COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 15 July 2013 T-PD(2013)05rev_en

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

(T-PD)

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

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 ;	

- ‘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.	
- ‘Employer’ means any natural or legal persons 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 Information and Communication Technologies (ICTs) for the collection and processing of personal data for employment purposes, employers shall ensure adequate data security.	DE: What does "directly identifying data" refer to? What is the distinction between it and "personal data"?

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.	
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 erase ~~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~~—~~ necessary ~~non-excessive~~.	DE: Special attention should be paid to the fact that the processing of the data must not lead to the creation of an overall picture of an employee's key intellectual and character traits. DE: We request clarification of the term "evaluation data".

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~~ The employee 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.	DE: "including correlated and/or analysed" should be included in the definition under paragraph 1. DE: This rule is very vague. The employee should always be informed about a change in the purpose.
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. In accordance with domestic law and practice, 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	DE: What type of "communication" is being referred to here? Should communication only be permitted on the basis of a relevant legal provision?
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).	DE: Is this also to apply across national borders and also to data transmitted to non-Member States?
8.3. Where adequate safeguards are provided in accordance with 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 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, if it is necessary : a. to determine his or her suitability for the present or future employment; b. to fulfil the requirements of preventive medicine; c. to safeguard the vital interest of the data subject; d. to allow social benefits to be granted**;** or e. 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 or other rules of professional secrecy. 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.	
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. ~~U~~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. 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.	
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 and a claim is not submitted by the applicant. 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.	
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 The use of the Internet and e-mail at working shall be in accordance with member states laws and practice. The following guidelines shall be considered by the Member States: 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.	
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.	
