COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Recommendation CM/Rec(2015)5
of the Committee of Ministers to member States
on the processing of personal data in the context of employment

(Adopted by the Committee of Ministers on 1 April 2015,
at the 1224th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity among its members;

Aware of the increasing use of new technologies and means of electronic communication in the relations between employers and employees, and the corresponding advantages thereof;

Believing, however, that the use of data-processing methods by employers should be guided by principles designed to minimise any risks that such methods might pose to employees' rights and fundamental freedoms, in particular their right to privacy;

Bearing in mind the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108, hereinafter the "Convention No. 108") and of its Additional Protocol regarding supervisory authorities and transborder data flows of 8 November 2001 (ETS No. 181), and the desirability of applying the principles to the employment sector;

Recognising also that the interests to be borne in mind when developing principles for the employment sector are individual or collective, private or public;

Considering that personal data in official documents held by a public authority or a public body may be disclosed by the authority or body in accordance with the domestic law to which the public authority or body is subject, thus reconciling access to such official documents with the right to the protection of personal data in accordance with the principles of the present recommendation;

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

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

Considering that, in light of such changes, Recommendation Rec(89)2 of the Committee of Ministers to member States on the protection of personal data used for employment purposes should be revised in order to continue to provide an adequate level of protection for individuals in the context of employment;

Recalling that Article 8 of the European Convention on Human Rights (ETS No. 5) protects the right to private life, including activities of a professional or business nature, as interpreted by the European Court of Human Rights;

Recalling the applicability of the existing principles set out in other relevant recommendations of the Committee of Ministers of the Council of Europe to member States, in particular Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation Rec(97)5 on the protection of medical data and Recommendation Rec(92)3 on genetic testing and screening for health care purposes;

Recalling the Guiding Principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance, adopted by the European Committee on Legal Co-operation (CDCJ) of the Council of Europe in May 2003, referred to in Resolution 1604 (2008) on video surveillance of public areas of the Parliamentary Assembly of the Council of Europe, which are especially relevant;

Recalling the European Social Charter (ETS No. 163), as revised on 3 May 1996, and the International Labour Office's 1997 Code of practice on the protection of workers' personal data,

Recommends that governments of member States:

– ensure that the principles contained in the appendix to the present recommendation, which replaces the above-mentioned Recommendation Rec(89)2, are reflected in the application of domestic legislation on data protection in the employment sector, as well as in other branches of law which have a bearing on the use of personal data for employment purposes;

– for this purpose, ensure that the present recommendation and its appendix are brought to the attention of the authorities established under domestic data protection legislation which are competent to supervise the implementation of such legislation;

– promote the acceptance and implementation of the principles contained in the appendix to the present recommendation by means of complementary instruments, such as codes of conduct, to ensure that the principles are well known, understood and applied by all employment sector participants, including representative bodies of both employers and employees, and are taken into account in the design and use of ICTs in the employment sector.

Appendix to the Recommendation CM/Rec(2015)5

Part I – General principles

1. Scope

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

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

2. Definitions

For the purposes of the present recommendation:

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

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

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

"Employment purposes" concerns the relations between employers and employees which relate to recruitment, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, as well as the planning and efficient running of an organisation and termination of the employment relationship. The consequences of the contractual relationship may extend beyond the term of the contract of employment;

"Employer" means any natural or legal person, public authority or agency that has an employment relationship with an employee or is considering such a relationship in respect of a job applicant and has the legal responsibility for the undertaking or establishment;

"Employee" means any natural person concerned under an employment relationship engaged by an employer.

3. Respect for human rights, dignity and fundamental freedoms

Respect for human dignity, privacy and the protection of personal data should be safeguarded in the processing of personal data for employment purposes, notably to allow for the free development of the employee's personality as well as for possibilities of individual and social relationships in the workplace.

