Rules no. 837/2006 on Electronic Surveillance of Iceland

21 mar. 2007

Art. 1.

Objective and scope

The objective of these rules is to promote a balance between, on the one hand, the right to privacy, and, on the other hand, the interest of data controllers in ensuring security and reasonable monitoring of employees and other persons, subject to electronic surveillance, e.g. by regulating the use of hardware and software in the interest of the relevant activity or operation.

The rules apply to electronic surveillance in the workplace, in schools, and in other areas generally traversed by a limited number of people. The rules apply irrelevant of the type of devices used, such as servers, devices to monitor telephone use, surveillance cameras, webcams, vehicle tracking systems, positioning systems etc. The rules do not apply to devices used to monitor attendance, e.g. time sheets.

Art. 2.

Definitions

For the purpose of these rules, words and terms shall have the following meaning:

1. Electronic surveillance: A constant or regularly repeated surveillance which involves the monitoring of individuals, with the use of remote controlled or automatic equipment. The term applies to:
   a. surveillance which involves personal data processing, or results in, is intened to result in, or can result in such processing; and
   b. surveillance not involving the collection of visual material or other personal data

2. Data controller: The party that determines the purpose of electronic surveillance, and decides upon the devices used, the method of surveillance, and the use of the collected information.

3. Private e-mail: E-mail, sent or received using hardware or software provided by the data controller, e.g. an employer, relating to the private life of an individual, not relating to the interests of the data controller or his activities or operations. Criteria on whether an e-mail can be regarded as private are e.g.:
   a. if the e-mail is identified as private in the subject line or if it can be manifestly concluded as private in other ways
   b. if the e-mail is stored in a separate folder in an e-mail system, either identified as private, or obviously containing private material

4. Internet use: The use of hardware or software, provided by the data controller, to browse the internet, to receive or send e-mail, or for instant messaging.

5. Logging: An operation to ensure traceability of processing operations in information systems (i.e. within log-files).

6. The Monitoring of telephone use: A constant or regular collection of information about the telephone use of an individual, e.g. by registering information about dialled numbers or recording telephone conversations.

7. A Vehicle Tracking System: An electronic equipment which is used or can be used for processing information about drivers of vehicles, including information about their routes and/or their way of driving.

8. An Electronic Positioning System: An electronic equipment which processeses or makes possible the processing of information about the positioning and whereabouts of individuals, such as RFID.

Art. 3

Discreet surveillance

Discreet surveillance is only permissable on the basis of a legal act or a court order.

Art. 4

Purpose

Electronic surveillance must be carried out for specified, explicit and legitimate purposes, such as security or property protection.

Art. 5

Porportionality
Electronic surveillance shall not be excessive in relation to the purposes for which it is conducted. Privacy rights of the individuals subject to surveillance shall be respected and any unnecessary interference with their privacy shall be avoided. When determining whether to conduct electronic surveillance, it should be established that the objectives of the surveillance can not be reached by other, reasonable, and less intrusive means.

Art. 6

The Workplace

Electronic surveillance for the purpose of monitoring workers’ efficiency is subject to the condition of an specific need, e.g. if:

a. employee supervision can not be managed by other means; or

b. safety of the monitored area can not be ensured by other means, e.g. from the point of view and in the light of legislation on hygiene and pollution control;

c. the surveillance is necessary on the basis of provisions of a wage contract or a similar agreement on terms of employment, e.g. when wages are based on performance-based or time-based systems.

Art. 7

Storage, disclosure, erasure,
and other processing of personal data

Personal data collected by electronic surveillance shall only be stored if necessary for the purposes of the surveillance.

Personal data, collected by electronic surveillance, shall be erased when there is no longer a reasonable need to retain them. A reasonable need can be based on provisions of law or the pending processing of data by a controller for the original purposes of the surveillance. Notwithstanding, personal data, collected by electronic surveillance, can not be retained for a longer period of time than 90 days, unless otherwise provided for by law. That does not apply to personal data, collected by logging or stored in backup files. Neither does it apply to data to be used for the purposes of existing legal proceedings.

Personal data, collected by electronic surveillance, can only be used for the purpose of their collection and only if necessary for that purpose. They shall not be further processed or disclosed, unless the data subject gives his consent or when permitted by the Data Protection Authority. Notwithstanding, data on accidents or alleged criminal activities, can be disclosed to the police.

