SZECSKAY | ÜGYVÉDI IRODA
ATTORNEYS AT LAW

H-1055 BUDAPEST, KOSSUTH TÉR 16-17
(MAIL: H-1245 BUDAPEST PF/POB 1228)
HUNGARY

TEL: +36 (1) 472 3000 • FAX +36 (1) 472 3001 • INFO@SZECSKAY.COM • WWW.SZECSKAY.COM

EMPLOYEE MONITORING FROM THE PERSPECTIVE OF HUNGARIAN DATA PROTECTION LAWS

While employers oftentimes wish to monitor the behavior of their employees, which generally is a rightful intention, it is also the employees' rightful expectation for the employer to respect their privacy and personal data. In this article, we provide a brief overview of the most important rules employers must observe when monitoring their employees.

Under the Hungarian Labour Code, an employer may inspect the work of its employees. However, there are certain mandatory rules employers must comply with when actually monitoring employee's behaviour.

The data commissioner has issued several opinions (aka information sheets) on the employer's control of the employee's use of Internet, email and cellular phone. They also addressed the issue of surveillance cameras at the workplace and to what extent and under what conditions employers may use them.

Under the Hungarian Data Protection Act, personal data may only be managed with consent from the person concerned. Personal data means any information relating to an identified or identifiable natural person and any reference drawn, whether directly or indirectly, from such information. In the course of data management, such information shall be treated as personal data as long as the data subject remains identifiable through it. 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/her physical, physiological, mental, economic, cultural or social identity.

For the purposes of the Data Protection Act, data management means any operation or set of operations that is performed upon data, whether or not by automatic means, such as collection, recording, arrangement, storage, adaptation or alteration, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction, and blocking them from further use. Photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images) also qualifies as data management.

SZECSKAY | ÜGYVÉDI IRODA
ATTORNEYS AT LAW

H-1055 BUDAPEST, KOSSUTH TÉR 16-17
(MAIL: H-1245 BUDAPEST PF/POB 1228)
HUNGARY

TEL: +36 (1) 472 3000 • FAX +36 (1) 472 3001 • INFO@SZECSKAY.COM • WWW.SZECSKAY.COM

It is worth noting that concerned person's consent means any freely given specific and informed indication of his / her wishes by which the person concerned signifies his / her agreement to his / her personal data being processed without limitation or with regard to specific operations. This means that for the purposes of the Data Protection Act, only consent that has been granted based on proper, complete and prior information given by the employer may be regarded as consent.

We now briefly address the various means through which employee behavior may be lawfully monitored.

1 Internet Use

The employer may monitor the use of Internet by the employees if

(i) the employer has previously informed the employees that Internet is provided specifically for work-related purposes and of the prohibition to use the Internet for private purpose and also of the employees' rights concerning data management and

(ii) the employees have given their written consent regarding monitoring as indicated under clause (i) above.

The monitoring must be proportionate with the aims wished to be achieved by the employer and must be justified by a lawful aim of the employer. Personal data can only be managed for specified and explicit purposes, where it is necessary for carrying out certain rights or obligations. This purpose must subsist in all stages of operations of data management. The personal data managed must be essential for the purpose for which they were collected, they must be suitable for achieving that purpose, and they may be managed to the extent and the duration necessary for achieving that lawful purpose.

If the employer has not prohibited or restricted the use of Internet for private purpose or has explicitly allowed private use, the employer may not lawfully monitor employees' Internet use.

It is worth noting that if the employer may monitor the use of Internet, it does not mean that the employer has the right to review all data collected through monitoring. The employer may only list the data downloaded and the sites visited; it may not review such data and sites.

H-1055 BUDAPEST, KOSSUTH TÉR 16-17
(MAIL: H-1245 BUDAPEST PF/POB 1228)
HUNGARY

TEL: +36 (1) 472 3000 • FAX +36 (1) 472 3001 • INFO@SZECSKAY.COM • WWW.SZECSKAY.COM

Of course, the employer may restrict the employees' use of Internet in a way that certain sites cannot be opened. In addition, the employer may also easily list the sites opened and files downloaded.

2 Email Use

If the employer wishes to monitor email correspondence, the employer must properly and completely inform the employees of the monitoring of email use in advance. The information must cover the following:

(i) purpose and duration of monitoring;

(ii) entity carrying out data management and

(iii) rights of the data subjects.

The employer must obtain prior written consent to such monitoring from the employees. Again, as indicated above, personal data may be managed only for specified and explicit purposes, where it is necessary for carrying out certain rights or obligations. This purpose must subsist in all stages of operations of data management. The personal data managed must be essential for the purpose for which they were collected, they must be suitable for achieving that purpose, and they may be managed to the extent and the duration necessary for achieving that purpose.

