INFORMATION SHEET No.135

CCTV'S at the Workplace: Processing of Personal Data Privacy

November 2017

Introduction

In Cyprus the processing of personal data is governed by the Processing of Personal Data (Protection of Individuals) Law of 2001 that came into force on 23 November 2001. The Law was introduced in the context of harmonization with the European Data Protection legislation and amended in 2003 in order to harmonise domestic legislation with the Directive 95/46/ EC and to address privacy issues arising out of the collection, storage, processing and use of personal data. The Data Protection Law in Cyprus will change on 25 May 2018 when the EU General Data Protection Regulation takes effect, replacing the Data Protection Law of 2001.

The installation and operation of CCTV's in the workplace is for the safety and security reasons. The employee's however, do not justify the function of cameras inside the office area on a daily basis. CCTV's operations is legitimate and lawful for security purposes in reception areas (Hotels), entrances and exits, cashier places, or places with electromechanical equipment of major infrastructure with the condition that the cameras are focusing and taking images only in the protected security area; cashier/ATM machines and more.

Employees have the right to privacy, especially inside their offices and the employers can deprive this right, with the installation and operation of CCTV's in a constant basis. The inside office area where the employee is working, is a place where employees have high expectations of privacy, and any interference in the private sphere of privacy must be justified. Some examples of camera installations in the workplace are the areas with electromechanical installations where the shift controller or the security officer can monitor the operations of high risk machinery in order to intervene directly in cases of security incident. Other places are military factories, banks, high-risk facilities. The purpose of installation shall be the security and safety, and not the monitoring of the actions of employees.

The processing that occurs during the operation of the business (even at night time) by cameras that are operating within the office, for safety and security purposes, shall be in line with the principles of necessity and proportionality of Data Protection law. More specifically, the data controller/employer in most of the cases seems to collect and processes more data than necessary to achieve the purpose of processing, taking into account that the use of these instruments leads to the monitoring of employees at the time of their work. The video capture of images from inside the office at the time that employees work could be regarded as excessive for purposes of the processing concerned.

Consent

An area of difficulty is where the giving of consent is a condition of employment. The employee is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In those situations consent is not freely given and is therefore unlawful.

According to the Council of Europe, freely given consent might not be considered as "freely given", in dependency relationships where there is a significant imbalance of economic power or other form of power between the data controller (the employer) and the data subject (the employee). As dependency relationship is considered the employer and the employee relationship. Reliance on consent should be confined to cases where the employee has a genuine free choice and is

subsequently able to withdraw the consent without detriment.

An Overview of the most common problems in the protection of personal data in the workplace is given by the Article 29- Data Protection Working Party Opinion 8/2001 on the processing of personal data in the employment context. The Opinion analysed the importance of consent as a legal basis for processing of personal data in the employment context and concluded that the economic inequality between the employer and the employee, it raises doubts whether the consent is freely given. The Working Party concluded that the circumstances in which the consent is given should be carefully considered when assessing the validity of consent in the employment context and in most cases it is observed that the Employer is collecting more data than what is required to meet the purpose of processing.

However, an example of a large Company which intends to create a list that contains the names of all employees, their position in the company and the business address, and the sole purpose of the use of the personal data is to improve the intragroup communication for assisting the employees to identify their colleagues in meetings, shall not be considered as a not freely given consent because the processing of images in the list does not have in itself negative consequences.

Individual Rights with Regard to Data Protection

The data subject (employee) shall obtain from the data controller (the employer in this case):

- Confirmation as to whether or not data relating to the employee are being processed
- Information at least as to the purposes of the processing, the categories of data concerned, and the recipient or categories of recipients to whom the data are disclosed
- Knowledge of the logic involved in any automatic processing of data concerning the Employee at least in the case of automated decisions.

Commissioner in Cyprus

Employee's (data subjects) have also the right to object on compelling legitimate grounds relating to his/her particular situation to the processing by the employer of data relating to them, and to receive compensation by damages as a result of unlawful processing operation or of any act incompatible with data protection legislation.

The Commissioner in Cyprus may apply to controllers or to any representatives or third parties the following administrative sanctions for breach of their obligations under the Processing of Personal Data (Protection of Individuals) Law of 2001 and any other legislation on the protection of individuals against the processing of personal data:

- warnings in relation to the data breach
- a fine of up to thirty thousand euros (€ 30.000)
- temporary revocation of license
- permanent revocation of license
- Removal of the files or the relevant personal data.

When processing employee's personal data, employers should always bear in mind fundamental data protection principles such as the following:

- **Legitimacy:** The processing of employees personal data must be legitimate.
- Transparency: Employees shall be aware of which data is the employer collecting about them (directly or from other sources), which are the purposes of processing operations envisaged or carried out with these data presently or in the future.
- **Finality:** Data must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes.
- **Proportionality:** The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Assuming that employees have been informed about the processing operation and assuming that such processing activity is legitimate and proportionate, such a processing still needs to be fair with the employee.
- **Security:** The employer must implement appropriate technical and organisational measures at the workplace to guarantee that the personal data of his employee is kept secured. Particular protection should be granted as regards unauthorised disclosure or access.
- **Accuracy and retention of the data:** The employer must take all the reasonable steps to ensure that inaccurate or incomplete data, having regard to the purposes for which they were processed or further collected, are erased or rectified.
- **Awareness of the staff:** Staff in charge or with responsibilities in the processing of personal data of other employee's need to know about data protection and receive proper training.

Conclusion

It arises from the above that any monitoring, must be a proportionate response by an employer to the risks it faces taking into account the legitimate privacy and other interests of employees and any personal data held or used in the course of monitoring must be adequate, relevant and not excessive for the purpose for which the monitoring is justified. Any monitoring must be carried out in the least intrusive way possible. It must be targeted on the area of risk, taking into account the data protection rules. Monitoring, including surveillance by camera, must be informed of the existence of the surveillance, the purposes for which personal data are to be processed and other information necessary to guarantee fair processing.

Additionally, not all problems that involve the processing of personal data are exclusively data protection ones. The legitimate interests of the employer justify certain limitations to the privacy of individuals at the workplace. Sometimes it is the Law or the interests of others which impose these limitations. However, no business interest may ever prevail on the principles of transparency, lawful processing, legitimisation, proportionality, necessity and others contained in Data Protection Legislation. Employees can always object to the processing when it is susceptible of unjustifiably overriding his/her fundamental rights and freedoms. Given the specificity of the employment relationship, consent will not normally be a way to legitimise the processing in the employment context. Where it is relied on, consent must always be freely given, specific and informed.

NOTES

The above is intended to provide a brief guide only. It is essential that appropriate professional advice is obtained. Totalserve Management Ltd will be glad to assist you in this respect. Please do not hesitate to contact us.