

**European Privacy Officers Forum (EPOF)**  
**www.epof.org**

**EPOF'S VIEWS ON THE COMMISSION'S INITIATIVE ON EMPLOYEE PRIVACY**

The European Privacy Officers Forum (EPOF) is composed of data protection compliance officers and internal legal counsels in charge of data protection in Europe from approximately twenty-five major European and global companies. As such, EPOF members have considerable experience dealing with the compliance challenges presented by the European privacy and data protection law regulations on a daily basis.

Now that the consultation of social partners in accordance with article 138, paragraph 2 of the EC Treaty has ended, DG Employment has expressed its intention to propose specific additional legislation that it considers would enhance the privacy protection currently afforded to employees in the EU. In this document, EPOF respectfully outlines areas of serious concerns, held by several of its members, regarding any proposed legislation. As requested by DG Employment in a meeting with EPOF in Brussels, this document includes examples of day-to-day company experiences with regard to employee data.

In its second stage consultation, which was launched on 30 October 2002, the Commission identified four issues that should be covered by new legislation:

- Employee consent with regard to the processing of personal data and invasions of privacy by the employer;
- Access to and processing of sensitive data, more specifically the processing of health data;
- Drug testing and genetic screening;
- Monitoring and surveillance.

Whether current legislative instruments on privacy and data protection, the Data Protection Directive 95/46 (the "Data Protection Directive"), the Electronic Communications and Privacy Directive 2002/58 and the safety and health directives, including Directive 90/270/EEC on the protection of workers with regard to the use of display screen equipment, sufficiently protect the privacy interests of employees is an important and complex public policy question. EPOF urges DG Employment to ensure that any new legislation or new requirements in this area be carefully thought through and not have adverse or unintended consequences.

EPOF recognizes that the employer/employee relationship may raise fact-specific privacy questions; however EPOF is of the opinion that these concerns are covered by the Data Protection Directive. Employment data protection questions are not substantially different from those arising in other areas covered by the Data Protection Directive, such as in the context of a customer/supplier relationship. The same rights and principles of consent, notice, choice, correction and redress apply and are adhered to. As privacy officers, we are (together with workers representatives in some countries) the advocates of the employees' data privacy rights. Concerns and complaints about a company's possible violation of data privacy laws are therefore addressed to us. As of today, the complaints we have received about the companies' handling of employee personal data are extraordinarily few. Our experience so

Co-Chairs:

Rosa Barcelo, DLA Caestecker, Louizalaan 106 Avenue Louise, B-1050 Brussels, Belgium  
rosa.barcelo@dla.com, Tel. +32-2-500 1542, Fax +32-2-500 1605  
Christopher Kuner, Hunton & Williams, Avenue Louise 326, B-1050 Brussels, Belgium  
ckuner@hunton.com, Tel. +32-2-643 5800, Fax +32-2-643 5822

## **European Privacy Officers Forum (EPOF)**

**www.epof.org**

far is that concerns, questions and potential conflicts can be worked out on the basis of the existing data privacy framework by applying the existing data privacy laws and the means of self-regulation successfully to protect the data and the interests of our employees. EPOF therefore strongly reiterates its view that there is no need for a special employee data protection directive.

There is another reason why we think that a special employee data protection directive would not add value to the current data protection laws. Any proposed Employee Directive would not remove existing variations in Member State's interpretation and implementation of the Data Protection Directive. A new directive would most likely be a minimum-directive, which means that differences in Member State laws would not be eliminated, as each Member State would still be authorized to set a higher standard. EPOF therefore objects to any new employment directive on the ground that it would do nothing to harmonize the laws of the Member States.

We believe that the questions relating to employee privacy could be answered by an analysis of the principles and rules of the Data Protection Directive. This analysis could result either in guidance by the Commission and the Data Protection Authorities or in industry initiatives undertaken to address the practical issues they have experienced in the employment context. Without endorsing either of these texts, we want to encourage efforts such as those of the UK Data Protection Commissioner and of the ILO who both worked on codes of conduct.

\* \* \*

For all of the above reasons, EPOF strongly urges DG Employment to reconsider the need for a new, additional Community-wide legislation in this area. Moreover, if the above arguments were not sufficient, we believe the following additional (non-exhaustive) comments on the four issues identified by the Commission raise further substantial concerns:

### **Consent**

EPOF takes the view that an employer must be able to process employee data on a day-to-day basis, relying on articles 7(b), 7(c) and 7(f) of the Data Protection Directive as a sufficient basis in most instances. Unfortunately these articles are often interpreted narrowly. In particular, article 7(f) has not been implemented or interpreted in Member States in a harmonious fashion. As a consequence, employers who respect the general data protection principles (and in particular the relevance, necessity and proportionality requirements) need to be able to rely on employee consent to ensure the legitimacy of necessary and harmless data processing.

