

## **Regulations on the processing of personal data (Personal Data Regulations).**

Laid down by the Royal Decree of 15 December 2000 pursuant to the Act of 14 April 2000 No. 31 on the processing of personal data (Personal Data Act), sections 3, 4, 12, 13, 14, 26, 30, 31, 32, 33, 41, 43, 44, 48 and 51. Issued by the Ministry of Justice and the Police, transferred to the Ministry of Labour and Government Administration by the Decree of 15 December 2000 No. 1263. Amended on 23 December 2003 No. 1798 (i.a. title), 6 May 2005 no. 408, 23 August 2005 no. 923, 16 February 2006 no. 200, 5 June 2007 no. 1092, 24 April 2008 no. 396 (ratifies earlier amendments), Regulation 29 January 2009 no. 84, 5 June 2009 no. 598.

### **Chapter 1. The scope of the Personal Data Act.**

#### ***Section 1-1. The Office of the Auditor General's processing of personal data***

When the Office of the Auditor General processes personal data as part of its control activities, such processing shall be exempted from sections 18, 27, 31 and 33 of the Personal Data Act.

The Personal Data Act in its entirety shall apply to all other processing by the Office of the Auditor General.

#### ***Section 1-2. Personal data processing that is necessary in the interests of national security***

Personal data processing that is necessary in the interests of national security or the security of allies, the relationship to foreign powers and other vital national security interests shall be exempted from section 44, first to third paragraphs, of the Personal Data Act, and from sections 31 and 33 of the Act.

Any disagreement between the data controller and the Data Inspectorate regarding the extent of the exemption shall be decided by the Privacy Appeals Board.

#### ***Section 1-3. Processing of personal data in the administration of justice, etc.***

The Personal Data Act shall not apply to matters that are dealt with or decided pursuant to the Acts relating to administration of justice (the Courts of Justice Act, the Criminal Procedure Act, the Civil Procedure Act and the Enforcement Act, etc.).

Amended by the Regulations of 23 December 2003 No. 1798 (in force from 1 January 2004). 5 June 2007 no. 1092 (in force January 2008), 24 April 2008 no. 396 (ratification).

(In section 1-3 the formula "Civil Procedures Act (*tvistemålsloven*)" is replaced by "Civil Procedures Act (*tvisteloven*)").

#### ***Section 1-4. Svalbard***

The Personal Data Act and appurtenant Regulations shall apply to data controllers who are established on Svalbard.

The Data Inspectorate may by individual decision grant dispensation from the individual provisions of the Personal Data Act if local conditions make this necessary.

### ***Section 1-5. Jan Mayen***

The Personal Data Act and appurtenant Regulations shall apply to data controllers who are established on Jan Mayen.

## **Chapter 2. Data security**

### ***Section 2-1. Proportionality requirements relating to the protection of personal data***

The provisions of this chapter shall apply to such processing of personal data as is carried out entirely or partly by automatic means where it is necessary, in order to prevent the danger of loss of life and health, financial loss or loss of esteem and personal integrity, to protect the confidentiality, availability and integrity of the data.

Where such a danger exists, the planned and systematic measures taken pursuant to these Regulations shall be proportional to the probability and consequence of breaches of security.

### ***Section 2-2. Orders from the Data Inspectorate***

The Data Inspectorate may issue orders regarding the protection of personal data, including the establishment of criteria for acceptable risk associated with the processing of personal data.

### ***Section 2-3. Security management***

The general manager of the enterprise run by the data controller is responsible for ensuring compliance with the provisions of this chapter.

The purpose of the processing of personal data and general guidelines for the use of information technology shall be described in security objectives.

Choices and priorities in security activities shall be described in a security strategy.

Use of the information system shall be reviewed regularly in order to ascertain whether it is appropriate in relation to the needs of the enterprise, and whether the security strategy provides adequate data security.

The result of the review shall be documented and used as a basis for any changes in security objectives and strategy.

### ***Section 2-4. Risk assessment***

An overview shall be maintained of the kinds of personal data that are processed. The enterprise shall itself establish criteria for acceptable risk associated with the processing of personal data.

The data controller shall carry out a risk assessment in order to determine the probability and consequences of breaches of security. A new risk assessment shall be carried out in the event of changes of significance for data security.

The result of the risk assessment shall be compared with the established criteria for acceptable risk associated with the processing of personal data, cf. first paragraph and section 2-2.

The result of the risk assessment shall be documented.

### ***Section 2-5. Security audits***

Security audits of the use of the information system shall be carried out regularly.

A security audit shall comprise an assessment of organization, security measures and use of communication partners and suppliers.

If the security audit reveals any unforeseen use of the information system, this shall be treated as a discrepancy, cf. section 2-6.

The result of the security audit shall be documented.

### ***Section 2-6. Discrepancies***

Any use of the information system that is contrary to established routines, and security breaches, shall be treated as a discrepancy.

The purpose of discrepancy processing shall be to re-establish the normal state of affairs, eliminate the cause of the discrepancy and prevent its recurrence.

If the discrepancy has resulted in the unauthorised disclosure of personal data where confidentiality is necessary, the Data Inspectorate shall be notified.

The result of discrepancy processing shall be documented.

### ***Section 2-7. Organization***

The distribution of responsibility for and authority governing the use of the information system shall be clearly established.

The distribution of responsibility and authority shall be documented and shall not be changed without the authorization of the data controller's general manager.

The information system shall be configured in such a way as to achieve adequate data security.

The configuration shall be documented and shall not be changed without the authorization of the data controller's general manager.

Use of the information system that has significance for data security shall be carried out in accordance with established routines.

### ***Section 2-8. Personnel***

Members of the staff of the data controller shall only use the information system to carry out assigned tasks, and shall be personally authorized to make such use.

The staff members shall have the knowledge necessary to use the information system in accordance with the routines that have been established.

Authorized use of the information system shall be registered.

### ***Section 2-9. Duty of confidentiality***

Members of the staff of the data controller shall be subject to a duty of confidentiality as regards personal data where confidentiality is necessary. The duty of confidentiality shall also apply to other data of significance for data security.

### ***Section 2-10. Physical security***

Measures shall be taken to prevent unauthorized access to equipment that is used to process personal data pursuant to these Regulations.

The security measures shall also prevent unauthorized access to other equipment of significance for data security.

Equipment shall be installed in such a way that influence from the environment in which it is operated does not significantly affect the processing of personal data.

### ***Section 2-11. Protection of confidentiality***

Measures shall be taken to prevent unauthorized access to personal data where confidentiality is necessary.

The security measures shall also prevent unauthorized access to other data of significance for data security.

Personal data that are transferred electronically by means of a transfer medium that is beyond the physical control of the data controller shall be encrypted or protected in another way when confidentiality is necessary.

As regards storage media that contain personal data where confidentiality is necessary, the need to protect confidentiality shall be shown by means of marking or in another way.

If the storage medium is no longer used for the processing of such data, the data shall be erased from the medium.

### ***Section 2-12. Securing of accessibility***

Measures shall be taken to secure access to personal data where accessibility is necessary.

The security measures shall also secure access to other data of significance for data security.

Preparations shall be made for alternative processing in the event of the information system being unavailable for normal use.

Personal data and other data that are necessary to restore normal use shall be copied.

### ***Section 2-13. Protection of integrity***

Measures shall be taken to prevent unauthorized changes in personal data where integrity is necessary.

The security measures shall also prevent unauthorized changes in other data of significance for data security.

Measures shall be taken to prevent malicious software.

### ***Section 2-14. Security measures***

Security measures shall prevent unauthorized use of the information system and make it possible to detect attempts to make such use.

Attempts to make unauthorized use of the information system shall be registered.

Security measures shall include measures that cannot be influenced or circumvented by members of the staff, and shall not be limited to actions that any individual member is supposed to carry out.

