the request of the Data Protection supervisory authority, employers should also be able to demonstrate their compliance with such principles and obligations. 3.3. The measures that employers should adopt These measures will depend on volume of the processing, the nature of the data concerned, the type of the activities being undertaken, and should also take into account possible consequences for data subjects. 3.4. When using ICTs for the ~~collection and~~ processing of personal data for employment purposes, employers shall ensure adequate data security.	**COMMENT 5:** Since the principle of minimisation is a general principle of data protection it should not be restricted to "directly identifying data" **COMMENT 6:** Which one? There might be – depending on the country – several supervisory authorities in the employment sector (e.g. for supervising work safety etc.). **COMMENT 7:** Since Principles 3.2. and 3.3. are closely connected they should be merged. **COMMENT 8:** "collection" is covered by the term "processing" (see Principle 1.3. 2nd indent)
4. *Collection of data* 4.1. Employers should collect personal data directly from the data subject concerned. When it is necessary, lawful and appropriate to collect and process data obtained from third parties or sources, for example to obtain professional references, the data subject should be informed. ~~and his or her consent should be obtained~~. 4.2. Personal data collected by employers for employment purposes should be relevant and not excessive, having regard to the nature of employment as well as the legitimate needs of the employer in connection with its activities. 4.3. Employers should refrain from seeking to obtain access to employees' private data which is	**COMMENT 9:** If data collection is lawful (i.e. provided by law), the consent of the data subject isn't needed. **COMMENT 10:** Relation to Principle 3.1.?

not necessary for assessment of his ability to carry out the duties and responsibilities of the job concerned. 4.4. ~~In case of online data that is publicly accessible,~~ Tthe employer should take appropriate measures to ensure that, only relevant, accurate and up-to-date data are used, thus avoiding misuse or unfair processing of that data in respect of their origin. 4.5. Health data may only be collected and processed for the purposes set out in principle 9.2 of this Recommendation.	**COMMENT 11:** This principle (which is a general principle of data protection) should not be restricted to cases of online data.
5. *Storage of data* 5.1. The storage of personal data is permissible only if the data has been collected in accordance with the requirements outlined in principles 4, 9, 14 to 20 and if the storage is intended to serve employment purposes. Such data should be relevant, adequate, accurate and non-excessive. Where this is not the case, the employer should refrain from using the data. ~~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. Such data should be relevant, adequate, accurate and non-excessive.~~	**COMMENT 12:** Since this is a general principle of data protection it should not be restricted to evaluation data and therefore transferred to paragraph 1.
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 is to be processed (including correlated and/or analysed) 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 the different context and to ensure that they are not used in a manner incompatible with the original purpose. Where important decisions affecting an employee are to be taken based on the processed data, he or she should be informed. 6.4. Without prejudice to principle 8, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principle of purpose specification in	

the subsequent use of the data. Where substantive changes in the processing occur, the persons concerned should be informed. The consent of the employee may also be required in appropriate cases as safeguard.	
7. *Communication of data to employee's representatives* 7.1. In accordance with domestic law and practice, or the terms of collective agreements, ~~some~~ personal data may be communicated to employees' representatives, but only to the extent that such data ~~is~~ are necessary to allow those representatives to properly represent the interests of the employees concerned. 7.2. The use of ICTs for trade union communications should be subject to appropriate agreements that set out, in advance, transparent rules prescribing their use and safeguards to protect confidential communications.	**Comment 13: (word some)** Which ones?
8. *External communication of data* 8.1. Personal data collected for employment purposes should only be communicated to public bodies acting in, and for the purposes of carrying out their official functions, 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 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 authorised or determined by domestic law (in particular where necessary for court proceedings). 8.3. Where adequate safeguards are provided by domestic law, personal data can be communicated among a group of companies for	

the purpose of discharging obligations created by law or collective agreements. The consent of the employee may also be required in appropriate cases as additional safeguard. 8.4. With regard to the public sector, other instruments providing for disclosure of personal data to ensure government 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. In particular, the legislation should contain provisions that require full respect of the principle of purpose specification and limit disclosure to relevant personal data.	
9. *Processing of sensitive data* 9.1 The processing of ~~personal~~ sensitive data referred to in ~~paragraph~~ Principle 1.3. of this Recommendation ~~Article 6 of Convention 108~~ is only possible in particular cases, where it is indispensable for the specific recruitment or to fulfil legal obligations related to the contract of employment. The processing is also conditional on the applicable law providing additional appropriate safeguards, complementing those set out in Convention 108. Appropriate safeguards shall aim~~ed~~ 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 ~~paragraph~~ Principle 18 of this Recommendation. 9.2. An employee or job applicant may 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; - to safeguard the vital interest of the data subject or other employees; - to allow social benefits to be granted; or - to satisfy judicial procedures.	**COMMENT 14:** See also comment on Principle 18. **COMMENT 15:** There might be cases when an employer needs to know medical data of an employee/job applicant in order to protect vital interests of other employees (for example in hospitals).

The processing of genetic data, to determine for instance the professional suitability of employees or job applicants, even with the consent of the person concerned, is prohibited. Processing of genetic data may exceptionally be authorised if it is provided by domestic law and subject to appropriate safeguards, for health reasons and 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, may not be collected from third parties or sources other than the employee concerned except with his express and informed consent or if otherwise determined by law, with appropriate safeguards. 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. Such data must either relate directly to the ability of the employee concerned to exercise his or her duties, or be necessary in support of measures to protect the employee's health or to prevent risks to others. Where such data are communicated to the employer, this should be to a holder of a duly authorised role such as personnel administration, health and safety at work and the information should only be communicated if it is indispensable for decision making by the latter and in accordance with provisions of domestic law. 9.5. Health data covered by medical confidentiality and - where their processing is lawful - genetic data, 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 data subject's right of access to his or her health data and genetic data should not be restricted unless access to such data could cause serious harm to the data subject. In such cases, the data may 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 ~~,and~~ such collection is ~~lawful and~~ authorised by a data protection authority, or the collection is mandatory	**COMMENT 16:** See also Principle 10.3. of R (89) 2 **COMMENT 17:** Are there any health data that are not covered by the obligation of medical confidentiality? **COMMENT 18:** See Principle 10.4. of R (89) 2.

according to ~~the~~ domestic law.	**COMMENT 19:** It should be made clear that data processing is lawful if consent is given **or** if the data protection authority authorises data processing **or** if data processing is provided by law (see also Art. 5.1. of the modernisation proposals of Convention 108 and Art. 7 of Directive 95/46/EC.
10. *Transparency of processing* 10.1. Employees should be provided with information concerning the personal data that is held by his or her employer. This information can be provided directly or via his or her 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 Article 8 of Convention 108, 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 and its possible use, including indirect monitoring. 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, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her.	**COMMENT 20:** The right to object is neither defined nor mentioned in this Principle (see proposal of the Republic of Austria on Principle 11.1.).

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. Employees should also be entitled to have personal data rectified or erased, if they are inaccurate and/or if the data has 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.**	**COMMENT 21:** See Principle 12.1. of R (89) 2.
11.2. The right of access should also be guaranteed in respect of evaluation data, including where such data relates 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. 11.3. 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.	
~~11.4. Un~~ An employee should also be able to obtain, on request, information regarding the reasons for data processing, the results of the processing and how they have been applied to him. ~~Employees should also be entitled to have personal data rectified or erased, if they are inaccurate and/or if the data has been processed contrary to the law or the principles set out in this recommendation.~~	**COMMENT 22:** The right to rectification/erasure is a general right and should therefore be transferred to Principle 11.1.
11.5 The employer should introduce general procedures to ensure that there is an adequate and prompt response where the right of access and rectification are exercised, in particular in large-scale entities or entities spread out across the country.	**COMMENT 23:** Since it is already mentioned in Principle 11.1. that response is to be given "without excessive delay" this paragraph seems to be redundant and should rather be mentioned in an Explanatory Memorandum.
11.6. Derogations to the rights referred to in paragraph 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 close 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.	**COMMENT 24:** This Principle should be brought in line with Principle 11.1. as proposed in this document
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. 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 ~~paragraph~~ Principle 1.3 or is required in the interests of a present or former employee. 13.2. Personal data submitted in furtherance of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made. 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, the data should only be stored for the shortest possible period and for only as long as it is necessary. 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 must, in principle, be deleted in due time, 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 the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted where it leads to the monitoring of a specific employee, or a specific group of employees. The use of video surveillance for the direct and principal purpose of monitoring employees' activity and behaviour or for monitoring occurrences at locations that are part of the most personal area of life of an employee is not permitted. 14.2 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, safety or work organisations. Before any monitoring can occur, or in circumstances where such monitoring may change, employees' representatives need to be consulted. 14.3 In the event of dispute or legal proceedings, employees should be able to obtain copies of the recording made.	**COMMENT 25: (words 'most personal area of life)** Toilets, dressing room **Comment 26:** Video surveillance is a particularly intense intrusion in the rights of data subjects and should therefore only be allowed under conditions as set out in Principle 14.2.
15. Internal reporting mechanism Where employers are obliged by law or internal rules to implement internal reporting mechanisms, such as hotlines, employers should secure protection of personal data of all parties involved. In particular, employers should ensure the confidentiality of the employee who reports on illegal or unethical conduct (e.g. a whistleblower). Personal data of the parties involved should be used solely for the purpose of appropriate internal procedures relating to the report, law or judicial order. Where applicable, employers should enable	

anonymous reporting. However, internal investigations should not be carried out on the sole basis of an anonymous report, except where it is circumstantiated and relates to serious domestic law infringements.	
16. Use of Internet and e-mails in the workplace 16.1 The employer should avoid unjustifiable and unreasonable interferences with employee's right to private life. This principle extends to all aspects of an employee's employment, including his or her use of any computer, smartphone or other digital device, either in the framework of the employer's intranet, extranet, or by using directly the internet or not, made available by the employer. It applies whether the device used by the employee is provided by the employer or the employee himself or herself. The persons concerned should be properly and periodically informed, through a clear privacy policy. The information provided should be kept up to date. This should be done taking into consideration principle 10 of the recommendation. The information should include the purpose of the processing, the preservation or back-up period of connection 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 of the existence of that possibility can only occur in accordance with the law and where strictly necessary for security, operational or other lawful reason, such as to monitor infringements to intellectual property of the employer. 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 absolute professional necessity. Further, this 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.	Comment 27 (words 'when feasible): There might be situations when an employee is fired and not allowed to return to his working place.
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 ~~the~~ necessary safeguards for the employee's right to privacy and protection of personal data. Employers shall in particular pay special attention to the purpose for which such devices are used. Notably, monitoring should not be the main purpose, but only an indirect consequence of action needed to protect production, safety or work organisations. 17.2 When an employee, following his or her employer's instructions or with the knowledge and approval of his or her employer, uses professional devices outside the company or institution premises, and by virtue of that use the employer acquire knowledge of the employee's location, the collection and further processing of that personal data must be exclusively limited to the strict verification of the fulfilment of professional duties or organisational aspects. 17.3 Employers shall apply appropriate internal procedures relating to the processing of that 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	**COMMENT 28:** For reasons of clarity and also for systematic reasons this Principle should be incorporated in Principle 9.

and only if accompanied by appropriate safeguards. 18.2 The processing of biometric data shall be subject to the requirements of security and proportionality. In this regard, careful consideration should be given to the implications of storage in a central database or alternative systems based on media made available solely to the individual concerned.	
19. Psychological tests, analyses and similar procedures Recourse to tests, analyses 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 conducted when strictly necessary. They should not take place without the employees or job applicants consent, and domestic law should provide appropriate safeguards. The employee's consent should be free, informed and without any financial or other compensation foreseen. The employee or job applicant should be informed in advance of the use that will be made of the results of these tests**,** analyses or similar procedures. ~~and, subsequently, the content thereof~~. Paragraph 11.2. applies correspondingly.	**COMMENT 29:** 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.	Comment 30: (word processors) See comment on Principle 1.3.
21. Obligations of the employer For all particular forms of processing, set out in Part II of this Recommendation, the employer should ensure that appropriate measures are taken to secure the respect of the following obligations:	

• 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 the persons concerned in advance. • Consult employees' representatives in accordance with domestic law or practice and, where appropriate, with the relevant collective agreements. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, their agreement should be sought. • Consult before the processing the national Data Protection supervisory authorities.	**COMMENT 31:** See comment on Principle 3.2.

