COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 30 May / may 2011 T-PD-BUR(2011) 02 prov MOS rev 4

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

LE BUREAU DU COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNES A CARACTERE PERSONNEL [STE n°108]

(T-PD-BUR)

Compilation of comments received on the Report on Recommendation No. R(89) 2 of 18 January 1989 regulating the use of personal data used for employment purposes

Compilation des commentaires reçus sur le rapport sur la Recommandation N°R (89) 2 du 18 janvier 1989 sur la protection de s données à caractère personnel utilisées à des fins d'emploi

Secretariat document prepared by
The Directorate General of Human Rights and Legal Affairs

Document préparé par
la Direction Générale des affaires juridiques et des droits de l'Homme

INDEX / TABLE DES MATIERES

STATES / ETATS

ALBANIA / ALBANIE

The Recommendation should definitely take into account the fact that the controllers of SNS already have independent obligations, especially in terms of information, defaults and proportionality. However, it would be useful to provide brief guidelines for cases where an employer collects and uses data relating to job applicants or employees more or less without their knowledge through an intermediary, under another name or using a pseudonym and combine it with other information. In principle, this data collection is not actually right, regardless of whether or not the employee is a member of the SNS (some SNS allow users to enter 'tagging' data for non-members).

Instead, there should be a separate discussion with reference to networks where only news of a work/professional nature is exchanged, which it would be appropriate to consider separately to the more 'private' SNS.

Collection of data using search engines or placing employees' data on the Internet

Similar considerations would be stipulated with respect to the periodic collection of data using search engines outside the organisational structure of work.

The problem of the 'open nature' of the Internet and the protection of the personal data of its users also applies, in fact, in relation to recruitment procedures and the employment relationship.

Search engines are part of everyday life for those using the Internet and technologies to search for information. As service providers, these search engines collect and process large quantities of data, also harvested via special means like cookies (IP addresses and search chronology; data provided to enjoy personalised services).

Search engines contribute towards making various and precious information easily accessible, with increasingly sophisticated opportunities thanks also to added-value services such as the profiling of physical people (known as 'people-search engines') and facial recognition software based on pictures.

The types of data that they aim to have collected, including sounds, pictures, videos and other formats, are manifold. Some search engines replicate data in temporary memories (known as caches). By reassembling general information of various types under single individuals, search engines can create new profiles, however incorrect, of a person who runs a significant risk in the event that the individual data making up this profile is browsed separately.

The capacity of search engines to assemble data can have a significant impact on a person's private and social life, especially if personal data derived from a search is incomplete, excessive or incorrect, or even to be deleted by virtue of the right to be forgotten. In spite of progress and efforts including those of data protection authorities, users are still not sufficiently aware of the consequences arising from the use of these services, or of the purposes, even if secondary in nature, of the operations which result from it.

Theoretically (even if it is not easy in reality for the average user), an employee can turn to the controller of a search engine to have personal data which is no longer useful for the purposes for which it was previously collected cancelled or rendered anonymous (particularly when the data no longer corresponds to the actual content published on the 'source' website). However, in the

same way as SNS, there is a specific need to encourage data collection by employers to be more pertinent and transparent.

If the Recommendation takes search engines into consideration, it could also, with reference to an entirely different aspect of the issue, take into account the fact that employers increasingly use the Internet and Intranet to develop their own websites for corporate or promotional reasons with regard to citizens, consumers and users. In this way, it would be possible to devote more attention to information for employees about data concerning them which is intended for publication, as well as to the principle of purpose.

Biometric data and RFID techniques

The Recommendation could expressly consider the significant use of innovative biometric, wireless and location systems and Radio Frequency Identification technologies (commonly known as 'RFID technology') for a variety of purposes and applications, some of which may violate human dignity and human rights or present major risks to the latter.

The employer is able to collect, sometimes in a non-transparent manner, various data relating to entries, movements and activities of people, especially if they are assigned to certain tasks. Personal data on employees is collected indirectly as well via surveillance by objects and products sold over the counter or wholesale which track their movements.

The use of chips, often invisible, is attractive to the employer because it has positive effects on work organisation and may be used easily even by means of portable devices or by placing them
inside objects, clothes or uniforms, sometimes with the consent (induced) of the parties concerned, but not always in observance of the principles of data protection, especially in relation to the absence of adequate information regarding the use of the data.

There are event systems that can be imbedded under a person's skin, who is then transformed into an 'antenna' or sensor, with little consideration of habeas corpus or the principle (which in this instance is turned on its head) according to which information systems should be of service to mankind.

It would be necessary to encourage the adoption of internal privacy policies which, together with the explanatory Memorandum, respect more specifically the principles of:

- necessity ;
- proportionality (also in relation to various biometric data, some of which present greater risk such as fingerprints and iris recognition, and other less invasive ones such as hand geometry) .
- purpose (exclusion of further use: for example, data from car park entries used surreptitiously to compare with attendance data) ;
- adequate and easily understandable information on the types of data, regarding the fact that the devices produce data even without the consciously active behaviour of the person concerned, regarding the possibility - if it exists - of switching devices on and off and the consequent effects, as well as all the intended uses of the data and how to exercise their right to be informed ;

- limitation of data storage time.

The reasonable use of these systems should take into account the fact that some options present more or less invasive effects: the use of verification, rather than identification techniques; the creation of a centralised database containing biometric data, rather than just placing it on a portable device at employees' disposal; the use of more powerful readers that read from a great distance; the adoption of solutions which do or do not allow the employee to switch off the device. In the presence of adequate guarantees, consent does not in any case, at least in general, seem to be the ideal foundation for these types of data processing.

Unique identifiers

If 'unique identifiers' are used in the workplace, it is easier to trace data relating to a single employee and create profiles in a scarcely visible manner as well. This may occur, for example, to profile employees based on the type and number and time spent in relation to documents they consult to which they have access (consider companies engaged in the production and distribution of multimedia products wanting to check for infringements of copyright by employees).

The issue would be treated organically as an integral part of the theme of monitoring employees, but specific attention would be devoted to the possible use of unique identifiers in so far as these can signal the existence of an intention a priori to trace an employee. In principle, tagging a document should not be linked to an individual unless it is indispensable to perform a certain service and there is full information and, where possible, consent.

Genetic data

Some employees have manifested significant interest in using genetic data before hiring employees in order to provide a fuller profile of candidates or to identify those not adapted to a particular job (for example, in the case of a declared illness or risk of illness), or to identify possible protective measures to improve the working environment.

This also presents possible risks of discrimination and serious violations of human dignity and the right of self-determination.

Genetic tests sometimes have an uncertain probabilistic and predictive value but regardless of this fact, processing genetic data for employment purposes must be prohibited in principle and admitted only in exceptional circumstances where it is used for purposes of a very different nature (like a case where an employee voluntarily produces documents which include genetic data, submitted to the company doctor at the workplace in order to have a measure introduced for his or her advantage or protection such as, for example, due to occupational illness or a dispute).

Data relating to seropositivity, AIDS or drugs or alcohol abuse

Limited revision of the Memorandum could be carried out also regarding the issue of seropositivity and AIDS, which poses similar problems of possible discrimination, but also requirements to protect the health of third parties such as, for example, assisted or transported third parties. More specifically, there could be mention of the reasonable tendency to selectively identify exceptional situations or jobs which really do expose other employees or third parties to health risks and which should therefore warrant an exemption from the tendency to prohibit processing of this data, in the presence of appropriate guarantees also in relation to the sphere of movement of the collected data and the dignity and right to protection of the parties concerned.

Access to medical records held elsewhere

There is an increase in the use of electronic medical records, meaning the collection of medical documentation on the past and present physical and mental state of an individual which allow a quick overview of rather delicate data for the purpose of medical treatment and other closely related purposes.

We suggest that after this paragraph to include the fact that medical records to the health of employees, are considered sensitive information and as a rule, their processing is prohibited, citing the exceptional cases when their processing shall be done.

Electronic medical records should be accessible (except by the interested party) only by health practitioners and personnel authorised by the health structures assisting in the treatment of the employee, moreover with 'record-specific' consultation rights. The main purpose of their consultation should remain that of facilitating the success of a medical treatment due to better information. Access for any other reason, including for employment purposes even if via experts or insurance companies, should be prohibited in principle. This is in reference either to possible direct online access by the employer (several devices based on tokens or electronic signatures are emerging on the market), or to indirect access by the employer who can put pressure on the employee to persuade him or her to provide the documentation in a manner that is neither voluntary nor based on free consent.

We suggest that after this paragraph to provide the obligation of health practitioners and personnel authorised by the health structures to maintain the confidentiality of personal data of employees.

Commensurate protection should be arranged also for off-line records.

5. The monitoring of employees

Reasonable expectation of privacy in the workplace

New technologies still represent a positive development in the working word, even if employers can also use them in ways that are injurious to fundamental rights and freedoms. Thanks to them, it is easier to analyse, reconstruct and profile the use of information systems for work purposes using, for example, navigation or traffic log files obtained from the proxy server or from other information recording instruments, which can also allow the employer to know the content of the communications.

Employees should not leave their own privacy and data protection rights outside the workplace. To the contrary, they should be able to claim a legitimate expectation of a certain level of privacy even in the workplace where they develop a significant part of their own relationships with other human beings. This expectation should not be undermined by the fact that the employee is using communication media and tools which belong to the employer.

The protection of private life includes the right to develop these relationships and these place limitations on the legitimate prerogative of the employer to carry out supervision activities. The employer has the right to encourage efficient management and to protect itself against liabilities and damages which employees' actions may give rise to. Monitoring and surveillance activities in the interests of the employer should however be lawful, transparent, effective and proportionate, and this reasonable approach would also avert possible negative effects on the quality of their professional relationship.

We think that it would be necessary after this paragraph to include the possibility that every employee, who has suffered damage as a result of an unlawful processing of his personal data, have the right to seek compensation to the employers for the damage caused.

The Recommendation could encourage a more common position on the subject and a further harmonisation of national practices and legislation with a global viewpoint which would also take into account the secrecy of correspondence and possible exemptions from it, as well as powers of information and co-decision which organisations representing employees exercise on the basis of the law or collective bargaining.

The modern notion of 'privacy' includes activities of a professional or commercial nature. The concept of secrecy of correspondence has also been amplified, developing into the new generation's 'secrecy of communications'.

The location and ownership of the electronic media used should not be a reason to exclude the secrecy of communications and correspondence. Online and traditional correspondence should not be treated differently without a valid reason: with given conditions, electronic mail would also be subject to similar, if not absolutely identical, considerations as traditional mail on paper. Already today, but even more so in the years to come, the evolution of working conditions makes it more difficult to establish a clear separation between working hours and private life. In particular, with the development of the 'home office' model, many employees continue to work at home or outside the office using IT infrastructures which may or may not be placed at their disposal by the employer for this purpose.

The specific considerations in this report relate to the most common situations in which employees may find themselves, but it is also taken into account that:

- More or less proportionate monitoring could be carried out for reasons other than safety or the prevention and verification of unlawful behaviour, such as for the purpose of random monitoring even of productivity and individual capacity or general monitoring of work or checking working hours;

- General monitoring may involve management figures (managing directors or managers), independent professionals operating in the workplace (doctors) or persons in charge of internal control in an unbiased position (audits or statutory auditors) or lastly, trade union organisations. In all these cases, there are specific problems which will be assessed separately;

- Some work activities (financial transactions, professional training for example in direct marketing or emergency calls) may justify, in the presence of adequate guarantees, the lawful and correct recording of external contents or data of communications or conversations for proof or research purposes .

- Secret spot checks may be set up by the employer at the request of judicial authorities or the police for the purpose of criminal justice pursuant to the law.

These considerations regard the predominant problem of Internet navigation and electronic mail, as well as the use of electronic devices placed at the employee's disposal, but also relate, with the necessary adaptations, to the more traditional issue of the monitoring of fixed-line telephones in the workplace.

Observance of the canons of data protection may also prevent problems relating to the admissibility of evidence in criminal, civil or employment cases.

Information

The employer should indicate in a clear and detailed manner in all instances the method of use permitted for the tools placed at their disposal and whether, monitoring will be carried out and if so, the indicators and methods which will be used. Information on the policy regarding the use of media and on monitoring should be clear, comprehensive, accurate and quickly accessible.

The information would be adapted to each work context (for example, for small concerns where there is constant interpersonal sharing of information resources) and expressed in a clear manner, and sufficiently publicised and updated periodically.

The employer should for example specify, where applicable:

- Internal rules on data and systems security or on the protection of company or professional secrecy envisage for any classes of employees, as well as the role of the system administrator and any relocation of servers in other countries;

- Any personal use of electronic communication tools permitted which is invoiced to the party concerned, or definitely not tolerated (for example, the downloading or possession of software or files that are wholly unrelated to work activity), providing an indication also of the possible consequences, preferably graduated according to the seriousness of the offence (having to also take into account the possibility of involuntary visits to websites due to unexpected actions by search engines, advertisements or typing errors);

- Any monitoring that the employer reserves the right to perform, providing an indication of the legitimate reasons for them and the methods used in principle, also in relation to cross-examination of interested parties;

- The log files in case any are kept, also in the form of back-up copies, and the persons who could have access to them.

Similar although not necessarily identical information should be provided to any trade union organisations which could play a role in terms of information, consultation or conciliation, especially on the introduction of significant changes when introducing new applications.

Adequate awareness initiatives would be studied vis-à-vis external parties that interact with the organisation if monitoring activities may involve them (e.g. message addressees).

Inspections: necessity and proportionality

In the Recommendation, also through the Memorandum, it could be highlighted that employers are expected to:

- Ensure the functionality and correct use of electronic media and define the methods in which they should be used, also taking into account regulations regarding rights and trade union relations;

- Adopt suitable security measures to ensure the availability and integrity of information and data systems.

We suggest that in addition to this point to note the fact that the level of security should be appropriate to the nature of data processing.

Also, we suggest to add a point in which to provide the obligation of employers to maintain the confidentiality of personal data that they process.

On the basis of determined, explicit and legitimate purposes, the employer could reserve the right to inspect the correctness of work performance and the use of work tools or to perform other types of inspection, for manufacturing, organisational or occupational safety (due to anomalies or for maintenance) requirements for example.

As already stated, activities whose primary purpose is remote monitoring, as in the examples below, should be prohibited:

- The systematic registration and possible reading of messages sent by electronic mail or of related external data, beyond what is technically necessary to deliver the service ;
- The systematic caching of web pages viewed by employees ;
- The secret analysis of portable computers entrusted to their care, during maintenance or replacement for example ;
- The secret reading and recording of typed characters using keyboards or similar devices.

The processing of data regarding an individual employee should be permitted when it is necessary in order to achieve the employer's legitimate interests (for example, to protect the working organisation from serious harm by stopping the leakage of confidential information) and does not infringe the fundamental rights of employees in an unjustifiable manner.

We suggest that in addition to this paragraph to provide that personal data of an employee may be processed if he has given his consent, for the preparation and performance of a contract to which he is a party, in order to protect his vital interests and to comply with a legal obligation of the employer.

Priority should be assigned to interventions of a preventive nature, also through the use of technological solutions.

CZECH REPUBLIC

Czech Office for Personal Data Protection would like to add several sectorial Positions to the complex Study by Mr. Buttarelli concerning PD used for employment purposes that were published by the Czech Office. The goal of the mentioned Positions is to explain application of the PDP to the employers and employees

1) In connection with the Office for PDP inspection´ s duty, based on legal provisions

2) In interaction with the new Czech Labor Code (especially Art. 316 of the Code that concern surveillance on the working place), Civil Code and special Acts provisions concerning working rights and obligations.

The legally balanced approach of both concerned parties – employee-employer - is taken as principle.

In addition it is necessary to mention the fruitful cooperation of the Office with the Czech Inspection of Labor.

The recently published book –detailed commentary on PD used for employment purposes - was published by Director of the Czech Office Administrative Procedure Department. The commentary deals with elementary legal problems in workplaces and new technological development as well.

The publication concerning PD used by employers is being prepared in cooperation of the Czech, Hungarian and Polish PDPA, supported by Leonardo da Vinci program. The brochure has to be published in the summer of the year 2011.

CYPRUS / CHYPRE

In reference to your email regarding the report prepared by Mr Giovanni Buttarelli regulating the use of personal data used for employment purposes we would like to inform you the following:

1. As a general comment we are of the opinion that a new detailed text should be adopted replacing entirely the previous Recommendation No. R (89) 2 of 18 January 1989 which is far from regulating the new growing developments over the last few years. This will be most helpful for countries where domestic employment Law or any other related Law does not specifically regulate the use and processing of employees' personal data by the employers i.e employees' monitoring, whistleblowing practices, biometric and RFID techniques and the exercise of access right.

2. Regarding video surveillance despite the fact that 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 Commission, still remains current and though as said in the report it is not necessary to be regulated in the new Recommendation we believe that since the new Recommendation will cover all aspects of the latest developments, at least a short reference to those principles should be included in the new text in order to be a complete and integrated text.

3. Referring to the employee's right to access his personal data and specifically in the case of an internal investigation after a third party's nominal accusation we believe that the text should provide for a more detailed reference.

DENMARK / DANEMARK

By e-mail of January 26 2011 you have requested the Danish Data Protection Agency to comment on Mr. Giovanni Buttarelli´s report on the Commitee of Ministeres Recommendation No. R(89) 2 of 18 Januar 1989 regulating the use of personal data used for employment purposes. In addition you have requested information on relevant domestic legislation.