4. Application of data processing principles

4.1. Employers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned.

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

5. *Collection and storage of data*

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

5.2. Personal data collected by employers for employment purposes should be relevant and not excessive, bearing in mind the type of the employment as well as the changing information needs of the employer.

5.3. Employers should refrain from requiring or asking an employee or a job applicant access to information that he or she shares with others online, notably through social networking.

5.4. Health data may only be collected for the purposes set out in principle 8.2 of the present recommendation.

5.5. The storage of personal data for employment purposes is permissible only if the data have been collected in accordance with the requirements outlined in principles 4, 9 and 14 to 20 of this recommendation and only for the time necessary to pursue the legitimate aim of the processing. These data should be relevant, appropriate and not excessive. When evaluation data relating to the performance or potential of an employee are stored, such data should only be used for the purpose of assessing professional skills.

6. *Internal use of data*

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

6.2. Employers should adopt data protection policies, rules and/or other instruments on internal use of personal data in compliance with the principles of the present recommendation.

6.3. Under exceptional circumstances, where data are to be processed for employment purposes other than the purpose for which they were originally collected, employers should take adequate measures to avoid misuse of the data for this different purpose and inform the employee. Where important decisions affecting the employee are to be taken, based on the processing of that data, the employee should be informed accordingly.

6.4. Without prejudice to principle 8, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principles of proportionality and purpose specification in the subsequent use of data. Every substantive change in the processing should be communicated to the persons concerned.

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

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

7.2. In accordance with domestic law and practice, the use of information systems and technologies for the communication of data to employees' representatives should be subject to specific agreements that set out, in advance, transparent rules prescribing their use and safeguards to protect confidential communications, in accordance with principle 10.

8. *External communication of data*

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

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

a. where it is necessary for employment purposes, the purposes are not incompatible with the purposes for which the data was originally collected and if the employee concerned or his or her representatives, as the case may be, are informed of this in advance;

b. with the express, free and informed consent of the employee concerned;

c. if the communication is provided for by domestic law and in particular when necessary for the purpose of discharging legal obligations or in accordance with collective agreements.

8.3. The provisions governing the disclosure of personal data to ensure transparency in the public sector (government and other public authority or body), including monitoring the correct use of public resources and funds, should provide appropriate safeguards for the employee's right to privacy and protection of personal data.

8.4. Employers should take appropriate measures to ensure that only relevant, accurate and up-to-date data are communicated externally, particularly in relation to data that is posted online and accessible to a wider public.

9. *Processing of sensitive data*

9.1. The processing of sensitive data referred to in Article 6 of Convention No. 108 is only permitted in particular cases, where it is indispensable for recruitment to a specific job or to fulfil legal obligations related to the employment contract within the limits laid down by domestic law and in accordance with appropriate safeguards, complementing those set out in Convention No. 108 and in the present recommendation. Appropriate safeguards should be 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 should be possible under conditions provided in Principle 18 of the present recommendation.

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

a. indicate his or her suitability for present or future employment;
b. fulfil the requirements of preventive medicine;
c. guarantee an appropriate rehabilitation or comply with any other work environment requirements;
d. safeguard the vital interests of the data subject or other employees and individuals;
e. enable social benefits to be granted;
f. respond to judicial procedures.

9.3. Genetic data cannot be processed, for instance, to determine the professional suitability of an employee or a job applicant, even with the consent of the data subject. The processing of genetic data may only be permitted in exceptional circumstances, for example to avoid any serious prejudice to the health of the data subject or third parties, and only if it is provided for by domestic law and subject to appropriate safeguards.

9.4. Health data and, where their processing is lawful, genetic data, should only be collected from the employee where it is provided for by law, and subject to appropriate safeguards.

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

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

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

9.6. Health data covered by the obligation of medical confidentiality and, where their processing is lawful, genetic data, where appropriate, should be stored separately from other categories of personal data held by employers. Technical and organisational security measures should be taken to prevent persons who do not belong to the employer's medical service having access to the data.