CYPRUS / CHYPRE

In reference to your email dated July 17th 2013 with regard to the Revised Draft Recommendation No: 89(2) I would like to inform you that we have neither specific comments nor drafted proposals. As a general comment we would expect more detailed guidance regarding the processing of biometric data in the framework of the employment context, and especially the processing of employees' fingerprints for the purpose of recording employees' attendance.

ESTONIA / ESTONIE

T-PD Secretariat
Data Protection and Cybercrime
DGI - Human Rights and Rule of Law
Council of Europe 26.09.2013

General comments: draft Recommendation on the protection of personal data used for employment purposes.

Estonian Data Protection Inspectorate asked from several interested parties for an opinion and/or comments on the draft recommendation. We received suggestions from Estonian Chamber of Commerce and Industry. These proposals are in a separate document.

We hereby would like to provide you with some general comments.

There has been some uncertainty regarding contacting referees indicated in CV-s. Employers need very clear indication whether they need to obtain additional consent or inform the applicant prior to contacting the referees.

Therefore we have made a proposal to add the following to Article 4.1.

4.1. Employers should collect personal data directly from the data subject concerned. When it is necessary, lawful and appropriate to collect and process data obtained from third parties or sources, for example to obtain professional references, the data subject should be informed and his or her consent should be obtained. If during the process of recruitment the data subject provides the employer with contacts of professional referees then the employer should be able to assume that the data subject has given a consent to contact these persons named in references.

Best regards,

Kaja Puusepp

Development Director

4. *Collection of data*	
4.1. Employers should collect personal data directly from the data subject concerned. When it is necessary, lawful and appropriate to collect and process data obtained from third parties or sources, for example to obtain professional references, the data subject should be informed and his or her consent should be obtained.	4.1. Employers should collect personal data directly from the data subject concerned. When it is necessary, lawful and appropriate to collect and process data obtained from third parties or sources, for example to obtain professional references, the data subject should be informed and his or her consent should be obtained. If during the process of recruitment the data subject provides the employer with contacts of professional referees then the employer should be able to assume that the data subject has given a consent to contact these persons named in references.
4.2. Personal data collected by employers for employment purposes should be relevant and not excessive, having regard to the nature of employment as well as the legitimate needs of the employer in connection with its activities.	
4.3. Employers should refrain from seeking to obtain access to employees' private data which is not necessary for assessment of his ability to carry out the duties and responsibilities of the job concerned.	
4.4. In case of online data that is publicly accessible, the employer should take appropriate measures to ensure that, only relevant, accurate and up-to-date data are used, thus avoiding misuse or unfair processing of that data in respect of their origin.	
4.5. Health data may only be collected and processed for the purposes set out in principle 9.2 of this Recommendation.	

ITALY / ITALIE

We support the draft Recommendation that reflects the purpose of modernizing data protection in an area, such as employment, which has undergone significant changes during the last few decades, in particular in respect of globalisation and new technologies.

We transmit few additional comments in respect of the latest version of the document that was circulated among T-PD members:

Principle 3.3: It may advisable to specify, at least in the Explanatory memorandum, that according to such principle appropriate simplified solutions should be adopted in small-scale working environments. By doing so, the principle would better reflect the title of the principle which explicitly refers to “simplification”.

3.4 There is probably no need to include data security among general principles considering that a specific section (principle 12) is devoted to that.

7.2 . Nowadays ICTs are the ordinary means for communication. Confidentiality for trade union communications could be be stated as a general principle without referring specifically to ICTs.

8.2 b it is doubtful that consent can represent the correct legal basis for communication of personal data to public bodies.

8.2.c “*determined* by domestic law” is not the correct wording. (“provided for by domestic law”?)

8.4 It may be advisable to consider additional safeguards in respect of the disclosure of personal data to ensure government transparency and/or to monitor the correct use of public resources. Specific reference may be done to the need to: a) identify the type of relevant information that could be disclosed; b) prevent sensitive data from being disclosed; c) avoid time-unlimited availability by determining proportionate time limits; d) consider the issue of availability of such information through external search engines.

9.4 The second sentence of principle 9.4 refers to genetic data that “relate directly to the ability of the employee concerned“. Are we sure that are genetic data that are strictly related to the employee’s capability? Do we have examples for that? Is it appropriate to provide that the communication of health/genetic data is given to personnel administration?

9.6 we would suggest the deletion of this principle: a) it is not clear to which kind of situations it refers to; b) some confusion is caused by terminology (are “data subject” and “employee” the same person?) c) it is probably too paternalistic to provide that the access to health/genetic data exercised by the data subject should be restricted in case such access could cause serious harm to the data subject.

18.2 Security and proportionality are general principles which apply to any data processing. We would suggest here to refer to ”strict” requirements of security and proportionality. Moreover, as WP29 stated in Opinion 3/2012, centralised storage of biometric data increases both the risk of the use of biometric data as a key to interconnect multiple databases and the specific dangers of the reuse of such data for incompatible purposes. Principle 18.2 could be therefore strengthened

by requesting that a careful assessment (rather than “consideration”) should be carried out in respect of storage of data, taking into account appropriate safeguards and security measures to avoid unlegitimate access to data, and showing a preference for alternative systems based on media made available solely to the individual concerned rather than central databases.

19. Principle 19 states that recourse to tests and similar procedures should only conducted when strictly necessary. It may be advisable to add that such necessity test should be related to the type and nature of the job activity, and add some additional safeguards, also in respect of the content of such tests, in particular by stating that only data that are strictly relevant for the pursued purpose should be processed.

draft recommendation	Amending proposals
Part I – General principles **1. *Scope and definitions*** 1.2. The principles set out in this recommendation apply to any collection and processing of personal data for employment purposes in both the public and private sectors. 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 the duties relating to those contracts. 1.3. For the purposes of this recommendation: - 'Personal data' means any information relating to an identified or identifiable individual ("data subject"); - 'Data processing' means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, 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,	Taking into account that "data collection" is activity covered by definition "data processing" (item 1.3.) it would be reasonable to delete words of "collection and" and to add provisions related to further processing of personal data as follows: **1.1. The principles set out in this recommendation apply to any processing of personal data for employment purposes in both the public and private sectors and to further processing of these data.** It is important that further processing of personal data have to be related with the primary purposes of data processing and upon giving of consent of data subject.

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; - 'Recipient' means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available, including when a transfer of data abroad is made through a service provider; - 'processing of sensitive data' covers the processing of genetic data, personal data concerning offences, criminal convictions and related security measures, the processing of biometric data uniquely identifying a person, as well as the processing of 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 of employees, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, as well as planning and organisation of work. The consequences of the contractual relationship may extend beyond the term of the contract of employment.	Taking into consideration that after the employee leaves the job data should partly processed or stored by the employer (for example for the purpose to present evidence to the tax administrator or etc.) the word of "dismissal" should be included as follows: "which relate to recruitment **and dismissal"** of employees." Also provisions related to the principles, scope of

	collected data of employee have to be deleted or stored certain period might be included to the Recommendation.
- 'Employer' means any natural or legal person who engages physical persons to perform required tasks in exchange of a salary and has the legal responsibility for the undertaking and/or establishment; - 'Employee' means any person engaged by an employer under a subordination relationship.	It is recommend the concept of "employee" to relate with data subject, that's employee first of all is data subject and then any person <…>.
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, also to allow the free development of employees' personality and to foster possibilities of individual and social relationship on the workplace.	
3. *Application of data processing principles: minimisation, accountability, simplification and data security* 3.1. Employers should minimise the collection and use of directly identifying data to only the data that necessary to the aim pursued in the individual cases concerned and should anonymise data when possible. 3.2. Employers should develop appropriate measures, including organisational ones, 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. 3.3. The measures that employers should adopt will depend on volume of the processing, the nature of the data concerned, the type of the activities being undertaken, and should also take into account possible consequences for data subjects. 3.4. When using ICTs for the collection and	Provisions relating to anonimisation of personal data should also be applied to the data transfer (When there no needs to transfer personal data of employee, anonymised data have to be transferred).

processing of personal data for employment purposes, employers shall ensure adequate data security.	
4. *Collection of data* 4.1. Employers should collect personal data directly from the data subject concerned. When it is necessary, lawful and appropriate to collect and process data obtained from third parties or sources, for example to obtain professional references, the data subject should be informed and his or her consent should be obtained. 4.2. Personal data collected by employers for employment purposes should be relevant and not excessive, having regard to the nature of employment as well as the legitimate needs of the employer in connection with its activities. 4.3. Employers should refrain from seeking to obtain access to employees' private data which is not necessary for assessment of his ability to carry out the duties and responsibilities of the job concerned. 4.4. In case of online data that is publicly accessible, the employer should take appropriate measures to ensure that, only relevant, accurate and up-to-date data are used, thus avoiding misuse or unfair processing of that data in respect of their origin. 4.5. Health data may only be collected and processed for the purposes set out in principle 9.2 of this Recommendation.	The proposal is to define the wording of "consent of employee" clearly, what consent have to be obtained from employee (for example, informed, unambiguous and etc.), when employer intend to process personal data and/or sensitive data of data subject. The same remark applies to points 6.4, 8.2 a, 8.3 of Draft.
5. *Storage of data* 5.1. The storage of personal data is permissible only if the data has been collected in accordance with the requirements outlined in principles 4, 9, 14 to 20 and if the storage is intended to serve employment purposes. Where this is not the case, the employer should refrain from using the data. 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. Such data should be relevant, adequate, accurate and	Since the employee's data can be stored short or long term (all life) by employer it is reasonable to foresee that data subject have to know about storage of his/her data and which entities stored his/her data.

non-excessive.	
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 is to be processed (including correlated and/or analysed) 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 the different context and to ensure that they are not used in a manner incompatible with the original purpose. Where important decisions affecting an employee are to be taken based on the processed data, he or she should be informed. 6.4. Without prejudice to principle 8, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principle of purpose specification in the subsequent use of the data. Where substantive changes in the processing occur, the persons concerned should be informed. The consent of the employee may also be required in appropriate cases as safeguard.	
7. ***Communication of data to employee's representatives*** 7.1. In accordance with domestic law and practice, or the terms of collective agreements, some personal data may be communicated to employees' representatives, but only to the extent that such data is necessary to allow those representatives to properly represent the interests of the employees concerned. 7.2. The use of ICTs for trade union communications should be subject to appropriate agreements that set out, in advance, transparent rules prescribing their use and safeguards to protect confidential communications.	The proposal is to harmonize the word of "communication" with the concept of "data processing" (for example, transferring, disclosing or other word).
8. ***External communication of data*** 8.1. Personal data collected for employment	The proposal is to harmonize the word of "communication" with the concept of "data processing" (for example, transferring, disclosing

purposes should only be communicated to public bodies acting in, and for the purposes of carrying out their official functions, 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 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 authorised or determined by domestic law (in particular where necessary for court proceedings). 8.3. Where adequate safeguards are provided by domestic law, personal data can be communicated among a group of companies for the purpose of discharging obligations created by law or collective agreements. The consent of the employee may also be required in appropriate cases as additional safeguard. 8.4. With regard to the public sector, other instruments providing for disclosure of personal data to ensure government 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. In particular, the legislation should contain provisions that require full respect of the principle of purpose specification and limit disclosure to relevant personal data.	or other word). It is considered whether the point 8.2.a of Draft can't be a lawful ground for data transfer to public bodies for other purposes as such, since when the data are transferred with the employee's consent or transferring is authorized by domestic law, in both cases the employer have to evaluate that other purposes have not to be incompatible with the purposes for which the data originally collected. The proposal is to delete this point a and provisions concerning compatibility of purpose foresee in point 8.2 first sentence of Draft. There can be other lawful grounds for data transfer to public bodies for other purposes, such as a contract to which the data subject is party is being concluded or performed; processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party to whom the personal data are disclosed, unless such interests are overridden by interests of the data subject.
9. *Processing of sensitive data* 9.1 The processing of personal data referred to in Article 6 of Convention 108 is only possible in particular cases, where it is indispensable for the specific recruitment or to fulfil legal obligations related to the contract of employment. The processing is also conditional on the applicable law providing additional appropriate safeguards,	The proposal is to foresee provisions regarding processing of personal data concerning offences, criminal convictions and related security measures, since there are provisions concerning processing of biometric data, genetic data, health data and etc. and such data can be collected by the employer.