With reference to paragraph 5.7. of the draft recommendation I can inform you that the Danish Data Protection Agency caused to specific complaints have drafted some guidelines on employers handling of e-mail-accounts of former employees. Among other issues the guidelines address the question of how long the account can be active after departure of the employee. The Danish Data Procection Agency finds that an e-mail-account should be active after departure in a period that is as short as possible. The timeframe must be fixed in consideration of the emplyoees position and functions and the period shall not exceed 12 months.

As soon as possible after departure auto reply must give information on leave and other relevant information and the e-mail-adress must be removed from the employers homepage etc. An active account shall in general only be used to receive e-mail and only one or few trusted emplyees should have access to the account.

With reference to paragraph 11.2 and the call for relevant legislation I can refer to the Danish Act on the use of healt data, etc. on the labour market. An English version of the act is available through the following link:
http://uk.bm.dk/Legislations/%7E/media/BEM/Files/English/Acts/Use%20of%20health%20data_act286.ashx

In general the act seeks to lay down provisions to prevent selection of workforce based on unregulated and arbitrary use of information on hereditary charateristics. Further the act applies to all heath data regardless of whether the information stem from genetic research or other sources.

FRANCE

1- Sur l 'étude relative à la Recommandation relative au Travail (R(89) 2

La position du représentant français est de reconnaître la nécessité exprimée par le rapporteur de mettre à jour et moderniser cette recommendation pour prendre en compte tous les changements technologiques intervenus depuis 1989.

Pour l'ensemble les commentaires du représentant français vont dans le sens de ceux exprimés par l''Espagne et le Portugal notamment sur le fait que si les principes généraux sont toujours d'application, il est important de voir en quoi les changements technologiques actuels peuvent impacter ces principes et nécessiter leur adaptation. Tout particulièrement les principes de proportionnalité, de transparence , d'information du salarié en particulier sur les destinataires des données collectées , de l'utilisation de son consentement du salarié et de son droit d'accès aux données collectées et traitées par l'employeur doivent être revus dans cette perspective.

La proposition d'insérer les mises à jour et les modifications spécifiques uniquement dans le Mémorandum pourrait être la solution juridique adaptée.

En revanche, nous pourrions avoir une réserve concernant l'utilisation des données biométriques et génétiques

---

On the study on Recommendation N°R (89)2

The position of the French representative is to recognize the need expressed by the rapporteur to update and modernize this recommendation uin order to take into account all the technological changes intervenend since 1989.

The comments of the French representative are in line with those expressed by the'Espagne and Portugal in particular the fact that if the general principles still apply, it is important to see how the current technological changes may impact these principles and require their adaptation. Especially priinciples of proportionality, transparency, information to the employee in particular about the recipients of collected data, using the consent of the employee and his right of access to data collected and processed by the employer must be reviewed from this perspective.

The proposal to include updates and changes only in the specific Memorendum could be the adapted legal solution .

However, it seems necessary to be cautious about admitting the use of biometrics and genetic data

ITALY / ITALIE

General observations

In general terms we support the valuable Report which raises manifold criticalities for data protection in the employment sector in the light of new technologies, new scenarios of workplace and globalization. We agree with the proposal of reviewing Recommendation (89)2 – that although still valid overall – needs some modernization in order to keep high the level of protection of individuals in a context that has undergone profound changes. In particular we support the proposal to create a new Recommendation instead of approving only single modifications to the existing texts. A new Recommendation would represent an overall framework, with a stronger impact, more accessible to readers and adequate to the new challenges raised in the employment sector over the last decades.
In general terms we also support the draft of the "new" Recommendation attached to the Report with the manifold elements that have been introduced. However, we suggest some modifications in track-changes that may hopefully clarify the text (and that we propose in a "word" version of the text; see below). We also point out that the proposal introduces a lot of innovative elements that may need a thorough background explanation. We suggest that the Explanatory Memorandum may play an essential role for that aim. This is particularly the case for paragraph 5.3 (collection of data related to the potential employee); paragraph 5.5 ("gradual" monitoring); paragraph 9.4 (transparency v. privacy).

1.The new context of the working world
The study conducted on the Recommendation was of a general nature with reference to a variety of new implementing problems, devoting particular attention to new technologies and their impact on the monitoring of employee's activities. This document takes into account the request for a concise report. Approximately 22 years have passed since the Recommendation was adopted. This considerable period of time is like a century in terms of technological development.

Work per se has changed a lot (in terms of subject matter, form, duration and intermediaries), as have the places where it is performed and the way in which it is organised.
Employers, employees and their needs have changed and the spectrum of personal data that is handled has also become broader (IP addresses, log files and location data, for example). This is not caused by new technologies alone.
There is a new international dimension to work, which is global and local at the same time, also due to the heavy use of outsourcing organised on a worldwide scale (for example, the offshoring of call centres). Manufacturing processes, even if coordinated in a more centralised manner, are at times fragmented in several countries throughout the world. In the not too distant future, there is the prospect of cloud computing, that is to say the development of information technologies which use hardware resources (storage, CPU) or software distributed remotely, therefore making it difficult to determine which law would apply to it.
There is significant fusion between public and private sector work: the first embodies the main typical contractual elements of the second. In the public sector and in some private situations (e.g. listed companies), a need for greater transparency is felt, which is sometimes guaranteed by law to control expenditure, for e-government or to ensure correct operation of public bodies or public interest bodies. This brings with it a greater requirement for the publicity, also online or at the request of interested parties, of personal data for competitive selection procedures, personal reference details, curricula vitae, positions and salary brackets. It is therefore even more necessary than in the past to explain in detail to employees what is 'public' or in any case 'knowable', within the context of their employment relationship.

Over the last few years there have been other, similar developments:

- as a result of legislation regulating financial services;

- due to the legal obligation for branch offices established in some countries (such as the USA) to also produce documents, materials and a lot of personal data regarding employees and directors electronically with reference to civil disputes (eDiscovery) or law enforcement proceedings, which sometimes conflicts with the protection of data in other countries;

- the detection of possible fraud, dangers and other serious risks that can damage clients, colleagues, shareholders, the public or the very reputation of the company, public body or foundation (known as 'whistleblowing'). we seize the opportunity to highlight the approval by the CoE Parliamentary Assembly of Resolution 1729 (2010) on the protection of "whistle-blowers". We take the liberty to point out that in the revision process of the principles on data protection in the employment sector it would be important to guarantee a coordination within the Council of Europe between the different groups working in interrelated subjects as in the case of whistleblowing that has obvious data protection implications (see for example the Wp29 Opinion 1/2006).

Regardless of the more modern internal organisation of work, personal data handled for work-related purposes increasingly travels the whole planet, not just within the confines of branch offices and subsidiaries. There are major risks, liabilities and uncertainties surrounding data being used more easily for other ends and in ways that are incompatible with the original objectives for which it was intended, or else lost or rendered accessible to third parties or within the workplace in an unauthorised and non-transparent manner.

As already noted, working methods have changed significantly over 22 years. Whereas, for example, teleworking is more widespread (although not used as intensively as expected), there are many more fragmented and temporary forms of work, including working for several employers, sometimes at the same time or via intermediary organisations operating online.

At the main, physical workplace (when this is the centre of work activities), the employer can be traced more easily using various mechanisms (access to information systems and offices; mobile devices; pagers; RFID readers). There are important developments in terms of data protection (for information and resulting from data use that is non-transparent or incompatible with the purposes for which the data was originally intended) due to work webmail systems, mobile telephones and smartphones, as well as specific work activities which make it possible to trace the position of equipment and people in great detail, also with the help of GPS systems (e.g. drivers of special vehicles and the transport sector).

New developments have also emerged from ubiquitous computing, a new post-desktop model of work organisation which envisages a different interaction between man and machine through which information processing is integrated within everyday objects and activities. Someone using ubiquitous computing engages or uses many computational devices and systems simultaneously in the course of normal work activities and may not be aware of the fact that they are performing operations and sending and receiving data.
With regard to the context of 1989, the following should also be highlighted:

- the growing importance of data protection in the domain of the protection of the physical health and safety of employees. For example, consider the role of the company doctor in the workplace, who must process data regarding health independently. In principle, the employer may not have access to this data, even though it is jointly responsible for

its secure processing. At times, data that is not always anonymous in relation to people outside the workplace must also be processed (for example, in companies carrying out dangerous activities);

- collective or company contracts, or primary or secondary legislation which grant trade organisations the right to access aggregate, anonymous or sometimes individual data. Moreover, trade organisations use - de facto or following agreement with the employer - information systems inside the workplace for information or promotion purposes which poses problems in its application;

- the tendency of employers to collect data outside the context of work, even without the knowledge of employees, from police forces or on the Internet using search engines and social networking sites for example, which presents new perspectives in relation to the analysis in the Memorandum (point 11).

All these new challenges are not always accorded enough attention by legislators (including European ones) and national supervisory authorities. Not infrequently, the principles of data protection that apply to the working world have remained the same general principles that are used for other public and private domains, with few principles specific to the working world.
The general canons of data protection laws remain valid and, in general, offer flexibility to the working world; however, they do not allow for the provision of more specific rules which might at times be necessary (consider, for example, the need to prevent discrimination in the workplace made possible by the use of genetic data).

In various countries however, new legislation to protect employees in different spheres and for different purposes from traditional data protection laws has appeared. This legislation lays down several rigorous restrictions, in principle prohibiting, for example, the collection of certain data or the use of certain questions or behavioural tests at the time of recruitment, even with the consent of the interested party.
The difference in the approach of national legislators in this area has only partially subsided. Still today, different categories of data are transferred to remote centralised databases of a parent company, based on the consent of the interested parties which however, in this case, would seem rather inappropriate in reality. Some companies use, albeit not on a large scale, standard contractual clauses which can be agreed between controllers and controllers or between controllers and processors, prepared or deemed adequate on the basis of a heated debate which developed in Europe and internationally. It should be noted that codes of practice (also called 'binding corporate rules') are progressively, albeit slowly, being developed whereby the multinational organisations in question establish internal measures as a guarantee for interested parties (audits, training programmes, privacy officer networks, systems for dealing with complaints, etc.) which are considered as 'binding' within the Group of companies and which are then examined by data protection authorities.

2. Guidelines for a revised Recommendation

Despite these profound changes in context, the Recommendation of 1989, having been drafted with farsighted legislative skill based on general and flexible sets of requirements, still remains valid overall, considering the fundamental guarantees provided by Convention 108 and its additional protocol.
It is believed that to date, there is justification for maintaining a specific recommendation on this subject, after however revising it to incorporate several targeted modifications, as well as a few selective additions aimed at developing the existing general principles which seem effective for the next few years as well.

For convenience, an organic text for a 'new' Recommendation is enclosed in annex which highlights these modifications and additions, making it possible to adopt either a new Recommendation to replace the previous one entirely (although it would contain, as already stated, only partial modifications and additions: it is the solution that is suggested), or to approve only single modifications and additions to the existing text of the Recommendation which would therefore formally remain in force.

In both cases, it would be necessary to adopt a comprehensive approach and to maintain a balance with the other recommendations of the Council of Europe pertaining to other sectors, some of which contain useful references for the working world (In particular Recommendations No R (86) on the protection of personal data used for social security purposes, No R (95) 4 on the protection of personal data in the telecommunications services sector, with particular reference to telephone services, and No R (97) 5 on the protection of data of a medical nature), reserving any circumscribed

- revisions of such instruments for other occasions. We suggest to explicitly consider Recommendation No. R (92) 3 on Genetic Testing and Screening for Health Care Purposes, stating that "Health service benefits, family allowances, marriage requirements or other similar formalities, as well as the admission to, or the continued exercise of, certain activities, **especially employment**, should not be made dependent on the undergoing of genetic tests or screening)". (Principle 6 - Non-compulsory nature of tests) . The recently adopted Recommendation on profiling may be mentioned too considering that the issue is taken into account by the draft Recommendation (See Principle 5.3 and 6.2).

Compared with the past, the workplace is now considered to be more of a social development where the worker has the right to develop his or her own personality, and this applies not only with regard to colleagues within the workplace as the Memorandum already emphasises.

Important case-law decisions recognise the employee's right to enjoy a reasonable sphere of privacy in his or her personal and professional relationships. It is a right which goes beyond the privacy; already guaranteed traditionally (company canteens, lockers, drawers, changing rooms and, within certain limits, behaviour outside the workplace). Employees advise of their need to use the Internet briefly for entirely private purposes during what are sometimes long working hours, to follow up a matter with a public office or a health structure for example. This could take place in a way and within limits that the employer would find acceptable and would be clearly defined. It would be necessary to declare in the introduction that there is a new framework internationally of case-law origin too which has further affirmed fundamental rights and freedoms in relation to data processing, thus contributing to the codification of new fundamental rights (for example, that of data protection or the sanctity of the virtual residence), affirming the dignity of employees in relation to remote monitoring, or providing better guarantees for various forms of habeas corpus or habeas data in relation to biometrics and genetic data.

The Recommendation should only contain technologically neutral principles that are also capable of withstanding technological development, which promises to be unremitting, for a few years without 'chasing after' specific technologies or applications which would only be considered expressly in a few parts of the text or in the Memorandum alone.

Nevertheless, a recommendation on this subject should no longer look at the aforementioned phenomenon from the historically outdated 'automation' viewpoint, as was the case in 1989 and should rather concentrate more on the 'virtual' aspect of many workplaces. Moreover, the existing

Recommendation looks in great detail at the 'Introduction' of information systems, rather than their operation, and this reference should also be adapted to suit today's realities as well. The use of technologies and systems is now, in fact, routine. The e-workplace is a diverse and inescapable reality and more rigorous attention to new applications is required.

The Recommendation should regulate the traditional employment relationship in the private and public sectors, essentially without distinction. It would then be useful to underline that any adaptations of its principles might be necessary for specific situations, particularly with respect to communications by employees subject to special obligations of professional secrecy (for example, industrial or company secrets or the protection of journalistic secrecy in publishing firms).

It would also be useful to devote more attention to growing data traffic in relation to only fixed-term or part-time employees, whose data is sometimes known by several employers and intermediaries at the same time, sometimes via online systems used even for welfare and social security purposes. This attention should also be directed at the duration of data storage of those not employed, or not passing behavioural tests or carrying out probationary periods.

It would be important to give a signal on the subject of interested parties exercising their rights to personal evaluation data. A reasonable balancing of the interests involved could allow the employee access to data regarding him or her when the evaluation process is concluded, without prejudice to employer's or third party's need for temporary protection; however, it should only be possible to change it in the traditional way based on common agreement.

Lastly, the new background of rights, starting with the protection of personal data, would make reflection on the current distinction between automated and non-automated processing desirable. A precise statement would be desirable however, even though the Recommendation already censures any possible circumvention in this respect (Point 1.1).

3. Development factors of new principles and whom they address

Alongside the specific modifications of existing provisions as indicated in annex, it would be advisable to introduce some guidelines which would be inspired by five new principles, some of which could moreover be useful in the future for recommendations in other sectors.

Privacy by design

The Recommendation should still focus primarily on the activities of data controllers. However, it would be useful to focus some attention on those who design, produce and distribute software and technologies (as well as researchers and bodies providing their certification or promoting standards), as well as service and access providers.

A preventive approach inspired by a rationale of privacy by design could reduce implementing problems, by encouraging the distribution of products with privacy oriented products which are more focused, already from a technical and organisational viewpoint, on the principles of necessity and proportionality. The negative fallout following the distribution and use of these products would thus be contained.

Accountability

It would be advisable to affirm the accountability of data controllers. In the working world too, there is a need to ensure that legal obligations and general principles are better translated into concrete best practices, so that data protection is more a part of the shared values of an organization than in the past and they are assigned more specific responsibilities within it.
This outcome could be promoted by encouraging data controllers to adopt technical and organisational measures to ensure that the aforementioned principles and obligations are

developed in reality and can be demonstrated to supervisory authorities by the data controller at their request.

The Memorandum could then suggest several examples of effective mechanisms, adapted according to each situation, which could support real data protection such as:

- updated processing inventories;
- binding internal procedures and/or policies defined prior to the introduction of new data or processing categories, with jobs and roles to be organised according to the importance of the case or event to clarify in advance, for example, how to provide adequate information to interested parties or how to give them adequate replies in the event that they exercise their rights or complain;
- privacy impact assessments for high-risk processing operations;
- the appointment of a data protection officer or a more precise assignment of responsibility
- to ensure a more organic management of data processing; the introduction of mechanisms for the internal audit or independent inspection of the state of progress in applying legislation;
- the identification of internal procedures to highlight security risks or breaches;
- training activities and certification at various levels, including management.

It should then be emphasised that this principle should not weigh down the obligations of data controllers, nor needlessly duplicate already existing ones; rather, it should help controllers to ensure de facto effective compliance and to be in a better position to demonstrate it in the event of inspections and disputes.

Principle of necessity
In concert with privacy by design, it would be useful to encourage that information systems and software are configured to reduce the use of personal and identification data to a minimum for the purposes required. Furthermore, it could be made clearer that employers should process data in the least invasive manner possible.

Prohibition on data-processing for the primary purpose of remote monitoring
For the protection of dignity to be more well-defined, it would be necessary to prohibit more explicitly activities which consist, even occasionally, in the processing of personal data for the direct and primary purpose of remote monitoring (physical or logical) of work and other personal conduct. Employers should abstain from using the results of this unlawful processing, even when employees are not aware of it.

However, processing which consists in such monitoring only indirectly, in so far as it is primarily a main work organisation or safety objective which renders it necessary, it could be deemed legitimate, but should be subject to adequate information including information to union bodies, and performed with their agreement where possible.

Principle of simplification for small concerns
Finally, it would be useful to follow a greatly simplified approach for small business concerns (small firms, craftsmen and laboratories) whereby a few adaptations to the implementing conditions would be encouraged so as to avoid excessive bureaucracy without damaging the level of protection.

