

## Internet Surveillance at the Work Place

### Issue

Email and internet access in the work place raise the issue of how the employer can monitor their use and limit their use for nonbusiness purposes. The employer has a legitimate interest in maintaining control over employee internet use in order to:

- limit the use to work related activities only and thus avoid a decrease in employee productivity;
- ensure the security of the IT infrastructure by banning certain activities and identifying the source of security breaches;
- avoid a waste of IT resources.

Restricting internet use is a labour law issue which is not addressed in detail here. The monitoring of the internet use of employees is an issue under both the Swiss Federal Data Protection Act and related labour laws. The Federal Data Protection and Information Commissioner also has issued guidelines on the issue.

### Principles applicable to the monitoring of internet use at the work place

Swiss labour law prohibits the use of control and monitoring devices for the purpose of monitoring the behaviour of employees at the work place, but allows the use of control and monitoring devices for other purposes, if necessary, provided the health and liberty of the employees is not compromised.

Prior to any monitoring, the employer should issue a detailed, written acceptable use policy setting out the purposes for which the employees may use internet access and the limitations that apply.

The employer is required to use adequate technical security measures, such as firewalls, to restrict infringements of the acceptable use policy, and keep such security measures technically up to date. Monitoring internet use is not a permissible alternative to reasonable technical security measures, but it may be used to complement them.

Systematic monitoring of an individual employee's internet use is prohibited. However, the monitoring of internet use through means that do not identify specific employees is allowed to ensure compliance with the acceptable use policy. Anonymous monitoring can be carried out without informing the employees. Monitoring using pseudonyms, i.e., with the possibility to identify the authors of abusive usage, may not be employed universally and may only be used if the employees have been notified in advance of its potential use.

If anonymous monitoring provides evidence of infringement of the acceptable use policy, then it is acceptable to begin monitoring which can identify the employee who is violating the acceptable use policy, provided that employees were notified in advance of the possible use of identity-based monitoring. Notices about identity-based monitoring should be given to employees in writing.

In addition, any monitoring needs to be performed in accordance with a monitoring policy which specifies who is in charge of the monitoring, what is monitored, who will be notified if an abuse is identified and what the consequences of such abuse are. It is recommended that this information be disclosed to employees, along with a statement of what action may be taken if the abusive use is believed to be a criminal act. The most straightforward way to provide this information is to give a copy of the monitoring policy to the employees. In practice, it often makes sense to establish a single policy which combines the acceptable use policy and the monitoring policy.

### **Principles applicable to the monitoring of employee emails**

In principle, the restrictions applicable to the monitoring of internet use also apply to the monitoring of employee emails. There are, however, specific rules due to the nature of email. For instance, a review of email traffic will include the email header and will therefore not be anonymous; emails are more likely to contain private information relating to employees; and employees can only exercise limited control on the emails they receive.

Because it is difficult to monitor email anonymously, a sporadic monitoring of email use, limited to the header information, is permitted. The monitoring must be done in accordance with a monitoring policy and an acceptable use policy must be issued to govern the use of email and, in particular, to prohibit certain uses of email. The employees also must be informed in writing in advance of any email monitoring and of the fact that the monitoring allows identification of both the employee and the sender or recipients of the email.

Notwithstanding the right to monitor the email header information, the employer may not access the content of an employee's private emails. Distinguishing between a private and business email is not always easy without examining an email's content. If there is doubt about the private or business nature of an email, the employee must be consulted and if the employee states that the email is private, it may not be accessed without the employee's consent.