Guideline

Confirmed on:	Confirmed by:
Co-operation procedure:	Reviewed on:

Rules in Swedish *Att hämta och öppna en arbetstagares e-post*

Approved by Rector November 2013

Retrieving and opening an employee's e-mail

Contents

Retrieving and opening an employee's e-mail 1
Basis 3
Legal stipulations governing the retrieval and opening of e-mail 3
Scope of the right to handle an employee's e-mail 3
What does the retrieval of e-mail messages mean? 3
What does the opening of e-mail messages mean? 3
Technical and functional requirements 3
Grounds of the employer's right to retrieve or open an employee's e-mail 4
With the employee's consent 4
Without the employee's consent 4
Procedure 4
General requirements 4
Before the retrieval/opening 5
Retrieval 5
Opening 6
After the retrieval/opening 6
Form templates for documentation 6
Power of attorney to read e-mail message contents 7
I hereby authorise 7
Report of retrieving messages belonging to the employer 8
Grounds for retrieval (check one or more options): 8
The retrieval was conducted by: 8
The retrieval was witnessed by: 8
COMPLETION INSTRUCTIONS: Report of retrieving messages belonging to the employer 9
People involved in the retrieval: 9
Report of opening a message belonging to the employer 10
Grounds for opening the message (check box): 10
Specification of the opened message: 10
The message was opened by: 10
The opening was witnessed by: 10

COMPLETION INSTRUCTIONS: Report of opening a message belonging to the employer 11
Specification of the opened message: 11
People involved in the opening: 11
Record of retrieving [and opening] an employee's e-mail messages 12
SAMPLE - Record of retrieving and opening an employee's e-mail messages 13

Basis

Legal stipulations governing the retrieval and opening of e-mail

The Finnish Constitution (731/1999, section 10) states that the secrecy of correspondence, telephony and other confidential communications is inviolable. This inviolability of secrecy also concerns e-mail correspondence. The Act on the Protection of Privacy in Electronic Communications (516/2004, Section 4) states that the identification data of messages is confidential. Identification data includes, for example, information about the parties of the e-mail correspondence.

The Act on the Protection of Privacy in Working Life (759/2004, Chapter 6, sections 18-20) grants the employer the right to retrieve and open electronic mail messages sent to or by an employee. This guideline is based on the stipulations outlined in the Act on the Protection of Privacy in Working Life.

Scope of the right to handle an employee's e-mail

The employer is only entitled to retrieve or open e-mail messages sent by or to the employee immediately[1] before the employee's absence or during the absence. Listing message titles outside this time frame is not allowed without the employee's consent.

What does the retrieval of e-mail messages mean?

The retrieval of e-mail messages means listing the message title data. The employee is only entitled to use the following title data:

- Sender
- Recipient
- Title or subject
- Date of sending.

The software typically used for reading e-mail messages can be used for retrieving messages, as well. The list resulting from the retrieval is similar to the list of Inbox messages displayed by regular e-mail applications.

The message contents are not read in conjunction with message retrieval.

The e-mail retrieval is a one-off action with a clear start and end point. It is not a continuous process.

What does the opening of e-mail messages mean?

The opening of e-mail messages means reading the message contents. This can only be done after retrieving the messages.

Technical and functional requirements

The employer must provide the employee, in advance, with at least one of the following options:

- The employee can authorise another employee to handle his/her e-mail in his/her absence.
- An automatic reply can be set to the employee's incoming messages.
- E-mail sent to the employee can be forwarded to another address approved by the employer.
- The message senders can choose to send messages related to the work task/service to the organisation (service) address instead of the employee's personal e-mail.

Specifications to the above clauses:

- The automatic reply function usually also responds to spam, which can increase the flow of advertising and junk mail. Hence, auto replies should be used with caution.

[1] The law does not define the term "immediately". It remains open for interpretation.

- Not all e-mail messages are located in the university's e-mail system. Messages may be saved on the employee's workstation, mobile devices or shared server disks.
- According to the University's e-mail rules, it is forbidden to forward work-related e-mail outside the University, for example, to Gmail or Hotmail accounts.