Security measures shall be documented.

### ***Section 2-15. Security in other enterprises***

The data controller shall only transfer personal data by automatic means to a person who satisfies the requirements of these Regulations.

The data controller may transfer personal data to any person if the transfer is carried out in accordance with the provisions of sections 29 and 30 of the Personal Data Act, or when it has been laid down by statute that requests may be made to obtain the data from a public register.

Data suppliers who carry out security measures, or make other use of the information system on behalf of the data controller, shall satisfy the requirements of this chapter.

The data controller shall clearly establish the distribution of responsibility and authority in respect of communication partners and suppliers. The distribution of responsibility and authority shall be described in a special agreement.

The data controller shall have knowledge of the security strategy of communication partners and suppliers, and regularly make sure that the strategy provides adequate data security.

### ***Section 2-16. Documentation***

Routines for using the information system and other data of significance for data security shall be documented.

The documentation shall be stored for at least five years from the time the document was replaced by a new, current version.

Records of authorized use of the information system and of attempts at unauthorized use shall be stored for at least three months. The same shall apply to records of all other events of significance for data security.

## **Chapter 3. Internal controls**

### ***Section 3-1. Systematic measures for processing personal data***

The data controller shall establish internal controls in accordance with section 14 of the Personal Data Act. The systematic measures shall be adapted to the nature, activities and size of the enterprise to the extent that is necessary in order to comply with requirements laid down in or pursuant to the Personal Data Act, with special emphasis on provisions laid down pursuant to section 13 of the Personal Data Act.

Internal controls entail that the data controller shall, *inter alia*, ensure that he has knowledge of current rules governing the processing of personal data, that he has adequate and up-to-date documentation for the implementation of the above-mentioned routines, and that this documentation is available to the persons it may concern.

The data controller shall also have routines for fulfilling his duties and the rights of data subjects pursuant to current rules of privacy, including routines for

- a) obtaining and verifying the consent of data subjects, cf. sections 8, 9 and 11 of the Personal Data Act,
- b) evaluating the purpose of personal data processing in accordance with section 11 a of the Personal Data Act,
- c) evaluating the quality of personal data in relation to the defined purpose of processing the data, cf. sections 11d and 11e, 27 and 28 of the Personal Data Act, and following up any discrepancies,
- d) replying to requests for access and information, cf. sections 16 to 24 of the Personal Data Act,
- e) complying with the data subject's demands for a bar on certain forms of personal data processing, cf. sections 25 and 26 of the Personal Data Act,

- f) complying with the provisions of the Personal Data Act regarding the obligation to give notification and to obtain a licence, cf. sections 31 to 33 of the Personal Data Act.

Data processors who process personal data on assignment for data controllers shall process the data in accordance with routines established by data controllers.

### ***Section 3-2. Dispensation***

The Data Inspectorate may grant a dispensation from all or parts of this chapter when special circumstances exist.

## **Chapter 4. Credit information services**

### ***Section 4-1. Relationship to the Personal Data Act***

The provisions of the Personal Data Act shall apply to the processing of personal data in credit information services unless these Regulations otherwise provide.

The Personal Data Act shall also apply to the processing of credit information relating to persons other than natural persons.

### ***Section 4-2. Definition of a credit information service***

For the purposes of this chapter, the term "credit information service" means activities which consist in providing information that throws light on creditworthiness or financial solvency (credit information). This chapter does not apply to the utilization of information within an enterprise, or in relation to enterprises within the same corporate group unless the information is provided by an enterprise operating a credit information service. Nor does it apply to the provision of information to another credit information enterprise to which this Act applies, provided that the information is to be utilized in this enterprise's own credit information service.

- The following services are not regarded as credit information services:
- a) notifications from public registers regarding rights in and charges on real or movable property,
  - b) notifications from banks (cf. the Act of 24 May 1985 No. 28 on Norges Bank and the Monetary System (the Norges Bank Act), the Act of 1 March 1946 No. 3 on the Norwegian State Housing Bank, the Act of 24 May 1961 No. 1 on Savings Banks, the Act of 24 May 1961 No. 2 on Commercial Banks) and from finance companies (cf. the Act of 10 June 1988 No. 40 on financial activities and financial institutions) in connection with withdrawals from accounts and the execution of payment services. The same applies when such notifications are transmitted for a bank or finance company by an outside enterprise,
  - c) notifications to the data subject,
  - d) the publication of publicly exhibited tax assessments pursuant to section 8-8 of the Act of 13 June 1980 No. 24 on Tax Assessment Administration (the Tax Assessment Act).
  - e) the Brønnøysund registers' processing of registers required by statute.
  - f) notices from the Chattels (Moveable Property) Register concerning registered distraint and actions to ascertain "no distrainable property".

Amended by Regulation 24 April 2008 nr. 396.

### ***Section 4-3. Disclosure of credit information***

Credit information may only be given to persons who have an objective need for it.

Credit information shall be provided in writing either by automatic means or in paper-based form. However, credit information may be given orally provided that it does not contain any data that can be cited against the data subject, or if the credit information must be given without delay for practical reasons. If credit information is given orally, the information and the applicant's name and address shall be recorded and kept on file for at least six months. If the information contains any data that can be cited against the data subject, it shall be confirmed in writing.

Credit information may be supplied by distribution of publications or lists, provided that the publication or list only contains data concerning business enterprises, and that the data is given in summary form. Such publications may only be given to persons who are members or subscribers of the credit information processor.

Agreements entailing that the applicant shall be given any information that comes to the knowledge of the credit information enterprise in the future may only be made in respect of information relating to business enterprises.

### ***Section 4-4. Right of access of and information to the data subject***

If credit information relating to natural persons is provided or confirmed in writing, the credit information enterprise shall at the same time send a duplicate, copy or other notification concerning the contents free of charge to the person about whom data has been requested. The data subject shall be invited to request that any errors be rectified.

The right of access of legal persons follows from section 18 of the Personal Data Act.

The data subject may also demand to be informed of what credit information has been provided about him in the last six months, to whom it was given and where it was obtained.

### ***Section 4-5. Permission to operate a credit information service***

An enterprise may not process personal data for credit information purposes until the Data Inspectorate has granted it a licence. The same applies to credit information for persons other than natural persons.

When deciding whether to grant a licence, sections 34 and 35 of the Personal Data Act shall apply. For enterprises over which foreign interests have a controlling influence, conditions may be laid down regarding the form of establishment and the composition of the company's management.

***Section 4-6. Validity of licences granted in pursuance of the Personal Data Filing Systems Act.***

Licences granted for personal data filing systems for use in a credit information service pursuant to section 9 of the Act of 9 June 1978 No. 48 on personal data filing systems, etc. shall apply as licences pursuant to section 4-5 of these Regulations, insofar as the licence is not contrary to the Personal Data Act.

***Section 4-7. The authority of the Data Inspectorate***

If special reasons so indicate, the Data Inspectorate may by individual decision exempt the data controller from obligations that follow from the provisions of this chapter.

**Chapter 5 Repealed by Regulation 5 June 2009 no. 598.**

**Chapter 6. Transfer of personal data to other countries**

***Section 6-1. The EU Commission's decisions concerning the level of protection in third countries***

The Commission's decisions pursuant to Directive 95/46/EF, Articles 25 and 26, cf. 31, shall also apply to Norway in accordance with the EEA Joint Committee's Decision No. 83/1999 (of 25 June 1999 regarding the amendment of Protocol 37 and Appendix XI of the EEA Agreement), unless the right of reservation is exercised.

The Data Inspectorate shall ensure compliance with the decisions.

Amended by the Regulations of 23 December 2003 No. 1798 (in force from 1 January 2004).

***Section 6-2. The Data Inspectorate's assessment of the level of protection in third countries***

If the Data Inspectorate concludes that a third country does not have an adequate level of protection for the processing of personal data, the Data Inspectorate shall notify the EU Commission and the other member states of its decision.