It is worth noting that any email sent to or received from a third party may not be reviewed. This is because the third party has not given his / her consent to such review / data management.

If the employer has provided an email account to the employees for work purposes, the employer may review the subject of the email, the name of sender and recipient, date and size of email. Following such review, the employer may require the employee to hand over to him a specific email. The employee may refuse to hand over an email only by way of reference to a third party's interest.

Instead of a total prohibition from using the work-related email account for private purposes, it is also possible to restrict the use of email, e.g. in a way that emails above a certain size may not be sent from the specific email account or no email may be sent to a specific addressee.

SZECSKAY | ÜGYVÉDI IRODA ATTORNEYS AT LAW

H-1055 BUDAPEST, KOSSUTH TÉR 16-17
(MAIL: H-1245 BUDAPEST PF/POB 1228)
HUNGARY

TEL: +36 (1) 472 3000 • FAX +36 (1) 472 3001 • INFO@SZECSKAY.COM • WWW.SZECSKAY.COM

It is worth noting that IT hosts may review email correspondence if such review is necessary for protecting the employer's IT system from viruses. However, it is essential that the information collected by the IT host through the review may not be handed over to third parties, including the employer.

3 Cellular Information

If the employer wishes to know where certain employees are during working hours, the employer must properly and completely inform the employees in advance of such monitoring during working hours. The information must cover the following:

(i) purpose and duration of monitoring;

(ii) entity carrying out data management;

(iii) rights of the data subjects.

The employer must obtain prior written consent to such monitoring from the employees. Personal data may be managed only for specified and explicit purposes, where it is necessary for carrying out certain rights or obligations. This purpose must subsist in all stages of operations of data management. The personal data managed must be essential for the purpose for which they were collected, they must be suitable for achieving that purpose, and they may be managed to the extent and the duration necessary for achieving that purpose.

The employer may under no circumstance monitor the location of its employees out of working hours.

It is worth noting that the employer may not monitor any private calls from office cellular phones nor may it list the calls placed by the employee. This is because the third party (the calling party or the person called) has not given his / her consent to such monitoring.

A practical proposal, as suggested by the data commissioner, is as follows: The employer sets a threshold (budget) for the employees up to which threshold the employer pays the cellular phone bill. This threshold may be determined in a way that it also covers the costs of some estimated private calls by the employees. The relevant employee then pays the amount exceeding the monthly threshold.

H-1055 BUDAPEST, KOSSUTH TÉR 16-17
(MAIL: H-1245 BUDAPEST PF/POB 1228)
HUNGARY

TEL: +36 (1) 472 3000 • FAX +36 (1) 472 3001 • INFO@SZECSKAY.COM • WWW.SZECSKAY.COM

4 Use of Surveillance Cameras

If an employer wishes to install surveillance cameras at the workplace, it must properly and completely inform all employees of the surveillance in advance. The information must cover the following:

(i) purpose and duration of surveillance;

(ii) entity carrying out data management;

(iii) rights of the data subjects and

(iv) whether the surveillance cameras record or simply show real time events without recording anything.

Personal data may be managed only for specified and explicit purposes, where it is necessary for carrying out certain rights or obligations. This purpose must subsist in all stages of operations of data management. The personal data managed must be essential for the purpose for which they were collected, they must be suitable for achieving that purpose, and they may be managed to the extent and the duration necessary for achieving that purpose.

An employer must obtain prior written consent from the employees if surveillance cameras are used to check the performance and/or presence of employees. No consent is needed if surveillance cameras are used to detect theft (e.g. if the cameras are installed in a warehouse). In this case, prior information is sufficient.

The use of surveillance cameras may not be secret. In addition, no surveillance cameras may be used in changing rooms, restrooms, toilets or kitchens. The surveillance cameras must be installed in such a way that they are clearly visible to those entering the relevant room and a sign must be posted at the entry of the rooms equipped with such cameras.

In addition to the above, the employer must ensure that the footage is deleted as and when necessary under the law.

SZECSKAY | ÜGYVÉDI IRODA ATTORNEYS AT LAW

H-1055 BUDAPEST, KOSSUTH TÉR 16-17
(MAIL: H-1245 BUDAPEST PF/POB 1228)
HUNGARY

TEL: +36 (1) 472 3000 • FAX +36 (1) 472 3001 • INFO@SZECSKAY.COM • WWW.SZECSKAY.COM

Although employees can request that the employer delete relevant footage relating to them, the employer may refuse this request if it turns out that the employee requesting deletion committed a theft which can be proven by the relevant footage.

The contents of this article are intended to provide only a general overview of the subject matter. Specialist advice should be sought for specific matters. Queries relating to this article should be addressed to the author at:

ZOLTAN.KOVACS@SZECSKAY.COM