Grounds of the employer's right to retrieve or open an employee's e-mail

With the employee's consent

As default, the employer is only entitled to retrieve or open its employee's e-mail with the employee's consent.

The consent for retrieving and opening e-mail messages is always the employee's choice; the employee cannot be obligated to giving his/her consent, and the employee can revoke this consent at any time.

If the employer does not have the employee's consent for retrieving or opening e-mail messages, the following procedure shall apply.

Without the employee's consent

The employer is only entitled to retrieve an employee's e-mail message without the employee's consent if there is justified reason to believe that the employee's e-mail contains one or more work-related messages that are crucial for the employer. A further prerequisite is that the employer doesn't have any other system for reviewing messages and their contents.

The employer can retrieve an employee's e-mail message without the employee's consent if the employee has died or is permanently prevented from performing his/her work duties.

If the employee is temporarily prevented from performing his/her work duties, the following conditions must be met in order for the employer to have the right to retrieve his/her e-mail messages:

- There is no other reasonable way to obtain the information or material contained in the e-mail message.
- The employee's consent cannot be obtained within a reasonable time, and the investigation of the matter cannot be delayed.
- The [information security officer] approves of the action and all of its phases are documented.

Example: *An employee is arranging a conference and has negotiated the arrangements with the speakers by e-mail. No one else knows the full list of agreed speakers and their contact information.*

Procedure

Deviations to this procedure can be made under a separate agreement. In the absence of any agreements, the following shall apply.

General requirements

The following general requirements must be met in order for the employer to be entitled to retrieve or open an employee's e-mail messages:

- The retrieval or opening of e-mail messages is based on a certain, specified task or role occupied by the employee.

– The above-specified technical and functional requirements**Error! Reference source not found.** are met.

As the primary option, the employee's supervisor must attempt to obtain the employee's consent. The clearest way to express such content is using a written power of attorney (Appendix 1: Power of attorney to read e-mail message contents). The procedures to be applied can also be agreed in conjunction with preparing the power of attorney. In other cases, the [information security officer] must be contacted before taking any action.

If it is not possible to obtain the employee's consent, the conditions outlined in the section "Without the employee's consent" must be fulfilled. In addition:

– The information on the message sender, recipient or title may not be processed more extensively than is necessary for the purpose of retrieving the message, and the persons processing the information may not disclose it to a third party during the employee's employment relationship or after its termination (Act on the Protection of Privacy in Working Life, Section 19).
– The employee's supervisor is responsible for ensuring that the level of confidentiality of the gained material, as well as the basis thereof, is determined and indicated with a stamp or in another acceptable way.

Before the retrieval/opening

The employee' supervisor ascertains the need to retrieve or open the employee's e-mail messages. If the need is justified, the supervisor confirms the justification by requesting the employee's consent to this, primarily in the form of a written power of attorney.

If such consent cannot be obtained, the employee's supervisor checks whether the employer is entitled to retrieve the employee's e-mail messages without his/her consent as outlined in this document. If the employee chooses not to give his/her consent, or if the above-specified preconditions for retrieving an employee's e-mail messages without consent are not met, this procedure is not applicable.

If the preconditions are met, the employee's supervisor contacts [the information security officer], who makes the necessary arrangements to retrieve and open e-mail messages and to ensure that no new messages can be sent to the employee's inbox. [An automatic reply can be set to the employee's e-mail account.]

The [information security officer] and the employee's supervisor jointly authorise a certain person to retrieve and open the employee's e-mail messages in question. Several persons can be authorised to do this if actions are needed with regard to several separate tasks or roles occupied by the employee.

Retrieval

The employee's e-mail messages from the defined period of time are retrieved from the IT systems with the help of each system's administrator.

The authorised person marks the messages that are to be opened in the retrieved list of messages. Based on the information displayed on the list, a justified connection must be found between each message marked for opening and the task or role that serves as grounds for retrieving and opening the e-mail messages.

A report of e-mail message retrieval is prepared (Appendix 2: Report of retrieving messages belonging to the employer) and the retrieved message list is attached to the report.