9.7. Health data related to third parties should not be processed under any circumstances unless full, unambiguous, free and informed consent is given by the data subject, or such processing is authorised by a data protection supervisory authority, or it is mandatory according to domestic law.

10. *Transparency of processing*

10.1. Information concerning personal data held by employers should be made available either to the employee concerned directly or through the intermediary of his or her representatives, or brought to his or her notice through other appropriate means.

10.2. Employers should provide employees with the following information:

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

10.3. A particularly clear and complete description must be provided of the categories of personal data that can be collected by ICTs, including video surveillance and their possible use. This principle also applies to the particular forms of processing provided for in Part II of the appendix to the present recommendation.

10.4. 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 through the information systems normally used by the employee.

11. *Right of access, rectification and to object*

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

11.2. An employee should be entitled to have personal data relating to him or her rectified, blocked or erased if they are inaccurate and/or if the data have been processed contrary to the law or the principles set out in the present recommendation. He or she should also be entitled to object at any time to the processing of his or her personal data unless the processing is necessary for employment purposes or otherwise provided by law.

11.3. The right of access should also be guaranteed in respect of evaluation data, including where such data relate to assessments of the performance, productivity or capability of the employee when the assessment process has been completed at the latest, without prejudice to the right of defence of employers or third parties involved. Although such data cannot be corrected by the employee, purely subjective assessments should be open to challenge in accordance with domestic law.

11.4. An employee should not be subject to a decision significantly affecting him or her, based solely on an automated processing of data without having his or her views taken into consideration.

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

11.6. Derogations to the rights referred to in paragraphs 10, 11.1, 11.2, 11.4 and 11.5 may be permitted if provided for by law and are 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, in the case of an internal investigation conducted by an employer, the exercise of the rights referred to in paragraphs 10 and 11.1 to 11.5 may be deferred until the closing of the investigation if the exercise of those rights would prejudice the investigation.

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

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

12. *Security of data*

12.1. Employers, or entities which may process data on their behalf, should implement adequate technical and organisational measures in response to periodic reviews of the organisation’s risk assessment and security policies and update them as appropriate. Such measures should be designed to ensure the security and confidentiality of personal data processed for employment purposes against accidental or unauthorised modification, loss or destruction of personal data, as well as against unauthorised access, dissemination or disclosure of such data.

12.2. In accordance with domestic law, employers should ensure adequate data security when using ICTs for any operation of processing of personal data for employment purposes, including their storage.

12.3. The personnel administration, as well as any other person engaged in the processing of the data, should be kept informed of such measures, of the need to respect them and of the need to maintain confidentiality about such measures as well.

13. *Preservation of data*

13.1. Personal data should not be retained by employers for a period longer than is justified by the employment purposes outlined in principle 2 or is required by the interests of a present or former employee.

13.2. Personal data submitted in support of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the job applicant. Where such data are stored with a view to a further job opportunity, the data subject should be informed accordingly and the data should be deleted if he or she so requests.

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

13.4. Personal data processed for the purpose of an internal investigation carried out by employers which has not led to the adoption of negative measures in relation to any employee should be deleted after a reasonable period, without prejudice to the employee's right of access until such deletion takes place.

Part II – Particular forms of processing

14. Use of Internet and electronic communications in the workplace

14.1. Employers should avoid unjustifiable and unreasonable interferences with employees' right to private life. This principle extends to all technical devices and ICTs used by an employee. The persons concerned should be properly and periodically informed in application of a clear privacy policy, in accordance with principle 10 of the present recommendation. The information provided should be kept up to date and should include the purpose of the processing, the preservation or back-up period of traffic data and the archiving of professional electronic communications.

14.2. In particular, in the event of 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, giving preference for non-individual random checks on data which are anonymous or in some way aggregated.

14.3. Access by employers to the professional electronic communications of their employees who have been informed in advance of the existence of that possibility can only occur, where necessary, for security or other legitimate reasons. In case of absent employees, employers should take the necessary measures and foresee the appropriate procedures aimed at enabling access to professional electronic communications only when such access is of professional necessity. Access should be undertaken in the least intrusive way possible and only after having informed the employees concerned.