If the Data Inspectorate, after assessing a specific case pursuant to Directive 95/46/EF, Article 26, no. 2, nevertheless permits the transfer of personal data to a third country that does not ensure an adequate level of protection pursuant to Directive 95/46/EF, Article 25, no. 2, the Data Inspectorate shall notify the EU Commission and other member states of its decision.

If the Commission or other member states object to the Data Inspectorate's decisions pursuant to the second paragraph, and the Commission takes steps, the Data Inspectorate shall ensure compliance with the decision.

Amended by the Regulations of 23 December 2003 No. 1798 (in force from 1 January 2004). 24 April 2008 no. 396 (ratification).

*Section 6-3. (Repealed by the Regulations of 23 December 2003 No. 1798, in force from 1 January 2004.)*

## **Chapter 7. Obligation to give notification and to obtain a licence**

### **I. Obligation to obtain a licence, etc.**

#### ***Section 7-1. Obligation to obtain a licence for the processing of personal data in the telecommunications sector***

Personal data processing by providers of telecommunication services for the purpose of customer administration, invoicing and the provision of services in connection with the subscriber's use of the telecommunications network shall be subject to licensing pursuant to the Personal Data Act.

For the purposes of these Regulations, the term "providers of telecommunication services" shall mean enterprises which for commercial purposes provide telecommunications wholly or partly by means of transmissions through the telecommunications network that are not broadcasts.

#### ***Section 7-2. Obligation to obtain a licence for the processing of personal data in the insurance sector***

Personal data processing by providers of insurance services (cf. Act of 10 June 1988 No. 39 on insurance activity) for the purpose of customer administration, invoicing and the implementation of insurance contracts shall be subject to licensing pursuant to the Personal Data Act.

#### ***Section 7-3. Obligation to obtain a licence for the processing of personal data by banks and financial institutions***

Personal data processing by banks and financial institutions (cf. the Act of 24 May 1985 No. 28 on Norges Bank and the Monetary System (the Norges Bank Act), the Act of 1 March 1946 No. 3 on the Norwegian State Housing Bank, the Act of 24 May 1961 No. 1 on Savings Banks, the Act of 24 May 1961 No. 2 on Commercial Banks), the Act of 10 June 1988 No. 40 on financial activities and financial institutions) for the purpose of customer administration, invoicing and the implementation of banking services shall be subject to licensing pursuant to the Personal Data Act.

#### ***Section 7-4. The authority of the Data Inspectorate***

If special reasons so indicate, the Data Inspectorate may decide that personal data processing covered by sections 7-14 to 7-17 and sections 7-21 to 7-25 of these Regulations shall nevertheless be regulated by sections 31 or 33 of the Personal Data Act.

Amended by the Regulations of 24 April 2008 no. 396.

### ***Section 7-5. Notification form***

Notification to the Data Inspectorate shall be given on a form prepared by the Data Inspectorate and pursuant to rules for submission that have been drawn up by the Data Inspectorate.

## **II. Processing that is exempt from the obligation to give notification**

### ***Section 7-6. Exemption from the obligation to give notification***

Processing covered by this chapter shall be exempt from the obligation to give notification pursuant to section 31, first paragraph, of the Personal Data Act. If sensitive data is processed, cf. section 2, subsection 8, of the Personal Data Act, the processing may be subject to licensing pursuant to section 33, first paragraph, of the Personal Data Act.

Exemption from the notification obligation presupposes that the personal data are processed in keeping with the purpose that follows from the individual provision. The provisions of the Personal Data Act regarding personal data processing in chapters I to V and VII to IX shall be complied with even if the processing is exempt from the obligation to give notification.

Amended by the Regulations of 23 December 2003 No. 1798 (in force from 1 January 2004). 24 April 2008 no. 396 (ratification).

### ***Section 7-7. Customer, subscriber and supplier data***

Processing of personal data concerning customers, subscribers and suppliers shall be exempt from the obligation to give notification pursuant to section 31, first paragraph, of the Personal Data Act. The same shall apply to data concerning a third person which is necessary for the fulfilment of contractual obligations.

Exemption from the notification obligation shall only apply if the personal data is processed as part of the administration and fulfilment of contractual obligations.

### ***Section 7-8. Information relating to housing matters***

The processing of personal data as part of the administration and fulfilment of obligations relating to the ownership or lease of real property shall be exempt from the obligation to give notification pursuant to section 31, first paragraph, of the Personal Data Act. This encompasses all leasing and ownership matters such as data relating to tenants in tenancy relationships, co-owners of jointly owned property and shareholders in housing cooperatives and housing cooperative stock corporations.

Amended by the Regulations of 23 December 2003 No. 1798 (in force from 1 January 2004), 24 April 2008 no. 396 (ratification).

### ***Section 7-9. Register of shareholders***

Personal data processing as required by section 4-5 of the Act of 13 June 1997 No. 44 on Limited Liability Companies (the Limited Liability Companies Act) and section 4-4 of the Act of 13 June 1997 No. 45 on Public Limited Liability Companies (the Public Limited Liability Companies Act) shall be exempt from the obligation to give notification pursuant to section 31, first paragraph, of the Personal Data Act.

Exemption from the notification obligation shall only apply if the purpose of the processing is to fulfil the obligations imposed on the individual company by company legislation.

Amended by the Regulations of 23 December 2003 No. 1798 (in force from 1 January 2004), 24 April 2008 no. 396 (ratification).

### ***Section 7-10. Keeping of mediation records***

Personal data processing in connection with the keeping of mediation records as required by the Act of 8 April 1981 No. 7 on Children and Parents (the Children Act) and the Act of 4 July 1991 No. 47 on Marriage shall be exempt from the obligation to give notification pursuant to section 31, first paragraph, of the Personal Data Act.

Exemption from the notification obligation shall only apply if the purpose of the processing is to verify that mediation has taken place, to evaluate and plan the mediation arrangement, or to provide a basis for statistical analyses.

### ***Section 7-11. Activity logs in EDP systems or computer networks***

Personal data processing as a consequence of the registration of activity (events) in an EDP system, and personal data processing relating to the use of system resources, shall be exempt from the obligation to give notification pursuant to section 31, first paragraph, of the Personal Data Act.

Exemption from the notification obligation shall only apply if the purpose of the processing is:

- a) to administer the system, or
- b) to uncover/clarify breaches of security in the EDP system.

Personal data that are revealed as a result of processing pursuant to the second paragraph may not subsequently be processed in order to monitor or check up on the natural person.

### ***Section 7-12. Privacy ombudsman***

The Data Inspectorate may consent to exemptions being granted from the obligation to give notification pursuant to section 31, first paragraph, of the Personal Data Act, if the data controller designates an independent privacy ombudsman who is responsible for ensuring that the data controller complies with the Personal Data Act and appurtenant Regulations. The

privacy ombudsman shall also maintain an overview of such data as are mentioned in section 32 of the Personal Data Act.

### **III. Processing that is exempt from the obligation to obtain a licence and the obligation to give notification**

#### ***Section 7-13. Exemption from the obligation to obtain a licence and the obligation to give notification***

Processing covered by this chapter shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Personal Data Act and from the obligation to give notification pursuant to section 31, first paragraph, of the said Act.

Exemption from the licensing obligation and the notification obligation presupposes that the personal data shall be processed in keeping with the purpose that follows from the individual provision. The provisions of the Personal Data Act regarding the processing of personal data in chapters I to V, and VII to IX, shall be complied with even if the processing is exempt from the licensing obligation and the notification obligation.

#### ***Section 7-14. Sensitive customer data***

The processing of sensitive personal data, cf. section 2-8 of the Personal Data Act, relating to customers shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Act and from the obligation to give notification pursuant to section 31, first paragraph, of the Act.