The person authorised to access the employee's e-mail messages, the system administrator(s) and [information security officer] or a person assigned by him/her must all be present when retrieving e-mail messages, and they all must sign the message retrieval report.

Opening

The messages that are marked for opening in the list of messages as described above are opened with the help of the system administrator. These messages can be provided for the authorised handler as printouts, in a folder, or on a memory medium.

The opened message must not be deleted from the original mailbox.

A report is written for every opened message (Appendix 3: Report of opening a message belonging to the employer) and signed by everyone present when the opening takes place (see item ”Retrieval” above). If several messages are opened on the basis of the same reason, this procedure can be reported in one joint document including an itemisation of the opened messages.

After the retrieval/opening

A record is prepared about the above-described procedure and the generated reports are attached to it (Appendix 4: Record of retrieving [and opening] an employee's e-mail messages). All persons who were present during the retrieval/opening must sign the record.

The [information security officer] delivers the record and its attachments to the University's registry office for storage. The registry office retains the records according to the information management plan.

The [information security officer] provides the employee in question with a copy of the record. The copy is delivered as a registered letter, and it must be free of charge for the recipient.

The [information security officer], the employee's supervisor and the employee schedule a meeting in which they address the case. The purpose of this meeting is to find out how corresponding situations could be avoided in the future.

Form templates for documentation

The forms referred to in the guideline for retrieving and opening an employee's e-mail messages, including completion instructions, are attached to the guideline as Appendices 1 - 4. These documents also include detailed descriptions of the preconditions required for the respective actions. Appendix 1 includes the employee's power of attorney expressing his/her consent to reading the contents of his/her e-mail messages. The report forms related to the retrieval and opening of e-mail messages, as well as the template of the record to which these reports are to be attached (Appendices 2 - 4), meet the requirements of reporting to the employee as stipulated in the Act on the Protection of Privacy in Working Life.

Attached to this guideline are the following samples of documents produced to verify the legality of the actions:

Appendix 1: Power of attorney to read e-mail message contents

Appendix 2: Report of retrieving messages belonging to the employer

Appendix 3: Report of opening a message belonging to the employer

Appendix 4: Record of retrieving [and opening] an employee's e-mail messages

Power of attorney to read e-mail message contents

The employee hereby provides another person, approved by the employer, with a power of attorney to read his/her e-mail messages when he/she is prevented from reading them or otherwise performing his/her duties. This power of attorney is granted voluntarily. The employee can revoke the power of attorney at any time. The power of attorney can be utilised in cases outlined in the Act on the Protection of Privacy in Working Life (759/2004, Sections 18-20).

I hereby authorise

_____

(person(s) approved by the signed employee's supervisor)

to read work-related e-mail messages sent to my e-mail account and to take any consequent action in the following situations (check one or more options):

- ☐ during my annual holiday when it lasts longer than ____ days
- ☐ during my leave of absence when it lasts longer than ____ days
- ☐ during my business trip when it lasts longer than ____ days
- ☐ during my training when it lasts longer than ____ days
- ☐ during my sick leave when it lasts longer than ____ days
- ☐ during the period from _____ to _____
- ☐ if the University or its unit has a compelling need to know the message contents
- ☐ after my death.

The person accessing my e-mail messages is allowed to

- ☐ forward messages related to my work tasks to the appropriate receivers
- ☐ perform actions described in an appendix.

The person accessing e-mail messages addressed to me is obligated to maintain their confidentiality and refrain from utilising any messages intended personally for me.

I have the right to cancel this power of attorney at any time. The cancellation becomes effective immediately as soon as the specified authorised persons are informed of it.

_____ _____

Date Power of attorney granted by - signature and name in block letters

_____ _____

Witnessed by - signature and name in block letters

Distribution: Registry office, (employee), (supervisor), (authorised person), (unit/department office)

The completed form is retained in the registry office for 10 years after the expiry of the power of attorney or after the end of the employee's employment relationship

Report of retrieving messages belonging to the employer

E-mail account owner, name and username: _____|_____

IT system in question: _____

Grounds for retrieval (check one or more options):

Reasons 1-3 and either 4 or 5-6 must exist.