complementing those set out in Convention 108. Appropriate safeguards shall aimed 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 paragraph 18 of this Recommendation. 9.2. An employee or job applicant may 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; - to safeguard the vital interest of the data subject; - to allow social benefits to be granted**;** or - to satisfy judicial procedures. The processing of genetic data, to determine for instance the professional suitability of employees or job applicants, even with the consent of the person concerned, is prohibited. Processing of genetic data may exceptionally be authorised if it is provided by domestic law and subject to appropriate safeguards, for health reasons and 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, may not be collected from third parties or sources other than the employee concerned except if otherwise determined by law, with appropriate safeguards. 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. Such data must either relate directly to the ability of the employee concerned to exercise his or her duties, or be necessary in support of measures to protect the employee's health or to prevent risks to others. Where such data are communicated to the employer, this should be to a holder of a duly authorised role such as personnel administration, health and safety at work. 9.5. Health data covered by medical confidentiality and - where their processing is lawful - genetic data, 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 data subject's right of access to his or her health data and genetic data should not be restricted unless access to such data could cause serious harm to the data subject. In such cases, the data may 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 and such collection is lawful and authorised by a data protection authority, or the collection is mandatory according to the law.	
10. *Transparency of processing* 10.1. Employees should be provided with information concerning the personal data that is held by his or her employer. This information can be provided directly or via his or her 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 Article 8 of Convention 108, 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 and its possible use, including indirect monitoring. 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.	The proposal is to foresee under which conditions (cases) such indirect monitoring is possible and also that the data subject have to be informed about such monitoring.
11. *Right of access, rectification and to object* 11.1. Employees should be able to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her. The communication 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. 11.2. The right of access should also be guaranteed in respect of evaluation data, including where such data relates 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. 11.3. 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. 11.4. Un employee should also be able to obtain, on request, information regarding the reasons for data processing, the results of the processing and how they have been applied to him. Employees should also be entitled to have personal data rectified or erased, if they are inaccurate and/or if the data has been processed contrary to the law or the principles set out in this recommendation. 11.5 The employer should introduce general procedures to ensure that there is an adequate and prompt response where the right of access and rectification are exercised, in particular in large-scale entities or entities spread out across the country. 11.6. Derogations to the rights referred to in paragraph 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 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 close 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 or to exercise the right 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.	According to Article 9 of the Convention the proposal is to add the point 10 of Draft, foreseeing derogation to the data subject's right to know (be informed) about the processing of his personal data. Also there is no mentioned the data subject's right to object to the processing of his personal data in the draft; is it possible to object to the processing of personal data; whether data subject can withdraw his/her consent or not to the processing

	of his personal data. According to this the proposal is to supplement the Draft.
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. 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.	The proposal is to foresee that further data transferring to third parties have to be ensured by using adequate technical and organizational measures.
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 paragraph 1.3 or is required in the interests of a present or former employee. 13.2. Personal data submitted in furtherance of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made. 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, the data should only be stored for the shortest possible period and for only as long as it is necessary. 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 must, in principle, be deleted in due time, 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 the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted where it leads to the monitoring of a specific employee, or a specific group of employees. 14.2 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, safety or work organisations. Before any monitoring can occur, or in circumstances where such monitoring may change, employees' representatives need to be consulted. 14.3 In the event of dispute or legal proceedings, employees should be able to obtain copies of the recording made.	The point 14 of Draft have to be clearly regulated foreseeing under which cases (purposes) such monitoring of employees is permitted or not available (for example in which places (dressing room, toilets, reception and etc.) video surveillance is not permitted or necessary), further using of recorded data and for what purposes (or maybe they can't be used for other purposes), information provided to the data subject concerning using such systems and technologies for the monitoring of employees. In point 14.2 of Draft it is proposed to add words "the rights and freedoms of employees or other persons" after the words "work organizations".
15. Internal reporting mechanism Where employers are obliged by law or internal rules to implement internal reporting mechanisms, such as hotlines, employers should secure protection of personal data of all parties involved. In particular, employers should ensure the confidentiality of the employee who reports on illegal or unethical conduct (e.g. a whistleblower). Personal data of the parties involved should be used solely for the purpose of appropriate internal procedures relating to the report, law or judicial order. Where applicable, employers should enable anonymous reporting. However, internal investigations should not be carried out on the sole basis of an anonymous report, except where it is circumstantiated and relates to serious domestic law infringements.	
16. Use of Internet and e-mails in the workplace 16.1 The employer should avoid unjustifiable	

and unreasonable interferences with employee's right to private life. This principle extends to all aspects of an employee's employment, including his or her use of any computer, smartphone or other digital device, either in the framework of the employer's intranet, extranet, or by using directly the internet or not, made available by the employer. It applies whether the device used by the employee is provided by the employer or the employee himself or herself. The persons concerned should be properly and periodically informed, through a clear privacy policy. The information provided should be kept up to date. This should be done taking into consideration principle 10 of the recommendation. The information should include the purpose of the processing, the preservation or back-up period of connection 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 of the existence of that possibility can only occur in accordance with the law and where strictly necessary for security, operational or other lawful reason, such as to monitor infringements to intellectual property of the employer. 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 absolute professional necessity. Further, this 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 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 the necessary safeguards for the employee's right to privacy and protection of personal data. Employers shall in particular pay special attention to the purpose for which such devices are used. Notably, monitoring should not be the main purpose, but only an indirect consequence of action needed to protect production, safety or work organisations. 17.2 When an employee, following his or her employer's instructions or with the knowledge and approval of his or her employer, uses professional devices outside the company or institution premises, and by virtue of that use the employer acquire knowledge of the employee's location, the collection and further processing of that personal data must be exclusively limited to the strict verification of the fulfilment of professional duties or organisational aspects. 17.3 Employers shall apply appropriate internal procedures relating to the processing of that data and shall notify it to the persons concerned in advance.	In point 17.1 of Draft it is proposed to add words of "the rights and freedoms of employees or other persons" after the words of "work organizations". The formulation of "exclusively limited to the strict verification" is evaluative nature and there have to be a concrete way such as agreement with employee, or regulated by rules of ethics.
18. Biometric data 18.1 The collection and further processing of biometric data should only be undertaken when it	

is necessary to protect the legitimate interests of the employer, employees or third parties, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards. 18.2 The processing of biometric data shall be subject to the requirements of security and proportionality. In this regard, careful consideration should be given to the implications of storage in a central database or alternative systems based on media made available solely to the individual concerned.	
19. Psychological tests, analyses and similar procedures Recourse to tests, analyses 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 conducted when strictly necessary. They should not take place without the employees or job applicants consent, and domestic law should provide appropriate safeguards. The employee's consent should be free, informed and without any financial or other compensation foreseen. The employee or job applicant should be informed in advance of the use that will be made of the results of these tests**,** analyses or similar procedures and, subsequently, the content thereof.	
20. Other processing posing specific risks to employees' rights 20.1 Employer or where applicable processors, should carry out a risk analysis of the potential impact of the intended data processing on the employee's rights and fundamental freedoms and design data processing operations in such a way as to prevent or at least minimise the risk of interference with those rights and fundamental freedoms. 20.2 Unless domestic law or practice provides other appropriate safeguards, the agreement of employees' representatives should be sought before the introduction or adaptation of ICTs where the information or consultation procedure referred to in principle 14 reveals such risks.	

21. Obligations of the employer For all particular forms of processing, set out in Part II of this Recommendation, the employer should ensure that appropriate measures are taken to secure the respect of the following obligations: • 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 the persons concerned in advance. • Consult employees' representatives in accordance with domestic law or practice and, where appropriate, with the relevant collective agreements. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, their agreement should be sought. • Consult before the processing the national supervisory authorities.	
Other comments	The proposal is to add provisions concerning transfer of personal data of employees to third countries in the Part I of Draft. It's debatable whether these guidelines should include provisions relating to the direct marketing, for example offering goods and services to the employee by employer or transferring of direct marketing massages with personal data of employee to third parties.

MONTENEGRO

MONTENEGRO
MINISTRY OF INTERIOR
Section for Personal Data Protection
and Free Access to Information
08 No
Podgorica, 23 August 2013

THE CONSULTATIVE COMMITTEE OF THE CONVENTIONFOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

STRASBOURG

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

The Ministry of Interior - Section for Personal Data Protection and Free Access to Information, as the Ministry responsible for personal data protection in Montenegro, examined the Draft Recommendation on the protection of personal data used for employment purposes.

Taking into account the issue addressed by the Draft Recommendation as significantly important, Montenegro welcomes the timeliness and comprehensiveness of the Draft Recommendation, and it considers that within the scope of personal data processing done by every individual county, it is necessary to further harmonise mutual practice aimed at achieving the largest possible extent of complementarity of the procedure in the Council of Europe member states. It is necessary to regulate this issue precisely, so as to present the high-quality contribution to the human rights protection system and provide supremacy of the rights in this sensitive field.

Concerning concrete proposals, we would like to point out the following:

- In regard to Part I – General principles, Montenegro has no remarks. We consider the topic properly covered, and the terms used present clear and logical sequence which properly conveys the message concerning general principles addressed in the given field;

- In regard to Part II - Particular forms of processing, I suggest the following:

- item 9.3 following the wording: “with appropriate safeguards“, the following should be added: “or if the individual gave explicit consent.“ We believe that in such a way active participation of the individual would be ensured in processing his/her data, as in addition to the legality principle, the consent principle would also be introduced, thus completing this issue;

- following the item 11.9, item 11.10 should be added worded as follows: “An employee has the right to know who and for which purposes used his/her data.“

- following the item 14.1, item 14.2 should be added worded as follows: “An employee shall sign the notification that he/she is informed on introducing ICTs.“

Finally, on behalf of Montenegro I would like to address appreciation to the Consultative Committee Secretariat for their support and excellent coordination, thus significantly contributing to the quality of the activities of our Committee. Montenegro remains open for further communication aimed at reaching the largest possible consensus in regard to this issue, thus providing grounds for more efficient and effective planning of activities in the field of data protection.

Please accept the assurances of my highest consideration.