4. Specific revisions or modifications
Considering the request for a brief document, the minor modifications made directly in the annexed text are not explained in full here. Instead, some issues which need to be revised in the Recommendations or the Memorandum are summarised. As already mentioned above, the former is still adequate for the purpose of regulating some issues. Therefore, it is proposed that some clarifications, examples, suggestions and specifications mentioned in this document which are not inserted in the text in annex would only be inserted in the Memorandum.

Collection of data from social networks

Various employers (and intermediaries) have become fully aware of the operation of virtual communities and other services hosted on the web, such as social network services (SNS). Users of these online communication platforms, which are experiencing exponential growth, input a lot of data and content which describe their habits, preferences, friendships and interaction with other users, assisting the creation of detailed profiles of people based on their interests and activities. Access to this data can be restricted to contacts which users have chosen, but some users do not restrict such access, accepting 'contacts' without worrying about the existence of a connection. Sometimes, it is possible to have contacts from third parties, even strangers, when all the members of an SNS can look at a profile, for example, or when data can be indexed by search engines within or outside of the SNS.
The default set-up, which can be harmful for privacy, is only changed by a minority of users.
The data can be used by third parties for various purposes, even commercial ones, and can pose risks including the loss of a commercial or employment opportunity. Whilst there are reports of various dismissals motivated by circumstances where employees have simply exchanged some self-deprecating remarks regarding their employment situation 'in private' on an SNS, various users continue to extol the legitimate expectation that personal data entered for the sole purpose of socialising on the Internet with certain people be processed in a lawful and proper manner.

The Recommendation should definitely take into account the fact that the controllers of SNS already have independent obligations, especially in terms of information, defaults and proportionality. However, it would be useful to provide brief guidelines for cases where an employer collects and uses data relating to job applicants or employees more or less without their knowledge through an intermediary, under another name or using a pseudonym and combine it with other information. In principle, this data collection is not actually right, regardless of whether or not the employee is a member of the SNS (some SNS allow users to enter 'tagging' data for non-members).
Instead, there should be a separate discussion with reference to networks where only news of a work/professional nature is exchanged, which it would be appropriate to consider separately to the more 'private' SNS.

Collection of data using search engines or placing employees' data on the Internet

Similar considerations would be stipulated with respect to the periodic collection of data using search engines outside the organisational structure of work.
The problem of the 'open nature' of the Internet and the protection of the personal data of its users also applies, in fact, in relation to recruitment procedures and the employment relationship. Search engines are part of everyday life for those using the Internet and technologies to search for information. As service providers, these search engines collect and process large quantities of data, also harvested via special means like cookies (IP addresses and search chronology; data provided to enjoy personalised services).
Search engines contribute towards making various and precious information easily accessible, with increasingly sophisticated opportunities thanks also to added-value services such as the profiling of physical people (known as 'people-search engines') and facial recognition software based on pictures.
The types of data that they aim to have collected, including sounds, pictures, videos and other formats, are manifold. Some search engines replicate data in temporary memories (known as caches). By reassembling general information of various types under single individuals, search engines can create new profiles, however incorrect, of a person who runs a significant risk in the event that the individual data making up this profile is browsed separately.
The capacity of search engines to assemble data can have a significant impact on a person's private and social life, especially if personal data derived from a search is incomplete, excessive or incorrect, or even to be deleted by virtue of the right to be forgotten.
In spite of progress and efforts including those of data protection authorities, users are still not sufficiently aware of the consequences arising from the use of these services, or of the purposes, even if secondary in nature, of the operations which result from it.
Theoretically (even if it is not easy in reality for the average user), an employee can turn to the controller of a search engine to have personal data which is no longer useful for the purposes for which it was previously collected cancelled or rendered anonymous (particularly when the data no longer corresponds to the actual content published on the 'source' website). However, in the same way as SNS, there is a specific need to encourage data collection by employers to be more pertinent and transparent.If the Recommendation takes search engines into consideration, it could also, with reference to an entirely different aspect of the issue, take into account the fact that employers increasingly use the Internet and Intranet to develop their own websites for corporate or promotional reasons with regard to citizens, consumers and users. In this way, it would be possible to devote more attention to information for employees about data concerning them which is intended for publication, as well as to the principle of purpose.

Biometric data and RFID techniques

The Recommendation could expressly consider the significant use of innovative biometric, wireless and location systems and Radio Frequency Identification technologies (commonly known as 'RFID technology') for a variety of purposes and applications, some of which may violate human dignity and human rights or present major risks to the latter.

The employer is able to collect, sometimes in a non-transparent manner, various data relating to entries, movements and activities of people, especially if they are assigned to certain tasks. Personal data on employees is collected indirectly as well via surveillance by objects and products sold over the counter or wholesale which track their movements.

The use of chips, often invisible, is attractive to the employer because it has positive effects on work organisation and may be used easily even by means of portable devices or by placing them inside objects, clothes or uniforms, sometimes with the consent (induced) of the parties concerned,

but not always in observance of the principles of data protection, especially in relation to the absence of adequate information regarding the use of the data.

There are event systems that can be imbedded under a person's skin, who is then transformed into an 'antenna' or sensor, with little consideration of habeas corpus or the principle (which in this instance is turned on its head) according to which information systems should be of service to mankind.

It would be necessary to encourage the adoption of internal privacy policies which, together with the explanatory Memorandum, respect more specifically the principles of:

- necessity ;
- proportionality (also in relation to various biometric data, some of which present greater risk such as fingerprints and iris recognition, and other less invasive ones such as hand geometry) ;
- purpose (exclusion of further use: for example, data from car park entries used surreptitiously to compare with attendance data) ;
- adequate and easily understandable information on the types of data, regarding the fact that the devices produce data even without the consciously active behaviour of the person concerned, regarding the possibility - if it exists - of switching devices on and off and the consequent effects, as well as all the intended uses of the data and how to exercise their right to be informed ;
- limitation of data storage time.

The reasonable use of these systems should take into account the fact that some options present more or less invasive effects: the use of verification, rather than identification techniques; the creation of a centralised database containing biometric data, rather than just placing it on a portable device at employees' disposal; the use of more powerful readers that read from a great distance; the adoption of solutions which do or do not allow the employee to switch off the device.
In the presence of adequate guarantees, consent does not in any case, at least in general, seem to be the ideal foundation for these types of data processing

Unique identifiers

If 'unique identifiers' are used in the workplace, it is easier to trace data relating to a single employee and create profiles in a scarcely visible manner as well. This may occur, for example, to profile employees based on the type and number and time spent in relation to documents they consult to which they have access (consider companies engaged in the production and distribution of multimedia products wanting to check for infringements of copyright by employees).
The issue would be treated organically as an integral part of the theme of monitoring employees, but specific attention would be devoted to the possible use of unique identifiers in so far as these can signal the existence of an intention a priori to trace an employee. In principle, tagging a document should not be linked to an individual unless it is indispensable to perform a certain service and there is full information and, where possible, consent.

Genetic data

Some employees have manifested significant interest in using genetic data before hiring employees in order to provide a fuller profile of candidates or to identify those not adapted to a particular job (for example, in the case of a declared illness or risk of illness), or to identify possible protective measures to improve the working environment.

This also presents possible risks of discrimination and serious violations of human dignity and the right of self-determination.

Genetic tests sometimes have an uncertain probabilistic and predictive value but regardless of this fact, processing genetic data for employment purposes must be prohibited in principle and admitted only in exceptional circumstances where it is used for purposes of a very different nature (like a case where an employee voluntarily produces documents which include genetic data, submitted to the company doctor at the workplace in order to have a measure introduced for his or her advantage or protection such as, for example, due to occupational illness or a dispute). *Data relating to seropositivity, AIDS or drugs or alcohol abuse* Limited revision of the Memorandum could be carried out also regarding the issue of seropositivity and AIDS, which poses similar problems of possible discrimination, but also requirements to protect the health of third parties such as, for example, assisted or transported third parties. More specifically, there could be mention of the reasonable tendency to selectively identify exceptional situations or jobs which really do expose other employees or third parties to health risks and which should therefore warrant an exemption from the tendency to prohibit processing of this data, in the presence of appropriate guarantees also in relation to the sphere of movement of the collected data and the dignity and right to protection of the parties concerned.

Access to medical records held elsewhere

There is an increase in the use of electronic medical records, meaning the collection of medical documentation on the past and present physical and mental state of an individual which allow a quick overview of rather delicate data for the purpose of medical treatment and other closely related purposes.
Electronic medical records should be accessible (except by the interested party) only by health practitioners and personnel authorised by the health structures assisting in the treatment of the employee, moreover with 'record-specific' consultation rights. The main purpose of their consultation should remain that of facilitating the success of a medical treatment due to better information. Access for any other reason, including for employment purposes even if via experts or insurance companies, should be prohibited in principle. This is in reference either to possible direct online access by the employer (several devices based on tokens or electronic signatures are emerging on the market), or to indirect access by the employer who can put pressure on the employee to persuade him or her to provide the documentation in a manner that is neither voluntary nor based on free consent. Commensurate protection should be arranged also for off-line records.

5. The monitoring of employees

Reasonable expectation of privacy in the workplace

New technologies still represent a positive development in the working world, even if employers can also use them in ways that are injurious to fundamental rights and freedoms. Thanks to them, it is easier to analyse, reconstruct and profile the use of information systems for work purposes using, for example, navigation or traffic log files obtained from the proxy server or from other information recording instruments, which can also allow the employer to know the content of the communications.

Employees should not leave their own privacy and data protection rights outside the workplace. To the contrary, they should be able to claim a legitimate expectation of a certain level of privacy even in the workplace where they develop a significant part of their own relationships with other human beings. This expectation should not be undermined by the fact that the employee is using communication media and tools which belong to the employer.

The protection of private life includes the right to develop these relationships and these place limitations on the legitimate prerogative of the employer to carry out supervision activities. The employer has the right to encourage efficient management and to protect itself against liabilities and damages which employees' actions may give rise to. Monitoring and surveillance activities in the interests of the employer should however be lawful, transparent, effective and proportionate, and this reasonable approach would also avert possible negative effects on the quality of their professional relationship.

The Recommendation could encourage a more common position on the subject and a further harmonisation of national practices and legislation with a global viewpoint which would also take into account the secrecy of correspondence and possible exemptions from it, as well as powers of information and co-decision which organisations representing employees exercise on the basis of the law or collective bargaining.

The modern notion of 'privacy' includes activities of a professional or commercial nature. The concept of secrecy of correspondence has also been amplified, developing into the new generation's 'secrecy of communications'.

The location and ownership of the electronic media used should not be a reason to exclude the secrecy of communications and correspondence. Online and traditional correspondence should not be treated differently without a valid reason: with given conditions, electronic mail would also be subject to similar, if not absolutely identical, considerations as traditional mail on paper. Already today, but even more so in the years to come, the evolution of working conditions makes it more difficult to establish a clear separation between working hours and private life. In particular, with the development of the 'home office' model, many employees continue to work at home or outside the office using IT infrastructures which may or may not be placed at their disposal by the employer for this purpose.

The specific considerations in this report relate to the most common situations in which employees may find themselves, but it is also taken into account that:

- more or less proportionate monitoring could be carried out for reasons other than safety or the prevention and verification of unlawful behaviour, such as for the purpose of random monitoring even of productivity and individual capacity or general monitoring of work or checking working hours;

- general monitoring may involve management figures (managing directors or managers), independent professionals operating in the workplace (doctors) or persons in charge of internal control in an unbiased position (audits or statutory auditors) or lastly, trade union organisations. In all these cases, there are specific problems which will be assessed separately;

- some work activities (financial transactions, professional training for example in direct marketing or emergency calls) may justify, in the presence of adequate guarantees, thelawful and correct recording of external contents or data of communications or conversations for proof or research purposes;

- secret spot checks may be set up by the employer at the request of judicial authorities or the police for the purpose of criminal justice pursuant to the law.

These considerations regard the predominant problem of Internet navigation and electronic mail, as well as the use of electronic devices placed at the employee's disposal, but also relate, with the necessary adaptations, to the more traditional issue of the monitoring of fixed-line telephones in the workplace.

Observance of the canons of data protection may also prevent problems relating to the admissibility of evidence in criminal, civil or employment cases.

Information

The employer should indicate in a clear and detailed manner in all instances the method of use permitted for the tools placed at their disposal and whether, monitoring will be carried out and if so, the indicators and methods which will be used.

Information on the policy regarding the use of media and on monitoring should be clear, comprehensive, accurate and quickly accessible.

The information would be adapted to each work context (for example, for small concerns where there is constant interpersonal sharing of information resources) and expressed in a clear manner, and sufficiently publicised and updated periodically. The employer should for example specify, where applicable:

- internal rules on data and systems security or on the protection of company or professional secrecy envisage for any classes of employees, as well as the role of the system administrator and any relocation of servers in other countries;

- any personal use of electronic communication tools permitted which is invoiced to the party concerned, or definitely not tolerated (for example, the downloading or possession of software or files that are wholly unrelated to work activity), providing an indication also of the possible consequences, preferably graduated according to the seriousness of the offence (having to also take into account the possibility of involuntary visits to websites due to unexpected actions by search engines, advertisements or typing errors);

- any monitoring that the employer reserves the right to perform, providing an indication of the legitimate reasons for them and the methods used in principle, also in relation to cross-examination of interested parties;

- the log files in case any are kept, also in the form of back-up copies, and the persons who could have access to them.

Similar although not necessarily identical information should be provided to any trade unionorganisations which could play a role in terms of information, consultation or conciliation, especially on the introduction of significant changes when introducing new applications.
Adequate awareness initiatives would be studied vis-à-vis external parties that interact with the organisation if monitoring activities may involve them (e.g. message addressees).

Inspections: necessity and proportionality

In the Recommendation, also through the Memorandum, it could be highlighted that employers are expected to:

- ensure the functionality and correct use of electronic media and define the methods in which they should be used, also taking into account regulations regarding rights and trade union relations;

- adopt suitable security measures to ensure the availability and integrity of information and data systems.

- On the basis of determined, explicit and legitimate purposes, the employer could reserve the right to inspect the correctness of work performance and the use of work tools or to perform other types of inspection, for manufacturing, organisational or occupational safety (due to anomalies or for maintenance) requirements for example.

As already stated, activities whose primary purpose is remote monitoring, as in the examples below, should be prohibited:

- the systematic registration and possible reading of messages sent by electronic mail or of related external data, beyond what is technically necessary to deliver the service ;

- the systematic caching of web pages viewed by employees ;

- the secret analysis of portable computers entrusted to their care, during maintenance or replacement for example ;

- the secret reading and recording of typed characters using keyboards or similar devices.

The processing of data regarding an individual employee should be permitted when it is necessary in order to achieve the employer's legitimate interests (for example, to protect the working organisation from serious harm by stopping the leakage of confidential information) and does not infringe the fundamental rights of employees in an unjustifiable manner.

Priority should be assigned to interventions of a preventive nature, also through the use of technological solutions.

Constant or prolonged indiscriminate or unjustified inspections, which are difficult moreover to easily legitimise through the employee's consent (inappropriate for the most part, and also insufficient in these cases, given the presence of third parties as well) are excluded.
In the event that it is intended to conduct inspections, the employer should check beforehand that they are indispensable for a certain objective and are commensurate with that objective, considering other methods of supervision which present less intrusion of personal privacy (avoiding, for example, the use of systems which perform automatic and constant inspections).
Furthermore, various software programmes are capable of automatically alerting the employee that a certain activity is not permitted or correct, and that activity may also be prohibited in a similarly automatic way, without formally reporting the prevented event.

Gradualness and proportionality should also guide cases where an omission on the part of the employee would be referred to his or her superiors and to the management (evaluation of the practicality of warnings at a lower level).

Internet

In order to reduce the risk of improper use of the Internet (browsing of non-relevant sites, file or software uploads or downloads, the use of network services for purposes unrelated to work), the employer should adopt appropriate measures, even by using filters, in order to avoid subsequent inspections of employees which could also moreover involve sensitive data.

These measures could, for example, consist in:

- a priori identification and specification of categories of sites which are definitely not related to work;

- ensuring that during inspections, only data that is anonymous or that does not allow the immediate identification of users is processed by used appropriate data aggregation techniques (for example, analysis of log files relating to web traffic of groups of employees only).

- The employer could obviously not provide employees with an e-mail account or Internet access, but when computers with Internet access are assigned, an extreme and total ban from using the Internet for personal reasons does not recognise the modern reality of work.

- The abuse of the Internet by employees could be identified using aggregated or anonymous data without analysing the content of the sites visited. Verification of navigation times or site categories most frequently visited could give sufficient assurance of the absence of abuse, even when such checks are performed in relation to the entire organisation or parts of it, instead of individual employees. When examining the latter, more specific inspections could be initiated if the first general checks bring possible abuses to light.

Electronic mail

In certain situations, especially in the absence of an explicit and reasonable internal policy in the workplace, the content of electronic mail messages - together with certain data external to the communications and the attached files - could be protected by a guarantee of secrecy of correspondence and communication, protected in some countries even at constitutional level. The inspection of an employee's correspondence or of his or her use of the Internet should only be deemed necessary in exceptional circumstances.

Sometimes, there could first and foremost be a doubt as to whether the employee receiving or sending a message is using their e-mail for personal or work purposes.
A proper policy could therefore clarify the legitimate expectations of confidentiality of the employee or third parties and could avoid the behaviour of the employer intending to discover the content of the messages being unlawful or incorrect in the case in question.