- ☐ **1.** The employee handles the tasks independently and the necessary information is not recorded in any other system
- ☐ **2.** It is evident that messages belonging to the employer have been sent or received
- ☐ **3.** It is necessary to obtain the information in question in order to manage matters
- ☐ **4.** The employee is permanently unavailable and his/her consent cannot be obtained
- ☐ **5.** The employee is temporarily unavailable and his/her consent cannot be obtained
- ☐ **6.** The employee's consent cannot be obtained within a reasonable time and the matter cannot be delayed.

Messages were retrieved on (date): _____ and it was discovered that

- ☐ **yes**, messages belonging to the employer were found and they need to be opened
- ☐ **no**, messages belonging to the employer that would need to be opened were not found.

A list of messages that were retrieved but not opened is attached to this report.

The list must contain message-specific data in the format in which it was reviewed. The reviewed data can comprise the message sender/recipient, title and sending date. The attachment is classified as secret under the Act on the Protection of Privacy in Electronic Communications (516/2004), Section 4).

The retrieval was conducted by:

Signatures of authorised persons _____

Name in block letters and title _____

Signature of system administrator _____

Name in block letters and title _____

The retrieval was witnessed by:

Signature of witness _____

Name in block letters and title _____

The original form is attached to the record and delivered to the registry office. A copy of the record and this form is delivered to the e-mail account owner without any undue delay.

COMPLETION INSTRUCTIONS: Report of retrieving messages belonging to the employer

This form must be completed when the University or its unit has a need to obtain information contained in e-mail messages sent or received by its employee as stipulated in the Act on the Protection of Privacy in Working Life (759/2004) but the employee is not available to provide this information, and the information has not been saved in any other system. If messages need to be retrieved from several systems, a separate copy of this form must be completed for each retrieval. This form is attached to the record prepared of the procedure.

The employee's name and user ID in the target system are entered on the form. In addition, the target system and the unit responsible for the administration of this system are specified. The information system in question can be an e-mail service or the user's disk space, for example, a home directory or a folder on the employee's workstation.

The measure may only be taken if options 1 - 3 and either 4 or 5 - 6 can be checked on the form (Act on the Protection of Privacy in Working Life , Section 19).

The retrieval is a one-off measure, and its implementation date is indicated on the form.

It is specified on the form whether messages that need to be opened were found.

For each message that is to be opened, the form ”Report of opening messages belonging to the employer" must be completed and attached to the procedure record.

A list of e-mail messages that were retrieved but don't need to be opened is attached to this form. The list displays the message data in the format in which it was reviewed. This format can vary depending on the e-mail application or retrieval method. The retrieval may only feature the following data: message sender/recipient, title and sending date. The handling of this message identification data is governed by the Act on the Protection of Privacy in Electronic Communications (516/2004). According to Section 4 of the Act, all messages, identification data and location data are confidential unless the Act or another Act provides otherwise.

People involved in the retrieval:

1. One or more person(s) jointly authorised by the [information security officer] and the supervisor of the employee in question
2. The system administrator that can make the retrieval possible
3. As a witness, the [information security officer] or a person assigned by him/her.

All participants must sign the form.

Report of opening a message belonging to the employer

E-mail account owner, name and username: _____|_____

IT system in question _____

Grounds for opening the message (check box):

☐ **1.** It is evident that the message to be opened belongs to the employer.

☐ **2.** It is necessary to obtain the information in question in order to manage matters.
Why? _____

☐ **3.** The sender/recipient of the message cannot be contacted in order to obtain the information.

All grounds must be valid.

Specification of the opened message:

Sender/Recipient _____

Message title/subject _____

Message date _____

The message was opened on (date) _____

Information about the message contents was provided to (names)

_____

_____

The message was opened by:

Signatures of authorised persons _____

Name in block letters and title _____

Signature of system administrator _____

Name in block letters and title _____

The opening was witnessed by:

Signature of witness _____

Name in block letters and title _____

The original form is attached to the record and delivered to the registry office. A copy of the record and this form is delivered to the e-mail account owner without any undue delay.

