Monitoring use of email and Internet and recording conversations (3/3/20)

The use of information technology at work is becoming increasingly common. For example, there are profilers that, for the purpose of setting the amount of a performance bonus, monitor how much time staff spend on the computer and particular applications, or assess Internet addresses they visit during working hours. Likewise, employers often monitor the use of email and the Internet or record staff conversations to monitor their daily routine and productivity. This article explores cases where this is permitted and where such monitoring or its extent infringes on staff privacy.

The employer's rights and obligations

The employer is permitted to monitor and restrict use of the Internet (e.g. ban a particular website) and the use of means of communication (put a limit on messaging, set up a spam filter etc) in order to –

- safeguard the network against threats (e.g. by banning potential malware);
- minimise the risk of allowing excessive use of the Internet and means of communication for private purposes (buying goods, social networking, travelling etc).

However, the employer is required by the GDPR[1] to notify staff of the aims and reasons for personal data processing.

For example, in its ruling of 3 April 2007 on Copland vs the UK, the European Court of Human Rights found a breach of article 8 of the European Convention on Human Rights because the company had not issued any internal policy to specify circumstances in which the employer is permitted to monitor how staff use the Internet, email and telephone.

The company secretly monitored a college worker's use of the Internet, email and telephone to find out whether she was excessively using the college's devices for private purposes.

In addition to the employer's duty of notification, staff must also be informed about the extent and nature of the employer's monitoring activities.

For example, in its ruling of 5 September 2017 on Bărbulescu vs Romania, the European Court of Human Rights found that although the worker had been notified of the company's internal policies, the employer had failed to inform the worker about the extent and nature of the employer's monitoring activities and ability to access the content of staff communications. This breached article 8 of the European Convention on Human Rights.

The employer had asked the worker to set up a Yahoo Messenger account for professional purposes. The employer had announced twice that the worker's email was being monitored. The worker was dismissed after the employer found the Yahoo Messenger account had been used for private purposes.

What the employer is not permitted to do

- The employer is not permitted to receive automatic copies of all emails received and sent by staff. This is excessive.

- The employer is not permitted to freely read staff emails even if the employer's devices are used. This is excessive.
- The employer is not permitted to retain information about all activities a worker has performed on computer unless an especially high security protection is required under certain conditions. Otherwise such monitoring of staff activities is illegal.
- The employer is not permitted to access staff usernames and passwords. However, if a worker is absent and any information they hold is necessary for performing certain functions and tasks, the employer may request access data from the system administrator. The same applies to the worker's email in their absence.
- Server audit trails may be stored for a certain period.
- The recording of staff conversations with the aim of training new recruits must not be done over a prolonged period or constantly. Recording staff conversations without a stated aim and reason is prohibited. The employer should assess whether this aim can be achieved by taking alternative measures or by processing a smaller amount of personal data.

Recommendations for employers

We recommend informing workers about –

- the aims and reasons for personal data processing;
- the extent and nature of the employer's monitoring activities;
- possible recipients of personal data; and
- the exercise of statutory rights (such as the right to access personal data and the right to adjust it under article 13 and 14 of the GDPR).

We recommend preparing this policy as a separate document rather than including it in the organisation's general policies.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) including articles 13(1)(c) and 14(1)(c)