12.7.2010

NOTICE TO MEMBERS

Subject: **Petition 1198/2009 by J.F.K. (Hungarian), on the invasion of workers' private sphere by multinational companies**

1. Summary of petition

The petitioner protests against the practise by multinational companies of checking employees' bags after work, camera surveillance during work and the requirement to submit a CV when applying for jobs. He considers this to be a violation of human rights and asks the Parliament to take steps to remedy the situation.

2. Admissibility

Declared admissible on 1 December 2009. Information requested from Commission under Rule 202(6).

3. **Commission reply**, received on 12 July 2010.

The petition

The petitioner objects to three types of practice carried out in Hungary by multinational companies such as Jabil, Nokia and Sanmina: 1) daily checks of employees by personal property guards (often involving body searches) on the premises of the multinational companies, 2) the obligation to submit a CV in advance when applying for employment, and, 3) offensive video surveillance at the workplace. He indicates that he does not have any evidence in support of his allegations, but explains that employees have to sign a separate agreement confirming not to use a mobile phone or a camera at the work place. He also claims that there are rules providing that images and sound for tape and video recordings may not be reproduced in an offensive manner, by harassing other persons, or recording against their will. In cases of extreme necessity, and for justified reasons, anyone may produce a

recording for the purpose of evidence.

The petitioner considers that such checks are humiliating, that the obligation to submit his CV in advance is unlawful data collection, and that the prohibition to use a camera phone at his workplace is a violation of his human rights. He asks that legal instruments be put in place to protect employees from the abovementioned practices.

The Commission's comments on the petition

The Data Protection Directive (*Directive 95/46/EC*[1]) provides the legal framework for the processing of personal data in all Member States. Should Member States not have complied with this implementing obligation, citizens can require the direct application of certain provisions of this Directive. In that regard the ECJ ruled in C-465/00[2] that certain provisions, such as Art. 6 (1) c) (principles relating to data quality: data have to be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed) and Art. 7 c) and e) (criteria for making data processing legitimate) have direct effect.

The Directive is only applicable to personal data within the meaning of Directive 95/46/EC. Art. 2 defines 'personal data' as any information relating to an identified or identifiable natural person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Directive 95/46/EC lays down the principles with which processing activity must comply with in order to be lawful. It also establishes certain rights for those individuals whose personal data are processed, so as to ensure compliance with their fundamental right to the protection of their personal data. The principles enshrined in Art. 6 are the foundation for the protection of personal data, since they concern the quality of the data when they are processed: the collection and the processing of personal data must be for specified and explicit purposes (purpose limitation principle), and personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (principle of proportionality) and, where necessary, kept up to date (Art. 6). Personal data must also be processed for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

Data processing (Art. 7) is only considered legitimate if

a) the data subject has unambiguously given his consent, or
b) processing is necessary for the conclusion of a contract binding on the data subject, or
c) as a legal requirement, or
d) to protect the vital interests of the data subject, or
e) for the performance of a task carried out in the public interest or in the exercise of official authority, or
f) in the legitimate interests of a natural or legal person, provided that the interests or the

[1] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995, p. 31.
[2] ECJ C-465/00, C-138/01 and C-139/01, *Rechnungshof and Österreichischer Rundfunk*, 20.5.2003, point 98ff.

rights and freedoms of the data subject are not overridden.

The data subject has the right to receive information concerning, access to, and rectification, deletion or blocking of, his personal data, as well as the right to effective redress for the unlawful processing of his data. These rights may be restricted insofar as it is necessary to safeguard, for example, not only national security and defense, but also for the purpose of criminal investigations and prosecutions.

Processing activities are supervised and controlled by public independent supervisory authorities (Art. 28), usually called "data protection authorities", which are the competent authorities to monitor the compliance of any processing of personal data at national level with the national legislation implementing the Directive.

Two issues have to be confirmed for the Data Protection Directive 95/46/EC to be applicable.

The most important issue is the one concerning the data processed, and if they fall under the definition of "personal data" of Art. 2 a). As far as the petitioner's second and third allegations are concerned, the data contained in a CV and recorded by video surveillance are personal data within the meaning of Directive 95/46/EC. As far as the first allegation is concerned, the physical body search does not fall within the scope of the Data Protection Directive.

The second relevant issue is to determine who processes the personal data. Depending on whether they are a data controller or merely a data processor, they must comply with a number of obligations. Multinational companies such as Jabil, Nokia and Sanmina are legal persons which themselves determine the purpose and means of the processing of the personal data they collect, such as the data contained in CVs or the data collected by video surveillance. By doing so they are considered data controllers within the meaning of Directive 95/46/EC, although they could delegate/subcontract the processing of personal data to processors who would carry out this task on their behalf.

1st allegation: Checks of employees by personal property guards (often involving body searches)

Under the Treaty on European Union and the Treaty on the Functioning of the European Union, the European Commission has no general powers to intervene in individual cases of alleged violations of fundamental rights. It can do so only if an issue of European Union law is involved.

In connection with the petitioner's complaint on the checks of employees by personal property guards at assembly plants, it should be pointed out that there is no specific EU legislation regulating this issue. For this reason it is not possible for the Commission to pursue this first allegation.