HEAD

Zora Čizmović

NORWAY / NORVÈGE

DRAFT RECOMMENDATION	AMENDING PROPOSALS
Part I – General principles **1. *Scope and definitions*** 1.3. The principles set out in this recommendation apply to any collection and processing of personal data for employment purposes in both the public and private sectors. 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 the duties relating to those contracts. 1.3. For the purposes of this recommendation: - 'Personal data' means any information relating to an identified or identifiable individual ("data subject"); - 'Data processing' means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, 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 ;	With the increased number of definitions included in the instrument, we propose that the definitions are set out in a separate provision (1*bis*), in order to obtain a more systematic structure
- '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; - 'Recipient' means a natural or legal person, public authority, service, agency	

or any other body to whom data are disclosed or made available, including when a transfer of data abroad is made through a service provider; - 'processing of sensitive data' covers the processing of genetic data, personal data concerning offences, criminal convictions and related security measures, the processing of biometric data uniquely identifying a person, as well as the processing of 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 of employees, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, as well as planning and organisation of work. The consequences of the contractual relationship may extend beyond the term of the contract of employment.	The definition should focus on "sensitive data" as such, and not on processing, which is defined in the second indent
- 'Employer' means any natural or legal person who engages physical persons to perform required tasks in exchange of a salary and has the legal responsibility for the undertaking and/or establishment; - 'Employee' means any person engaged by an employer under a subordination 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, also to allow the free development of employees' personality and to	

foster possibilities of individual and social relationship on the workplace.	
3. *Application of data processing principles: minimisation, accountability, simplification and data security* 3.1. Employers should minimise the collection and use of directly identifying data to only the data that necessary to the aim pursued in the individual cases concerned and should anonymise data when possible. 3.2. Employers should develop appropriate measures, including organisational ones, 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. 3.3. The measures that employers should adopt will depend on volume of the processing, the nature of the data concerned, the type of the activities being undertaken, and should also take into account possible consequences for data subjects. 3.4. When using ICTs for the collection and processing of personal data for employment purposes, employers shall ensure adequate data security.	
4. *Collection of data* 4.1. Employers should collect personal data directly from the data subject concerned. When it is necessary, lawful and appropriate to collect and process data obtained from third parties or sources, for example to obtain professional references, the data subject should be informed and his or her consent should be obtained. 4.2. Personal data collected by employers for employment purposes should be relevant and not excessive, having regard to the nature of employment as well as the legitimate needs of the employer in connection with its activities. 4.3. Employers should refrain from seeking to obtain access to employees' private data which is not necessary for assessment of his ability to carry out the duties and responsibilities of the job concerned. 4.4. In case of online data that is publicly accessible, the employer should take appropriate measures to ensure that, only relevant, accurate	The concept of "private data" appears unclear, and we question the advantages of using this term. We observe that an exemplification of data which are considered to be private is planned in the explanatory memorandum, but are not sure a categorisation of "private" and "non-private" data

and up-to-date data are used, thus avoiding misuse or unfair processing of that data in respect of their origin. 4.5. Health data may only be collected and processed for the purposes set out in principle 9.2 of this Recommendation.	is useful or even feasible. As an alternative, we propose to focus on *personal data not relevant for the particular employment situation* – thus building on a more flexible standard.
5. *Storage of data* 5.1. The storage of personal data is permissible only if the data has been collected in accordance with the requirements outlined in principles 4, 9, 14 to 20 and if the storage is intended to serve employment purposes. Where this is not the case, the employer should refrain from using the data. 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. Such data should be relevant, adequate, accurate and non-excessive.	The provision regulates employers' *storage* of data, and subsequent *use* should not be mentioned here. Any restrictions on subsequent use should instead be set out in principles 6-8
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 is to be processed (including correlated and/or analysed) 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 the different context and to ensure that they are not used in a manner incompatible with the original purpose. Where important decisions affecting an employee are to be taken based on the processed data, he or she should be informed. 6.4. Without prejudice to principle 8, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principle of purpose specification in the subsequent use of the data. Where substantive changes in the processing occur, the persons concerned should be informed. The consent of the employee may also be required in appropriate cases as safeguard.	We are worried the obligation following from point 6.2 is too onerous – in particular on small-size enterprises – and propose that it be modified, e.g. by inserting the term *"where appropriate"*
7. *Communication of data to employee's*	

representatives 7.1. In accordance with domestic law and practice, or the terms of collective agreements, some personal data may be communicated to employees' representatives, but only to the extent that such data is necessary to allow those representatives to properly represent the interests of the employees concerned. 7.2. The use of ICTs for trade union communications should be subject to appropriate agreements that set out, in advance, transparent rules prescribing their use and safeguards to protect confidential communications.	We question the value of this provision in addition to point 3.4 on data security
8. *External communication of data* 8.1. Personal data collected for employment purposes should only be communicated to public bodies acting in, and for the purposes of carrying out their official functions, 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 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 authorised or determined by domestic law (in particular where necessary for court proceedings). 8.3. Where adequate safeguards are provided by domestic law, personal data can be communicated among a group of companies for the purpose of discharging obligations created by law or collective agreements. The consent of the employee may also be required in appropriate cases as additional safeguard. 8.4. With regard to the public sector, other instruments providing for disclosure of personal	We fail to see which situations are aimed at in point 8.3, and ask that it be clarified

data to ensure government 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. In particular, the legislation should contain provisions that require full respect of the principle of purpose specification and limit disclosure to relevant personal data.	
9. *Processing of sensitive data* 9.1 The processing of personal data referred to in Article 6 of Convention 108 is only possible in particular cases, where it is indispensable for the specific recruitment or to fulfil legal obligations related to the contract of employment. The processing is also conditional on the applicable law providing additional appropriate safeguards, complementing those set out in Convention 108. Appropriate safeguards shall aimed 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 paragraph 18 of this Recommendation. 9.2. An employee or job applicant may 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; - to safeguard the vital interest of the data subject; - to allow social benefits to be granted**;** or - to satisfy judicial procedures. The processing of genetic data, to determine for instance the professional suitability of employees or job applicants, even with the consent of the person concerned, is prohibited. Processing of genetic data may exceptionally be authorised if it is provided by domestic law and subject to appropriate safeguards, for health reasons and in particular to avoid any serious prejudice to the health of the data subject or third parties.	The use of the term "possible" in this context is not appropriate, and we propose to replace it with the term *"permitted"* or a similar expression We are somewhat worried about the scope of point 9.2, and propose the following modification: "*In accordance with member state law*, an employee or job applicant may *only* be asked questions concerning his or her health and/or be medically examied …"

9.3. Health data and - where their processing is lawful - genetic data, may not be collected from third parties or sources other than the employee concerned except if otherwise determined by law, with appropriate safeguards. 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. Such data must either relate directly to the ability of the employee concerned to exercise his or her duties, or be necessary in support of measures to protect the employee's health or to prevent risks to others. Where such data are communicated to the employer, this should be to a holder of a duly authorised role such as personnel administration, health and safety at work. 9.5. Health data covered by medical confidentiality and - where their processing is lawful - genetic data, 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 data subject's right of access to his or her health data and genetic data should not be restricted unless access to such data could cause serious harm to the data subject. In such cases, the data may 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 and such collection is lawful and authorised by a data protection authority, or the collection is mandatory according to the law.	It is unclear to us what situations are aimed at in point 9.7, and we ask for further elaboration
10. *Transparency of processing* 10.1. Employees should be provided with information concerning the personal data that is held by his or her employer. This information can be provided directly or via his or her representative. Except in relation to employees' name and habitual residence or establishment, employers should provide employees with the following information:	In order to avoid the obligation becoming too onerous, it should be specified that the right to receive information only applies *"upon request"*

- 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 Article 8 of Convention 108, 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 and its possible use, including indirect monitoring. 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.	

POLAND / POLOGNE

We welcome proposed amendments, which greatly expand existing provisions, and thus enhance the protection of rights of employees. We would like nevertheless, present some remarks.

To begin with the question of appropriate legal basis, we suggest that in point 3.1., relevant reference should be made in order to raise the awareness of the employers, that they can collect data only if there is a proper legal basis. This would also seem complementary to the mentioned rules of necessity as well as data minimisation. The amendment wording would be as follows: *"Employers should minimise the collection and use of directly identifying data to only the data that* ***is*** *necessary to the aim pursued in the individual cases concerned,* ***where relevant in line with additional conditions and safeguards set out in internal law,*** *and should anonymise data when possible."* Similarly in point 4.2., the abovementioned amendment seems justified: "*Personal data collected by employers for employment purposes* ***where relevant in line with additional conditions and safeguards set out in internal law*** *should be relevant and not excessive, having regard to the nature of employment as well as the legitimate needs of the employer in connection with its activities."* The abovementioned remark is also true in relation with psychological tests, analyses and similar procedures, as stated in point 19. Our proposition would be: *"Recourse to tests, analyses 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 conducted when strictly necessary* ***where relevant in line with additional conditions and safeguards set out in internal law****."*;

Secondly, we are of the opinion, that the point 8.2. a) seems to be a little bit too vague. It says, that: *"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: where 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".* It results from the above, that it is possible to disclose to wide range of entities personal data of the employees, once the purpose is not incompatible and they have been informed. It seems that there could exist additional obligations, such as obligation of having written agreement, at least in the EU member states. Therefore, some reference to applicable law or to the protection of rights of data subject. The proposed wording could be as follows: "*where the communication is necessary for employment p0urpose, the purposes are not incompatible with the purposes for which the data was originally collected, the employees concerned or their representatives, as the case may be are informed of this,* ***where relevant in line with additional conditions and safeguards set out in internal law."***

Additionally, it could be also worth consider, to indicate in an explanatory memorandum, with relation to point 18.2. concerning biometric data, that in case of processing of such data, due consideration should be paid to the question of selection of possibly less intrusive category of biometric data. In order to avoid such threats as for instance revealing of health condition.

SWEDEN / SUEDE

Sweden's General comments regarding the revisited draft of the Recommendation on the protection of personal data used for employment purposes

1. In order for the Recommendation to remain valid despite the constant development of new technologies the Recommendation should not be too detailed and, to the extent possible, neutral as regards the technology. The current draft is still quite detailed and certain provisions still has too much focus on specific technologies (for example e-mails, Internet and intranets). Hence, there is a risk that the Recommendation will quite quickly be outdated. *It should therefore be considered to move such provisions to the Explanatory Memorandum*. The high amount of details could also make the recommendation difficult to understand and apply for employers, employees and representatives**.**

2. In some articles the consent of the employee is required. To use the employee's consent as a legal basis for processing may be problematic as the employee is often in a position of dependence in relation to the employer. It may, thus, be put in question to what extent an employee may provide a freely given consent. It should therefore be considered to require another legal basis such as the weighing of the interest between the employer's need to process data on one hand and respect for the employee's privacy on the other hand (as provided for in article 7 f of directive 95/46/EC).

3. In some aspect,the Recommendation contains rules that are not primarily data protection issues, but rather issues of privacy in working life in a broader perspective. It is questionable whether it is appropriate to add such rules in this Recommendation. This needs in any case to be clarified.

4. As a general remark to the use expressions such as "domestic law", "regulated by law", "legal obligations" etc throughout the Recommendation Sweden would like to draw attention to the fact that labour market issues in Sweden, according to long-standing tradition, mainly are regulated by the parties on the labour market through collective agreements. Moreover, case-law from the Labour Court is of great importance since it often delivers generally applicable rulings with guiding principles and establishes general legal principles. Therefore, where the Recommendation says domestic law, laid down by law, lawfully, regulated etc this will in Sweden be interpreted as also covering collective agreements, general legal principles and guiding case-law. *This should be described in the Explanatory Memorandum*. The Swedish system has in fact been tried by the ECtHR in a decision as to the admissibility of an application (no 46210/99 by Inga-Lill Wretlund).

Although the obligation in question (to submit to drug testing as was the case in question) did not follow from legislation, the ECtHR observed that labour market issues are, according to long-standing tradition in Sweden, mainly regulated by the parties on the labour market through collective agreements. The ECtHR noted that the employer's right to manage and organise the work is a principle agreed upon by those parties and the Labour Court had established that this right constitutes a general legal principle. According to the Labour Court's case-law, the employer may have a right to carry out control measures as part of the right to manage and organise the work. The Labour Court had concluded, before the events of the present case, that such control measures could include drug and alcohol tests. Also in the judgment in the present case, the Labour Court considered that the tests in question were naturally connected with activities of the company in question and that the right to order employees to undergo such tests therefore could be seen as part of the company's right to manage and organise the work according to the central collective agreement.