Art. 8

Vehicle Tracking Systems

The use of vehicle tracking systems and electronic positioning systems are only permissible in case of a specific need, e.g. significant security factors, by consent of the data subject, or according to other specific authorisation, e.g. by wage contracts or provisions of law. The use of vehicle tracking systems for the purposes of monitoring the positioning and whereabouts of drivers are subject to the condition of a specific need to reach lawful and reasonable objectives.

Art. 9

E-mail and Internet Use

Private e-mail can not be viewed except when expressly needed, e.g. in the case of a computer virus or for similar technical purposes.

Data on internet browsing, connections to websites, and data volume of an employee or a student can be viewed, if there is a substantiated suspicion that the relevant individual is violating law, or rules by the employer or school authorities. In case of suspicion of criminal activities, the police should be contacted.

When viewing the use of e-mail or internet, the employee or student should be notified beforehand and give the possibility to attend the viewing. That does not apply if the attendance of the individual is not possible, e.g. because of his serious illness. If the individual can not attend the viewing he shall have the possibility of appointing a representative.

At the termination of employment, an employee should be given the possibility to erase or copy e-mail not relating to the employer’s activities. E-mail of students should be erased at the end of their school attendance, provided that they have had adequate time to make personal copies. Information on employees’ or students’ use of the internet shall not be viewed after termination of employment or end of school attendance, unless the conditions of para. (1)-(3) are fulfilled, or otherwise provided by law.

Art. 10

Duty of information
The controller of electronic surveillance shall adopt rules and/or provide the individuals subject to the surveillance with information, by which these rules are not referring to a notification according to Art. 48 of Act no. 81/2003 on Telecommunication. Before the provisions of such rules by the controller are applied, they shall be presented by verifiable means, e.g. at the time of signing an employment agreement.

Rules or information according to para. (1) shall address the purpose of the surveillance, who shall have access to the collected data, and for how long the data will be retained. A wage contract or a binding agreement between the parties, ensuring the data subject further rights prevails over such rules.

Otherwise, where relevant, information should be given on the following:

a. The type of equipment used, e.g. digital cameras, vehicle tracking systems, or sound recording devices.

b. The right to object to the surveillance and the consequences of such an objection.

c. Access rights and the right to correction or erasure.

d. Rules on internet use, e.g. whether it is forbidden to download and/or forward by e-mail illegal and/or pornographic material.

e. The processing of private e-mail and other e-mail.

f. Whether telephone use is monitored, and whether the private use of telephones is restricted.

g. The consequences of violating rules on e.g. the use of telephones or internet.

h. Other information, in so far as such information is necessary with regard to the specific circumstances, to enable the data subject to protect his interests.

The provisions of para. (1)-(3) do not apply when it is clear that the individual, subject to the surveillance, already has knowledge of the items stipulated in the paragraphs.

Art. 11

Obligation to notify

A controller of electronic surveillance shall notify the Data Protection Authority of the surveillance, in accordance with Rules on the Obligation to Notify and Processing which Requires a Permit. The notification shall contain information on how the surveillance is conducted, what information has been supplied about it, and other items specified in Art. 32 of Act no. 77/2000 on the Protection of Privacy as regards the Processing of Personal Data.

Art. 12

Access rights

The subject of electronic surveillance has the right to access collected data relating to him, e.g. by listening to sound recordings, in accordance with Art. 18 of Act no. 77/2000 on the Protection of Privacy as regards the Processing of Personal Data, provided that provisions of Art. 19(2) do not apply. A request for such access can be submitted either orally or in writing.

The controller or, where relevant, the data processor, shall provide the access as promptly as possible and no later than within a month after receiving a request according to para. (1). A disagreement thereof can be resolved by the Data Protection Authority. In such cases the Data Protection Authority can order the controller to retain the data until it has reached a conclusion.

Art. 13

Cessation of Electronic Surveillance

The Data Protection Authority can order the cessation of electronic surveillance, violating the provision of these rules, and the erasure of the data collected by the surveillance equipment.

Art. 14

Legal Basis

These rules, adopted in accordance with Art. 37(5) of Act no. 77/2000 on the Protection of Privacy as regards the Processing of Personal Data, cf. Art. 5 of Act no. 81/2002, shall enter into force immediately.

Upon their entry into force, rules no. 888/2004 on Electronic Surveillance shall be repealed.

The Icelandic Data Protection Authority, 19. September 2006