Our experience so far, is that employees accept consent as a valid basis of processing of their data. Eliminating the ability to rely on consent would reduce the flexibility of companies and deprive employees and companies of a way to interact responsibly.

Besides, the consent option may be appropriate also in specific circumstances, such as: in the event that a company would like to use the image of its employees in advertising campaigns for company products or if a company wants to make commercial use of employees' data, such as the provision of employee contact details to direct marketing companies. In the data

**European Privacy Officers Forum (EPOF)**  
**www.epof.org**

processing reality of a company, consent may also be used for example for specific employee groups such as managers or executives. As in the case of the customers, consent should remain a valid basis to obtain permission to collect and transfer data.

For these reasons, it is clear to the privacy officers of EPOF that the use of employees' consent, which is recognized by the Data Protection Directive in articles 7(a) and 26 (1).(a), can and should be retained as a valid option in the employer/employee relationship context.

**Special Categories of data/Health data**

EPOF disagrees with the Commission's view that there is a need to prohibit the use of sensitive data in the employment context except in cases provided by law. Indeed, today only a few Member States' laws contain such types of provisions, and we fear that Member States' laws may not encompass all situations where such types of data have to be processed in an employment context. EPOF is also concerned by the suggestion of the Commission that processing such types of data must systematically be subject to prior Data Protection Authorities approvals. Indeed, companies would be in a more secure situation if, instead of having to wait for an approval, they were given clear guidelines as to what are considered as acceptable data processing activities in this field.

Besides, in some instances it is necessary or recommended to process sensitive data of employees in other situations than those identified by the Commission in its consultation paper (see examples in Annex 1).

EPOF suggests the development of communication to employers emphasizing the sensitive nature of this data and its processing in certain contexts, guidelines for acceptable practices and explanation of the need for additional control and audit measures to ensure the protection of the employee's interests (such as collection limitation, and enhanced security).

**Drug testing and genetic screening**

With regard to the subject of drug testing and genetic screening, EPOF does not see the need for Community action. Genetic screening data would be categorized as processing sensitive data under the Data Protection Directive and therefore would either not be collected by companies under the general prohibition of article 8, or if companies came into possession of such data, through medical reports for example, their use would be limited by the Data Protection Directive obligations.

Drug testing may be appropriate and necessary when a person is working in a high risk or safety-sensitive position, especially when there is a reason to believe that a person is engaging in unauthorized or illegal drug use. Appropriate restrictions can be established for protecting the confidentiality of the drug test results and for protecting the privacy of the individual when providing the urine or other sample to be tested. Proper chain-of-custody procedures can ensure the accuracy of the test result and its relationship to the employee who gave the original sample. Employers have no problem complying with these procedures that maintain privacy for the person and his test results. However, employers --who know their workforces, workplaces and risks best-- need to be given some flexibility to decide when

## **European Privacy Officers Forum (EPOF)**

**www.epof.org**

drug testing may be appropriate or necessary. They should not be limited to testing only for certain reasons or in connection with certain jobs.

For example, in one work location, the employees came to the management because they were concerned about a particular group of workers who might be using drugs. While the workers were not in safety sensitive positions, the complaining employees were concerned about other areas of the facility that contained hazardous materials and machinery, to which the drug-using workers may have access. The complaining employees requested that the employer implement a drug-testing program for all employees in the facility.

We believe this is an area that can be adequately and appropriately addressed without the need for a EU directive. Alternatively, we would like to ensure that employers retain flexibility, as appropriate and as needed, consistent with the description above.

### **Monitoring and surveillance**

EPOF wants to stress that an employer has a series of legitimate interests in protecting its network, its equipment and the information stored in it and indeed, may be required to do so by other EC Directives, including the Data Protection Directive. The interests include, but are not limited to:

- Protecting the network against attacks (i.e. viruses and intrusion);
- Ensuring availability of the network (i.e. uptime, bandwidth);
- Keeping control over the costs of network operations (i.e. data storage, bandwidth, amount of data traffic);
- Safeguarding the company against illegal use of the network/equipment (e.g. illegal software, spamming, child pornography, harassment, libel); and
- Protecting confidential data and business secrets from being disclosed to unauthorized users or in a non-secure manner.

Annex 2 provides a non-exhaustive list of practical concerns and comments, following the order adopted by the Commission in its second stage consultation paper.

### **Conclusion**

In sum, EPOF joins the many stakeholders who believe that there is no compelling need for additional legislation on employee privacy and data protection. The existing European and national legislative framework sufficiently protects the rights of the employees. EPOF does believe that there is room for improvement through harmonization between Member States, for example, in the area of network monitoring.