In these circumstances, the ECtHR was satisfied that the measure challenged by the applicant had a sufficient basis in Swedish law and thus was “in accordance with the law” within the meaning of Article 8 § 2 of the Convention.

DRAFT RECOMMENDATION	AMENDING PROPOSALS
Part I – General principles **1.** ***Scope and definitions*** **1.4.** The principles set out in this recommendation apply to any collection and processing of personal data for employment purposes in both the public and private sectors.	
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 the duties relating to those contracts.	**Question**: Does the sentence " *to help employers discharge the duties*" refers to the competency match or does it also include other measures, e.g. financial assistance given to enable a job? The meaning of this sentence need to be further explained.
1.3. For the purposes of this recommendation: - 'Personal data' means any information relating to an identified or identifiable individual ("data subject"); - 'Data processing' means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, 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; - '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; - 'Recipient' means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available, including when a transfer of data abroad is made	**Question**: The scope of "*where no automated processing is used"* seems to be wider than the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. What is the reason? .

through a service provider;

- ‘processing of sensitive data’ covers the processing of genetic data, personal data concerning offences, criminal convictions and related security measures, the processing of biometric data uniquely identifying a person, as well as the processing of 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 of employees, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, as well as planning and organisation of work. The consequences of the contractual relationship may extend beyond the term of the contract of employment.

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, also to allow the free development of employees’ personality and to foster possibilities of individual and social relationship on the workplace.

2XX - *Public access to official documents*	***Public access to official documents*** **(New article) :**
	Sweden would like to propose a new article regarding the public access to official documents. 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 public access to such official documents with the right to the protection of personal data pursuant to this Recommendation. **Justification:** The principle of public access to official documents means that the public has the right to access official documents. This principle shall not be infringed if there is no ground to withhold information in public documents. In Sweden this principle is protected by the constitution.
3. *Application of data processing principles: minimisation, accountability, simplification and data security*	
3.1. Employers should minimise the collection and use of directly identifying data to only the data that necessary to the aim pursued in the individual cases concerned and should anonymise data when possible.	
3.2. Employers should develop appropriate measures, including organisational ones, 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.	
3.3. The measures that employers should adopt will depend on volume of the processing, the nature of the data concerned, the type of the activities being undertaken, and should also take into account possible consequences for data subjects.	

3.4. When using ICTs for the collection and processing of personal data for employment purposes, employers shall ensure adequate data security.	
4. *Collection of data* 4.1. Employers should collect personal data directly from the data subject concerned. When it is necessary, lawful and appropriate to collect and process data obtained from third parties or sources, for example to obtain professional references, the data subject should be informed and his or her consent should be obtained.	4.1. Employers should, when appropriate, collect personal data directly from the data subject concerned or when it is necessary, lawful and appropriate, collect and process data obtained from third parties or sources, for example to obtain professional references. ~~the data subject should be informed and his or her consent should be obtained~~ **Justification**: It should be considered whether the current wording of article 4.1 may lead to unrealistic results. For example, does it prevent a company from collecting information on a person it whishes to "headhunt" before approaching this person with an offer (the current wordin requires consent or prior information)?
4.2. Personal data collected by employers for employment purposes should be relevant and not excessive, having regard to the nature of employment as well as the legitimate needs of the employer in connection with its activities.	
4.3. Employers should refrain from seeking to obtain access to employees' private data which is not necessary for assessment of his ability to carry out the duties and responsibilities of the job concerned.	
4.4. In case of online data that is publicly accessible, the employer should take appropriate measures to ensure that, only relevant, accurate and up-to-date data are used, thus avoiding misuse or unfair processing of that data in respect of their origin.	

4.5. Health data may only be collected and processed for the purposes set out in principle 9.2 of this Recommendation.	**4.5 Question**: With reference to the principles in article 9, Sweden wonder if the possibility of collecting health data for health and safety statistics fits within the current wording. For the preventive work environment and in order to avoid accidents and occupational diseases it is important that health data can be collected to form the basis of work environment statistics.
5. *Storage of data*	
5.1. The storage of personal data is permissible only if the data has been collected in accordance with the requirements outlined in principles 4, 9, 14 to 20 and if the storage is intended to serve employment purposes. Where this is not the case, the employer should refrain from using the data.	**Suggestion:** 5.1. The storage of personal data is permissible only if the data has been collected in accordance with the requirements outlined in principles 2x, 4, 9, 14 to 20 and if the storage is intended to serve employment purposes. Where this is not the case, the employer should refrain from using the data. **Justification:** The last sentence of the article stipulates that the employer shall refrain from using personal data in circumstances other than those contained in the first sentence. Information about individuals may appear in public documents of the Swedish authorities. Provisions which contain restrictions on use that are focused on personal data may in some cases be interpreted as prohibiting the disclosure of public documents. It is therefore important that the recommendation is designed to clarify that the restriction does not constitute such an obstacle. If it is so that the restriction only applies to the Authority's use of the data in their activities and not the right of the public to access the data than the article should not pose a problem
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. Such data should be relevant, adequate, accurate and non-excessive.	
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 is to be processed (including correlated and/or analysed) 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 the different context and to ensure that they are not used in a manner incompatible with the original purpose. Where important decisions affecting an employee are to be taken based on the processed data, he or she should be informed.	
6.4. Without prejudice to principle 8, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principle of purpose specification in the subsequent use of the data. Where substantive changes in the processing occur, the persons concerned should be informed. The consent of the employee may also be required in appropriate cases as safeguard.	
7. *Communication of data to employee's representatives*	
7.1. In accordance with domestic law and practice, or the terms of collective agreements, some personal data may be communicated to employees' representatives, but only to the extent that such data is necessary to allow those representatives to properly represent the interests of the employees concerned.	7.1. In accordance with domestic law and practice, or the terms of collective agreements, some personal data may be communicated to employees' representatives, but only to the extent that such data is necessary to allow those representatives to properly represent the interests of the employees concerned or if necessary for the fulfilment and supervision of obligations laid down in collective agreements. **Justification**: According to long-standing tradition in Sweden, labour market issues are, mainly regulated by the parties through collective agreements. In our system the trade unions thus have right to access to data in order to be able to control the fulfilment of the obligations in the collective agreements not only for single employees but also in order to be able to monitor the application and enforcement of the system as such.

7.2. The use of ICTs for trade union communications 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, and for the purposes of carrying out their official functions, 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 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 authorised or determined by domestic law (in particular where necessary for court proceedings).	
8.3. Where adequate safeguards are provided by domestic law, personal data can be communicated among a group of companies for the purpose of discharging obligations created by law or collective agreements. The consent of the employee may also be required in appropriate cases as additional safeguard.	

8.4. With regard to the public sector, other instruments providing for disclosure of personal data to ensure government 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. In particular, the legislation should contain provisions that require full respect of the principle of purpose specification and limit disclosure to relevant personal data.	**Suggestion:** *The second sentence in 8.4 should be deleted* With regard to the public sector, other instruments providing for disclosure of personal data to ensure government 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. ~~In particular, the legislation should contain provisions that require full respect of the principle of purpose specification and limit disclosure to relevant personal data.~~ **Justification:** It is unclear whether the second sentence implies a restriction of the principle of public access to official documents. There is therefore a risk that the right of access to official documents, which in Sweden is constitutionally protected, can be restricted. The second sentence should for that reason be deleted
9. *Processing of sensitive data*	
9.1 The processing of personal data referred to in Article 6 of Convention 108 is only possible in particular cases, where it is indispensable for the specific recruitment or to fulfil legal obligations related to the contract of employment. The processing is also conditional on the applicable law providing additional appropriate safeguards, complementing those set out in Convention 108. Appropriate safeguards shall aimed 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 paragraph 18 of this Recommendation. 9.2. An employee or job applicant may 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;	

	New paragraph *(c).* to guarantee an appropriate rehabilitation or in any other way comply with work environment requirements **Justification:** A new paragraph regarding rehabilitation and work environment is necessary. An employer must sometimes treat health data in order to fulfill its obligations with regard to occupational health and rehabilitation
- to safeguard the vital interest of the data subject;	~~c~~ d~~.~~;
- to allow social benefits to be granted**;** or	~~d~~ e
- to satisfy judicial procedures	~~E~~ f
The processing of genetic data, to determine for instance the professional suitability of employees or job applicants, even with the consent of the person concerned, is prohibited. Processing of genetic data may exceptionally be authorised if it is provided by domestic law and subject to appropriate safeguards, for health reasons and 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, may not be collected from third parties or sources other than the employee concerned except if otherwise determined by law, with appropriate safeguards.	
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. Such data must either relate directly to the ability of the employee concerned to exercise his or her duties, or be necessary in support of measures to protect the employee's health or to prevent risks to others. Where such data are communicated to the employer, this should be to a holder of a duly authorised role such as personnel administration, health and safety at work.	**Question and modification:** Sweden would like a clarification on what is covered by "*Medical confidentiality."* The wording could pose a problem if the medical information only can be handled by personnel who are bound by "medical confidentiality". For example; Swedish employment Agency handles a variety of information of a medical nature, such as to facilitate people with disabilities access to employment. Personnel at the Employment agency are not bound by "medical confidentiality"; they are instead bound by other provisions on confidentiality such as The Public Access to Information and Secrecy Act (Offentlighets- och sekretesslagen 2009:400). Sweden would therefore like to suggest the

	following **modification** on 9.4 *first sentence:* 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 by others who, in accordance with domestic law, may have access to such data.
9.5. Health data covered by medical confidentiality and - where their processing is lawful - genetic data, 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.	**Question:** A clarification is needed on the wording "should be stored separately from other categories of personal data". Can health data be stored on the same database as other personal data?
9.6. The data subject's right of access to his or her health data and genetic data should not be restricted unless access to such data could cause serious harm to the data subject. In such cases, the data may be communicated to the employee through a medical practitioner of his or her choice.	**Modification:** The data subject's right of access to his or her health data and genetic data should not be restricted unless access to such data could cause serious harm to the data subject. Any such restriction must be in accordance with domestic law. In such cases, the data may be communicated to the employee through a medical practitioner of his or her choice. **Justification:** It is not possible under Swedish law, as a general rule, to prevent individuals to have access to information about them. This right to access, which also serves to protect the privacy of individuals, should therefore not be limited if it is otherwise provided by domestic law.
9.7. In any circumstances health data related to third parties will not be processed unless full unambiguous informed consent is given and such collection is lawful and authorised by a data protection authority, or the collection is mandatory according to the law.	

10. *Transparency of processing*	
10.1. Employees should be provided with information concerning the personal data that is held by his or her employer. This information can be provided directly or via his or her 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 Article 8 of Convention 108, 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 and its possible use, including indirect monitoring. 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, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her. The communication 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.	**Question:** A clarification is needed in 11.1, whether the term "confirmation of the processing" means that the individual has a right to know what information is treated and not only that the data is being processed.

11.2. The right of access should also be guaranteed in respect of evaluation data, including where such data relates 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.	
11.3. 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.	
11.4. Un employee should also be able to obtain, on request, information regarding the reasons for data processing, the results of the processing and how they have been applied to him. Employees should also be entitled to have personal data rectified or erased, if they are inaccurate and/or if the data has been processed contrary to the law or the principles set out in this recommendation.	
11.5 The employer should introduce general procedures to ensure that there is an adequate and prompt response where the right of access and rectification are exercised, in particular in large-scale entities or entities spread out across the country.	
11.6. Derogations to the rights referred to in paragraph 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 data subject or the rights and freedoms of others.	

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. 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 paragraph 1.3 or is required in the interests of a present or former employee.	