In order to prevent a regrettable dispute, the employer could for example:

- recognise the employee's right to use a further e-mail address for private use, or encourage the additional use of e-mail addresses shared within the same unit by several employees;

- ensure that in the event of absence from the workplace, the system has a function which automatically communicates coordinates from another useful point of contact;

- pre-establish a procedure that allows access to the work-related e-mail without conflict in cases of necessity during an employee's absence, in a transparent and correct manner that the employee has already been informed of, and which can theoretically allow him or her to ensure that a person they trust assists the opening of the e-mail;

- insert a warning for recipients in some e-mail messages to underline the 'work' nature of the messages and the fact that the contents of the reply can be known.

The inspection of e-mails could become necessary in order to obtain confirmation or proof that the employee has completed certain prohibited actions in relation to which the employer must defend its own interests. Consider, for example, the case where the employer has a secondary liability for the actions of its employees, it has to detect the presence of viruses, or guarantee the security of the information system or even gain access without fail to the e-mail of the employee who is absent due to illness or holidays.

At least at the beginning, the monitoring of electronic mail should in principle be limited to data regarding the size of the exchange of correspondence and the length of communications, rather than interesting themselves in their content, if this is sufficient to satisfy the employer's concerns. Access to the content of electronic mail simultaneously involves other persons, inside or outside the organisation, whose consent cannot be obtained.

Following an unsuccessful anonymous inspection, a general warning could be given concerning significant improper use of IT tools accompanied by an invitation to a number of employees to adhere to the instructions provided.

Finally, in the event of any maintenance of the information system, access to personal data on paper or memories assigned to employees should in principle be prevented.

Data storage

Developing the theme of the principle of necessity, software must be programmed to cancel personal data relating to Internet access and electronic traffic (by recording over it, for example) periodically and automatically. In the absence of particular technical or security requirements, temporary storage of data relating to the use of electronic tools should be justified for a proven purpose, within the limits of the predetermined time required to achieve it. Exceptional prolongation of storage times should only occur due to extremely unusual technical or security requirements or due to justice or defence-related necessity.

On the basis of the principle of proportionality, the employer should not retain data resulting from inspection activities for a longer time period than necessary for the reason declared, with the legitimate exception of defence and justice requirements. Data should not be used for other purposes.

6. Video surveillance

Dating back circa 8 years, 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 at its 78th meeting on 20-23 May 2003 remain current and it does not seem necessary to expand upon them in the Recommendation in connection with the employment relationship.
In order to avoid overloading the Recommendation and modifying it in an excessively general or fragmented manner on the specific secondary subject of video surveillance, it is suggested not to insert new provisions on this matter and to make a simple reference to these either in the introduction or in greater depth in the Memorandum, also in order to provide a global view of the issues involved. A similar reference was made in the introduction by Recommendation of the Parliamentary Assembly of 2008 on video surveillance in public places.

7. Conclusions

Some 22 years have elapsed since the adoption of Recommendation No R 0(89) 2, but the text is still topical in various parts, to some extent as a result of the farsighted technique used in its drafting at the time, based on general principles.
There have nevertheless been substantial changes in the organisation of labour in the meanwhile, due in part to the development of new technologies, search engines, social networks and biometric data, so the background now delineated is very different.
It would be useful, therefore, to include some guidance in the Recommendation or Memorandum derived from recently evolved general principles in connection with technological development, in a technologically neutral fashion (privacy by design; accountability; necessity; the data-processing ban with the primary aim of remote monitoring; simplification). With particular reference to the monitoring of employees' work, only a few amendments and additions would be useful, and in some cases only in the Memorandum, while arranging for a full replacement of the Recommendation for the interpreter's convenience.
Necessity, proportionality and transparency could have a positive effect on the prevention of tension in the workplace, by balancing the employer's various requirements for the monitoring of employees and the proper use of electronic work instruments against employees' legitimate expectations, to enable them to enjoy a degree of confidentiality and form their personality in the workplace.

The Guiding Principles of 2003 on video surveillance are still topical, and a simple reference to them may suffice.

Appendix 1: Draft Recommendation CM/Rec(2010)… of the Committee of Ministers to member states on the protection of personal data used for employment purposes.
(Adopted by the Committee of Ministers on … 2010 at the … meeting of the Ministers' Deputies)

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

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

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

Believing, however, that the use of **data processing methods, in particular automatic processing,** by employers should be guided by principles which are designed to minimise any risks which such methods could possibly pose for the rights and fundamental freedoms of employees, in particular their rights to privacy **and protection of personal data**;

Bearing in mind in this regard the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 **and of the Additional Protocol regarding Supervisory Authorities and Transborder Data Flows of 8 November 2001**, and the desirability of adapting them to the particular requirements of the employment sector; Recognising also that the interests to be borne in mind when elaborating principles for the employment sector are of an individual as well as collective nature; Aware of the different traditions which exist in the member states in regard to regulation of different aspects of employer-employee relations, regulation by law being only one method of regulation;

Aware of the changes which have occurred internationally in public and private employment, in production processes, and in the globalisation thereof facilitated by innovative technologies intended to bring about further and strong development.

Supprimé : the fact that

Supprimé : designed

Considering that such changes make it necessary to revise the terms of Recommendation No. 89 (2) on the protection of personal data used for employment purposes in order to continue ensuring a high level of protection in accordance with Convention 108;

Deeming it unnecessary to incorporate into that new recommendation further specific principles governing the use of video surveillance since 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 Council of Europe's European Committee on Legal Co-operation (CDCJ) in May 2003' and referred to in Resolution 1604 (2008) of the Parliamentary Assembly of the Council of Europe are still topical;

Recalling in this context Article 6 of the European Social Charter of 18 October 1961 **and the International Labour Office's 1997 Code of Practice on the Protection of Workers' Personal Data.**

Recalling that the notion of "private life" stated by Article 8 of the European Convention of Human Rights as interpreted by the European Court of Human Rights, includes activities of a professional or business nature since it is in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. (Niemietz v. Germany - *Application no. 13710/88)*

Recommends that the governments of member states:

- ensure that the principles contained in the recommendation are reflected in the application of domestic legislation on data protection to the employment sector, as well as in other branches of the law bearing on the use of personal data for employment purposes;

- for this purpose, ensure that the recommendation is brought to the attention of the authorities established under domestic data protection legislation which are competent to supervise implementation of such legislation;

- promote acceptance and implementation of the principles contained in the recommendation by ensuring its wide circulation among representative bodies of both employers and employees. Maybe one could add a reference to the fact that the governments of member states should encourage such bodies to introduce and promote self-regulation mechanisms, such as codes of conducts ensuring respect for privacy and data protection in accordance with the principles of the Recommendation.
  Moreover, considering that Principle 3 is devoted to privacy by design, one may also include designers and suppliers of technologies among the addressees of the Recommendation as was done in Recommendation on profiling.

Decides that this recommendation is to replace Recommendation No. 89 (2) on the protection of personal data used for employment purposes.

Appendix to the Recommendation

1. *Scope and definitions*
1.1. The principles set out in this recommendation apply to the collection and use of personal data for employment purposes in both the public and private sectors.
These principles apply to automatically processed data as well as to other data on employees which are held by employers, in so far as such information is necessary to make automatically processed data intelligible, **or used in any way to take important decisions. By analogy, they apply, where appropriate, to any personal data relating to individuals outside the workplace which are processed for work safety purposes, and also to trade union organisations.**

Supprimé : security

Manual processing of data should not be used by employers in order to avoid the principles contained in this recommendation.
1.2. Notwithstanding the principle laid down in paragraph 1.1, second sub-paragraph, a member state may extend the principles of this recommendation to manual processing in general. 1.3. For the purposes of this recommendation:

- The expression ‘personal data’ covers any information relating to an identified or identifiable individual. An individual shall not be regarded as ‘identifiable’ if identification requires an unreasonable amount of time, cost and manpower.

- The expression ‘employment purposes’ concerns 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.

1.4. Unless provisions of domestic law exist to the contrary, the principles of this recommendation apply, where appropriate, to the activities of employment agencies, whether in the public or private sector, which collect and use**, also through online information systems,** personal data so as to enable **one or more contracts of employment, including simultaneous or part-time contracts,** to be established between the persons registered with them and prospective employers**, or to help discharge the duties relating to those contracts.**

Supprimé : contemporaneous

1.5. This recommendation does not, to the extent necessary for the protection of state security, public safety and the suppression of criminal offences, apply to confidential information collected or held by employers for employment purposes on persons recruited for posts or who work in jobs closely related to these matters.

2. *Respect for privacy and human dignity of employees* ***and protection of personal data*** Respect for **privacy, human** dignity **and protection of personal data, also as regards the possibility of employees' developing their personality** in social and individual relations at the place of work, should be safeguarded in the collection and use of personal data for employment purposes.

3. *Necessity, accountability and simplifications*

Supprimé : *development of other principles*

3.1 The information systems, computer software programs and electronic devices used for employment purposes should be configured, as the case may be certified and applied in any way to the working environment, in such a way as to minimise the use and storage of personal data, as well as to limit the use of directly identifying data to what is necessary for the aims pursued in the individual cases concerned. *(we are not sure that the wording "as the case may be certified and applied in any way to the working environment" is clear)*

Supprimé : only that

***3*.2. The employer should develop effective measures to ensure that the principles and obligations relating to data processing for employment purposes are respected in practice, and to enable this to be demonstrated adequately at the request of the supervisory authority.**

3.3. Appropriate simplified solutions should be adopted in small-scale working environments.

4. *Information and consultation of employees*

4.1. **The installation and use of information systems, computer software programs and electronic devices for the direct and principal purpose of remotely monitoring the working activity or actions or whereabouts of employees should not in principle be permitted.**

4.2. In accordance with domestic law or practice and, where appropriate, in accordance with relevant collective agreements, employers should, in advance, fully inform or consult their employees or the representatives of the latter about the introduction**,** adaptation **and operation of information systems, computer software programs and electronic devices** for the collection and use of **personal data necessary for requirements relating to production or safety or work organisation.**

4.3. **The employer should take appropriate measures, as may be found appropriate by DPAs, to assess the impact of any data processing which poses specific risks to the right to privacy, human dignity and protection of personal data, and to process such data in the least invasive manner possible.** The agreement of employees or their representatives should be sought before the introduction or adaptation of such systems, **programs or** devices where the

information or consultation procedure referred to in paragraph 4.2 reveals **such risks** unless domestic law or practice provides other appropriate safeguards.

5. *Collection of data* ***and particular forms of processing or of information***

5.1. Personal data should in principle be obtained from the **person concerned. (S)He** should be informed when it is appropriate to consult sources outside the employment relationship.
5.2. Personal data collected by employers for employment purposes should be relevant and not excessive, bearing in mind the type of employment as well as the evolving information needs of the employer.
5.3. In the course of a recruitment **or promotion** procedure, the data collected should be limited to such as are necessary to evaluate the suitability of **the persons concerned** and their career potential.
In the course of such a procedure, personal data should be obtained solely from the individual concerned. Subject to provisions of domestic law, sources, **including those from consultancies or social networks for the development of professional relationships,** may only be consulted with her/his consent or if (s)he has been informed in advance of this possibility. **Profiling of the person concerned based on the secret collection of data from search engines should in principle be prohibited. An employer should not persuade the person concerned to provide access to his electronic medical records held by third parties.**
In any event, appropriate measures should be taken so that also in the case of data readily accessible in electronic communications networks available to the public, only relevant, accurate and up-to-date data are used, thus also avoiding misinterpretation or unfair processing of that data in the light of the context of its origin.
5.4. Recourse to tests, analyses and similar procedures designed to assess the character or personality of the individual should not take place without his consent or unless domestic law provides other appropriate safeguards. If (s)he so wishes, (s)he should be informed **in advance of the use that will be made** of the results of these tests**, analyses or procedures and, subsequently, the content thereof.**
5.5 The processing of biometric data to identify or authenticate individuals should be based on scientifically recognised methods. In principle, it should be permitted only where it is necessary to protect the primary interests of the employer or to protect the personal integrity and health of employees or third parties. (*The notion of "primary interest" may need some clarification, for example in the Explanatory Memorandum, in order to avoid defeating the provision. We also wonder whether the possible intervention of DPAs, for example through prior checking, should be mentioned.*)
5.6. With regard to possible processing of personal data relating to Internet or Intranet pages viewed by the employer, preference should be given to choice, with the persons concerned being properly informed, in conformity with paragraphs 4 and 12, of preventative measures such as:

- **the configuration of systems or use of filters which prevent particular operations, as the case may be (such as uploading and downloading of particular contents);**
- **the identification of sites which are or are not deemed to relate to the work carried out;**
- **the implementation of a possible tiered monitoring system on personal data, providing first for non-individual random checks on data which are anonymous or in some way aggregated (for example, by production unit).**
- **where an employee uses, with the employer's authorisation, equipment which may reveal his whereabouts, in particular outside working hours, appropriate arrangements should be ade so that data relating to his whereabouts are not used and are automatically deleted as soon as possible.**

Supprimé : viewed
Supprimé : in
Supprimé :
Supprimé : grading
Supprimé : of possible monitoring

Appropriate internal procedures relating to the processing of that data should be established and notified to the persons concerned in advance.

5.7 Without prejudice to paragraph 4, first sub-paragraph, the employer should in principle refrain from systematically viewing the content of emails which are sent to an employee to whom an individual email inbox has been assigned or which are sent by him.

Where possible, preference should be given to assigning employees email addresses which can be , immediately traced to posts rather than individuals ,

Appropriate instructions should also be issued so that where an employee is absent the email system automatically communicates the details of another point of contact, indicating that the employee is temporarily absent. In exceptional cases, where the employee is absent, an appropriate procedure should cover the opening of solely work-related emails, after the employee himself has been informed, and, where appropriate, in the presence of a representative of his choice.

In order to inform the addressee that the email system is used purely for professional purposes, an appropriate warning should be inserted in emails sent by the employee.

Supprimé : are

Supprimé : traceable

Supprimé : not to individuals but

Supprimé : .

6. *Storage of data*

6.1. The storage of personal data is permissible only if the data have been collected in accordance with the rules outlined in paragraph **5** and if the storage is intended to serve employment purposes.

Where those rules are not complied with, the employer should refrain from using the data. (should this principle be extended also to the respect of the rules outlined in paragraph 4?)

6.2. The data stored should be accurate, where necessary kept up to date, and represent faithfully the situation of the employee. They should not be stored or coded in a way that would infringe an employee's rights by allowing him to be characterised or profiled without his knowledge.

Where the use of biometric data is permitted under paragraph 5.5, they should not, as a rule, be stored in a database, and preference should be given, where appropriate, to biometric identification or authentication systems based on media made available solely to the person concerned.

6.3. Where judgmental data are stored relating to the performance or potential of individual employees, such data should be based on fair and honest evaluations and must not be insulting in the way they are formulated.

7. *Internal use of data*

7.1. Personal data collected for employment purposes should only be used by employers for such purposes.

With due regard to the principles of relevance and accuracy, and with regard in particular to largescale or territorially extensive working environments, certain personal data could be made easily identifiable in internal communication networks in order to speed up the performance of the work carried out and facilitate interaction with other employees. (*This paragraph may need some clarifications. In particular one may provide that legal tools –at least policy documents- should identify the main characters and modalities of such communication.*)

Supprimé : .

7.2. Where data are to be used for employment purposes other than the one for which they were orig-inally collected, adequate measures should be taken to avoid misinterpretation 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 the employee are to be taken, based on data so used, he should be informed.

7.3. The interconnection of files containing personal data collected and stored for employment purposes is subject to the provisions of paragraph 6.2.

7.4. Without prejudice to Article 9, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to respect for the principle of purpose specification in the subsequent use of the data, also as regards any changes in processing

of which the persons concerned must be informed in the due respect of applicable law and as may be found appropriate by DPAs

8. ***Communication of data and use of information systems for the purpose of employee representation***

8.1. In accordance with domestic law and practice or the terms of collective agreements, personal data may be communicated to employees' representatives in so far as such data are necessary to allow them to represent the interests of the employees.

8.2. The use of information systems for trade union communications should form the subjectmatter of appropriate agreements with the employer designed to lay down in advance transparent rules permitting correct use and to identify safeguards to protect any confidential communications.

9. *External communication of data* ***and dissemination***

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

9.2. 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 enterprises in the same group, should only take place: a. where the communication is necessary for employment purposes which are not incompatible with the purposes for which the data were originally collected and where employees or their representatives are informed of this; or b. with the express and informed consent of the individual employee; or c. if the communication is authorised by domestic law, **in particular where necessary for judicial purposes or to exercise a right before a judge.**

9.3. **With the consent of the employee or on the basis of adequate safeguards provided by national legislation, personal data can be communicated within a group of enterprises for the purpose of discharging duties provided for by law or collective agreements relating to work and social security and welfare for employees, or to optimize the allocation of human resources.**

9.4. **With regard in particular to the public sector, the law should reconcile the right to privacy and protection of personal data with the requirements relating to transparency or monitoring of the correct use of public resources and funds. To that end, professional categories or profiles should be identified for which specific disclosure obligations are applicable under the law with regard to specific items of information , as also the contents of the information that may be disclosed. , Account should be taken to the possibility of identifying them more easily where they can be traced through external search engines.**

9.5. **When the work tasks entail a constant relationship with the public or where this is necessary to meet requirements relating to transparency vis-à-vis users, consumers and citizens, appropriate measures and safeguards may be adopted to make the employee concerned directly or indirectly identifiable. To that end one may also rely – if appropriate -, on an identification code allocated to and displayed by the employee or another personal reference.**

10. *Transborder data flows*

10.1 Transborder transfers of personal data collected and stored for employment purposes should be sub-ject to the principles stated in paragraphs **7 and 9**.

