

WORKING WELL IN NETWORKS (Summary)

The use of e-mail and the internet within organisations has increased significantly over the past few years. More and more employees have access to the World Wide Web via a computer at their workstation. At the same time, there are increasing fears that these resources will be used in an improper and risky manner. Employers are keen to monitor such use, whilst employees are quick to regard this as a violation of their personal privacy. This report is a guide intended to assist employers, works councils and individual employees in formulating company policy with regard to the monitoring of e-mail and internet use that does justice to the privacy of employees.

The rules that feature in this report apply to the internet in all its manifestations: older applications such as e-mail, internet sites, newsgroups and chat, as well as the more modern versions such as WAP. Each new variant has new possibilities, but also presents new risks for the employer and the employee. For the employer this can include the security of the network, combating 'prohibited use' or protecting the good name of the organisation. For employees, monitoring often places their entitlement to privacy under pressure, however it also affects their right to freedom of expression or to gather information.

During working hours, employees are subject to certain restrictions of their fundamental rights. This does not mean that, in protecting his or her interests (for example combating misuse by means of monitoring e-mail or internet use), an employer can push the fundamental freedoms of his or her employees aside. The protection of privacy in the workplace has been laid down in the form of a whole range of legislation and regulations. On the basis of Article 8 of the ECHR, an employee is entitled to a certain degree of confidential communication in the workplace without interference by his or her employer. On the basis of the concepts of being a good employee and good employment practice in the Dutch Civil Code, both parties must adhere to both responsible use of e-mail and the internet and careful policy in respect of monitoring. The Works Councils Act [Wet op de ondernemingsraden] provides works councils with a right of approval with regard to the introduction of this type of policy. Finally, the Dutch Data Protection Act [Wet bescherming persoonsgegevens, Wbp] provides a framework with regard to how personal data in relation to e-mail and internet use should be dealt with.

On the basis of labour law and legislation on privacy, rules of thumb have been formulated with regard to the use and monitoring of e-mail and internet in the workplace. These rules of thumb are intended to serve as a guide for the drawing up of proper and careful policy within workers' organisations. In order to enlarge the applicability of the rules of thumb, the Dutch Data Protection Authority (Dutch DPA) [College Bescherming Persoonsgegevens (CBP)] has developed general regulations for the use of e-mail and internet. These are intended to serve as an instrument to enable organisations, companies and works councils to apply the rules of thumb to their own policy.

Rules of thumb for monitoring the use of e-mail and the internet

General

1. Treat business online in the same manner as offline.
2. Set up clear rules with the agreement of the works council.
3. Publish the rules in a way that is accessible for the employee.
4. Determine to what extent private use of the facilities is permitted.
5. Make prohibited use impracticable as far as possible through the use of software.
6. Make reports and user statistics anonymous.
7. Take into consideration the system back-ups.
8. Guarantee the integrity of the system manager.
9. Discuss detected behaviour with the person concerned as soon as possible.
10. Grant access to the data.
11. Periodically evaluate the rules.

E-mail and internet

12. Try to separate business and private mail and avoid monitoring private mail wherever possible.
13. Limit monitoring to the objective formulated. Provide for a relevant control mechanism.
14. Minimize the monitoring of observance (tailored work).
15. Limit the logging of network use to the data traffic. Do not save the logged data for any longer than is necessary.
16. Avoid privileged information from members of the works council and company doctors in electronic messages.