EPOF would welcome the opportunity to discuss the positions taken in this paper with the Commission at any time.

**European Privacy Officers Forum (EPOF)**  
**www.epof.org**

**ANNEX 1 – SPECIAL CATEGORIES OF DATA/HEALTH DATA**

Examples where processing of sensitive data may occur in an employment context:

- Processing of criminal convictions related data should be made with care and extra protection. However, limiting by law the possibility for an employer to verify the criminal background of its employees to only those employees who have specific functions would be too restrictive. Indeed, the activities or specific situation of some companies may require them to check the criminal background of all employees, whatever their function. This could be the case if the activities of the company are particularly sensitive (defense-related activities, manufacturing dangerous goods etc) or if the company is exposed to specific risks, such as terrorist attacks.

We doubt that a law could encompass all situations where such types of processing would be acceptable. This is why we would favour a dialog between relevant parties in order to issue guidelines addressing specific situations. Guidelines have the advantage of flexibility; they can be revised to address situations not contemplated originally. Instead of subjecting all such types of processing to Data Protection Authorities' approval, it would be preferable that such Authorities issue clear guidelines as to what practices are acceptable.

- Large companies need to automate their internal control mechanisms to ensure compliance with company processes and with laws. Failure to do so could expose companies to major risks, including criminal sanctions, in the event an employee acting for the company does not comply with a legal requirement. For instance companies need to implement tools to ensure that at various stages of a product development or of a project all regulatory steps have been made (for instance the approval of an antitrust authority or a safety authority). These tools contain milestones and actions to be complied with by employees. If an employee fails to take the required action, then the system automatically keeps that information and sends a reminder to the employee. If the failure relates to an obligation triggering criminal sanctions, then such information is processed by the system for very legitimate purposes of ensuring compliance. Companies should not be prohibited from using tools necessary for them to track whether in their business activity they comply with the law.
- There are other situations than those mentioned by the Commission, where processing data “revealing” ethnic origin may be legitimate for a company. Some interpret article 8.1 of the Data Protection Directive as applying to photographs as they may “reveal” the ethnic origin of a person. However for security purposes or even to improve the communication between employees, companies need to keep photographs of their employees. Prohibiting the processing of “ethnic revealing data” for other purposes than those where the laws authorize a distinction between workers could then prevent the implementation of badges bearing employee photographs or employee directories with photographs.
- Similarly, some companies have departments which handle the business trip reservations for the company employees. Such departments may need information

## European Privacy Officers Forum (EPOF)

[www.epof.org](http://www.epof.org)

which can reveal the “ethnic origin” of the employees, e.g. in informing airline companies of the meal preferences of the employee (e.g. requests for “Kosher” meals...). Instead of prohibiting the processing of such data, which is in no way discriminatory, it would make more sense to restrict its use to this very specific purpose and its access only to the relevant department in charge of travel arrangement. Mere compliance with the principles of the Data Protection Directive would achieve this result.

- It would be difficult to keep some health data separate from other data, as the Commission suggests. Taking the example of maternity leaves: in most countries, maternity leaves have a certain duration provided by law. A company must process this type of information in its employment databases in order to anticipate the employee’s return date the employee (to reactivate access to the company systems, to organize work allocation within the concerned service).
- The previous example is an example of a situation where it is not possible to limit access to this health information only to healthcare professionals or people bound by medical confidentiality. The same conclusions can be drawn about other health data processing activities identified in the Commission’s paper: processing of disability information to determine whether a worker is fit for a particular employment (the HR manager and the department manager need to be involved in making this assessment before offering a new position to a disabled employee); processing of health information to determine entitlement to social benefits (here also HR managers and people in charge of payroll activities may need health data related information); people responsible for occupational health and safety compliance issues in companies are most of the time dedicated people but are not healthcare professionals or alike.
- There are several instances where companies would have to process data relating to trade union membership and where such processing is not intended for discriminatory purposes at all. In some countries for example, trade union fees are deducted from employees’ payroll and directly paid by the company to the trade union. Also, if an employee requests a leave of absence in order to attend a works council or union meeting, this leave and the reason for the leave will be recorded by its employer.

**European Privacy Officers Forum (EPOF)**  
**www.epof.org**

**ANNEX 2 – MONITORING AND SURVEILLANCE**

These comments follow the order of the Commission's paper:

- It may be necessary for a company to take rapid action to install monitoring devices for a temporary period in order to protect the interests of the company or of its employees as a result of a specific threat (e.g. suspicion of theft or trade secrets leaks). If companies were bound to follow a procedure as heavy and lengthy as the information and consultation of workers representatives, there are high risks that the wrongdoing would have occurred before the end of the consultation procedure. For security reasons, information and consultation of workers representatives in case of specific investigations should not be required.