11. *Particular categories of data*

11.1. Personal data relating to racial origin, political opinions, religious or other beliefs, sexual life or criminal convictions, referred to in Article 6 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, should only be collected and stored in particular cases**, where it is necessary to do so to carry out work pursuant to the contract of employment,** within the limits laid down by domestic law and in accordance with appropriate

Supprimé : .

Supprimé : form the subject-matter of

Supprimé : communication

Supprimé : bargaining

Supprimé : facilitate the optimum

Supprimé : by identifying

Supprimé : in¶ respect of which there are requirements relating to the publication of certain information

Supprimé : and

Supprimé : type

Supprimé : of the relevant notices which, for homogeneous classes, can be made public, that is to say

Supprimé : ¶ by also considering the

Supprimé : With regard in particular

Supprimé : to work-related tasks which involve a

Supprimé : in any way for

Supprimé : where sufficient also on the sole basis of the¶ direct recognition of

Supprimé : assigned

safeguards provided therein. In the absence of such safeguards, such data should only be collected and stored with the express and informed consent of the employees. Isnt' it a case of non freely-given consent?

11.2. An employee or job applicant may only be asked questions concerning his state of health and be medically examined in order:

a. to determine the suitability of an employee or job applicant for his present or future employment;

b. to fulfil the requirements of preventive medicine; or

c. to allow social benefits to be granted.

In principle, it should be prohibited to collect and use genetic data to determine the professional suitability of employees or job applicants, even with the consent of the person concerned. Provision may be made for exceptions only within the limits laid down by domestic law and where there are appropriate safeguards, which should also provide for the prior involvement of the supervisory authorities, for the sole purpose of adopting, at the request of the employee, the measures necessary to improve his health, safety and working conditions.

11.3. Health data **and, in any event, genetic data,** may not be collected from sources other than the employee concerned except with his express and informed consent or in accordance with provisions of domestic law.

11.4. Health data covered by medical secrecy **and, in any event, genetic data,** should only be stored by personnel who are bound by rules on medical secrecy. The information should only be communicated to other members of the personnel administration if it is indispensable for decision-making by the latter and in accordance with provisions of domestic law.

11.5. Health data covered by medical secrecy **and, where necessary, genetic data the processing of which is lawful,** should be stored separate from other categories of personal data held by the employer. Security measures should be taken to prevent persons outside the medical ser-vice having access to the data.

11.6. The data subject's right of access to his health data **and genetic data** should not be restricted unless access to such data could cause serious harm to the data subject, in which case the data may be communicated to him through a doctor of his choice.

11.7. The employer should process any health data relating to third parties in so far as is necessary to discharge obligations laid down by law or collective agreements, while maintaining the safeguards relating to the health data of employees.

12. ***Transparency of processing***

12.1. Information concerning personal data held by the employer should be made available either to the employee concerned directly or through the intermediary of his representatives, or brought to his notice through other appropriate means. This information should specify the main purposes of storing the data, the sort of data stored, the categories of persons or bodies to whom the data are regularly communicated and the purposes and legal basis of such communication.

In this context, a particularly clear and complete description must be provided of the type of personal data which can be collected by means of computer systems, programs or electronic devices which enable them to be monitored indirectly by the employer, and of their possible use. A similar description should be provided of the use of Radio Frequency Identification (RFID) technology, the possible use of personal identification codes, and also the role of any system administrators in relation to data processing.

12.2. The information should also refer to the rights of the employee in regard to his data, as provided for in paragraph **13** of this recommendation, as well as the ways and means of exercising the right of access.

12.3 The information referred to in the preceding paragraph should be provided and updated in due time and, in any event, before the employee carries out the activity or action concerned, and made readily available also through the information systems normally used by the employee.

Mis en forme : Police :(Par défaut) Arial, 11 pt

Mis en forme : Police :(Par défaut) Arial, 11 pt, Soulignement

Mis en forme : Police :(Par défaut) Arial, 11 pt, Soulignement

Mis en forme : Police :(Par défaut) Arial, 11 pt

Supprimé : bargaining

Mis en forme : Police :(Par défaut) Arial, 11 pt

13. *Right of access and rectification*

13.1. Each employee should, on request, be enabled to have access to all personal data held by his employer which concern him and, as the case may be, to have such data rectified or erased where they are incorrect or held contrary to the principles set out in this recommendation. **He should also be granted the right to know the origin thereof, and the parties to which the data have been, or could be, communicated. To that end, in particular in large-scale or territorially extensive places of work, the employer should introduce general preventative procedures to ensure that there is an adequate and prompt response where the rights are exercised.**

Supprimé : identity of the

13.2 The right of access should be granted also to personal assessment data, also where they relate to assessments of the productivity or capability of the employee provided for in paragraph 5.3, at least when the assessment process has been completed, without prejudice to the right of defence of employers or third parties involved; although they cannot be directly rectified by the employee, purely subjective assessments should be open to challenge in the manner laid down in domestic legislation.

13.3. Exercise of the rights referred to in paragraph **13.1** may, in the case of an internal investigation conducted by the employer, be deferred until the close of the investigation if the result of the investigation would be otherwise threatened. **However, internal investigations should not be carried out on the basis of an anonymous report, except where it is circumstantiated and relates to serious infringements which should be identified by domestic law or a decision of the supervisory authority.**

13.4. When an employee is faced with a decision based on automatic processing of data held by an employer, he should have the right to satisfy himself that the data have been lawfully processed. Could there be a right of opposition against decisions based on the sole basis of automatic processing?

13.5. Except where provisions of domestic law exist to the contrary, an employee should be entitled to designate a person of his choice to assist him in the exercise of the right of access or to exercise the right on his behalf.

13.6. If access to data is refused or if a request for rectification or erasure of any of the data is denied, domestic law should provide a remedy.

14. *Security of data*

14.1. Employers or firms which may process data on their behalf should implement adequate technical and organisational measures**, which are constantly updated as new technologies are developed,** designed to ensure the security and confidentiality of personal data stored for employment purposes against unauthorised access, use, communication or alteration.

14.2. 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.

15. *Conservation of data*

15.1. Personal data should not be stored by an employer for a period longer than is justified by the pur-poses outlined in paragraph 1.3 or is required in the interests of a present or former employee.

15.2. 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.

15.3. Where such data are stored with a view to a further job application, **the person concerned should be informed in due time and** the data should be deleted if the candidate concerned so requests.

Where it is necessary to store data submitted in furtherance of a job application for the purpose of defending legal actions, the data should only be stored for a reasonable period.

15.4 Personal data stored for the purpose of an internal investigation carried out by the employer which has not led to the adoption of negative measures in relation to any

employee should in principle be deleted in due time, without prejudice to the right of access up to the time at which they are deleted.

PORTUGAL

The Portuguese Expert to the T-PD takes du note of the Report presented to the T-PD by Mr. Giovanni Buttarelli under the title "Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation" and would like to convey to the T-PD some remarks.

Please regard these remarks as only preliminary and without prejudice to further written remarks to be sent as appropriate.

Mr. Buttarelli's text is divided into an analysis of today's situation of the use of personal data within the labour world and what he calls an organic proposal of a new text for the Recommendation (from page 18 to the end).

The author is to be congratulated on a good assessment of the present interactions of the use of technologies aimed to the use of information, more specifically of personal data within the working context.

The author's proposal for a draft of a revised Recommendation on the protection of personal data used for employment purposes is a very complete and complex text going beyond a set of general formulations about the subject rather entering into some kind of a regulation approach duly justified taking into attention the complexity of the subject.

The complexity of the subject can be perceived if we keep in mind its interactions with areas such as the respect for privacy and Human Rights in general, professional secrecy, protection of intellectual property, contractual complexity specific to the working world, namely the one derived from collective employment contracts where decisions that may affect a large group of workers' personal data (among other aspects, naturally) are taken by their representatives in order to fit collective interests, protection of public interests (mainly thinking of public workers, namely civil servants), State secrets, etc. Also nearly all branches of the Law are concerned, from civil law to criminal law/disciplinary law, to tax law or administrative law.

All this complexity is also to be analyzed within the framework of technological progress that contributes to large extent to empty old conceptual borders, making difficult to find where ends what is private life and starts the working life or admissible manifestations of private life within the work environment, or the interactions of what is behind geographical borders with what is borderless.

We propose the Bureau to analyze the possibility to, alternatively - within the general framework of the revision of Convention 108 - consider the eventual draft of an additional Protocol or a specific Chapter within the Convention itself, or else to revise the present Recommendation by drafting - from Mr. Buttarelli's work - a less detailed text more concise text."

SPAIN / ESPAGNE

Please, find below the comments and suggestions by the Spanish Data Protection Agency to the "Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation", drafted by our friend and colleague Giovanni Buttarelli. We sincerely apologise for responding so late.

First of all, we would like to express that we share most of the concerns stated in the report. We agree that circumstances in the work environment have significantly changed from 1989. The development and implementation of new technologies have had, in that sense, a crucial impact on work relationships, and had also affected workers' privacy. Thus, we share with the author the perception that amending and updating the Recommendation is more than necessary.

While bearing in mind the above, it is true that the Recommendation general principles remain still valid, so our work should be focused on providing added value to the existing text, more than on a radical redesigning of it.

We share most of the development factors identified by the report. Privacy by design, accountability and data minimisation have become widely accepted principles, and it seems appropriate to integrate them into the Recommendation. Moreover, scalability can also be an important factor, insofar as processing activities by SMEs do not usually raise the same concerns that those ones carried out by big companies.

We also recognise remote monitoring as an issue. However, a general prohibition does not seem to be the best solution. In our opinion, remote monitoring could be legitimate in a number of cases, even as a primary purpose. We would be more in favour of a precautionary approach, based on the necessity of establishing appropriate guarantees to fairly carry out this kind of processing.

Although social networks are clearly one of the key points in the supervisory authorities' agenda, in our view we should not focus our efforts only in this service. Technological neutrality should be one of our corner stones, as stated in the document. There are currently many different ways through which Internet users can post information in the Internet: forums, blogs, micro-blogging platforms… And we should realise that new services, applications and realities could also success in future, posing new risks to privacy. In our opinion, we should distinguish between publicly available and limited-access information, without targeting social networks as such. Further discussion is needed in order to apply concepts such as "data which are manifestly made public by the data subject" in a coherent way, and to define how to enforce the proposed principles and obligations.

A similar remark can be made when dealing with RFID. There is a number of traceability, geolocation and attendance control techniques that does not entail the use of RFID technologies.

The screening and monitoring of browsing activity and emails by employers is also a challenging issue. In this case, workers' expectations of privacy become essential. As stated above when referring to remote monitoring, a general prohibition does not seem to be the solution. Proportionality and information are critical in this context, as it has been properly addressed in the text.

It is quite common that companies enter into group insurance policies, meal vouchers and other similar agreements in order to provide additional advantages to its workers. Sometimes, workers'

relatives are also beneficiaries of such agreements. These issues could be covered in the chapter dealing with external communication of data.

We welcome the organic text proposed by Mr. Buttarelli, as a useful first step to improve the current Recommendation. In general terms, we share the opinion raised by our colleague and friend Mr. João Cabral, who stated that a less detailed and more concise text would be desirable. Of course, we also have a number of remarks to the proposed version. However, and taking into account that we are still in a very preliminary stage, as well as the comments expressed above, we considered it inefficient to carry out a detailed analysis of the current wording in an exhaustive way. In any case, it would be a pleasure for us to discuss any specific point with our colleagues within the T-PD.

SWITZERLAND / SUISSE

Observations préliminaires

Nous avons examiné le projet de révision de la recommandation n° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi de M. Giovanni Buttarelli dans sa version de décembre 2010. A cet effet, nous avons procédé à une consultation des organes intéressés en Suisse. Les réponses reçues ne nous permettent pas (encore) de fournir une prise de position consolidée présentant la position officielle de la Suisse sur ce projet.

1. Remarques générales

Dans l'ensemble nous saluons le projet de révision de la recommandation. Il conviendra cependant d'examiner l'opportunité de réécrire l'ensemble de la recommandation, notamment pour la mettre en concordance avec les recommandations les plus récentes.

2. Propositions de modifications :

Préambule

Préambule	**Observations et propositions**
Cons. 3	Remplacer « informatique » par « automatisé » et biffer « notamment automatisé »
Cons. 8	Nous proposons la rédaction suivante : « Conscient que les changements intervenus dans le monde du travail du fait notamment du recours aux technologies de l'information et des communications et de la globalisation des activités et des services imposent de compléter ou de modifier les principes de l'annexe à la présente recommandation ;
Cons. 9	Biffer ; relève plutôt de l'exposé de motifs
Annexe à la recommandation	**Observations et propositions**
1.1, 2e al.	Nous proposons la modification suivante : « Ces principes s'appliquent au traitement automatisé de données à caractère personnel. Ils s'appliquent également aux informations sur les employés détenues par les employeurs dans la mesure où elles sont nécessaires pour rendre intelligible le traitement automatisé des données ou prendre des décisions [importantes]. De même, ces principes …. »
1.2.	A l'instar d'autres recommandations, nous proposons de remplacer « traitements manuels » par « traitements non automatisés »
1.3.	Il conviendrait de s'interroger sur la nécessité de définir le terme « employé ». Nous proposons de modifier la définition des données à caractère personnel pour l'aligner sur les recommandations les plus récentes et notamment celle sur le profilage :

	« L'expression « données à caractère personnel » signifie … identifiable. Une personne physique n'est pas considérée comme « identifiable » si cette identification nécessite des délais ou des activités déraisonnables. » Nous proposons également d'introduire une définition des données sensibles : « L'expression « données sensibles » désigne les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou les autres convictions, et les données à caractère personnel relatives à la santé ou à la vie sexuelle ou concernant des condamnations pénales, ainsi que les autres données définies comme sensibles par le droit interne. Les données de santé se réfèrent également aux données génétiques. Les données biométriques sont assimilées à des données sensibles. » Nous proposons également d'introduire les définitions de traitement, de responsable de traitement et de sous-traitant. L'expression « système d'information » pourrait éventuellement également faire l'objet d'une définition, dans laquelle on reprendrait les éléments de programme informatique, matériel, dispositif électronique, y. c. système de vidéosurveillance. Il en va de même de l'expression « à des fins d'emploi », à savoir notamment collecte de données portant sur les aptitudes du travailleur à remplir son emploi, nécessaires au recrutement, à l'élaboration et l'exécution d'un contrat de travail, nécessaires aux obligations légales en relation avec un emploi (sécurité sociale, prévoyance, prévention, santé, etc.) ou découlant de conventions collectives de travail
1.4.	Remplacer « utilisent » par « traitent ». Que veut-on dire par « contemporain », ne s'agit-il pas plutôt de « contrat temporaire » ?
1.5	Nous proposons de biffer cette exception formulée de manière trop générale et d'examiner la possibilité de dérogations à certains principes (notamment information, droit d'accès)
2-	Nous proposons la rédaction suivante : « Le respect des libertés et droits fondamentaux, et notamment du droit à la vie privée et à la protection des données à caractère personnel, et du principe de non discrimination doit être garanti lors de la collecte et du traitement de données à caractère personnel à des fins d'emploi, notamment pour permettre aux employés le développement de leur personnalité et préserver leur possibilité de relations sociales et individuelles sur le lieu de travail. »
3.1	Cet article ne devrait pas mener à une obligation de l'employeur (ou respectivement un droit de l'employé), de devoir utiliser ou ne pas utiliser certains programmes informatique ou dispositifs électroniques. Au contraire, l'employeur devrait pouvoir choisir librement les programmes informatiques et les dispositifs électroniques qu'il considère adéquats mais il doit les utiliser et les configurer et/ou organiser ces opérations de manière à respecter les règles de protection des données et notamment le principe de minimisation des données.

4.1	L'article 4.1 n'est pas à sa place car il ne concerne pas «l'information et la consultation des employé» ; il serait plus judicieux de le placer à l'article 5 ou dans un nouvel article spécifique concernant la surveillance. Nous proposons en outre de formuler ce principe comme suit : « Le recours à des systèmes d'information, de programmes informatiques et de dispositifs électroniques, tels que les systèmes de vidéosurveillance sur le lieu de travail devrait être limité uniquement à des exigences organisationnelles et/ou de production, ou à des fins de sécurité au travail. Il ne devrait pas avoir pour but la surveillance délibérée et systématique de la qualité et de la quantité de travail individuel sur le lieu de travail, ainsi que le contrôle à distance du comportement ou de la position des employés. »
4.3	La première phrase de ce principe pourrait être déplacée dans le principe 2.
5.1	Remplacer « recueillies » par « collectées »
5.3	Est-ce qu'on peut exclure d'utiliser des données existantes en cas d'avancement. En effet, l'employeur devrait aussi pouvoir utiliser les données existantes dans le dossier de l'employé, notamment qualification, formation, etc., pour autant que cela se fasse de manière transparente. Qu'entend-on par réseaux de communication électronique à disposition du public ? S'agit-il des réseaux sociaux, uniquement ? Il conviendra de préciser au moins dans l'exposé des motifs.
5.4	Concernant l'information sur le contenu, nous proposons de prévoir une possibilité pour l'employeur de différer cette information lorsqu'il a un intérêt légitime à ne pas divulguer l'information, notamment lorsque l'employeur effectue des évaluations sans impliquer directement l'employé (par exemple examen de la qualité d'une prestation à la clientèle, fréquent dans les instituts de sondage ou de renseignements téléphoniques). La possibilité de telle évaluation doit cependant être connue des employés. « L'employeur peut différer l'information sur le contenu aussi longtemps qu'il a un intérêt légitime l'emportant sur l'intérêt ou les droits et libertés fondamentaux de l'employé. »
5.5	Il conviendra de préciser dans l'exposé de motifs en quoi la biométrie est susceptible de protéger l'intégrité personnelle et la santé des employés ou de tiers. En outre, le recours à la biométrie devrait prendre en compte les principes figurant en conclusion du rapport d'étape sur la biométrie.
5.6 – 5.7	Cette disposition contient plusieurs idées et il conviendra d'en revoir l'articulation. Certains éléments touchent par exemple plutôt à la sécurité des données, notamment en relation avec l'utilisation d'Internet / Intranet. C'est le cas de la configuration des systèmes et de l'identification de catégories de sites. D'autres relèvent de la surveillance des employés, à l'instar du principe 4.2 ou de règles de comportement de l'employé.