2nd allegation: unlawful data collection by request a CV of a potential future employee

Nowadays positions in companies are filed after interested and eligible candidates have undergone a selection process. This generally comprises a pre-selection stage which is carried out on the basis of the CVs which are submitted by interested candidates in advance. The

processing of data contained in CVs falls within the scope of the Data Protection Directive 95/46/EC, and is subject to the principles of legitimacy, necessity and proportionality (Art. 6 of the Directive).

In most cases the processing of data submitted in form of CVs can be justified as legitimate because it is

- carried out with consent of the data subject (Art. 7a) or
- it is necessary for the performance of an employment contract between an employer and an employee (Art. 7 b) or
- part of the legitimate interest pursued by the employer with a view to knowing which qualifications potential future employees have obtained in order to best match the open position with the most suitable person (Art. 7f).

The processing of personal data collected from CVs must be proportionate to the legitimate objectives pursued, and should particularly offer the least intrusive means of data processing. Provided that sufficient safeguards are in place, such processing for the stated reasons would be in compliance with Directive 95/46/EC. Such safeguards could comprise, for instance

- informing employees of the identity of the data controller and the purpose of the surveillance and other information necessary to guarantee fair processing in respect of the data subject (Art. 11);

- informing the data subject of the right to rectify the data concerning him and – particularly for ultimately unsuccessful candidates – the right to erasure.

The simple fact that a potential employer asks for an advance copy of the CV of a potential employee cannot be considered as unlawful data collection, as is alleged by the petitioner.

3rd allegation: video surveillance at the workplace

Video surveillance falls within the scope of the Data Protection Directive 95/46/EC. The data protection principles, in particular the principles of legitimacy, necessity and proportionality (Art. 6 of the Directive) apply to any processing of personal data through video-surveillance equipment.

The Article 29 Working Party (WP29)[1] has issued two opinions regarding video surveillance in the workplace[2] which provide guidance on how to apply the provisions of the Data Protection Directive to video surveillance. According to these opinions, the lawfulness of video surveillance in the workplace depends on several factors:

[1] The *Working Party on the protection of individuals with regard to the processing of personal data* (WP29) was set up by Art. 29 of the Data Protection Directive 95/46/EC. It is composed of representatives of the national data protection authorities. It acts independently and it is advisory to the Commission.

[2] *Opinion 8/2001 (WP48) on the processing of personal data in the employment context*, *Working Document of 25 November 2002 (WP67) on the processing of personal data by means of video surveillance* and *Opinion 4/2004 (WP89) on the processing of personal data by means of video surveillance.*

First, the purpose of the processing: video surveillance systems can be justified if they are deployed, subject to appropriate safeguards, to meet production or occupational safety requirements, or for security reasons. The different interests at stake should be taken into account on a case-by-case basis, and against the background of the specific context.

The installation of video-surveillance systems by companies for the purposes of production safety requirements or security reasons (to prevent theft of electronic products or of technological research) may be legitimate, to the extent that it is necessary for the purposes of the legitimate interest of these companies ("data controller") to ensure security of the premises and to prevent theft of technological research and business secrets, and this interest is not overridden by the interests of the employees (Art. 7f).

It is also possible that the use of video-surveillance systems is justified in order to protect a vital interest of the data subject, such as for reasons of occupational safety, ie.: from accidents during production (Art. 7 d).

Second, the necessity and proportionality of the processing: the deployment of video surveillance equipment needs to be proportionate to the legitimate objectives pursued and should particularly utilise the least intrusive means of data processing. The interests of the employer in putting up video surveillance equipment have to be balanced against the interests of the employee to obtain the protection of his personal data. This can only be done if appropriate safeguards are in place. Only then would video surveillance be in compliance with Directive 95/46/EC. Such safeguards could comprise for instance

- no installation of video surveillance equipment in bathrooms, shower-rooms, lockers and recreational areas;

- information to employees about the identity of the data controller and the purpose of the surveillance, and other information necessary to guarantee fair processing in the respect of the data subject;

- a limitation of the duration of retention of the videos;

- independent supervision by the national data protection authorities which are competent to monitor compliance with national data protection law implementing Directive 95/46/EC and provide the suitable safeguards and requirements for the system to be lawful.

Finally the data controller has the obligation (Art. 11) to inform the persons who enter a place under video surveillance, in a visible, clear and explicit way that they are being monitored. In the case of video surveillance equipment deployed at workplaces, workers' representatives should also be informed.

Conclusions

As concerns the first allegation regarding checks on employees in particular body searches, this matter falls outside the scope of Union law and can therefore not be pursued by the Commission.

As regards the other allegations, the petitioner did not submit any evidence establishing that the subsidiaries of the multinationals Jabil, Nokia and Sanmina had violated Directive 95/46/EC.

The petitioner is invited to address any allegations he might have against these multinationals, and which are linked to a violation of his rights to data protection, to the national data protection authority in Hungary:

Hungarian Data Protection Commissioner
Nádor str. 22.
1051 Budapest
Tel: (+36 1) 475 7100, (+36 1) 475 7186
Fax: (+36 1) 269 3541
E-mail: adatved@obh.hu