

## **MONITORING IN WORKING LIFE**

### **Report 2005:3 Summary in English**

The Data Inspection Board has previously investigated how personal data is processed in working life to check up on employees. The conclusions drawn by the Data Inspection Board from that investigation are presented in the Data Inspection Board report 2003:3 “The processing of personal data to check up on employees”.

In order to follow the development in this field, the Data Inspection Board has extended the investigation during 2005, by controlling the processing of personal data by more employers. In the new project the Data Inspection Board has examined the employers’ control of the use of the Internet and e-mail of the employees, and to what extent the workers are being monitored by means of processing of biometric data and surveillance cameras. The supervision comprises different companies and public authorities than those examined in the previous project.

The supervision was initiated by letting 103 companies and public authorities, chosen at random, answer a number of questions in writing in a questionnaire regarding the use of the Internet and e-mail of the employees and the monitoring that exists by means of processing of biometric data and surveillance cameras.

After the answers of the questionnaires had been put together, 15 of these companies and public authorities were inspected on the spot. The Data Inspection Board primarily selected companies and public authorities that had worked out guidelines regarding monitoring the use of the Internet of the employees respectively had begun the processing of biometric data. In two cases IT-security inspections were carried out.

### **Most employers have regulations on how the Internet and e-mail may be used**

Most employers had some sort of documented IT-policy that more or less regulated the right of the employees to use the Internet and e-mail. In most workplaces the employees had the right to use the Internet and e-mail for private purposes, with certain restrictions.

### **Half of the employers monitor the use of the Internet of the employees -but not with the aim of checking what the employees do during working hours**

Approximately half of the employers stated that they carry out some sort of checks concerning the use of the Internet of the employees. They often stated that the purpose of the control was security-related, that there were technical reasons or that it was in order to investigate a suspected legal offence. However, it was very unusual that employers monitored the use of the Internet in order to check what the employee was doing during working hours. On the other hand, an increasing common purpose of the checks was to try to obstruct surfing on unethical websites. Nevertheless, the inspections showed that many of the employers did not have a clear conception of what was to be considered as unethical in this context.

## **Few employers monitor the e-mails**

Only a few employers stated that they monitored the use of the Internet by employees. At the routine control the employers went through log files first of all. A routine investigation of the contents of the e-mails did not exist in any of the cases. Fundamentally, the individual ran the risk of being checked only if an e-mail had caused virus attacks, overloading of the system or if suspicion of a legal offence had occurred.

## **Lack of information – what is allowed and how is the check carried out?**

The Data Inspection Board has, within the scope of the project, examined the written information that employers provided employees with more closely, concerning the monitoring of the use of the Internet and e-mail that existed at the workplace. In approximately half of the investigated cases the standard of the information material of the employers was good. Just over ten percent of the employers involved in the investigation did not have any guidelines at all.

A common lack in the information was that there were no clear regulations concerning the use of the Internet by the employee. From the information it was only concluded that the employee was not allowed to use the Internet and e-mail in “doubtful and non-serious contexts” and that they should be used in accordance with “implicit ethical regulations”.

Furthermore, nearly half of the employers who carried out some sort of check concerning the employees’ use of the Internet were lacking regulations as to how this check was to be carried out. The corresponding figure regarding monitoring of e-mail was 20 percent. A quarter of the employers who carried out checks did not provide the employees with any kind of information regarding the control.

Even though it has become more common that consent is obtained for the checks that are carried out, this was only applied in a minority of the cases. In a little more than a third of the cases the checks were performed under some sort of trade union agreement.

## **Few have procedures when it comes to deleting data**

The answers of the questionnaires and experience from the inspections showed that it is still common that employers do not have any procedures when it comes to deleting data in accordance with the Personal Data Act. The Data Inspection Board considers that data that is the basis of the employer’s monitoring of the employee’s use of the Internet and e-mail in normal cases should not be kept longer than three months.

The Data Inspection Board has been able to notice that some employers use specific blocking programs that prevent surfing on unethical websites. Thanks to the blocking program this part of the purpose is served without any intrusive or extensive monitoring of the employees.

## **It is very unusual to use biometry**

The processing of employees’ biometric data was still something very unusual. Just one of the investigated employers used the biometric data of the employees for

authentication/verification or identification procedures. A few of the employers stated that they were planning to begin processing biometric data of the employees in the future. The Data Inspection Board points out certain issues in the report that an employer has to bear in mind when considering beginning such processing.

### **Camera surveillance is unusual and is not used for measurement of performance**

Camera surveillance of employees in the workplace where the public does not have access was also rather unusual. Eight employers claimed that such surveillance was carried out in a way that was comprised by the Personal Data Act. The monitoring that existed was carried out for security and technical reasons as well as in order to obstruct and investigate illegal activities. The monitoring was not performed in any case with the purpose of checking the work achievements of the employee. The areas at which the cameras were aimed were of the kind that the employee may pass through, but not generally carry out his work in.

Regarding the camera surveillance that existed, the Data Inspection Board noticed two major defects:

- In several cases the recordings were kept for a long time, or there were no regulations regarding how long the recording could be kept. With regard to the purposes of monitoring that were stated in the answers of the questionnaires, the Data Inspection Board considers that it should be an objective in the normal case to delete the recordings daily or weekly.
- The information provided to the employees is insufficient. In the opinion of the Data Inspection Board, the requirements of the Personal Data Act go beyond the demand for information concerning camera surveillance in the Act on general camera surveillance. In the cases where the camera surveillance is comprised by the Personal Data Act it is therefore not enough to put up signs in the spaces where the camera surveillance is carried out, which was the case among some of the employers in this study.

In conclusion, it could be added that the project has shown that many employers have technical possibilities to perform an extensive control of the use of the Internet and e-mail by employees, but in the present situation few employers take advantage of these possibilities. There are significant defects regarding the information provided to the employees concerning the limited control that is performed today. Many employers also need to improve information regarding how the IT tools may be used.