COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 01 December 2010 T-PD-BUR(2010)11

THE BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(T-PD-BUR)

22nd meeting
15-17 November 2010
Strasbourg, G04

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

By Giovanni Buttarelli

December 2010 version

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

INDEX

ANNEXE

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').

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) 1 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.

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 organisation 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 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.

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.

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 fact that the changes which have occurred internationally in public and private employment, in production processes, and in the globalisation thereof facilitated by innovative technologies designed to bring about further and strong development make it necessary to revise the terms of Recommendation No. 89 (2) on the protection of personal data used for employment purposes;

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,**

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.

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 security purposes, and also to trade union organisations.**

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 contemporaneous 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.**

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, development of other principles and simplifications*

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 only that necessary for the aims pursued in the individual cases concerned.

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 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. 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 ex-cessive, 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 con-cerned. 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 his consent or if 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 viewed in 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 he so wishes, 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.

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 content);**

- **the identification of sites which are or are not deemed to relate to the work carried out;**

- **the grading of possible monitoring on personal data, providing first for non-individual random checks on data which are anonymous or in some way aggregated (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**

made so that data relating to his whereabouts are not used and are automatically deleted as soon as possible.

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 are immediately traceable not to individuals but to posts.

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.

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.**

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 large-scale 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.

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 in the subsequent use of the data, also as regards any changes in processing of which the persons concerned must be informed.

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 subject-matter 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 form the subject-matter of communication within a group of enterprises for the purpose of discharging duties provided for by law or collective bargaining relating to work and social security and welfare for employees, or to facilitate the optimum 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 by identifying professional categories or profiles in respect of which there are requirements relating to the publication of certain information, and also the type of the relevant notices which, for homogeneous classes, can be made public, that is to say by also considering the possibility of identifying them more easily where they can be traced through external search engines.**

9.5. **With regard in particular to work-related tasks which involve a constant relationship with the public or where necessary in any way for 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, where sufficient also on the sole basis of the direct recognition of an identification code assigned to 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 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.

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 bargaining, 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.

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 held contrary to the principles set out in this recommendation. **He should also be granted**

the right to know the origin thereof, and the identity of 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.

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.

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.