Exemption from the licensing obligation and the notification obligation shall only apply if the data subject has consented to the registration and processing of the sensitive data, and the data are necessary for the fulfilment of a contractual obligation.

Personal data may only be processed as a necessary part of the administration and fulfilment of contractual obligations.

#### ***Section 7-15. Associations' membership data***

Associations' processing of membership data shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Act and from the obligation to give notification pursuant to section 31, first paragraph, of the Act.

As regards the processing of sensitive personal data, the exemption from the licensing obligation and the notification obligation shall only apply if the data subject has consented to the registration and processing of the sensitive data, and the data have a close and natural connection with membership of the association.

The personal data may only be processed as a necessary part of the administration of the association's activity.

### ***Section 7-16. Personnel registers***

Employers' processing of non-sensitive personal data relating to current or former employees, personnel, representatives, temporary manpower and applicants for a position shall be exempt from the obligation to give notification pursuant to section 31, first paragraph, of the Personal Data Act.

If sensitive personal data are processed, the processing shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Personal Data Act, but subject to the obligation to give notification pursuant to section 31, first paragraph. The exemption from the licensing obligation shall apply provided that:

- a) the data subject has consented to the processing or the processing is laid down by law,
- b) the data are related to the employment relationship,
- c) the personal data are processed as part of the administration of personnel.

However, the obligation to give notification pursuant to the second paragraph shall not apply to the processing of

- a) data concerning membership in trade unions as mentioned in section 2, subsection 8e of the Personal Data Act,
- b) necessary information on absence and information that must be registered under the Act of 17 June 2005 no. 62 relating to the Working Environment, Working Hours and Employment Protection etc. (Working Environment Act) section 5-1.
- c) data that are necessary to adapt a work situation for health reasons.

Amended by Regulations 23 December 2003 no. 1798 (in force 1 January 2004), 16 February 2006 no. 200, 24 April 2008 no. 396 (ratification).

### ***Section 7-17. Personal data relating to public representatives***

The processing of personal data relating to the elected or appointed representatives of bodies established pursuant to the Act of 25 September 1992 No. 107 on municipalities and county municipalities (the Local Government Act) or the Act of 7 June 1996 No. 31 on the Church of Norway (the Church Act) shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Personal Data Act and from the obligation to give notification pursuant to section 31, first paragraph.

The same shall apply to the processing of personal data relating to representatives of the Storting or to members of the Storting's standing committees.

### ***Section 7-18. Processing of personal data by courts of justice***

Personal data processing by courts of justice in connection with the activity of the courts (including registration procedures and notarial functions and the like that are carried out by a judge's office) shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Personal Data Act and from the obligation to give notification pursuant to section 31, first paragraph.

### ***Section 7-19. Processing of personal data by supervisory authorities***

The Data Inspectorate's processing of personal data pursuant to section 42 of the Personal Data Act shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Personal Data Act and from the obligation to give notification pursuant to section 31, first paragraph.

Records as mentioned in section 42, third paragraph, no. 1, of the Personal Data Act shall also contain information concerning the Data Inspectorate's personal data processing.

The first and second paragraphs shall apply correspondingly to the Privacy Appeals Board.

### ***Section 7-20. Pupil and student data at schools and universities, etc.***

The processing of personal data relating to pupils and students that is carried out pursuant to the Act of 17 July 1998 No. 61 on primary and secondary education (the Education Act) or the Act of 12 May 1995 No. 22 on universities and colleges (the University Act) or Act of 1 April 2005 no. 15 relating to Universities and University Colleges (Universities Act) or following the consent of the individual student or guardian, is exempted from the obligation to obtain a licence under the Personal Data Act section 33 first paragraph and from the obligation to give notice under the Personal Data Act section 31 first paragraph.

Added by Regulation of 23 December 2003 no. 1798 (in force 1 January 2004), cf. Regulation of 24 April 2008 no. 396 (ratification).

### ***Section 7-21. Information about children in kindergarten and supervised afternoon activities***

Processing of personal data about children in kindergarten or supervised afternoon activities under the Act of 17 June 2005 no. 64 relating to Day Care Institutions (Day Care Institution Act) and Act of 17 July 1998 no. 61 relating to Primary and Secondary Education (Education Act) or following the consent of the guardian, is exempted from the obligation to obtain a licence under the Personal Data Act section 33 first paragraph and from the obligation to give notice under the Personal Data Act section 31 first paragraph.

Added by Regulation of 23 December 2003 no. 1798 (in force 1 January 2004), cf. Regulation of 24 April 2008 no. 396 (ratification).

## **IV. Processing that is exempt from the obligation to obtain a licence, but subject to the obligation to give notification**

### ***Section 7-22. Exemptions from the obligation to obtain a licence***

Processing covered by this chapter shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Personal Data Act. However, notification of the processing shall be given pursuant to section 31, first paragraph, of the Personal Data Act.

Exemption from the licensing obligation shall only apply if the personal data are processed in keeping with the purpose that follows from the individual provision. The provisions of the Personal Data Act regarding personal data processing in chapters I to V and VII to IX shall be complied with even if no licence is required.

Amended by the Regulations of 23 December 2003 No. 1798 (in force from 1 January 2004, formerly section 7-20), cf. Regulation of 24 April 2008 no. 396.

### ***Section 7-23. Client records***

Processing of personal data in connection with activities that are regulated by the Act of 13 August 1915 no. 5 relating to the Courts of Justice (Courts of Justice Act) Chapter 11 on Legal Aid Work and Lawyers, Act of 15 January 1999 no. 2 relating to Audit and Auditors (Auditors Act), Act of 29 June 2007 no. 73 relating to Estate Agency (Estate Agency Act), and Act of 29 June 2007 no. 75 relating to Securities Trading (Securities Trading Act) are exempted from the obligation to obtain a licence under the Personal Data Act section 33 first paragraph.

The exemption from the licensing obligation shall only apply for processing within the bounds of the legislation mentioned in the first paragraph.

Amended by Regulation of 23 December 2003 no. 1798 (in force 1 January 2004, former section 7-21), cf. Regulation of 24 April 2008 no. 396 (ratification).

### ***Section 7-24. Records of money laundering and processing of associated personal data***

The processing of personal data by an institution that has a reporting obligation in connection with a statutory investigation and reporting duty under the Act of 20 June 2003 no. 41 relating to Measures to Combat the Laundering of Proceeds of Crime etc (Money Laundering Act), cf. Regulation of 10 December 2003 no. 1487 relating to Measures to Combat the Laundering of Proceeds of Crime etc (Money Laundering Regulation), are exempted from the obligation to obtain a licence under the Personal Data Act section 33 first paragraph. The exemption only applies to information obtained through the institution's investigations under the Money Laundering Act.

The exemption from the licensing obligation shall only apply if

- a) processing is exclusively of data obtained from the institution's investigations under the Money Laundering Act, and
- b) the personal data is processed for the purposes that follow from the Money Laundering Act and associated Regulation.

Amended by Regulation of 23 December 2003 no. 1798 (in force 1 January 2004, former section 7-22), cf. Regulation of 24 April 2008 no. 396 (ratification).

***Section 7-25. Processing of patient records by healthcare personnel and social workers not subject to public authorisation or holding a licence.***

The processing of patient/client data by health or social welfare professionals who are not subject to official authorisation shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Personal Data Act.

Exemption from the licensing obligation shall only apply if the personal data are processed in connection with:

- a) treatment and follow-up of individual patients, or
- b) preparation of statistics.

Amended by the Regulations of 23 December 2003 No. 1798 (in force from 1 January 2004, formerly section 7-23), 24 April 2008 no. 396 (ratification).

***Section 7-26. Processing of patient records by healthcare personnel subject to public authorisation or holding a licence***

The processing of patient/client data by officially authorized health professionals and health professionals who have been granted a licence, cf. sections 48 and 49 of the Act of 2 July 1999 No. 64 on health care personnel shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Personal Data Act.