13.2. Personal data submitted in furtherance of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made. 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, the data should only be stored for the shortest possible period and for only as long as it is necessary.	**Article 13.2 should be deleted** since it is in conflict with the right to information according to the Swedish Discrimination Act chapter 2, Section 4 In case Article 13.2 is not deleted it has to be redrafted as follows: **13.2, third sentence**: 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 only be stored for the shortest possible period and for only as long as it is necessary. **Justification:** According to the Swedish Discrimination Act a job applicant has the right to receive written information from the employer regardless of the possibility of a future legal action. Article 13.2 is in in conflict with the Discrimination Act. **Chapter 2, Section 4** If a job applicant has not been employed or selected for an employment interview, or if an employee has not been promoted or selected for education or training for promotion, the applicant shall, upon request, receive written information from the employer about the education, professional experience and other qualifications that the person had who was selected for the employment interview or who obtained the job or the place in education or training
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 must, in principle, be deleted in due time, without prejudice to the employee's right of access up to the time at which they are deleted.	**Question:** Sweden would like a clarification on what is meant by "due time"? Repeated abuses that may lead to termination of employment must be documented for some time. All events do not take place at once. Each event may not be sufficient for termination of employment, whereas, several repeated events may constitute grounds for termination or dismissal
13.4 New paragraph.	13.4 New paragraph *Sweden would like to propose a new paragraph in accordance with the principle of the public access to official documents, as suggested in the new article 2.x.* **Suggestion:** Preservation of data must be compatible with the purpose set out in article 2.X . **Justification:** There is a risk that limitation on preservation of data laid down in paragraph 13.1-13-3 can come into conflict with the principle of public access to official documents as suggested

	in the new article 2.X.
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 the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted where it leads to the monitoring of a specific employee, or a specific group of employees.	
14.2 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, safety or work organisations. Before any monitoring can occur, or in circumstances where such monitoring may change, employees' representatives need to be consulted.	Such systems should be allowed, if legitimate necessary and regulated, ~~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, safety or work organisations. Before any monitoring can occur, or in circumstances where such monitoring may change, employees' representatives need to be consulted. ***Justification:*** There are several cases where surveillance is necessary and the proposed article that this should not in principle be permitted is not in line with existing and well-grounded needs. The article should therefore instead be formulated as seen above, i.e laying down the prerequisites under which such surveillance should be allowed.
14.3 In the event of dispute or legal proceedings, employees should be able to obtain copies of the recording made.	
15. Internal reporting mechanism Where employers are obliged by law or internal rules to implement internal reporting mechanisms, such as hotlines, employers should secure protection of personal data of all parties involved. In particular, employers should ensure the confidentiality of the employee who reports on illegal or unethical conduct (e.g. a whistleblower). Personal data of the parties involved should be used solely for the purpose of appropriate internal procedures relating to the report, law or judicial order.	

Where applicable, employers should enable anonymous reporting. However, internal investigations should not be carried out on the sole basis of an anonymous report, except where it is circumstantiated and relates to serious domestic law infringements.	
16. Use of Internet and e-mails in the workplace	
16.1 The employer should avoid unjustifiable and unreasonable interferences with employee's right to private life. This principle extends to all aspects of an employee's employment, including his or her use of any computer, smartphone or other digital device, either in the framework of the employer's intranet, extranet, or by using directly the internet or not, made available by the employer. It applies whether the device used by the employee is provided by the employer or the employee himself or herself. The persons concerned should be properly and periodically informed, through a clear privacy policy. The information provided should be kept up to date. This should be done taking into consideration principle 10 of the recommendation. The information should include the purpose of the processing, the preservation or back-up period of connection data and the archiving of electronic messages.	The employer should avoid unjustifiable and unreasonable interferences with employee's right to private life. This principle extends to all aspects of an employee's employment, including his or her use of any ~~computer, smartphone or other~~ digital device, ~~either in the framework of the employer's intranet, extranet, or by using directly the internet or not, made available by the employer.~~ **Justification:** The current article is to detailed and has too much focus on specific technologies (for example e-mails, smartphones, Internet and intranets). Hence, there is a risk that the article and the Recommendation will quite quickly be outdated. *It should therefore be considered to move such provisions to the Explanatory Memorandum and redraft the article as technical neutral as it is possible*.
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 of the existence of that possibility can only occur in accordance with the law and where strictly necessary for security, operational or other lawful reason, such as to monitor infringements to intellectual property of the employer. 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 absolute professional necessity. Further, this must be undertaken in the least intrusive way possible and only after having informed the employees concerned.	The article should be deleted. **Justification** The article can be difficult to apply in practice. It is for example difficult to determine what is work-related emails and private email before opening the email, if it does not emerge from the subject line. If the article is not deleted, Sweden would like to suggest the following **modification**: Access to professional emails of employees who have been informed of the existence of that possibility can only occur ~~in accordance with the law and~~ where ~~strictly~~ necessary for security, operational or other lawful reason, such as to monitor infringements to intellectual property of the employer. 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 ~~absolute~~ professional necessity. Further, this must be undertaken in the least intrusive way possible and only after having informed the employees concerned. **Justification:** In Sweden, the employee's right to privacy is mainly regulated by practices and principles; so is it regarding the use of emails and computers at the workplace. Regarding the wording “absolute”: It can be difficult to know the scope of “absolute” professional before the employer has access to the emails.
16.4 In any case, the content, sending and receiving of private emails at work shall not be monitored.	**Comments and question:** As mentioned in paragraph 16.3, it is difficult to determine what is work-related emails and private email if the emails are sent or received through the employer's computer or from the employer´s email account. How would this be ensured?

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 at his or her presence.	The article should be deleted **Justification**: It is not appropriate to regulate in detail how the employee´s account must be deactivated or how the content should be recover upon an employee's departure. The circumstances may often be that the employee is unable or unwilling to attend when the contents of the account are stored, but where it is nevertheless necessary to store the content of the account inter alia due to legal obligations or operational reasons. If the article is not deleted, Sweden would like to suggest the following **modification** in **the second sentence**: If the employer needs to recover the contents of the employee's account for the efficient running of the company, he shall do so in connection to ~~before~~ the departure of the employee and if possible at his or her presence
	16.6 New paragraph *Sweden would like to propose a new paragraph in accordance with the principle of the public access to official documents, as suggested in the new article 2.x (a similar new paragraph is also suggested, see 13.4).* **Suggestion:** Preservation of data must be compatible with the purpose set out in article 2.X. **Justification:** There is a risk that the paragraphs 16.1-16.5 can come into conflict with the principle of public access to official documents as suggested in the new article 2.X.
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 the necessary safeguards for the employee's right to privacy and protection of personal data. Employers shall in particular pay special attention to the purpose for which such devices are used. Notably, monitoring should not be the main purpose, but only an indirect consequence of action needed to protect production, safety or work organisations.	
17.2 When an employee, following his or her employer's instructions or with the knowledge and approval of his or her employer, uses professional devices outside the company or institution premises, and by virtue of that use the employer acquire knowledge of the employee's location, the collection and further processing of that personal data must be exclusively limited to the strict verification of the fulfilment of professional duties or organisational aspects.	**Question:** It can be difficult to draw the line of what "professional duties" and "organisational aspects" means. The meaning of this sentence may therefore need to be further explained.
17.3 Employers shall apply appropriate internal procedures relating to the processing of that data and shall notify it to the persons concerned in advance.	
18. Biometric data 18.1 The collection and further processing of biometric data should only be undertaken when it is necessary to protect the legitimate interests of the employer, employees or third parties, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards.	
18.2 The processing of biometric data shall be subject to the requirements of security and proportionality. In this regard, careful consideration should be given to the implications of storage in a central database or alternative systems based on media made available solely to	

the individual concerned.	
19. Psychological tests, analyses and similar procedures	
Recourse to tests, analyses 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 conducted when strictly necessary. They should not take place without the employees or job applicants consent, and domestic law should provide appropriate safeguards. The employee's consent should be free, informed and without any financial or other compensation foreseen. The employee or job applicant should be informed in advance of the use that will be made of the results of these tests**,** analyses or similar procedures and, subsequently, the content thereof.	Recourse to tests, analyses 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, necessary and regulated.~~be conducted when strictly necessary.~~ ~~**Justification:**~~ The article run a risk of being too strict since it does not reflect the functioning of the labour market. It should therefore be considered whether the current wording may lead to unrealistic result.
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. Obligations of the employer	
For all particular forms of processing, set out in Part II of this Recommendation, the employer should ensure that appropriate measures are taken to secure the respect of the following obligations:	

• 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 the persons concerned in advance.	
• Consult employees' representatives in accordance with domestic law or practice and, where appropriate, with the relevant collective agreements. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, their agreement should be sought.	**Question :** Sweden would like to request a clarification on the reference of "Their agreement" in the second sentence. Does it refer to the representatives or to the employees? .
• Consult before the processing the national supervisory authorities.	~~Consult before the processing the national supervisory authorities~~ • Follow the specific guidelines that the national supervisory authorities may have developed, and the assurance that in cases of doubt, or if there is a requirement in domestic law, has consulted with such authority. **Justification:** It should not be an obligation to consult the national supervisory authority before the processing of personal. Such obligation is not possible to implement in practical terms.

SWITZERLAND / SUISSE

PROJET DE RECOMMANDATION	PROPOSITIONS REDACTIONNELLES DE MODIFICATION
Partie I – Principes généraux **1. *Champ d'application et définitions*** 1.1. Les principes de la présente recommandation s'appliquent à la collecte ou le traitement de données à caractère personnel à des fins d'emploi dans les secteurs public et privé. 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, contrats à temps partiel inclus, entre les personnes concernées qui figurent sur leurs listes et d'éventuels employeurs, ou afin de faciliter les démarches dérivant desdits contrats. 1.3. 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 ; lorsque 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 ; – « 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 ; – « traitement de données sensibles » couvre le traitement de données génétiques ou de données concernant des infractions, condamnations pénales et mesures de sûreté connexes, le traitement de données biométriques identifiant un individu de façon unique ainsi que le traitement de 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 apparentés, qui assure 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 employeur relatifs au recrutement des employés, à l'exécution du contrat de travail, à la gestion, y compris les obligations découlant de la loi ou de conventions collectives, ainsi que la planification et l'organisation du 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 qui engage une personne physique d'exécuter des tâches précises en échange d'un salaire et qui a la responsabilité légale de l'entreprise ou de l'établissement ; – « employé » signifie toute personne engagée par un employeur au terme d'un lien de subordination ;	

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, également 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.	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, ~~également~~ 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 : minimisation, responsabilisation, simplification, sécurité 3.1. Les employeurs devraient minimiser la collecte des données à ce qui est directement pertinent et nécessaire pour atteindre l'objectif déterminé dans les cas individuels concernés et lorsque ceci est possible, procéder à l'anonymisation des données. 3.2. Les employeurs devraient développer des mesures appropriées, y compris organisationnelles, 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. 3.3. Les mesures adoptées par l'employeur devraient être en fonction du volume du traitement, de la nature des données concernées, de la catégorie des activités entreprises et tiendront également compte des implications possibles pour les personnes concernées. 3.4. A travers l'utilisation des systèmes et technologies d'information pour la collecte et le traitement de données à caractère personnel à des fins d'emploi l'employeur doit veiller à appliquer les principes de sécurité.	3.1. Les employeurs devraient ~~minimiser~~ limiter la collecte des données à ce qui est directement pertinent et nécessaire pour atteindre l'objectif déterminé dans les cas individuels concernés et lorsque ceci est possible, procéder à l'anonymisation des données. 3.2. Les employeurs devraient développer des mesures appropriées, ~~y compris organisationnelles~~, (C : à mettre dans l'exposé des motifs) 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. 3.3. Les mesures adoptées par l'employeur devraient être ~~en fonction du~~adaptées au volume ~~du traitement, de~~et à la nature des données ~~concernées~~traitées, ~~de la catégorie des~~aux activités entreprises ; ~~et~~ elles tiendront également compte des implications possibles pour les droits et les libertés fondamentales des personnes concernées. 3.4. L'employeur devrait veiller à assurer la sécurité des données lors ~~A travers~~de l'utilisation des systèmes et technologies d'information pour la collecte et le traitement de données à caractère personnel à des fins d'emploi ~~l'employeur doit veiller à appliquer les principes de sécurité~~.
4. *Collecte des données*	