6.1	Remplacer « paragraphe » par «principe ». S'agit-il uniquement du principe 5. Ne faudrait-il pas y inclure les principes 2 et suivants
6.2	Concernant les données biométriques, il faudrait, dans l'exposé des motifs au moins, expliciter quant un enregistrement est envisageable dans une base de données. Par exemple est-ce envisageable pour des raisons de preuve ? ou pour permettre la réutilisation des données biométriques à des fins opérationnelles, notamment pour améliorer l'efficacité ou la qualité ?
7.1	Le 2e alinéa, même s'il est pertinent, relève plutôt de l'exposé des motifs.
7.2	Remplacer « utilisées » par « traitées »
7.4	Nous proposons le libellé suivant : « Sans préjudice des dispositions de l'article 9, lors de changements au sein de l'entreprise, de fusions ou d'acquisitions, le principe de finalité devrait être respecté pour le traitement de données à caractère personnel. En particulier, des modifications dans les modalités du traitement des données devraient être communiquées aux employés. »
8.1	Nous sommes d'avis qu'un tel accès ne devrait être autorisé qu'en cas de consentement de l'employé ou lorsque les données sont mises à dispositions sous forme anonyme.
9.	Nous proposons l'intitulé suivant : « communication des données à caractère personnel »
9.3	Nous proposons de modifier la fin du principe comme suit : « … sécurité sociale pour les employés, ainsi que pour permettre une meilleure affectation et une administration efficace des ressources humaines. »
9.4	Nous proposons la formulation suivante : « Dans le secteur public, la communication de données à caractère personnel ou l'accès à ces données à des fins de transparence ou de contrôle en cas d'utilisation de ressources et de fonds publics n'est licite que si la loi prévoit des garanties appropriées au respect de la vie privée. » Dans l'exposé de motifs, on pourrait reprendre – sous l'angle des garanties appropriées -, l'idée de concilier les intérêts en présence notamment en distinguant des catégories ou des profils professionnels pour lesquels il est nécessaire de publier certaines informations, ainsi que la typologie des informations pertinentes qui peuvent être rendues publiques, en fonction des classes homogènes et ce, en tenant compte de la possibilité d'en prendre connaissance plus facilement s'il est possible de les retrouver à l'aide de moteurs de recherche externes.
9.5	Nous proposons de mettre un point après « l'employé concerné » et de mettre la fin de la phrase dans l'exposé de motifs.

10	Il n'est pas certain que ce principe soit encore nécessaire dans sa formulation actuelle.
11.1	Si on introduit – comme proposé ci-dessus – une définition des données sensibles, le principe devrait être reformulé comme suit : 11. Données sensibles 11.1 « Les données sensibles ne devraient être collectées … » Nous proposons également de couvrir la phrase précontractuelle (recrutement) lorsque de telles données sont pertinentes pour déterminer l'aptitude du candidat à un emploi.
11.2	Le 2e alinéa consacré aux données génétiques doit être aligné sur le principe 4.9 de la recommandation sur les données médicales qui restreint la collecte et le traitement des données génétiques uniquement à des raisons de santé et notamment pour éviter tout préjudice sérieux à la santé de la personne concernée ou de tiers. Il faudrait dès lors biffer « de ses conditions de sécurité ou de ses fonctions » et prévoir la protection de la santé des tiers (voir également l'exposé des motifs de la recommandation sur les données médicales et l'état d'avancement des travaux du CDBI concernant l'utilisation des données génétiques à des fins d'emploi).
11.4	Nous proposons de biffer « en tout état de cause »
11.5	A quoi se réfère « si nécessaire » ? au traitement ou à l'enregistrement séparé ? Nous proposons la formulation suivante « Les données de santé couvertes par le secret médical et les données génétiques, lorsque leur traitement est nécessaire et autorisé par le droit interne, devraient être enregistrées … »
11.7	Nous avons des doutes sur la pertinence d'un tel principe.
12	Ce chapitre doit être revu pour tenir compte des exigences actuelles en matière d'information (voir notamment les dernières recommandations)
13.1	Nous proposons la modification suivante : « … dans la présente recommandation. Il devrait également se voir reconnaître le droit de connaître toutes les informations sur l'origine des données et l'identité des personnes… »
13.2	Nous proposons la formulation suivante : « L'employé devrait également avoir accès aux données à caractère personnel d'ordre subjectif, y compris celles relatives aux appréciations de la productivité ou du potentiel de l'employé prévues au principe 5.3. L'information peut être différé aussi longtemps que le processus d'appréciation n'est pas terminé ou que les données sont nécessaires à

	l'employeur ou à tiers pour défendre ses droits. L'employeur devrait en particulier indiquer l'actualité et la fiabilité de ces données, dans la mesure où ces informations ne ressortent pas des données elles-mêmes ou des circonstances. L'employé devrait pouvoir obtenir la rectification des données fausses ou si la rectification n'est pas possible, pouvoir contester les appréciations purement subjectives, selon les modalités prévues par le droit interne. »
13.3	Le terme «circonstancié» et «graves violations» devraient être clarifiés dans l'exposé des motifs
14.1	Dans l'exposé des motifs, il faudrait préciser que les entreprises devraient néanmoins être autorisées à utiliser leur infrastructure pour une période de temps raisonnable, si l'investissement respectif n'était pas déraisonnable au moment de leur acquisition/développement.

UNITED KINGDOM / ROYAUME-UNI

Comments on the Explanatory Memorandum

The UK broadly supports the new principles outlined in the Study. Our comments in relation to selected points raised in each section are set out below:

1. The new context of the working world

We consider that cloud computing is already a reality, rather than being in the "not too distant future". We also consider that the extension of Freedom of Information powers is another relevant development which indicates the need for greater transparency.

2. Guidelines for a revised recommendation

The UK would welcome a technologically neutral Recommendation and would welcome the extension of the principle of necessity to the 'use' of as well as the collection of personal data. However, any changes must take into account the impact on businesses. We believe that the resource implications for businesses, particularly small and medium sized ones in the current economic climate must be proportionate to the actual benefits delivered by increased safeguards for more transparent processing.

The Bureau may wish to consider whether questions and answers to employee evaluations should be disclosed, with the result that the same questions would be unusable for future recruitment.

3. Development factors of new principles and whom they address:

We would welcome clarification of what constitutes "high-risk" processing and believe that Privacy Impact Assessments ("PIAs") should not be limited to high risk processing operations, but rather that the risk of processing should be determined by carrying out a PIA.

We welcome the principle of simplification for small concerns, but would prefer that this be extended to Small and Medium Enterprises ("SMEs") to protect the interests of medium-sized as well as small businesses.

4 and 5. Specific revisions or modifications and the monitoring of employees

We consider that employers should be able to legitimately monitor their employees' use of their systems for the use of inappropriate websites, official time spent on personal web surfing and inappropriate uses of business email.

We believe it is right that employers should not be prohibited from using information from social networks in certain circumstances, to prevent harm to the business and its employees. Therefore we welcome that "monitoring and surveillance activities in the interests of the employer should however be lawful, transparent, effective and proportionate, and this reasonable approach would also avert possible negative effects on the quality of their professional relationship."

We are aware that a "guarantee of secrecy" concerning employees' correspondence and communication is a qualified guarantee, rather than absolute. We also believe that "the inspection of an employee's correspondence… should only be deemed necessary where the employer has reasonable grounds to suspect that an employee's use of electronic communications and internet is

contrary to its internal policies or otherwise involves unlawful practice" rather than the current wording "in exceptional circumstances".

Comments on the draft Recommendation

Section 4.1 – We consider that there are circumstances where the use of such systems should be permitted, for example, when employees work on a flexi-time basis and the employer needs a record of their working hours.

Section 4.3 – This section states that "the agreement of employees or their representatives should be sought before the introduction or adaption of such systems". Our experience is that it is not always appropriate to use consent as a condition in relationships between employees and employers, as it is unlikely to be freely given and is capable of being withdrawn.

Section 5.1 - We feel that the wording "person concerned" is too ambiguous and would prefer to clarify this to "data subject" if that is what is meant in this sentence.

Section 5.3 - The method of framing 4.1 (above) may also be necessary to clarify the sentence in 5.3 which currently states that "profiling of the person concerned based on the secret collection of data from search engines should in principle be prohibited". If the section explained in what circumstances it would not be prohibited, this would make it much clearer for employers.

We note that electronic medical records have been singled out in 5.3. This raises the question about whether this should be extended to paper copies as well.

Section 5.4 – As above, we believe that consent is not always reliable in employer/employee relationships, particularly where recruitment is concerned and the effect of withdrawing consent means that the subject will no longer be considered for a job.

Section 5.6 – The second line of 5.6 contains a reference to "pages viewed by the employer", but we believe that this may be a typing mistake and means to refer to the employee.

We consider that the reference to automatic deletion in 5.6 could be widened as the deletion of this data may need to be done manually.

Section 5.7 - We are not convinced of the practicality of assigning email addresses which are traceable by post, rather than name. The proliferation of common job titles in larger organisations may lead to emails going astray and personal information being misplaced/misused. There is also a question around transparency for customers about who they are dealing with. The Bureau may also wish to consider the cost implications of changing to such a system.

Section 11.1 – We consider that "where it is necessary to do so to carry out work pursuant to the contract of employment" may be too narrow and that this could be extended to cover pension systems.

Section 11.6 – The Bureau may wish to consider replacing "doctor" with 'medical practitioner' as the data subject may not wish to see a doctor.

Section 13.1 – We consider that there may need to be some exemptions put in place for particular circumstances where it may not be appropriate to inform the employee that their information is being processed. For example, article 29(1) of the Data Protection Act in the UK provides an exemption in this respect for personal data processed for the prevention or detection of crime, the

apprehension or prosecution of offenders and the assessment or collection of any tax or duty or of any imposition of a similar nature etc.

Section 13.3 – The Bureau may wish to consider whether legitimate investigations may be deterred or prohibited, which would be an undesirable result of this section. Investigation may be necessary to find evidence of infringement, so it may not be practical to state that unsubstantiated reports should be ignored even if they relate to a serious infringement and may not take into account whistle-blowing procedures. The Article 29 Working Group in the European Union published an opinion on whistle-blowing in 2006, which can be found here: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf.
It may be helpful for any revision to this Recommendation to take into account this report.

OBSERVER / OBSERVATEUR

ASSOCIATION FRANCOPHONE DES AUTORITES DE PROTECTION DES DONNEES PERSONNELLES (AFAPDP)

Commission Nationale de l'Informatique et des Libertés (CNIL)

PROJET DE RECOMMENDATION CM/REC(2010)... DU COMITE DES MINISTRES AUX ETATS MEMBRES SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL UTILISEES A DES FINS D'EMPLOI.

(Adopté le ... 2010 par le Comité des Ministres
lors de la ... réunion des Ministres délégués)

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

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

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

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

Supprimé : informatique

Supprimé : notamment automatisé,

Ayant à l'esprit les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, **ainsi que celles du Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données du 8 novembre 2001,** et compte tenu de la nécessité d'adapter ces dispositions aux exigences propres au secteur de l'emploi ;

Reconnaissant également que, lors de l'élaboration de principes dans le secteur de l'emploi, il doit être tenu compte aussi bien des intérêts individuels que des intérêts collectifs ;

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

Rappelant dans ce contexte l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 et l'article 6 de la Charte sociale européenne du 18 octobre 1961,

Conscient que les changements survenus dans la dimension internationale du travail dans le secteur public et privé, dans les processus de production et dans leur mondialisation favorisée par des technologies innovantes qui feront l'objet de

développements futurs et intenses, imposent la révision de certaines dispositions de la Recommandation N° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi ;

Étant donné qu'il n'est pas nécessaire d'introduire, aux termes de ladite nouvelle Recommandation, d'autres principes spécifiques concernant l'utilisation d'instruments de vidéosurveillance, dès lors que les «principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance » adoptés en mai 2003 par le Comité européen de coopération juridique (CDCJ) du Conseil de l'Europe, rappelés dans la Résolution 1604 (2008) de l'Assemblée parlementaire du Conseil de l'Europe, demeurent valides ;

Supprimé : Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance

Supprimé : adopted by the Council of Europe's European Committee on Legal Co-operation (CDCJ) in May 2003»

Rappelant, dans ce contexte, l'article 6 de la Charte sociale européenne du 18 octobre 1961 **et le Code de conduite du Bureau international du travail de 1997 sur la protection des données à caractère personnel,**

Recommande aux gouvernements des Etats membres :

- d'assurer que les principes contenus dans la présente recommandation soient reflétés dans la mise en oeuvre des législations nationales relatives à la protection des données dans le secteur de l'emploi ;

Commentaire [o1] : Il nous semble que la référence aux législations nationales couvre déjà les autres branches du droit

Supprimé : , ainsi que dans d'autres branches du droit portant sur l'utilisation de données à caractère personnel à des fins d'emploi

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

- de promouvoir l'acceptation et l'application des principes contenus dans la présente recommandation en assurant une large diffusion de celle-ci auprès des organes représentatifs des employeurs et des employés ;

Décide que la présente recommandation remplace la Recommandation N°R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi.

Annexe à la Recommandation

Commentaire [k2] : Distinguer ces deux points. Il conviendrait de traiter d'abord le champ d'application (1.1 et 1.2 ainsi que 1.4 et 1.5) et ensuite prévoir une partie distincte sur les définitions (1.3)

1. *Champ d'application et définitions*

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

Ces principes s'appliquent aux données traitées automatiquement ainsi qu'aux autres informations sur les employés détenues par les employeurs dans la mesure où ces informations sont nécessaires pour rendre intelligibles les données traitées **automatiquement ou utilisées pour prendre des décisions produisant des effets juridiques à l'égard des personnes concernées. De même, ces principes s'appliquent, s'il y a lieu, aux données à caractère personnel relatives à des personnes extérieures au lieu de travail traitées à des fins de sécurité du travail, ainsi qu'aux organisations syndicales.**

Supprimé : d'importantes

Un traitement de données ne devrait pas être effectué de façon non automatisée par un employeur dans le but d'échapper aux dispositions de la présente recommandation.

Supprimé : par voie manuelle

1.2. Nonobstant le principe énoncé au deuxième alinéa du paragraphe 1.1, un Etat membre peut
étendre les principes énoncés dans la présente recommandation à tous les traitements non automatisés.

1.3. Aux fins de la présente recommandation :

– L'expression «données à caractère personnel» signifie toute information concernant une personne physique identifiée ou identifiable. Une personne physique n'est pas considérée comme identifiable si cette identification nécessite des délais, et des activités déraisonnables.

– L'expression «à des fins d'emploi» concerne les rapports entre employés et employeurs 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.

1.4. Sauf législations nationales contraires, les principes de la présente recommandation s'appliquent, dans les cas appropriés, aux activités des agences pour l'emploi, dans les secteurs public et privé, qui collectent et utilisent, **notamment par l'intermédiaire de systèmes d'information en ligne,** des données à caractère personnel afin de permettre l'établissement **d'un ou de plusieurs contrats de travail contemporains ou à temps partiel** entre les personnes qui figurent sur leurs listes et d'éventuels employeurs, **ou afin de faciliter les démarches dérivant desdits contrats.**

1.5. La présente recommandation ne s'applique pas, dans la mesure nécessaire à la protection de la sécurité de l'Etat, de la sûreté publique et de la répression des infractions pénales, aux informations confidentielles collectées ou détenues par l'employeur à des fins d'emploi sur des personnes recrutées pour un emploi ou exerçant un emploi en relation étroite avec ces domaines.

*2. Respect de la vie privée **et de la protection des données à caractère personnel***

Le respect de la vie privée **et la protection des données à caractère personnel** dans les relations sociales et individuelles sur leur lieu de travail, devraient être préservés lors de la collecte et de l'utilisation de données à caractère personnel à des fins d'emploi.

3.1. Prise en compte de la vie privée dès la conception (« privacy by design »)

Les systèmes d'information, les programmes informatiques et les dispositifs électroniques utilisés à des fins d'emploi devraient être configurés, voire certifiés. Ils devraient s'adapter à chaque lieu de travail afin de réduire au minimum l'utilisation et la conservation des données à caractère personnel, notamment des données permettant une identification directe, qui ne sont pas nécessaires pour atteindre les objectifs propres à chaque situation.

3.2. Mise en œuvre des principes relatifs à la protection des données

L'employeur devrait développer des mesures appropriées visant à garantir que les principes et les obligations en matière de traitement des données aux fins d'emploi soient réellement respectés. Il devrait en outre de démontrer, sur demande, aux autorités de contrôle que les mesures appropriées ont été prises.

Supprimé : manuels

Commentaire [o3] : Nous suggérons de rajouter éventuellement certaines définitions pour des termes utilisés à plusieurs reprises dans la recommandation, comme par exemple: système d'information, programme informatique, dispositif électronique, responsable de traitement, sous-traitant, traitement, employé, employeur, représentant du personnel

Supprimé : des coûts

Commentaire [o4] : Par ailleurs la définition de la Convention 108 pourrait être amenée à évoluer à l'avenir. Convient-il dès lors d'introduire une définition spécifique dans cette recommandation ?