Exemption from the licensing obligation shall only apply if the personal data are processed in connection with:

- a) treatment and follow-up of individual patients,
- b) work as an appointed expert, or
- c) preparation of statistics.

Amended by the Regulations of 23 December 2003 No. 1798 (in force from 1 January 2004, formerly section 7-24), 24 April 2008 no. 396 (ratification).

***Section 7-27. Research projects***

Personal data processing in connection with a research project shall be exempt from the obligation to obtain a licence pursuant to section 33, first paragraph, of the Personal Data Act. Exemption from the licensing obligation shall only apply if all the conditions set out in points a)-e) are satisfied:

- a) first-time contact is established on the basis of publicly available information or through a person who is professionally responsible at the enterprise where the respondent is registered, or the respondent personally contacts the project manager or the latter's representative,
- b) the respondent has consented to all parts of the study. If the respondent is a minor or a person adjudicated incompetent, another person with authority to give consent on behalf of the respondent may give such consent,
- c) the project shall be terminated at a time that is established prior to commencement of the project,

- d) the material collected is anonymised or erased upon completion of the project, and
- e) the project does not make use of the electronic alignment of personal data filing systems.

Amended by the Regulations of 23 December 2003 No. 1798 (in force from 1 January 2004, formerly section 7-25), 24 April 2008 no. 396 (ratification).

## **Chapter 8. Video surveillance**

### ***Section 8-1. Scope***

This chapter applies to video surveillance, cf. section 36 of the Personal Data Act.

### ***Section 8-2. Securing of image recordings***

Image recordings shall be secured pursuant to section 13 of the Personal Data Act regarding data security and the provisions of chapter 2 of these Regulations.

### ***Section 8-3. Police use of image recordings***

Section 11, first paragraph, letter c), of the Personal Data Act shall not preclude police use of image recordings in its possession, in connection with the prevention of criminal acts, in connection with the investigation of accidents or in cases concerning a search for missing persons.

### ***Section 8-4. Erasure of image recordings***

Image recordings shall be erased when there is no longer any objective ground for storing them, cf. section 28 of the Personal Data Act.

Image recordings shall be erased not later than seven days after the recordings are made. However, the obligation of erasure pursuant to the preceding sentence shall not apply if the image recording is likely to be turned over to the police in connection with the investigation of criminal acts or accidents. In such cases, image recordings may be stored for a period not exceeding 30 days.

Image recordings made on postal or bank premises shall be erased not later than three months after the recordings were made.

The obligation of erasure pursuant to the second and third paragraphs shall not apply

- a) to image recordings that are in the possession of the police,
- b) to image recordings that may be of significance for the security of the realm or its allies, its relationship with foreign powers and other vital national security interests, or
- c) where the subject of the image recording consents to the image recordings being stored for a longer period of time.

If the obligation of erasure pursuant to the first paragraph arises for image recordings that have been turned over to the police by other persons, the police may return the recording

to the said persons, who shall erase it as soon as possible if the time limit pursuant to the second and third paragraphs has expired.

If there is a special need to store a recording for a longer period of time than that laid down in the second and third paragraphs, the Data Inspectorate may grant an exemption from these provisions.

### ***Section 8-5. Right of access***

As regards image recordings to which section 37, second paragraph, of the Personal Data Act applies, the provisions regarding right of access pursuant to section 18 of the Personal Data shall apply. In other cases, the subject of the image recording may demand access to the parts of the image recordings in which the subject appears, if the image recordings are stored for a period exceeding seven days.

Right of access pursuant to the first paragraph, second sentence, shall not apply to image recordings that are in the possession of the police, or image recordings that may be of significance for the security of the realm or its allies, other vital national security interests and the relationship to foreign powers.

## **Chapter 9. Examination of e-mail box etc.**

The chapter is amended by the Regulations of 29 January 2009 No 84 (in force from 1 March 2009).

### **Section 9-1. Substantive scope of the Act etc.**

This chapter concerns the employer's right to examine an employee's email box etc.

The term employee's email box means an email box that the employer has placed at the disposal of the employee for use at work in the business. The rules apply in the same way for the employer's right to explore and examine the employee's personal space in the business' computer network and in other electronic communications media and electronic systems that the employer has placed at the disposal of the employee for use at work in the business. The provisions shall also apply to the employer's examination of information that the employee has deleted from the aforementioned spaces, but which is stored as back-up copies or similar that the employer can access.

These rules shall apply equally to present and former employees as well as other persons who perform or have performed work for the employer.

These rules shall apply equally where data processing is entrusted to a Data Processor.

These rules shall apply insofar as they are appropriate for the examination by a university or university college of the email boxes of students, and for the examination by organisations and associations of the email boxes of volunteer workers and trusted officials.

### ***§ 9-2. Criteria for examination***

An employer may only explore, open or read email in an employee's email box

- a) when necessary to maintain daily operations or other justified interest of the business,
- b) in case of justified suspicion that the employee's use of email constitutes a serious breach of the duties that follow from the employment, or may constitute grounds for termination or dismissal.

An employer is not entitled to monitor employees' use of electronic systems, such as the Internet, beyond what follows from this Regulation, section 7-11.

### ***§ 9-3. Procedures for examination***

The employee shall be notified wherever possible and given an opportunity to speak before the employer makes the examination under this Chapter. In the notice the employer shall explain why the criteria in section 9-2 are believed to be met and advise on the employee's rights under this provision. The employee shall wherever possible have the opportunity to be present during the examination, and shall have the right to the assistance of an elected delegate or other representative.

If the examination is made with no prior warning, the employee shall receive subsequent written notification of the examination as soon as it is done. This notification must – besides the information mentioned in the first paragraph, second sentence – contain details of the method of examination, the emails or other documents that were opened, and the result of the examination, cf. section 2-16.

The exemptions from the right to information in the Personal Data Act, section 23 will apply in the same way. The exemptions also cover the subsequent notification under the second paragraph.

The examination shall be conducted in such a manner that the data are left unchanged if possible so that information obtained can be verified.

If examination of an email box reveals no documentation that the employer is entitled to examine under section 9-2 letters a and b, the email box and the documents it contains must be closed forthwith. Any copies must be deleted.

### ***Section 9-4. Deletion etc on termination of employment***

When the employment ends the employee's email box and similar are to be discontinued and contents not necessary for day-to-day operation of the business should be deleted without undue delay. The Personal Data Act, section 28 will apply in the same way.

### ***Section 9-5. Prohibition of non-compliance with this chapter***

The issuance of instructions or making of agreements – concerning the employer's right to examine employee emails or similar – that fail to comply with the provisions in this chapter to the detriment of the employee is prohibited.

These amendments enter into force with effect from 1 March 2009.

## **Chapter 10. Miscellaneous provisions**

Amended by the Regulations of 29 January 2009 No 84 (in force from 1 March 2009, former chapter 9).

### ***Section 10-1. The Privacy Appeals Board***

The Privacy Appeals Board shall deal with appeals against the decisions of the Data Inspectorate as mentioned in section 42, fourth paragraph, of the Personal Data Act and

appeals against the individual decisions of the Data Inspectorate pursuant to these Regulations.

The King will appoint personal deputies for the five members of the Board who are appointed by the King pursuant to section 43, second paragraph, of the Personal Data Act. The deputy members shall be appointed for the same term as the members.

The Privacy Appeals Board shall have a secretariat that shall facilitate the work of the Privacy Appeals Board and otherwise prepare matters for consideration by the Board.

The Privacy Appeals Board shall reach decisions by a simple majority vote. The decisions shall state whether they were reached unanimously. In the event of dissent, grounds for the minority view shall also be stated. To the extent that the decisions are not exempt from public disclosure, they shall be compiled in a record book that is open to the public.