14.4. The content, sending and receiving of private electronic communications at work should not be monitored under any circumstances.

14.5. On an employee's departure from an organisation, the employer should take the necessary organisational and technical measures to automatically deactivate the employee's electronic messaging account. If employers need to recover the contents of an employee's account for the efficient running of the organisation, they should do so before his or her departure and, when feasible, in his or her presence.

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

15.1. The introduction and use of information systems and technologies for the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted. Where their introduction and use for other legitimate purposes, such as to protect production, health and safety or to ensure the efficient running of an organisation has for indirect consequence the possibility of monitoring employees' activity, it should be subject to the additional safeguards set out in principle 21, in particular the consultation of employees' representatives.

15.2. Information systems and technologies that indirectly monitor employees' activities and behaviour should be specifically designed and located so as not to undermine their fundamental rights. The use of video surveillance for monitoring locations that are part of the most personal area of life of employees is not permitted in any situation.

15.3. In the event of dispute or legal proceedings, employees should be able to obtain copies of any recordings made, when appropriate and in accordance with domestic law. The storage of recordings should be subject to a time limit.

16. Equipment revealing employees' location

16.1. Equipment revealing employees' location should be introduced only if it proves necessary to achieve the legitimate purpose pursued by employers and their use should not lead to continuous monitoring of employees. Notably, monitoring should not be the main purpose, but only an indirect consequence of an action needed to protect production, health and safety or to ensure the efficient running of an organisation. Given the potential to violate the rights and freedoms of persons concerned by the use of these devices, employers should ensure all necessary safeguards for the employees' right to privacy and protection of personal data, including the additional safeguards provided for in principle 21. In accordance with principles 4 and 5, employers should pay special attention to the purpose for which such devices are used and to the principles of minimisation and proportionality.

16.2. Employers should apply appropriate internal procedures relating to the processing of these data and should notify the persons concerned in advance about them.

17. Internal reporting mechanism

17.1. Where employers are obliged by law or internal rules to implement internal reporting mechanisms, such as hotlines, they should secure the 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 (such as whistleblowers). Personal data of the parties involved should be used solely for the purpose of appropriate internal procedures relating to the report and as required by law, or as may be required for subsequent judicial proceedings.

17.2. Under exceptional circumstances, employers may enable anonymous reporting. Internal investigations should not be carried out on the sole basis of an anonymous report, except where it is duly circumstantiated and relates to serious infringements of domestic law.

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 employers, employees or third parties, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards, including the additional safeguards provided for in principle 21.

18.2. The processing of biometric data should be based on scientifically recognised methods and should be subject to the requirements of strict security and proportionality.

19. Psychological tests, analysis and similar procedures

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

19.2. The employee or the job applicant should be informed in advance of the use that will be made of the results of these tests, analysis or similar procedures and, subsequently, the content thereof. Principles 11.1 and 11.2 apply accordingly.

20. Other processing posing specific risks to employees' rights

20.1. Employers or, where applicable, processors, should carry out a risk analysis of the potential impact of any intended data-processing on the employees' 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 analysis reveals risks of interference with employees' rights and fundamental freedoms.

21. ***Additional safeguards***

For all particular forms of processing, set out in Part II of the present recommendation, employers should ensure the respect of the following safeguards in particular:

a. inform employees before the introduction of information systems and technologies enabling the monitoring of their activities. The information provided should be kept up to date and should take into account principle 10 of the present 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;

b. take appropriate internal measures relating to the processing of that data and notify employees in advance;

c. consult employees' representatives in accordance with domestic law or practice, before any monitoring system can be introduced or in circumstances where such monitoring may change. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, the agreement of employees' representatives should be obtained;

d. consult, in accordance with domestic law, the national supervisory authority on the processing of personal data.