Commentaire [k5] : Faire remonter avant le 1.3

Commentaire [o6] : Faire remonter avant le 1.3.
Par ailleurs, ce point 1.5 n'est-il pas rédigé en termes trop généraux ? En effet, la CNIL est par exemple très souvent confrontée au cas de personnes privées d'un emploi dans le domaine de la sécurité et ce après consultation des fichiers régaliens relatifs aux infractions et aux condamnations.
Ce type de cas serait-il exclu du champ de la recommandation ?

Commentaire [o7] : La dignité humaine ne nous semble pas être l'objet de la recommandation. Par ailleurs, plusieurs éléments composant la dignité humaine ne sont pas abordés dans cette recommandation (intégrité physique, harcèlement, libe ... [1]

Supprimé : *de la dignité humaine*

Supprimé : et de la dignité humaine

Supprimé : notamment relativement à la possibilité pour les employés de ... [2]

Commentaire [k8] : Réécriture de ce paragraphe

Supprimé : *<#>Nécessité, développement de certains principes et simplifications*¶

Supprimé : le cas échéant

Supprimé : , et, en tout état de cause

Supprimé : ainsi que de

Supprimé : efficaces

Ces mesures appropriées devraient être adaptées à la nature des données traitées au regard de l'activité et de la taille de l'entité concernée.

4. *Information des employés et consultation des représentants du personnel*

4.1. L'installation et l'utilisation de systèmes d'information, de programmes informatiques et de dispositifs électroniques utilisés essentiellement afin de contrôler à distance le travail, le comportement ou la localisation géographique des employés, ne devraient, en principe, pas être autorisées, sauf si des garanties appropriées sont prévues.

4.2. Conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives, les employeurs devraient informer ou consulter leurs employés ou les représentants de ceux-ci préalablement à l'introduction, à la modification **et au fonctionnement** de systèmes **d'information, de programmes informatiques et de dispositifs électroniques** pour la collecte et **l'utilisation des données à caractère personnel nécessaires aux fins de la production, de la sécurité ou de l'organisation du travail.**

La personne est informée de :
a) l'identité du responsable du traitement et, le cas échéant, de son représentant;
b) les finalités du traitement;
c) toute information supplémentaire telle que:
- les catégories de données concernées,
- les destinataires ou les catégories de destinataires des données,
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

Cette information peut être assurée sur tout support utile. Lorsque des moyens spécifiques de surveillance des employés sont mis en œuvre, la diffusion d'une charte informatique, rappelant l'utilisation qui doit être faire des outils mis à disposition des employés, devrait être encouragée. En outre, il convient d'informer les employés lorsqu'une sanction disciplinaire est envisagée à leur encontre.

4.3. **L'employeur devrait adopter des mesures appropriées pour évaluer l'impact d'éventuels traitements de données qui menacent précisément le droit au respect de la vie privée, la dignité humaine et la protection des données à caractère personnel, et pour traiter ces données de la façon la moins intrusif possible.** L'accord des représentants du personnel devrait être recherché avant l'introduction ou la modification de tels systèmes, **programmes** ou dispositifs lorsque la procédure de consultation mentionnée au paragraphe 4.2 révèle **ce type de risques,** à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationales.

5. *Collecte des **données et formes particulières de traitement ou d'informations***

5.1. Les données à caractère personnel devraient en principe être recueillies directement auprès de **l'intéressé.** Lorsqu'il convient de consulter des tiers, par exemple pour des références professionnelles, **l'intéressé** devrait en être informé préalablement.

5.2. Les données à caractère personnel collectées par les employeurs à des fins d'emploi devraient être pertinentes et non excessives, compte tenu du type d'emploi ainsi que des besoins évolutifs d'information de l'employeur.

Supprimé : **, et pour pouvoir le prouver de manière adéquate sur demande des autorités de contrôle.** ¶

Mis en forme : Justifié, Interligne : simple

Supprimé : *employés*

Commentaire [o9] : Nous suggérons d'insérer les points 3.1 et 3.2 à la fin de la recommandation.

Supprimé : 3.3. **Les petites entreprises devraient adopter des solutions simplifiées adaptées.**

Supprimé : **directement et**

Supprimé : **position**

Commentaire [k10] : Ce paragraphe n'a pas sa place ici. Il serait utile de créer une partie spécifique sur la surveillance ou le contrôle des salariés. Cette partie pourrait notamment traiter de la vidéosurveillance, de la géolocalisation, du contrôle par l'employeur des connexions internet et de la messagerie électronique, etc.

Supprimé : **invasive**

Supprimé : des employés ou de leurs

Supprimé : **menace**

Commentaire [o11] : Un tel paragraphe sur l'évaluation d'impact pourrait être placé à la fin de la recommandation, avec la partie 3.2 sur l'accountability

Supprimé : sources en dehors des contrats de travail

Supprimé : **ce dernier**

5.3. Au cours d'une procédure de recrutement **ou d'avancement** , la collecte de données des candidats ou des employés devraient se limiter à celles qui sont strictement nécessaires pour évaluer leurs compétences ainsi que l'aptitude à occuper de nouvelles fonctions

Au cours d'une telle procédure, les données à caractère personnel devraient être recueillies uniquement auprès de l'individu concerné. **Le profilage de l'intéressé basé sur la collecte déloyale de données provenant de moteurs de recherche devrait être, en principe, interdit. L'employeur ne devrait pas inciter l'intéressé à lui fournir un accès à son dossier électronique de sécurité sociale conservé par des tiers.**

Il conviendrait, en tout état de cause, de prendre des mesures appropriées afin que, parmi les données facilement accessibles sur des réseaux de communication électronique à disposition du public, seules les données pertinentes, exactes et mises à jour soient utilisées, ce qui éviterait que ces données soient mal interprétées ou traitées de façon déloyale.

5.4. Le recours à des tests, à des analyses et à des procédures analogues destinés à évaluer le caractère ou la personnalité d'une personne ne devrait pas se faire sans son consentement, ou à moins que d'autres garanties appropriées ne soient prévues par le droit interne. La personne concernée devrait pouvoir, si elle le désire, connaître **au préalable les modalités d'utilisation** des résultats de ces tests, **les analyses ou les procédures et, par la suite, leur contenu.**

Aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement de ces tests, analyses ou procédures.

De même, l'établissement du profil du candidat ou de l'employé doit être basé sur des données objectives, permettant d'établir les grands traits de personnalité de la personne, et en aucun cas révéler des données relatives à la santé de la personne.

Ces tests doivent être pertinents et se fonder sur des méthodes scientifiquement reconnues.

5.5. Le traitement des données biométriques visant à identifier ou authentifier les personnes devrait se fonder sur des méthodes scientifiquement reconnues. En principe, le traitement de ces données ne devrait être permis que lorsqu'il est nécessaire et proportionné à la protection des intérêts légitimes de l'employeur ou de l'employé.

5.6. Eu égard à 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, sous réserve d'en informer les intéressés conformément aux paragraphes 4 et 12, les mesures préventives suivantes :

la configuration de systèmes ou l'utilisation de filtres qui permettent d'empêcher l'accès à certains sites (comme les *fora* de discussion) ou de télécharger des contenus précis ;

l'identification de catégories de sites jugés comme corrélés ou non au travail de l'employé ;

la graduation des éventuels contrôles relatifs aux données à caractère personnel, moyennant notamment dans un premier temps le recours à des contrôles non individuels.

Si l'employé utilise, conformément à l'autorisation donnée par son employeur, des appareils susceptibles de signaler l'endroit où il se trouve en dehors de ses heures de travail, il conviendrait de permettre que ces dispositifs soient désactivés et d'adopter des

Supprimé : des employés

Supprimé : les données collectées auprès des candidats

Supprimé : des **intéressés** et leurs perspectives de carrière.

Commentaire [o12] : Il nous semble que le problème principal n'est pas celui des réseaux sociaux professionnels ou des sociétés de conseil. En effet, ce sont ces réseaux et ces sociétés (et non les employeurs) qui doivent obtenir le consentement de la personne ou les informer. Ce n'est pas à l'employeur de le faire.

Il nous semble en revanche que le vrai « risque » réside dans l'utilisation de données personnelles figurant sur des réseaux sociaux « privés ». Il serait plus utile ainsi d'intégrer une partie sur l'utilisation par l'employeur de ces données sur des réseaux sociaux privés.

Commentaire [k13] : Ne faudrait-il pas distinguer les réseaux professionnels pour lesquels un accord n'est pas nécessaire, des réseaux privés pour qui la consultation doi... [3]

Supprimé : Sous réserve des dispositions du droit inter... [4]

Supprimé : **occulte**

Commentaire [o14] : Si l'on aborde la question des rése... [5]

Commentaire [k15] : Il s'agit d'une autre problématique r... [6]

Supprimé : **en raison de leur provenance**

Supprimé : Rappeler qu'a

Supprimé : ne pourra être prise sur le seul fondeme... [7]

Supprimé : et valables d'un point de vue scientifique

Supprimé : **primordiaux**

Supprimé : **pour protéger l'intégrité personnelle e**... [8]

Supprimé : **, selon le cas, certaines opération**

Supprimé : **s**

Supprimé : **téléverser**

Mis en forme : Police :(Par défaut) Arial, Italique

Supprimé : **dans un premier temps des contrôles pa**... [9]

Supprimé : **biens**

Supprimé :

mesures permettant d'empêcher que ces données soient utilisées. Une purge des données devrait également être fixée.

Il conviendrait de définir des procédures internes relatives au traitement de ces données en les portant préalablement à la connaissance des intéressés.

5.7. Sans préjudice des dispositions du paragraphe 4, point 1, l'employeur devrait, en principe, s'abstenir de consulter systématiquement le contenu des messages de courrier électronique adressés à ou envoyés par un employé possédant une boîte de courrier électronique identifiée.

Il conviendrait également de fournir des instructions afin que, en l'absence d'un employé, le système de messagerie électronique signale l'absence temporaire de l'employé et communique automatiquement les coordonnées d'un autre contact utile. Pour des situations exceptionnelles, en cas d'absence d'un employé, une procédure ad hoc devrait contrôler uniquement l'ouverture des messages électroniques qui concernent le travail, si possible en prévenant l'employé en question, et, le cas échéant, en présence d'une personne de confiance désignée par ce dernier.

En cas d'utilisation à des fins personnelles du système de messagerie électronique, un avertissement adéquat devrait figurer dans le contenu ou l'objet des messages envoyés par l'employé.

6. *Pertinence des données*

6.1. L'enregistrement de données à caractère personnel n'est possible que si les données ont été collectées conformément aux règles définies au paragraphe **5** et si l'enregistrement est réalisé à des fins d'emploi. **En cas de manquement à ces règles, l'employeur doit supprimer les données en question.**

6.2. Les données traitées devraient être exactes, mises à jour si nécessaire, et reproduire fidèlement la situation de l'employé. Elles ne devraient pas être traitées d'une manière qui puisse porter atteinte aux droits de l'employé en permettant par exemple d'établir son profil sans qu'il en ait connaissance.

Si l'utilisation des données biométriques est permise aux termes du paragraphe 5.5., elles ne devraient pas, en principe, être traitées dans une base de données, la préférence devant être accordée, selon les cas, à des systèmes d'identification ou d'authentification biométrique basés sur des supports mis à la disposition exclusive de l'intéressé.

6.3. Lorsque des données appréciatives relatives à la productivité ou à la potentialité des employés sont enregistrées, elles devraient être fondées sur des évaluations équitables et loyales ; elles doivent être formulées de manière objective.

7. Principes de finalité et proportionnalité

7.1. Les données à caractère personnel collectées ne devraient être traitées par l'employeur pour des finalités déterminées et légitimes et ne devraient pas être utilisées de manière incompatible avec ces finalités.

Supprimé : **et de les effacer automatiquement le plus vite possible.**

Commentaire [o16] : Ce point 5.7 devrait être intégré dans la partie évoquée ci-dessus sur la surveillance des salariés.

Supprimé : ¶
Si possible, il serait préférable d'attribuer aux employés des adresses de courrier électronique qui ne fassent pas référence immédiatement à des personnes mais à des fonctions. ¶

Supprimé : **Afin d'informer le destinataire sur**

Supprimé : **l'**

Supprimé : **exclusivement professionnelles**

Supprimé : **s**

Commentaire [o17] : Nous nous interrogeons sur le sens de la proposition. Nous proposons de viser la nécessité pour l'employé d'indiquer les messages envoyés à des fins personnelles.

Supprimé : *Enregistrement*

Supprimé : **s'abstenir d'utiliser**

Supprimé : enregistrées

Supprimé : enregistrées

Supprimé : ou codées

Supprimé : de le caractériser ou

Supprimé : **enregistrées**

Commentaire [k18] : Remonter ce paragraphe au 5. 5 où l'on évoque la biométrie

Supprimé : ne

Supprimé : pas

Supprimé : insultantes dans la manière dont elles sont formulées

Supprimé : *Utilisation interne*

Supprimé : *des données*

Mis en forme : Justifié

Supprimé : à des fins d'emploi

Supprimé : utilisées

Supprimé : .

Supprimé : que

Supprimé : cette seule

Supprimé : qu'à de telles fins

Dans le respect des principes de pertinence et d'exactitude, notamment eu égard à des entreprises de grande dimension ou dispersées sur le territoire, l'accès à certaines données à caractère personnel pourrait être facilité sur les réseaux de communication interne afin que la prestation de travail soit exécutée avec davantage de célérité et pour faciliter l'interaction avec les autres employés.

Commentaire [o19] : Nous suggérons de retirer ce paragraphe de la recommandation car il concerne davantage l'organisation interne de l'entreprise.

7.2. Lorsque des données doivent être utilisées à des fins d'emploi autres que celles pour lesquelles elles ont été initialement collectées, des mesures appropriées devraient être prises pour assurer qu'elles ne soient pas utilisées de manière incompatible avec le but initial. En cas de décision concernant l'employé, fondée sur des données ainsi utilisées, celui-ci devrait en être avisé.

Supprimé : pour éviter que ces données ne soient mal interprétées dans un contexte différent et

Supprimé : importante

Commentaire [o20] : Serait-il utile de donner des exemples concrets comme la mesure de la diversité, lutte contre la fraude, contre la corruption, etc ?

7.3. Les dispositions du paragraphe 7.2 s'appliquent à la mise en relation de fichiers contenant
des données à caractère personnel collectées et enregistrées à des fins d'emploi.

7.4. Sans préjudice des dispositions de l'article 9, en cas de changements au sein de la société, de fusions et d'acquisitions, il convient de veiller au respect du principe de finalité dans l'utilisation des données, notamment eu égard à d'éventuelles modifications des modalités de traitement des données dont les intéressés doivent être informés.

8. Communication de données et utilisation de systèmes d'information aux fins de représentation des employés

8.1. Conformément aux législations et pratiques nationales et aux conventions collectives, des données à caractère personnel peuvent être communiquées aux représentants des employés, dans la mesure où de telles données sont nécessaires pour permettre à ces derniers de représenter les intérêts des employés.

8.2. L'utilisation de systèmes 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 permettant une utilisation appropriée, ainsi qu'à identifier des garanties à titre de protection d'éventuelles communications confidentielles.

9.*Communication externe* ***et transmission*** *des données*

Supprimé : ***diffusion***

9.1. 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 et dans les limites des obligations légales de l'employeur ou conformément à d'autres dispositions du droit interne.

Supprimé : pour les besoins de leurs fonctions officielles

Supprimé : que

9.2. La communication de données personnelles à d'autres entités, y compris aux entreprises du même groupe, ne devrait s'effectuer que :

Supprimé : des organismes publics dans le cadre de leurs missions ou à des parties autres que des organismes publics

Supprimé : les

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 ou leurs représentants en sont informés ; ou

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

c. si la communication est autorisée par le droit interne, **notamment si cela s'avère nécessaire en cas d'action en justice ou en vue de l'exercice d'un droit devant une instance judiciaire.**

9.3. En cas de consentement de l'employé ou en fonction de garanties appropriées prévues par la législation nationale, des données à caractère personnel peuvent faire l'objet d'une communication dans le cadre de groupes de sociétés afin d'exécuter les obligations prévues par la loi ou par la convention collective en matière de travail, de prévoyance et de sécurité sociale pour les employés, c'est-à-dire pour permettre la meilleure affectation de ressources humaines.

9.4. Concernant le secteur public, la loi devrait concilier le droit au respect de la vie privée et à la protection des données avec les exigences de transparence ou de contrôle en cas d'utilisation de ressources et de fonds publics, en distinguant des catégories ou des profils professionnels pour lesquels il est nécessaire de publier certaines informations, ainsi que la typologie des informations pertinentes qui peuvent être rendues publiques, en fonction de classes homogènes et ce, en tenant compte de la possibilité d'en prendre connaissance plus facilement s'il est possible de les retrouver à l'aide de moteurs de recherche externes.

9.5. Dans le cas de fonctions professionnelles impliquant des relations constantes avec le public ou lorsque des exigences de transparence à l'égard des usagers, des consommateurs et des citoyens le rendent nécessaire, il est possible d'adopter des mesures et des garanties appropriées pour rendre directement ou indirectement identifiable l'employé concerné, dès lors qu'il suffit de connaître directement un code d'identification attribué à l'employé ou une autre référence personnelle.

10. Flux transfrontières de données

10.1. La communication transfrontière de données à caractère personnel collectées et enregistrées à des fins d'emploi devrait être régie par les principes énoncés aux paragraphes **7 et 9.**

11. Catégories particulières de données

11.1. Les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, les données relatives à la vie sexuelle ou à des condamnations pénales, visées à l'article 6 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ne devraient être collectées et enregistrées que dans des cas particuliers, **lorsque cela est indispensable à l'exécution des prestations dérivant du contrat de travail,** dans les limites prévues par le droit interne et conformément aux garanties appropriées y figurant. En l'absence de telles garanties, ces données ne devraient être collectées et enregistrées qu'avec le consentement exprès et éclairé des employés.