### ***Section 10-2. Communications that contain a personal identity number***

Postal communications that contain a personal identity number shall be designed in such a way that the number is not accessible to persons other than the addressee. The same shall apply to communications that are transmitted by means of telecommunications.

### ***Section 10-3. Penalties***

Anyone who wilfully or through gross negligence omits to comply with the provisions of chapters 2 through 7 and sections 8-2, 8-3, 8-4, second to sixth paragraph, or section 8-5 of these Regulations shall be liable to fines or imprisonment for a term not exceeding one year or both.

An accomplice shall be liable to similar penalties.

## **Chapter 11. Concluding provisions**

Amended by the Regulations of 29 January 2009 No 84 (in force from 1 March 2009, former chapter 10).

### ***Section 11-1. Commencement***

These Regulations shall enter into force on 1 January 2001.

From the same date the following shall be appealed:

- a) the Regulations of 21 December 1979 No. 7 relating to personal data filing systems, etc. and to the delegation of authority
- b) the Regulations of 21 December 1979 No. 22 pursuant to the Act relating to personal data filing systems, etc.
- c) The Delegation of Authority of 30 September 1988 No. 758 pursuant to the Personal Data Filing Systems Act
- d) the Regulations of 12 December 1988 No. 1010 on annual tax for enterprises that are subject to an obligation to obtain a licence pursuant to the Personal Data Filing Systems Act
- e) the Regulations of 1 July 1994 No. 536 on the use of image recordings made in connection with video surveillance

- f) the Regulations of 23 March 1995 No. 267 on exemption from the obligation of financial institutions, etc. to obtain a licence for personal data filing systems in cases concerning money laundering
- g) the Delegation of Authority of 22 May 1995 No. 486 to the Data Inspectorate.

Amended by Regulation of 29 January 2009 no. 84 (in force 1 March 2009, former section 10-1).

## Remarks

### *Remarks on section 7-27*

The starting point for this provision is that no licensing obligation is established, rather a notification obligation. The former section 7-27 established criteria for how the initial contact should be established, consent, time of project conclusion, anonymisation or deletion at the end of the project, and a ban on electronic alignment of personal data records. The privacy protection elements that these criteria protected are also protected in the present legislation. How initial contact is established is largely a research ethics issue, albeit such that certain procedures are less problematic in a privacy perspective than others. The Data Inspectorate is confident that the Research Ethics Committee (REK) and Data Protection Officers look after this aspect. That consent is the clear general rule for processing of personal data follows directly from the PDA, section 8 and 9. In so far as the Data Protection Officers can accept exceptions from the general rule, it is expected that the researcher justifies his need for this in a satisfactory manner. The justification will be a key element in the Data Inspectorate's subsequent review. Additionally there is the assumption that for a consent to be valid, information must be given about how long the personal data will be stored, cf. section 2 no. 7. This requirement follows also from the information obligation under section 19 and following. Anonymisation or deletion should normally take place at project end. When it comes to electronic alignment this is not intrinsically problematic from a privacy perspective. The numbers included, the variables, and whether the material is anonymised (disidentified) immediately after the comparison is made, are all more important.

The condition is made that for an exemption to apply the project must be recommended by a Data Protection Officer. There is the further condition for the project that it is recommended by a Regional Committee on Medical Research Ethics (Research Ethics Committee, REK), if the project includes medical and healthcare research. This change thus represents a restriction in the licensing duty, but an expanded notification duty for researchers at institutions associated with a Data Protection Officer. For institutions not associated with a Data Protection Officer, however, it means an expansion of the licensing obligation.

For projects that are not deemed to be medical or healthcare research it is sufficient to have the advice of the Data Protection Officer. Since there is presently only a requirement for referral [to a higher authority] in medical and healthcare research, this assumes special care by researchers in other areas of society. At the same time it demands that the Data Protection Officer is familiar with research ethics and will, on his/her own initiative, refer projects which are deemed ethically dubious to a committee. The Data Protection Officers should also refer cases for which recommendation seems problematic to the Data Inspectorate, or advise the Data Inspectorate to undertake a prequalification process.

In the second paragraph of the provision a distinction is drawn with research projects of large scale and long duration, and research into such large data sets that are not pseudonymised or disidentified in some other secure manner. This also covers the establishment of large collections (records) of personal data, intended as the basis for other individual projects. The scope here must be related both to the number of people involved as research subjects and the amount of information recorded for each individual. The exemption from the licensing obligation will not apply to registers of this kind.

When it comes to the point that the exemption does not include research projects of large scale it is assumed that projects covering 5000 research subjects qualify as large scale. The

reason for the figure 5000 is that by far the majority of projects embrace a much lower number of participants, at the same time as the large population health studies are always subject to prequalification. Given the requirement for duration, this number seems reasonable from a privacy point of view.

As for duration, it is assumed that a typical doctoral thesis will last 3-6 years, and that projects lasting longer than that can be termed “permanent”. Even so, the assumption here is that only projects with a duration of more than 15 years are considered permanent. This time scale implies that if a project which was not initially expected to last more than 15 years in fact exceeds this duration, then the requirement for prequalification (a licence) will arise.

Research into large data sets is nonetheless exempted from the licensing obligation if the material held by the researcher is pseudonymised or disidentified in some other secure manner. The requirement for pseudonymisation or disidentification in some other secure manner means that the researcher, or the institution for which the researcher works, cannot save the connection key. Also implicit in this is that the number and type of parameters cannot be by nature such that it is possible to retro-identify the set members.

The large population studies performed by the Norwegian Institute of Public Health (FHI), the JANUS data bank and the so-called twins register/ heredity register at the University of Oslo are typical examples of registers that are not exempt from the licensing duty. These are extensive registers, both in terms of duration, number of data subjects (respondents), and volume of information recorded. It is not a deciding factor for whether a study is subject to a licensing requirement that it deals with biological material. Public health surveys which also collect biological material are unlikely to be covered by the exemption. However, this will be on the basis that the studies are by their nature permanent and form the basis for individual projects and studies.

Processing of information in individual projects based on a licensed register must be considered on the merits of the project under the licensing terms and this provision. The licensing duty will not be maintained on a general basis for access to data in the large licensed registers set up in response to regulation.

In distinguishing projects exempted from the licensing duty and other projects, it is the individual researcher who, jointly with the Data Protection Officer, can best assess the concerns that speak for prequalification of the individual project. This may be because of the numbers of people involved, the sensitivity of the information, or the duration of the project. Projects are often different by nature, at the same time as it is not solely the quantitative factors that will decide the matter, but the scope of the personal data to be collected and analysed.

In the second paragraph it is also pointed out that the exemption does not cover so-called “absentee analyses” unless these are based on consent. Absentee analyses means analyses of the distribution of education, income and benefits and so on, among people attending and people not attending, to calculate the importance of the non-attendance. In a privacy perspective, non-consensual absentee analyses do not have a special place, and must therefore be subject to prequalification by the Data Inspectorate. The reason that such analyses offer peculiar privacy issues is that persons who have chosen to avoid a study are still included. The Data Inspectorate understands that in some contexts there may be a need to assess the composition of the selected group, but when these analyses assume that relatively many details will be collected about people who have refused to take part, and who presumably

expect the researcher to respect their position, there arises a need for special assessment if we are to include acceptance of such non-respondents against their will.

The processing of health data in connection with medical research is often a matter that comes under the remit of the Health Registers Act (Personal Health Data Filing System Act). The provisions in the Personal Data Act and Personal Data Regulation regarding notification duty, however, will also apply to projects under the remit of the Health Registers Act. It follows from the Health Registers Act, section 5, that health data may only be processed electronically when permitted under the PDA, section 9 and section 33, or where it follows from the Act, and processing is not prohibited on some other legal ground. The PDA, section 33 concerns the licensing obligation. It further follows from the Health Registers Act, section 36 that, in so far as no other rule follows from that Act, the Personal Data Act and Personal Data Regulation will provide further rules.