4.1. L'employeur devrait collecter les données à caractère personnel auprès de la personne concernée directement. Lorsqu'il est nécessaire, légal et approprié de collecter et traiter des données obtenues auprès des tiers ou auprès des sources externes à la relation d'emploi, notamment s'agissant de références professionnelles, la personne concernée devrait en être informée et son consentement devrait être assuré.	4.1. L'employeur devrait collecter les données à caractère personnel directement auprès de la personne concernée ~~directement~~. Lorsqu'il est nécessaire, légal et approprié de ~~collecter et~~ traiter des données ~~obtenues~~ collectées auprès des ~~tiers ou auprès des sources externes à la relation d'emploi~~, (C : à mettre dans l'exposé des motifs, une source externe est un exemple de tiers) notamment s'agissant de références professionnelles, la personne concernée devrait en être informée et ~~son consentement devrait être assuré~~y avoir préalablement consenti.
4.2. Les données à caractère personnel collectées par l'employeur à des fins d'emploi devraient être pertinentes et non excessives, eu égard à la nature d'emploi ainsi qu'aux besoins légitimes de l'employeur en lien direct avec ses activités.	
4.3. L'employeur devrait éviter d'obtenir accès à des données privées qui ne sont pas nécessaires pour évaluer aptitude professionnelle de l'employé à occuper le poste concerné.	4.3. L'employeur ne devrait ~~éviter d'obtenir~~avoir accès à des données privées ~~qui~~ que si et dans la mesure où elles ~~ne~~ sont ~~pas~~ absolument nécessaires pour évaluer l'aptitude professionnelle de l'employé à occuper le poste concerné.
4.4. L'employeur devrait prendre des mesures appropriées afin de s'assurer que lorsque des données en ligne sont accessibles au public, seules les données pertinentes, exactes et mises à jour soient utilisées, afin d'éviter que ces données ne soient mal interprétées ou traitées de façon déloyale au regard de leur origine.	
4.5. Les données relatives à la santé ne peuvent être collectées qu'à des fins définies, prévues au principe 9.2 de la présente recommandation.	4.5. Les données relatives à la santé ne peuvent être collectées ~~qu'à des fins définies~~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 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 et si l'enregistrement est	5.1. L'enregistrement de données à caractère personnel 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 et si l'enregistrement est

réalisé à des fins d'emploi. Dans le cas contraire, l'employeur devrait s'abstenir d'utiliser les données. 5.2. Lorsque des données appréciatives relatives à la productivité ou à la potentialité des employés sont enregistrées, de telles données ne devraient servir qu'à évaluer les compétences professionnelles. Ces données devraient être pertinentes, adéquates et non-excessives.	réalisé à des fins d'emploi. ~~Dans le cas contraire, l'employeur devrait s'abstenir d'utiliser les données.~~ Comment : Peut éventuellement être rappelé dans l'EM. Le mettre dans la recommandation, donne l'impression qu'il serait mieux de ne pas les traiter, mais qu'il y a des cas où on peut fermer les yeux ! Si maintien la phrase, elle devrait être plus affirmative.
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 personnelles. 6.3. Lorsque des données doivent être traitées (mises en corrélation et/ou analysées) à des fins d'emploi pour d'autres finalités 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 pour s'assurer qu'elles ne soient pas utilisées de manière incompatible avec le but initial. En cas de décision importante concernant l'employé, fondée sur des données ainsi traitées, celui-ci devrait en être avisé. 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 du principe de spécification de la finalité dans l'utilisation ultérieure des données. Lorsque des modifications substantielles du traitement interviennent, la personne concernée doit en être informée. Le consentement des employés pourrait être requis dans certains cas en tant que garantie supplémentaire.	Comment : [mot finalités] Dans l'exposé des motifs, il conviendra de donner des exemples de situations dans lesquelles l'employeur peut traiter des données pour d'autres finalités. 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 ~~du~~ des principes de proportionnalité et [de spécification de] (C : est-ce que c'est nécessaire ?) la finalité dans l'utilisation ultérieure des données. Lorsque des modifications substantielles du traitement interviennent, la personne concernée doit en être informée. Le consentement des employés pourrait être requis dans certains cas en tant que garantie supplémentaire.
7. *Communication de données aux*	

représentants des employés 7.1. Conformément aux législations et pratiques nationales et aux conventions collectives, certaines données à caractère personnel peuvent être communiquées aux représentants des employés, dans la mesure uniquement où de telles données sont nécessaires pour permettre à ces derniers de représenter de façon appropriée les intérêts des employés concernés. 7.2. L'utilisation de systèmes et technologies d'information pour des communications à caractère syndical 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 ne devraient être communiquées à des organismes publics pour l'accomplissement de leur mission que dans les limites des obligations légales de l'employeur ou conformément à d'autres dispositions du droit interne. 8.2. La communication de données personnelles 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. 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 autorisée ou déterminée par le droit interne (notamment si cela	8.2. La communication de données personnelles 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. 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 ~~autorisée ou déterminée~~prévue par le droit interne (~~notamment si cela s'avère nécessaire en cas d'action en justice~~). (C : à mettre dans l'exposé des motifs)

s'avère nécessaire en cas d'action en justice). 8.3. Selon les garanties appropriées prévues par le droit interne, des données à caractère personnel peuvent être communiquées au sein d'un groupe de sociétés afin d'exécuter les obligations prévues par la loi ou par les conventions collectives. Le consentement de l'employé peut aussi être requis. 8.4 Dans le secteur public, d'autres instruments prévoyant des dispositions sur la divulgation de données à caractère personnel afin de garantir la transparence et/ou le contrôle de l'utilisation des ressources et de fonds publics, devrait 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. La législation devrait notamment inclure des dispositions requérant le plein respect du principe de finalité et limitant la divulgation de données à caractère personnel à des données pertinentes.	8.3. ~~Selon les garanties appropriées prévues par le droit interne, des données à caractère personnel peuvent être communiquées au sein d'un groupe de sociétés afin d'exécuter les obligations prévues par la loi ou par les conventions collectives~~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 garanties appropriées prévues par le droit interne. Le consentement de l'employé peut aussi être requis. 8.4 Dans le secteur public, ~~d'autres instruments prévoyant des dispositions sur~~les dispositions régissant la divulgation de données à caractère personnel afin de garantir la transparence et/ou le contrôle de l'utilisation des ressources et de fonds publics, devrai~~t~~ent 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. [La législation devrait notamment inclure des dispositions requérant le plein respect du principe de finalité et limitant la divulgation de données à caractère personnel à des données pertinentes.] (C : à mettre éventuellement dans l'exposé des motifs comme illustration des garanties appropriées)
9. Traitement de données sensibles 9.1. Le traitement des données personnelles visées à l'article 6 de la Convention 108, est possible 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. 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,	9.1. Le traitement des données ~~personnelles visées à l'article 6 de la Convention 108~~sensibles au sens du principe 1.3 de la présente Recommandation, est possible 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 biometriques est sujet aux dispositions du paragraphe 18 de cette Recommandation.	notamment le risque de discrimination. Le traitement des données ~~biometriques~~ biométriques est sujet aux dispositions du paragraphe 18 de cette Recommandation.
9.2. Un employé ou un candidat à un emploi ne peut être interrogé sur son état de santé et/ou faire l'objet d'un examen médical qu'à des fins définies pour :	9.2. Un employé ou un candidat à un emploi ne peut être interrogé sur son état de santé et/ou faire l'objet d'un examen médical qu'à ~~des~~ fins ~~définies pour~~de :
a. déterminer son aptitude à un emploi actuel ou futur ;	a. déterminer son aptitude à un emploi actuel ou futur ;
b. couvrir les besoins de la médecine préventive ;	b. couvrir les besoins de la médecine préventive ;
c. sauvegarder les intérêts vitaux de la personne concernée ;	c. sauvegarder les intérêts vitaux de la personne concernée ;
d. octroyer des prestations sociales ; ou	d. octroyer des prestations sociales ; ou
e. répondre à une procédure judiciaire.	e. répondre à une procédure judiciaire.
Le traitement de données génétiques, pour déterminer par exemple l'aptitude professionnelle des employés ou des candidats lors de l'instauration d'un contrat de travail, même avec le consentement de l'intéressé, est interdit.	Le traitement de données génétiques, pour déterminer par exemple l'aptitude professionnelle des employés ou des candidats lors de l'instauration d'un contrat de travail, même avec le consentement de l'intéressé, est interdit.
Le traitement de données génétiques peut cependant être autorisé par le droit interne et moyennant des garanties appropriées pour des raisons de santé et uniquement pour éviter tout préjudice sérieux à la santé de la personne concernée ou de tiers.	Le traitement de données génétiques peut cependant être ~~autorisé~~ prévu par le droit interne et moyennant des garanties appropriées ~~pour des raisons de santé~~, ~~et~~ uniquement pour éviter tout préjudice sérieux 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 peuvent être collectées auprès d'autres sources que l'employé lui-même, sauf dispositions contraires prévues par la loi, avec des garanties appropriées.	9.3. Les données de santé et - lorsque leur traitement est licite - les données génétiques, ~~ne peuvent être collectées auprès d'autres sources que l'employé lui-même,~~ ne devraient être collectées qu'auprès de l'employé lui-même, sauf dispositions contraires prévues par la loi, ~~avec~~ moyennant des garanties appropriées.
9.4. Les données de santé couvertes par le secret médical et - lorsque leur traitement est licite - les données génétiques, ne peuvent être	

traitées que par le personnel lié par le secret médical. Ces données devraient soit se rapporter directement à l'aptitude de l'employé à exercer ses fonctions où être nécessaires pour prendre des mesures en faveur de la santé de l'employé ou pour prévenir un risque pour d'autres personnes. Lorsque ces données sont communiquées à l'employeur, cette communication devrait etre faite à un titulaire dûment autorisé tel que l'administration du personnel, de santé et de la sécurité au travail. 9.5. Les données de santé couvertes par le secret médical et - lorsque leur traitement est licite - les données génétiques 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 de la personne concernée à ses 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 la personne concernée. Dans ce cas, ces données pourraient 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 (C : dans l'exposé des motifs il faudrait préciser dans quel cas l'employeur peut traiter des données concernant la santé des tiers) ne feront objet d'un traitement, à moins que la personne concernée ait donné son consentement informé et non-équivoque, et que ce traitement soit légal et autorisé par l'autorité de contrôle compétente et que la collection des données est indispensable à l'exécution des obligations prévues par la loi.	9.4. Les données de santé couvertes par le secret médical et - lorsque leur traitement est licite - les données génétiques, ne ~~peuvent~~ devraient être traitées que par ~~le~~ du personnel lié par le secret médical. Ces données devraient ~~soit~~ a. se rapporter directement à l'aptitude de l'employé à exercer ses fonctions, ou b. ~~où~~ être nécessaires pour prendre des mesures en faveur de la santé de l'employé ou c. être nécessaire pour prévenir un risque pour d'autres personnes. Lorsque ces données sont communiquées à l'employeur, cette communication devrait ~~etre~~ être faite à ~~un titulaire~~une personne dûment autorisée et en charge par exemple ~~tel que~~de l'administration du personnel, de la santé et de la sécurité au travail. 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 son consentement informé et non-équivoque, et que ce traitement ~~soit légal~~ne soit prévu par la loi ou qu'il ne soit ~~et~~ autorisé par l'autorité de contrôle compétente et que la ~~collection~~ collecte des données ~~est~~ ne soit indispensable à l'exécution des obligations ~~prévues par la loi~~légales.
10. *Transparence du traitement* 10.1. L'employeur devrait fournir à l'employé d'informations concernant ses données à	10.1. ~~L'employeur devrait fournir à l'employé d'informations concernant ses données à~~

caractère personnel détenues par lui. Ces informations pourraient être fournies soit directement, soit par l'intermédiaire des représentants de l'employé. Outre 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 à l'article 8 de la Convention 108, 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, une description particulièrement claire et complète devrait être fournie concernant les catégories des données à caractère personnel qui peuvent être collectées au moyen de systèmes et technologies d'information et leur utilisation potentielle, y compris la surveillance indirecte. (C : Donner dans l'exposé des motifs des exemples de surveillance indirect) Ce principe est également valable 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 ne réalise l'activité ou le comportement qui est visé, puis mises à disposition au moyen de systèmes d'information habituellement utilisés par l'employé.	~~caractère personnel détenues par lui~~L'employé devrait obtenir des informations sur les données à caractère personnel détenues par son employeur.. Ces informations pourraient lui être fournies ~~soit~~ directement~~, s~~ ou~~oit~~ par l'intermédiaire de ses~~s~~ représentants ~~de l'employé~~. Outre 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 à ~~l'article 8 de la Convention 108~~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, une description particulièrement claire et complète devrait être fournie concernant les catégories des données à caractère personnel qui peuvent être collectées au moyen de systèmes et technologies d'information et leur utilisation potentielle, y compris la surveillance indirecte. Ce principe est également valable pour toutes les formes particulières de traitement des données à caractère personnel prévues à la partie II de la présente Recommandation.