More generally, the terminology “consulted” should be clarified, so that it is not interpreted as tantamount to prior approval. Indeed, a prior approval process may lead in some companies to a systematic refusal of monitoring devices, even harmless tools implemented for mere security reasons. In addition, the procedure should be set within a specific timeframe to avoid lengthy delays in the implementation of tools, which are strategic to the security of a company.

- EPOF believes that it is not realistic to require companies to get all monitoring systems checked by supervisory authorities before implementation. The workload of supervisory authorities and the rapid change of technologies would indeed lead a prior check system to unduly delay the implementation of strategic tools, in particular those which are customarily used by a wide range of companies or harmless tools such as security related devices. A prior check raises the same issue as the consultation of workers representatives in instances where the monitoring activity would be incidental to investigate a specific and temporary case of wrongdoing. In such a situation, a prior check should not be required.

More generally, it seems necessary to clarify the scope of the prior check and to specify whether it would amount to a prior authorization.

- Regarding continuous monitoring, such type of monitoring should also be authorized for the purposes of ensuring compliance with the company policy on the use of company-owned equipment. Dependent on the circumstances and on the equipment to be monitored, such monitoring might be continuous or at random. For instance, companies should be able to operate on a continuous basis software tools, which enable the screening of attachment types (such as MP3) or specific words in emails, or devices, or which for example enable the company to track (on a continuous basis) phone-call duration.
- Companies should have the possibility to use tools, which are originally intended for a security purpose for other legitimate purposes, as long as they comply with data protection/labour law obligations (notice to employees, information of workers representatives). For instance a company having implemented a badge system to ensure access security to its site should not have to set up a separate badge system if, afterwards, it wants to use a badge system to check work attendance. Also, companies need to be able to use security systems (CCTV, access systems, firewalls, etc) and to

## European Privacy Officers Forum (EPOF)

[www.epof.org](http://www.epof.org)

analyse the data thereby created, such as log files to ensure the security of their networks in order to verify the behaviour of a given employee in specific circumstances, e.g. in the event a third party company complains of attacks or wrongdoings by the employing company on its site or network. Indeed, the third party company would have evidence on its own system that its network has been attacked via the employing company's computer system and the employing company must be able to investigate internally the origin of the claimed attack.

- Regarding the Commission's proposal on automated monitoring, EPOF is concerned by the generality of the statement as it goes beyond what is provided under article 15 of the Data Protection Directive. The text should be put in line so that it applies only to "automated individual decisions".
- The Commission should clarify whether there is an intended difference between continuous monitoring and routine monitoring.

EPOF believes that routine monitoring should be authorized not only in the event of automated monitoring for purposes of security and proper operation of the system but also for the purpose of ensuring compliance with the employer's internal policy. For instance technology can be used for legitimate reasons to monitor traffic in order to prevent MP3 files, files of a large size or even trade secrets to be sent via the company's network. Notably, companies have serious reasons to prohibit and monitor MP3 attachments; not only they use a lot of bandwidth and occupy a lot of storage place, but also they might infringe intellectual property rights and be the source of claims against the company.

- A rule prohibiting in all instances the control of the content of private emails creates a mechanism for fraud. Indeed, if sexual harassment is committed by email, the concerned emails are unlikely to be deemed as "professional emails" and because of such a rule the employer would not be in a position to assist its employees who are victims of such harassment. MP3 files, which are often prohibited attachments by companies' policies, are also usually included in private emails. To identify such MP3 files, accessing the email content is necessary. Also, a person disclosing its employer's trade secrets could easily commit such a wrongdoing by merely specifying in its email header "personal".

EPOF believes that a total prohibition is unworkable and would lead to unintended consequences, because it is in practice impossible to distinguish among private and professional emails. A reasonable employer who needs to access the content of emails sent or received by its system (for instance to investigate whether antitrust rules have been complied with in a given deal) will, as a principle, not be interested to look at emails which are not relevant to the investigation, in particular those appearing as "private". Such emails would therefore be set aside from the investigation. However, one cannot rule out that, in the framework of the investigation, emails of private nature be opened, either because they are not identified as such or because it is via a private email that a wrongdoing has been committed. The rule should find a balance between the privacy rights of employees and the legitimate interests of employers to protect their business, their reputation and the interests of other employees. EPOF

## **European Privacy Officers Forum (EPOF)**

**[www.epof.org](http://www.epof.org)**

believes that privacy interests can be secured by putting in place procedural protections in the way the investigations can be carried out and in particular by the use, where relevant, of software programs which make automatic searches of key words or attachments types.

- The particular protection granted to communication to occupational health professionals and workers representatives must be reasonable and not require the implementation of a parallel email system for instance.