The amendment does not affect the licensing or notification duty for studies that have already commenced. The amendment should however be invoked if the nature of the study changes in a manner making it necessary to submit a change notice or apply for a change in the licence.

0 Added by Regulation of 6 May 2005 no. 408 (in force 1 July 2005), cf. Regulation 24 April 2008 no. 396.

## **Remarks on Personal Data Regulation Chapter 9:**

### **In respect of section 9-1**

The scope of the provisions is examination of an employee's email box etc. The term etcetera refers to section 9-1, second paragraph, where a further list of electronic media and documents covered by the employer's examination right is provided.

The employer is the instance that, under the Personal Data Regulation, will be held to be the Data Controller (*behandlingsansvarlig*) under the Personal Data Act. Often this will be a legal person. In practice therefore, in the same way that the employer's duties may be devolved on the person who has the day-to-day responsibility for running the business, the Data Controller's duties may be devolved on the person who has the day-to-day responsibility for running the business. This however will not prevent the business being organised as seems most appropriate, and for decisions about examination (access to data) being reached by other persons than the general manager in charge of day-to-day operations. In all cases it will be the general manager and board of directors who have ultimate responsibility for compliance with the Regulation in the business. It may happen that the employer prefers to engage an external party to investigate the business. If an investigation committee is set up to investigate parts of the business, then this committee will not have other rights of examination of employee emails than are held by the employer. The employer must, in the event, confer powers to the committee to make examinations of employee emails based on the considered presumption that a legal basis for such examination exists under section 9-2. The committee in such cases will be deemed the Data Processor (*datahandler*) on behalf of the employer, and a contract setting out rights and duties will need to be drawn up in accordance with the PDA, section 15. When the rules become effective for the rights of universities and colleges to examine students' email boxes, the institution in question will be deemed the employer, and the student in question will be deemed the employee.

This provision will apply to the employer's examination of the employee's email box and specific documents within it, and of other electronically stored documents and

communications media made available to the employee for use at work. The provisions will therefore cover examination of text messages stored in a mobile phone placed at the disposal of the employee by the employer, examination of the employee's personal space in the data network of the business, and examination of other hand-held devices besides mobile phones provided they belong to the employer, but have been placed at the employee's personal disposal for execution of the work. The provisions will not, by contrast, apply to the employer's examination of documents stored in spaces or on systems which must be deemed shared by employees of the business. In these spaces all persons with access (log-in) rights will be allowed to read all documents stored there.

The second paragraph, final sentence is a reiteration that the provision applies not simply to the electronic aids and storage media that the employer has placed at the disposal of the employee, but also to examination of possible copies that the employer has made, typically on back-up tape.

One condition that applies is that the systems are intended for use at work. If the systems are placed at the employee's disposal for private use, then the rules governing the employer's right of examination will not apply. Such will be the case, for instance, if the employer offers the employee the loan of a mobile phone handset without there being an assumption that the phone must be used at work. In such cases the rules governing examination of the email box will not apply.

Nor does the examination right apply to systems that the employee personally owns. This means that the employer is not entitled to examine documents stored in the employee's private systems, even when the system is sometimes used for work-related activities. The reliance on an external Data Processor to operate the computer systems does not release the employer from his Data Controller responsibilities under the Personal Data Act. It therefore makes no difference to the employer's examination right or the employee's protection from such examination whether the employer operates the server or other systems where the information is stored, or whether such operation is entrusted to a Data Processor. The crucial thing is that the information is subject to the employer's Data Controller responsibility.

It is further intended that the rules will provide protection also to students at the country's universities and colleges, and to volunteer workers and trusted officials in organisations and associations to the extent appropriate for such groups.

### **In respect of section 9-2**

This provision contains alternative grounds for the employer's examination of employee emails. The basic requirement is that examination must be necessary for a specific purpose. This follows directly from the Personal Data Act, incidentally, and is reiterated specifically in this provision. An assessment must be made whether the examination is necessary for the operation of the business. In making this necessity assessment the employer's need for examination in order to protect his interests must be weighed against the employee's need for privacy and protection of his correspondence.

The necessity test in **letter a** demands a specific evaluation in each case of whether there is a qualified need to open the email box in order to protect the justified interest that the employer feels he has. This regard for the proper and rational commercial running of the business and so forth will in and of itself constitute a justified interest of the employer, but if examination

is not needed in order to protect such interest in the specific case facing the employer, then examination may not take place. If protection of business operations can be achieved by other and less intrusive means, then examination of the email box will not be necessary, and thus also by corollary not permitted by the Regulation.

No special rules are set forth to regulate examination in the absence of the employee or regarding the time factor in such a case. Absence and length of absence will be an element in the overall assessment of whether the examination is necessary. Such an arrangement means greater flexibility than fixed time limits. It is always necessary to make an overall necessity assessment. One element in a necessity assessment, to give an example, would be if the employee has provided for forwarding of business-related emails, or selected an automatic response stating where business-related emails should be sent in the employee's absence. Such automatic forwarding or message service may reduce the employer's need to examine the emails. It may nonetheless happen that examination is deemed necessary even when the employee has just popped out for lunch, for example. A case in point might be where the employer has reason to believe that an offer with a tight deadline is pending in the employee's emails which demands action before the employee returns.

The necessity assessment in letter a is linked to protection of the day-to-day operation and other justified interests of the business. This harmonises well with the wording of the PDA, section 8, which sets out the basic criteria for processing of personal data. The assessment required to be made under the PDR, section 9-2, now lies close to the assessment that the Data Controller is required to make under the PDA, section 8, letter f. Accordingly, "justified interests" must be held up as the legal standard. The yardstick must therefore be what one in general considers to be the legitimate concerns of a business. A further standardisation of such interests is something that should be developed in practice.

Under **letter b** the employer may examine emails where a justified suspicion exists that use of the email account may give grounds for termination or dismissal. This may embrace use of the electronic communications systems for actions that may be, but are not necessarily, a criminal offence, of which are clearly not in the interests of the business or employer. Examples could be use of the computer system for the promulgation of spam or emails with other malicious content. It is important to have in mind, however, that receipt of emails with disloyal content is not grounds for examination, because it is something that lies outside the employer's control.

This alternative b may also give rise to examination in cases where there is a suspicion that the employer's systems are being used to harass colleagues, or for criminal offences that may impact the employer, such as use of the employer's systems to download illegal material, like child pornography, or illegal file-sharing. The action must be so serious, however, as to give grounds to terminate the employment.

The requirement for a justified suspicion that circumstances may exist that could bring about the termination or dismissal of an employee also means that the employer must have more than a vague supposition. The employer must have specific information that gives grounds to suppose that the email box may contain information about such circumstances as are mentioned in the Regulation. This might be tip-offs from colleagues, or information obtained from general administration of the business' IT systems, see PDR, section 7-11.

When applying the rules at a university or college a great deal is required initially for examination of student emails to be deemed necessary to protect the day-to-day operation of the institution. On the other hand, the need for insight may be greater in some situations, such as the need to investigate possible cheating at examination time. The criteria for email examination will also be met if there is a justified suspicion that student use of emails represents a gross breach of the obligations that follow from the relationship between institution and student, or may provide a basis for exclusion or expulsion, cf. Universities Act, section 4-8.

It is emphasised moreover that the provisions about examination of emails do not limit the employee's duty on his own initiative to inform the employer of emails with a work-related content. This applies in both private and public business and may for instance be significant in relation to an employer's obligations under the Archives Act and Bookkeeping Act. Thus the employee is bound to ensure that the employer has access to archivable materials. In this connection the employee may, especially in connection with absence, wish to give the employer access to his email box. The employee may in such instances give the employer access to his email box without being asked. An example of how this may be done is for the employee to phone the employer to state that a document from a given sender is waiting in his inbox, and give the employer permission to forward the document for processing.