11.2. Un employé ou un candidat à un emploi ne peut être interrogé sur son état de santé et faire l'objet d'un examen médical qu'aux fins suivantes :

Commentaire [o21] : Nous estimons que le consentement de l'employé ne peut de façon générale être accepté pour la communication des données. Le lien hiérarchique entre l'employeur et l'employé ne permet pas d'obtenir un consentement libre.

Cette position résulte également largement de l'avis 8/2001 du G29 sur la protection des données dans le contexte professionnel. Il y est précisé que le traitement de données ne devrait pas se fonder sur le consentement. L'on ne peut recourir au consentement strictement au cas où le travailleur est complètement libre de le donner et a la possibilité d'y renoncer sans préjudice.

La CNIL accepte le consentement du salarié par exemple lorsque ce dernier communique son CV aux fins d'une bourse d'emploi interne à un groupe de sociétés.

Commentaire [o22] : Il pourrait être utile de viser d'autres cas, dont la sauvegarde de la vie de la personne, la réalisation de l'intérêt légitime de l'entreprise sous réserve de ne pas méconnaître les droits et libertés fondamentaux de la personne concernée, etc.

Commentaire [o23] : Cf. commentaire ci-dessus sur le consentement

Commentaire [o24] : Ce paragraphe nous paraît devoir être revu largement. Il convient notamment de faire référence à l'exigence d'une protection adéquate pour permettre un flux transfrontières. De même, il pourrait être utile de faire référence à l'adoption d'instruments spécifiques comme des clauses contractuelles, des règles internes d'entreprise, prévoir certaines exceptions, etc.

Commentaire [o25] : Peut-être serait-il utile de rappeler, à l'instar de la Convention 108, le principe d'interdiction du traitement des données sensible, et prévoir ensuite les cas dans lesquels il est possible de traiter ces données.

Commentaire [o26] : Là encore nous suggérons de retirer cette phrase, le consentement ne nous paraissant pas acceptable dès lors qu'il n'est pas libre.

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

b. couvrir les besoins de la médecine préventive ; ou

c. bénéficier de prestations sociales.

En principe, il devrait être interdit de collecter et d'utiliser des données génétiques lors de l'instauration d'un contrat de travail, même avec le consentement de l'intéressé. Des dérogations exceptionnelles pourraient être prévues dans les seules limites prévues par le droit national et en présence de garanties appropriées et documentées qui devraient également prévoir une participation préventive des autorités de contrôle, uniquement afin d'adopter, à la demande l'employé, les mesures nécessaires à l'amélioration de son état de santé, de ses conditions de sécurité ou de ses fonctions.

11.3. Les données de santé **et, en tout état de cause, les données génétiques** ne peuvent être collectées auprès d'autres sources que l'employé lui-même que si des garanties appropriées sont prévues par le droit interne.

11.4. Les données de santé couvertes par le secret **médical et, en tout état de cause, les données génétiques,** devraient **être traitées exclusivement** par le personnel soumis aux règles sur le secret médical. Ces informations ne devraient être communiquées à des membres du service du personnel que si cela est indispensable à la prise de décisions par ce service et conformément au droit interne.

11.5. Les données de santé couvertes par le secret médical **et, si nécessaire, les données génétiques dont le traitement est autorisé,** devraient être enregistrées séparément des autres catégories de données détenues par l'employeur. Des mesures de sécurité devraient être prises pour éviter que des personnes étrangères au service médical n'aient accès à ces données.

11.6. Le droit d'accès de la personne concernée à ses données médicales 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 lui être communiquées par l'intermédiaire du médecin de son choix.

11.7. L'employeur devrait traiter les éventuelles données sur la santé relatives à des tiers si cela est indispensable à l'exécution des obligations prévues par la loi ou par la convention collective, dans le respect des garanties prévues pour les données sur la santé des employés.

12. ***Transparence du traitement***

12.1. Des informations sur les données à caractère personnel détenues par l'employeur devraient être mises à la disposition du travailleur concerné, soit directement, soit par l'intermédiaire de ses représentants, ou être portées à sa connaissance par d'autres moyens appropriés. Ces informations devraient spécifier les principales finalités de ces données, le type de données enregistrées, les catégories de personnes ou d'organes auxquels les données sont régulièrement communiquées, et la base juridique de cette communication.

Dans ce contexte, une description particulièrement claire et complète devrait être fournie relativement à la typologie des données à caractère personnel qui peuvent être collectées au moyen de systèmes d'information, de programmes ou de dispositifs

Commentaire [o27] : Serait-il utile de détailler ce que l'on entend par « prestations sociales » ?

Supprimé : octroyer

Supprimé : s

Commentaire [o28] : Est-il seulement possible de déterminer le comportement professionnel par des données génétiques ? Si tel est le cas, n'est-ce pas un principe d'interdiction totale ?
Nous suggérons de supprimer cette référence au comportement professionnel.
De même les dérogations prévues ensuite semblent à examiner avec davantage de précaution et méritent plus ample réflexion.

Dans un autre contexte, l'article L-1141-1 du code français de la santé publique pose un principe général d'interdiction, sans dérogation possible :
« Les entreprises et organismes qui proposent une garantie des risques d'invalidité ou de décès ne doivent pas tenir compte des résultats de l'examen des caractéristiques génétiques d'une personne demandant à bénéficier de cette garantie, même si ceux-ci leur sont transmis par la personne c ... [10]

Supprimé : pour déterminer le comportement professionnel des employés ou des candidats

Commentaire [o29] : Nous pensons qu'il n'est pas souhaitable d'accepter de collecter des données génétiques auprès d'autres sources et qu'il convient d ... [11]

Supprimé : sans le consentement exprès et éclairé de ce dernier ou

Supprimé : conformément aux dispositions du

Commentaire [o30] : Là encore veut-on viser l'autorisation du traitement de données génétiques dans le domaine des ressources humaines ?

Commentaire [o31] : Quels cas sont visés par ce paragraphe ?

Commentaire [o32] : Il nous apparaît plus opportun de supprimer cette partie et de viser au point n° 4 les dispositions spécifiques sur l'obligatio ... [12]

Commentaire [o33] : Il ne s'agit pas d'une simple mise à disposition de l'information mais soit d'une obligation d'information soit d'un droit d'accès. ... [13]

Supprimé : les finalités

électroniques permettant à l'employeur de les contrôler indirectement, ainsi que sur leur utilisation potentielle. Une description semblable devrait être fournie concernant l'emploi de technologies de Radio Frequency Identification (RFID), l'éventuelle utilisation de codes d'identification personnels, ainsi que concernant le rôle des éventuels administrateurs de système par rapport au traitement des données.

12.2. Ces informations devraient également faire mention des droits de l'employé au regard de ses données, tels qu'ils sont prévus au paragraphe 13 de la présente recommandation, ainsi que des modalités d'exercice du droit d'accès.

12.3. Les informations indiquées aux termes des paragraphes précédents devraient être fournies et mises à jour en temps utile et, en tout état de cause, 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.

13. *Droit d'accès et de rectification*

13.1. Tout employé devrait pouvoir avoir accès, sur demande, à toutes les données à caractère personnel le concernant détenues par son employeur, et obtenir, le cas échéant, la rectification ou l'effacement de telles données lorsque ces dernières sont détenues en contravention des principes posés dans la présente recommandation. **Il devrait également se voir reconnaître le droit de connaître leur origine, les finalités pour lesquelles ces données sont traitées, l'identité des personnes auxquelles les données ont été ou sont susceptibles d'être communiquées, et la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé.**

Á cette fin, particulièrement pour les entités de grande dimension ou dispersées sur le territoire, l'employeur devrait prévoir des procédures préventives d'ordre général afin de garantir que le contrôle soit adéquat et rapide en cas d'exercice de ces droits. L'employeur devrait centraliser le droit d'accès auprès d'un service afin de permettre que la demande soit rapidement traitée.

13.2. L'employé devrait également avoir accès aux données à caractère personnel d'ordre appréciatif, y compris celles relatives aux appréciations de la productivité ou du potentiel de l'employé, prévues au paragraphe 5.3., au moins lorsque le processus d'appréciation est terminé et si une décision a été prise à l'égard de la personne sur la base de ces appréciations. L'employé dispose également d'un droit de rectification et de formuler des observations selon les modalités prévues par la loi nationale.

13.3. Dans le cas d'une enquête interne effectuée par l'employeur, l'exercice des droits mentionnés au paragraphe 13.1 peut être différé jusqu'à la conclusion de cette enquête, si cet exercice risque de nuire au résultat de l'enquête. **Cependant, un signalement anonyme ne saurait être à l'origine d'enquêtes internes, sauf si ce signalement est circonstancié et concerne de graves violations identifiées par le droit national ou par une décision de l'autorité de contrôle.**

13.4. Lorsqu'une décision découlant d'un traitement automatisé des données détenues par l'employeur est opposée à l'employé, ce dernier devrait avoir le droit de s'assurer que ces données ont été licitement traitées.

Commentaire [o34] : Il convient aussi de prévoir l'information sur le droit d'opposition. Cf. notre commentaire ci-dessous.

Commentaire [o35] : Vise-t-on ici le cas de l'obligation d'informer le salarié en cas de modification des finalités, des types de données traitées, etc ? Si tel est le cas, pourrait-on envisager la formulation suivante : « la personne concernée doit être tenue informée de toute modification des finalités pour lesquelles ces données sont traitées, du type de données enregistrées, des catégories de personnes ou d'organes auxquels les données sont régulièrement communiquées, ou de la base juridique de cette communication »

Supprimé : et

Supprimé : dans les lieux de travail

Supprimé : , le besoin de l'employeur ou de tiers de se défendre étant temporairement écarté ; mê

Supprimé : me si l'employeur ne les rectifie pas directement, les appréciations purement subjectives devraient pouvoir être contestées selon les modalités prévues par le droit national.

13.5. 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 pour exercer ce droit en son nom.

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

Remarque générale : il nous paraît indispensable d'intégrer un article sur le droit d'opposition, en s'inspirant notamment de la Convention 108 ou de la formulation de la Directive 95/46/CE.

14. Sécurité des données

14.1. Les employeurs ou les entreprises auprès desquelles les données peuvent être sous-traitées devraient mettre en œuvre des mesures techniques et organisationnelles appropriées **et constamment mises à jour par rapport au développement des nouvelles technologies** pour garantir la sécurité et la confidentialité des données à caractère personnel enregistrées à des fins d'emploi, contre tout accès, utilisation, communication ou modification non autorisés.

14.2. L'employeur et le sous-traitant devraient signer un contrat comportant l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoyant que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

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

Supprimé : <#>¶

15. Conservation des données

15.1. Un employeur ne devrait pas conserver 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.

15.2. 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.

15.3. 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 soutenir d'éventuelles actions en justice, il est nécessaire de conserver les données fournies à l'occasion d'une candidature, ces données ne devraient être conservées que pendant une période raisonnable.

15.4. Les données à caractère personnel enregistrées du fait d'une enquête interne réalisée par l'employeur et qui n'a entraîné l'adoption d'aucune mesure négative à l'égard des

employés devraient, en principe, être effacées en temps utile, sous réserve du droit d'accès jusqu'au moment où elles seront effacées.

Remarque générale :

- **Serait-il possible d'agrémenter la recommandation avec des exemples concrets type « mise en place de dispositifs d'alerte professionnelle » (whistleblowing) ou procédures de Discovery. Des éléments pourraient être mentionnés dans les parties relatives à la collecte des données ou aux transferts ?**

Commissariat à la protection des données de l'Île Maurice

Il semble que le document est principalement axé sur les devoirs et obligations de l'employeur et les droits de l'employé.

Cependant, il serait probablement opportun d'inclure aussi des conseils pratiques a l'employé comme de limiter la diffusion extensive de ces données sur le site physique ou technologique du travail, et de lui indiquer quels sont les types de données qu'il doit ou peut divulguer et qu'il ait aussi une maitrise adéquate des outils informatiques pour limiter des abus par l'employeur, par le biais des cours ou programmes de training informatique du système opérant de l'entreprise, dispensés par l'employeur.

Commission d'accès à l'information du Québec

La CAI du Québec souhaite apporter quelques commentaires sur le projet de recommandation du T-PD (comité consultatif Convention 108) relatif aux données personnelles utilisés aux fins d'emploi.

Tout d'abord, nous souhaitons saluer la qualité et la richesse du document présenté pour observations.
Un travail important de recherche et de consolidation a été fait et constitue sans aucun doute une excellente base de travail.
Nous constatons que des principes issus des Standards de Madrid (« imputabilité » ou « Accountability » et « prise en compte de la vie privée dès la conception » ou « privacy by design ») ont été introduits dans le projet de recommandation : nous nous en félicitons.

Nous souhaitons donc faire part de quelques commentaires généraux sur le projet de recommandation (annexe 1 du document transmis):

- Certains termes tels que « contrat contemporain » et « petite entreprise » pourraient être précisés (p. 22),

- Nous pensons qu'il est important de rappeler le principe de minimisation lors de la collecte, et pas seulement lors de l'utilisation (art 3.1 p. 22),

- S'agissant des problématiques de géolocalisation, il pourrait être recommandé de prévoir la possibilité d'arrêter le dispositif en dehors des heures de travail,

- En outre, la recommandation mériterait peut être d'être plus précise concernant les données biométriques, notamment en déconseillant l'usage de bases de données centralisées et en encourageant les systèmes d'identifications basés sur des supports individuels,

- Enfin, nous suggérons d'évoquer en p. 26 l'hypothèse dans laquelle l'employeur gère le plan collectif d'assurance médicaments, négocié avec une société d'assurance.

Page 55: [1] Commentaire [o7] **omr** **29/03/2011 10:12:00**

La dignité humaine ne nous semble pas être l'objet de la recommandation. Par ailleurs, plusieurs éléments composant la dignité humaine ne sont pas abordés dans cette recommandation (intégrité physique, harcèlement, liberté d'expression, etc)

Page 55: [2] Supprimé **omr** **02/03/2011 15:26:00**

notamment relativement à la possibilité pour les employés de développer leur personnalité

Page 57: [3] Commentaire [k13] **kgs** **29/03/2011 10:12:00**

Ne faudrait-il pas distinguer les réseaux professionnels pour lesquels un accord n'est pas nécessaire, des réseaux privés pour qui la consultation doit être interdite car déloyale.

Page 57: [4] Supprimé **omr** **03/03/2011 11:13:00**

Sous réserve des dispositions du droit interne, d'autres sources, **dont celles en provenance de sociétés de conseil ou de réseaux sociaux dédiés au développement de relations professionnelles**[k1]**,** ne peuvent être consultées que si la personne concernée y a consenti ou si elle a été informée au préalable de cette possibilité.

Page 57: [5] Commentaire [o14] **omr** **29/03/2011 10:12:00**

Si l'on aborde la question des réseaux professionnels, il nous semble important de distinguer les réseaux sociaux privés et professionnels.

Page 57: [6] Commentaire [k15] **kgs** **29/03/2011 10:12:00**

Il s'agit d'une autre problématique relative à la collecte de données sensibles. Nous suggérons de déplacer cette partie au sein de l'article 11.

Page 57: [7] Supprimé **omr** **02/03/2011 12:28:00**

ne pourra être prise sur le seul fondement de ces tests.

Page 57: [8] Supprimé **omr** **02/03/2011 15:55:00**

pour protéger l'intégrité personnelle et la santé des employés ou de tiers

Page 57: [9] Supprimé **omr** **02/03/2011 16:00:00**

dans un premier temps des contrôles par sondages non individuels sur des données anonymes ou groupées (par exemple, par unité de production).

Page 61: [10] Commentaire [o28] **omr** **29/03/2011 10:12:00**

Est-il seulement possible de déterminer le comportement professionnel par des données génétiques ? Si tel est le cas, n'est-ce pas un principe d'interdiction totale ?
Nous suggérons de supprimer cette référence au comportement professionnel.
De même les dérogations prévues ensuite semblent à examiner avec davantage de précaution et méritent plus ample réflexion.

Dans un autre contexte, l'article L-1141-1 du code français de la santé publique pose un principe général d'interdiction, sans dérogation possible :

« Les entreprises et organismes qui proposent une garantie des risques d'invalidité ou de décès ne doivent pas tenir compte des résultats de l'examen des caractéristiques génétiques d'une personne demandant à bénéficier de cette garantie, même si ceux-ci leur sont transmis par la personne concernée ou avec son accord. En outre, ils ne peuvent poser aucune question relative aux tests génétiques et à leurs résultats, ni demander à une personne de se soumettre à des tests génétiques avant que ne soit conclu le contrat et pendant toute la durée de celui-ci."

Page 61: [11] Commentaire [o29] **omr** **29/03/2011 10:12:00**

Nous pensons qu'il n'est pas souhaitable d'accepter de collecter des données génétiques auprès d'autres sources et qu'il convient de supprimer cette référence aux données génétiques.

Page 61: [12] Commentaire [o32] **omr** **29/03/2011 10:12:00**

Il nous apparaît plus opportun de supprimer cette partie et de viser au point n° 4 les dispositions spécifiques sur l'obligation d'information (en s'inspirant notamment de l'article de la Directive 95/46/CE) et de préciser les dispositions relatives au droit d'accès dans le point n°13

Page 61: [13] Commentaire [o33] **omr** **29/03/2011 10:12:00**

Il ne s'agit pas d'une simple mise à disposition de l'information mais soit d'une obligation d'information soit d'un droit d'accès.