Regulations on control measures for employees covered by the Act relating to employment protection, etc. for employees on board ships (Ship Labour Act)

Legal basis: Laid down by the Norwegian Maritime Authority on 25 January 2019 under the Act of 21 June 2013 No. 102 relating to employment protection, etc. for employees on board ships (Ship Labour Act) section 9-1 fourth paragraph, cf. Formal Delegation of 3 July 2013 No. 974.

Chapter 1. General provisions

Section 1. *Scope of application*

These Regulations shall apply to the right to implement control measures for employees working on board Norwegian ships and mobile offshore units.

Section 2. *Supervision*

The Norwegian Data Protection Authority shall supervise compliance with the provisions of these Regulations.

Chapter 2. Camera surveillance

Section 3. *Conditions for camera surveillance*

Camera surveillance is allowed only if the company regards it necessary in order to prevent any dangerous situations and to ensure the safety of employees and others, or if there is a specific need for surveillance.

Camera surveillance means continuous or regularly repeated monitoring of persons by means of a remote-controlled or automatically operated surveillance camera or similar device which is permanently fixed. Camera surveillance means monitoring with and without the possibility of video and audio recording. The same applies to dummy security cameras, signs, boards, etc. that give the impression of camera surveillance.

Section 4. *Notification of camera surveillance*

If camera surveillance is used in accordance with these Regulations, the company shall, as responsible party, use signs or other means to communicate that the facilities are being monitored and whether the surveillance includes audio recordings.

Section 5. *Release of camera surveillance data*

Camera surveillance data in accordance with these Regulations may only be released to other parties than the company if:

a) the data subject has given his/her consent;
b) the release to the police is connected to the investigation of a criminal offence or accident and the statutory duty of secrecy does not interfere with the release; or
c) the release is required by law.

Section 6. *Erasure of camera surveillance data*

Camera surveillance data shall be erased not later than seven days after the recording was made. If the surveillance data is likely to be released to the police in connection with an investigation of a criminal offence or accident, the surveillance data may be stored for a period not exceeding 30 days.

Recordings made at business premises where payment instruments or IDs are used or at premises offering postal or bank services shall be erased not later than three months after the recordings were made.

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

a) to surveillance data 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

b) when the data subject consents to the surveillance data being stored for a longer period of time.

If there is a particular need to store surveillance data for a longer period of time than what is specified in the first and second paragraphs, the Norwegian Data Protection Authority may grant an exemption from these provisions.

Section 7. ***Validity of previously granted exemptions***

Exemptions granted by the Norwegian Data Protection Authority in accordance with section 8-4 sixth paragraph of the Regulations of 15 December 2000 No. 1265 on the processing of personal data (Personal Data Regulations) on storage of camera surveillance data are valid in accordance with these Regulations.

Chapter 3. The employer’s access to e-mails and other electronically stored information

Section 8. ***Scope of this chapter***

This chapter applies to the employer’s right to access information stored on:

a) an e-mail account provided by the employer for use at work;

b) an employee's personal storage area on computer networks or other electronic devices provided for the employee for use at work.

The provisions apply accordingly to the right of access to information which has been deleted from sites mentioned in the first paragraph, but still exists in backup systems, etc.

This chapter applies to current and former employees.

Section 9. ***Invariability of the provisions***

Laying down instructions or entering into agreements that depart from the provisions of this chapter to the detriment of the employee is not permitted.

Section 10. ***Conditions for access to e-mails, etc.***

The employer is only entitled to access information stored on sites specified in section 8 when:

a) this is necessary to attend to daily tasks or other justified interests of the company; or

b) there is a justified reason to suspect that the employee's use of an e-mail account or electronic devices entails gross breaches of the duties that follow from the employment or that could provide grounds for termination or dismissal.

The employer has no right to monitor the employee’s use of electronic devices, including use of the Internet, unless the purpose of the monitoring is to:

a) manage the company's computer network; or

b) identify or resolve security breaches in the network.

Section 11. ***Access procedures***

The employee shall, as far as practicable, be notified and given the opportunity to make a statement before the employer may access information. The notice shall include a justification of why the conditions of access are considered to be met and information about the employee's rights under this provision.

The employee has the right to object pursuant to Article 21 of the General Data Protection Regulation.

If practicable, the employee shall be given the opportunity to be present when such access takes place. Furthermore, the employee is entitled to be accompanied by a trade union representative or other person of their choice.

If access is made without prior notice or without the employee being present, the employee shall be notified in writing as soon as the data has been accessed. This notification shall include the information referred to in the first paragraph second sentence, as well as information on which method of access was used, which e-mails or other documents were opened and the result of the access process.

The exemptions from the right to information, cf. section 16 of the Personal Data Act, shall apply accordingly.

Access shall take place in such a way that, as far as practicable, the information will not be altered, and the information provided can be verified.

Opened e-mails, documents and such that prove to be unnecessary or irrelevant for the purpose of access shall be closed immediately. Any copies shall be deleted.

Section 12. ***Deletion of information at the end of the employment relationship***

The employee’s e-mail account shall be closed upon termination of the employment, unless there is particular reason for keeping the e-mail account open for a short period of time after the termination.

Information referred to in section 8 first paragraph (a) and (b) which is not necessary for the day-to-day running of the business shall be deleted within a reasonable time after the termination of the employment relationships.

Section 13. ***Entry into force***

These Regulations enter into force immediately.