In section 9-2 it is also emphasised that the Regulation does not constitute a legal basis for continuous monitoring of the employee's use of electronic means of communication. The provisions in the Regulation only apply to examination in isolated cases for specific purposes. A historical log of the computer system would constitute a form of monitoring or surveillance of the employee's use of the system. The reference to the Regulation, section 7-11 concerning insight and use of a computer system log is therefore meant to clarify that, while monitoring is permitted in certain cases, it is only permitted for the clearly defined purposes stated in the Regulation (administration of and/or detection and resolution of security breaches in the computer systems).

The provision gives the employer the right to examine an employee's email box in certain cases. On the other hand, this right of insight cannot set aside the employee's statutory duty of confidentiality. This is of special relevance to research staff, who, since they may have a statutory duty to maintain secrecy, cannot necessarily give the employer all information that they possess. Also correspondence between the employee and an elected delegate or safety delegate may be confidential, and thus not open to the employer's right of examination.

### **In respect of section 9-3**

The employee shall be notified wherever possible that examination will take place, and be given the opportunity to speak. The phrase "wherever possible" indicates that notification is not an absolute requirement, but should be sought. The provision should be understood such that notification can be omitted if, under section 9-2, immediate examination is warranted, for instance where this is necessary to sustain day-to-day operation of the business. The time element will thus be a key evaluation factor when deciding if notification of the employee is possible. Where the employer has time to contact the employee and give notice of the examination, such notice must be given. The employer must be able to justify the reason that notice was not given if notice is omitted.

An employer may fear that the employee can tamper with or destroy evidence if notification of the examination is given. To assist in such situations, the employer may make a mirror

image of the areas in the electronic network that he has a legal basis for examining, so as to secure a correct instantaneous image of the material that can be reconstituted if it is suspected that alterations have been made. Such mirror image will give both the employer and the employee confidence that it is possible to detect any alteration of the information, whether made by the employee after being informed of the upcoming examination, or of changes made by the very process of examination. Both the police and public supervisory agencies make use of mirror images in their investigations. Nor is it unnatural for an employer to make a mirror image in a case that he considers offers a legal basis for performing an examination of the employee's emails or similar. The examination of the mirror image is naturally subject to the same rules as for examination of emails.

It follows from the provision that the exemptions from the right to see information listed in the PDA, section 23, will apply here. This means, among other things, that if there is suspicion of a criminal offence, it may be possible to omit notification, as authorised in the PDA, section 23, first paragraph, letter b. This provision covers by its wording and legal preamble investigations by the Department of Public Prosecution, and investigations and enquires made by a public supervisory agency (like the Tax Authorities). The provision thus does not initially apply to the employer's own investigation. Whether the criteria for omitting notification are met will depend on a specific assessment of the circumstances. The opportunity to make a mirror image to secure evidence will be one element in this assessment. Where, under the PDA, section 23, there is a legal basis for the omission of notification, then also the duty to notify in retrospect under section 9-3, second paragraph, will not apply. The employer shall wherever possible be given the opportunity to be present during the supervisory inspection and shall have the right to be assisted by a representative. Despite the above, situations may be imagined where the employee does not want elected delegates or others to see the content of an email box. Therefore it is not an absolute requirement that the employee shall have representation against his will. The employee may therefore actively oppose representation while the employer makes the examination. But a situation where the employee is left to take the initiative to be present in person or be represented must not occur. This follows from the wording "be given the opportunity" to be represented. At a university or college the board of directors will propose or nominate persons who can assist the student as a person of trust in cases concerning examination of an email box, although the student may opt for a different representative.

The information that the employer learns from the examination may only be used in accordance with the PDA, sections 8, 9 and 11. Among other things this limits the use of information to fulfilling the specific purpose that justified the examination. Other usage must be authorised by the PDA, section 11. Especially relevant in this assessment is the PDA, section 11-c, stipulating that, without the consent of the data subject, future use of the information must not be incompatible with the original purpose. It must be assumed that if the examination is performed in pursuance of section 9-2 letter a or b, then it will take a great deal before other use of the information, besides the use that follows from the examination basis, will be compatible with the original purpose. It is further assumed that the boundaries that sections 8, 9 and 11 set up for use of the information obtained from the examination of the employee's email box will sufficiently preclude the employer's further use of the information, since there will be no legal basis for such further use. Accordingly, it is not considered necessary to stipulate further provisions about confidentiality, or rules for use of the information obtained by examination.

#### **In respect of section 9-4**

An employment may end in many ways: the employee may give notice, or may be given notice. Other less common situations may arise due to the death of the employee, the employee may go missing or become comatose, or may leave the workplace for an indefinite period, and these cases will also be covered by this provision.

The next of kin following a death are not necessarily entitled to see the deceased's emails etc. The same goes for his decedent estate. A specific evaluation must be made under sections 8, 9 and 11. The interests of any third persons will weigh heavy.

The general rule under this Regulation is that the contents of the email box, and the contents of other electronic communications media that the employee had at his disposal, or documents stored in electronic form in the employee's personal space in the business network, are to be erased upon termination of the employment, provided the running of the business does not require continued storage of the information. The most practical solution is for the employee to delete emails and other documents with a private content, and give the employer access to all documents with a work-related content. It is not always the case that employment ends in a manner that enables the employee to review and sort through his electronic communications and documents. Indeed, it is not infrequently the case that the email box contains archivable material when employment ends. The employer in such cases should, within a reasonable time period, arrange for an assessment of whether there are grounds for further action or whether the documents should be deleted under the PDA, section 28. Just what constitutes a reasonable time period needs to be assessed specifically, but the expectation must be that the employer makes an assessment within a six-month period after the employment ends. In such cases a specific search should be performed for work-related documents to assure continued storage of those documents that are of significance for the operation of the business, with a view to deleting the others.

Even if the email box is deleted, it is not necessarily the case that the information on back-up copies and similar will disappear. It is appropriate that the employer, for some time after the end of an employment relationship, can process information about the former employee. Examination of such information in back-up copies and similar can, however, only take place subject to the conditions in section 9-2 being fulfilled. A typical case will be where the employer needs to examine the material to search out contracts and other documents necessary for the day-to-day running of the business. Personal data on back-up copies should also be deleted after a certain time period, as there will no longer exist a justified need for them. Most businesses have routines for regular deletion or over-writing of back-up copies, for instance about every six months. Such routines will also ensure that documentation on back-up copies gets erased within a reasonable time. Where the employer lacks routines for deletion of back-up copies he must implement special measures to protect the privacy of employees who have left.

A contract for closure of the email box when the employment ends should be signed at a time when the employee is not under pressure to allow examination by the employer. At the time of appointment the employee may feel bound to sign a contract that allows examination by the employer, because it appears to be a condition of employment. The employee will likely feel less pressure upon termination of the employment, and this may therefore be a better occasion on which to sign such a contract.

### **In respect of section 9-5**

The purpose of the Regulation is to clarify the employer's right to conduct examinations in certain cases, and to protect the employee against unreasonable controls by the employer. In light of this the parties may not by agreement or instruction stipulate conditions for the employer's right to examine the employee's emails that offer weaker employee protection than the Regulation. The parties are however free to make agreements to amplify and define the provisions in the Regulation to offer better employee protection than the Regulation. The provisions concerning the employer's right to examine the employee's email box etc are formulated in rather general and discretionary terms. As a result, there are no criminal sanctions associated with breach of the rules. On the other hand, the general rules in the Personal Data Act about reactions in the case of breaches of rules that are issued under, or in pursuance of, the Personal Data Act, will apply, including the Data Inspectorate's opportunity to impose Data Offence Fines and coercive fines.