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 ou frais excessifs, 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.	11.1 Les employés devraient pouvoir obtenir, à leur demande, à intervalle raisonnable et sans délai ou frais excessifs, 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. 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 l'employeur ou de tiers de se défendre. Les appréciations purement subjectives devraient pouvoir être contestées selon les modalités prévues par le droit interne, même si l'employé ne peut les rectifier directement.	
11.3. 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 soit pris en compte.	
11.4. Un employé doit également obtenir, à sa demande, des informations concernant les motifs du traitement des données, les résultats du traitement et les moyens par lesquels ces résultats lui sont appliqués. L'employé devrait également avoir le droit d'obtenir la rectification ou l'effacement de ses données personnelles en cas d'inexactitude et/ou lorsqu'elles sont traitées en violation du droit interne ou des principes énoncés dans cette Recommandation.	
11.5. L'employeur devrait prévoir des procédures d'ordre général afin de garantir que le contrôle soit adéquat et rapide en cas d'exercice du droit	

d'accès et de rectification, particulièrement pour les entités de grande dimension ou dispersées sur le territoire. 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 pourrait 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 ou afin d'exercer ce droit 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. Des 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 autorisés. 12.2. 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 paragraphe 1.3. ou que ne le nécessite l'intérêt d'un employé actuel ou d'un ancien employé. 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 qu'une offre d'emploi n'interviendra pas. (C : Préciser dans l'exposé des motifs que 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 d'éventuelles actions en justice, il est indispensable de conserver les données fournies à l'occasion d'une candidature, ces données ne devraient être conservées que pendant la période la plus courte possible et uniquement pour la durée nécessaire.	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 ~~d'éventuelles actions~~une action (C : Cette conservation ne peut se faire que s'il y a un degré élevé de certitude qu'une action aura lieu). en justice, il est indispensable de conserver les données fournies à l'occasion d'une candidature, ces données ne devraient être conservées que ~~pendant la période la plus courte possible et uniquement pour la durée nécessaire~~pour la période nécessaire à l'action en justice. .

13.4. 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 mesure négative à l'égard des employés doivent en principe être effacées dans les meilleurs délais, sans préjudice de l'exercice du droit d'accès de l'employé jusqu'à ce qu'elles soient effacées.	13.4. 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 mesure négative à l'égard des employés doivent ~~en principe~~ être effacées dans les meilleurs délais, sans préjudice de l'exercice du droit d'accès de l'employé jusqu'à ce qu'elles soient effacées. Comment : Le maintien de en principe suggère qu'il y a des exceptions. Si c'est le cas, il faudrait le prévoir.
Partie II – Formes particulières de traitement	
14. *Systèmes et technologies d'information pour le contrôle du travail des employés, incluant la vidéosurveillance* 14.1 L'introduction et l'utilisation de systèmes et technologies d'information utilisés directement et essentiellement afin de contrôler à distance le travail et le comportement des employés, conduisant à une surveillance délibérée et systématique d'un employé en particulier, ou d'un groupe d'employés spécifiques, ne doit pas être autorisées. 14.2 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 ou de l'organisation du travail de l'établissement. Avant l'introduction d'un système de surveillance ou lorsqu'un système existant doit être modifié, les représentants des employés devront être consultés. 14.3 En cas de litige ou d'action en justice, les employés devraient pouvoir obtenir communication des enregistrements réalisés.	14.2 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 ou de l'organisation du travail de l'établissement. Avant l'introduction d'un système de surveillance ou lorsqu'un système existant doit être modifié, les représentants des employés devront être consultés. Les employés devraient en être informés de manière adéquate Comment : Par exemple dans un règlement interne.

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 verts, 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 personnelles 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 circonstancié et concerne de graves infractions au droit interne.	Les personnes concernées par un signalement devraient en être informées de manière appropriée afin qu'elles puissent faire valoir leurs droits.
16. Utilisation de l'Internet et des messages électroniques sur le lieu de travail	Est-ce que il ne faut pas mentionner qu'il faudra rédiger un règlement de surveillance qui a comme contenue aussi l'accès aux messages électroniques?
16.1 L'employeur devrait éviter des atteintes injustifiées/déraisonnables au droit au respect de la vie privée de l'employé. Ce principe s'éteint à tous les dispositifs utilisés par un employé, y compris son ordinateur, Smartphone ou autre appareil numérique, soit à travers l'utilisation d'intranet et extranet, soit à travers l'utilisation directe ou indirecte d'internet, mis à disposition par l'employeur. Ce principe s'applique de manière identique en débit du fait que le dispositif utilisé par l'employé est assuré par l'employeur ou l'employé. Les employés doivent être convenablement et périodiquement informés à l'aide d'une déclaration claire en matière de respect de la vie privée. L'information fournie doit être mise à jour, et le droit d'information doit être mis en œuvre conformément au principe 10 de la	16.1 L'employeur devrait éviter des atteintes injustifiées/déraisonnables au droit au respect de la vie privée de l'employé. Ce principe ~~s'éteint~~ s'étend à tous les dispositifs techniques et aux systèmes d'information et de télécommunication utilisés par un employé~~, y compris son ordinateur, Smartphone ou autre appareil numérique, soit à travers l'utilisation d'intranet et extranet, soit à travers l'utilisation directe ou indirecte d'internet, mis à disposition par l'employeur. Ce principe s'applique de manière identique en débit du fait que le dispositif utilisé par l'employé est assuré par l'employeur ou l'employé.~~ (C : à mettre dans l'exposé des motifs) Les employés doivent être convenablement et périodiquement informés à l'aide d'une déclaration claire en matière de respect de la vie

Recommandation et elle information doit inclure la finalité du dispositif, la durée de conservation ou de sauvegarde des données de connexion et l'archivage des messages électroniques. 16.2 En ce qui concerne plus particulièrement l'éventuel traitement de données à caractère personnel figurant sur des pages du réseau Internet ou Intranet consultées par l'employé, il conviendrait d'adopter les mesures préventives, telles que la configuration de systèmes ou l'utilisation de filtres qui peuvent empêcher certaines opérations, le cas échéant, et la graduation des éventuels contrôles relatifs aux données à caractère personnel, moyennant dans un premier temps des contrôles par sondages non individuels sur des données anonymes ou groupées. 16.3 L'accès aux messages électroniques professionnels des employés qui ont été préalablement informés de l'existence de cette éventualité, ne peut survenir qu'en conformité avec la législation et si cela est strictement nécessaire pour des raisons de sécurité, de fonctionnement de l'entreprise ou pour d'autres raisons légitimes, telles que pour contrôler les infractions à la propriété intellectuelle de l'employeur. En cas d'absence d'un employé, l'employeur devrait prendre les mesures nécessaires et à prévoir les procédures appropriées visant à permettre l'accès aux messages électroniques professionnels, uniquement lorsqu'un tel accès est absolument nécessaire d'un point de vue professionnel. Par ailleurs, ce traitement doit intervenir de la façon la moins intrusive possible et uniquement après avoir informé l'employé ou les employés concerné(s). 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	privée. L'information fournie doit être mise à jour, et le droit d'information doit être mis en œuvre conformément au principe 10 de la Recommandation et ~~elle~~ l'information doit inclure la finalité du dispositif, la durée de conservation ou de sauvegarde des données de connexion et l'archivage des messages électroniques. Comment : Préciser dans l'exposé des motifs que cette information peut se faire dans le cadre d'un règlement intérieur sur l'utilisation des moyens informatiques et la surveillance.

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 en sa présence.	
17. Appareils permettant de géolocaliser les employés 17.1 Tandis que les appareils permettant de localiser les employés peuvent être utilisés dans l'intérêt des employés (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 personnelles et au respect de la vie privée. 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. 17.2 Lorsqu'un employé, conformément aux instructions de son employeur ou après s'être assuré que l'employeur en connaisse au préalable les modalités et en accord avec ce dernier, utilise des appareils professionnels en dehors de l'entreprise ou de l'institution, et qu'en vertu de cette utilisation, l'employeur peut localiser l'employé, la collecte et d'autres traitements de ces données personnelles doivent être exclusivement limités à la stricte vérification de l'exécution des tâches professionnelles ou d'autres aspects en termes d'organisation. 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 puis le traitement de données biométriques ne devraient être réalisés que lorsque nécessaire à la protection des intérêts légitimes de l'employeur, des employés ou des	

tiers et devraient s'accompagner de garanties appropriées, et uniquement lorsqu'il y a impossibilité d'utiliser d'autres méthodes alternatives de traitement qui sont moins intrusives pour la vie privée. 18.2 Le traitement des données biométriques doit être soumis à des exigences de sécurité et de proportionnalité. A cet égard, une attention particulière devrait être accordée aux implications d'un enregistrement effectué dans une base de données centralisée ou à des systèmes alternatifs basés sur des supports mis à la disposition exclusive de la personne concernée.	
19. Tests psychologiques, analyses et procédures analogues Le recours à des tests, à des analyses et à des procédures analogues effectués par des professionnels spécialisés, couverts par le secret professionnel et destinés à évaluer le caractère ou la personnalité d'un employé ou d'un candidat à l'emploi ne devraient se faire qu'en cas de stricte nécessité. Ils 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. Le consentement de l'employé doit être libre, éclairé et sans contrepartie financière ou autre envisagée. L'employé ou le candidat à l'emploi devraient pouvoir, s'ils ou elles le désirent, 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 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. A moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationales, l'accord des représentants des employés devrait être recherché préalablement à l'introduction ou à la modification des systèmes de surveillance lorsque la procédure de consultation mentionnée au principe 14 révèle une possibilité d'atteinte.	
21. Obligations de l'employeur Pour toutes formes particulières de traitement, établies dans la Partie II de cette Recommandation, l'employeur est tenu de prendre des mesures pour le respect des obligations suivantes : • Informer les employés préalablement à 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 personnes concernées. • Consulter les représentants des employés, conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives pertinentes. 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 avant tout traitement les autorités nationales de contrôle.	• Consulter, conformément à la législation nationale ~~avant tout traitement~~ les autorités nationales de contrôle sur les traitements de données à caractère personnel.