COMPLETION INSTRUCTIONS: Report of opening a message belonging to the employer

This form must be completed if the University or its unit opens an e-mail message belonging to an employee under the Act on the Protection of Privacy in Working Life (759/2004). **Before opening, the message must be retrieved, and the retrieval must be documented using the form** ”Report of retrieving messages belonging to the employer”. If it is necessary to open several messages, a separate copy of this form must be completed for each message. The report of message retrieval and this form are both attached to the record prepared of the measures.

The employee's name and user ID in the target system are entered on the form. In addition, the target system and the unit responsible for the administration of this system are specified. The information system in question can be an e-mail service or the user's disk space, for example, a home directory or a folder on the employee's workstation.

Messages can only be opened if all grounds specified on the form are valid (Act on the Protection of Privacy in Working Life, Section 20). In addition, the need to open the message must be justified.

Specification of the opened message:

- Sender (From) or Recipient (To) of the message
- Contents of the message Subject field
- Reception/sending date of the message.

In addition, the date of opening the message and the person(s) informed about the message contents are specified on the form.

People involved in the opening:

1. One or more person(s) jointly authorised by the [information security officer] and the supervisor of the employee in question
2. The system administrator that can make the opening possible
3. As a witness, the [information security officer] or a person assigned by him/her.

All participants must sign the form.

SECRET (Reason, legal clause)

Record of retrieving [and opening] an employee's e-mail messages

<*Name of the employee*> (hereinafter: the Employee) works in the <*unit*> of the University and his/her tasks include <*the task(s) related to the need to access messages*>.

<Explanation why the existence and contents of the messages must be reviewed.>

As stipulated in Section 18 of the Act on the Protection of Privacy in Working Life (759/2004), the e-mail service <*specify*> used by the Employee has enabled the Employee to <*check the available options*>

☐ use an out-of-office auto reply
☐ direct work-related e-mail messages to another employee
☐ provide another employee with rights to read his/her received messages.

☐ The Employee has utilised these possibilities <*description*: *how*>.
☐ The Employee has not utilised these possibilities.

<*Specification whether the Employee has been asked for consent to read his/her messages, whether he/she has voluntarily given such consent, or why such consent cannot have been requested*>.

TO BE ADDED IF NEEDED:

The delivery of new messages to the Employee's Inbox was prevented <*date*> and an automatic reply message was set to instruct senders to send messages to the address <*organisation address*>.

On the above-specified grounds, the Employee's e-mail messages were retrieved under Section 19 of the Act on the Protection of Privacy in Working Life <*date(s)*> to ascertain whether the Employee has received or sent messages containing information crucial to the University immediately before or during his/her absence. A report of the retrieval is attached as Appendix 1.

In conjunction with the message retrieval it was discovered that the Employee's Inbox <*contains/does not contain*> messages that need to be opened.

TO BE ADDED IF NEEDED:

Consequently, the Employee's e-mail messages were opened under Section 20 of the Act on the Protection of Privacy in Working Life <*date(s)*> . A report of the opening is attached as Appendix 2.

Place and date	<*the Employee's supervisor's signature and name in block letters*>
	<*others involved, signature and name in block letters*>
Appendices	1 Report of retrieving messages belonging to the employer 2. Report of opening a message belonging to the employer
Distribution	Registry office, <*Employee*>

SECRET (Reason, legal clause)

SAMPLE - Record of retrieving and opening an employee's e-mail messages

Robert Researcher works in the YY department of the XX school of Aalto University, and his tasks include the practical arrangements of the symposium that will take place on 31 May 2010.

Mr. Researcher is on sick leave as of 15 March 2010 due to a serious accident. As Mr. Researcher has personally negotiated with the symposium participants about their schedules and presentation topics, it is evident that his e-mail Inbox contains messages that are crucial in order to continue the symposium arrangements.

The YY department's e-mail service used by Mr. Researcher has enabled and allowed him to direct his work-related messages to another employee, as is referred to in Section 18 of the Act on the Protection of Privacy in Working Life (759/2004).

Mr. Researcher has not utilised this possibility.

Due to his current health status, it is not possible to request his consent for retrieving and possibly opening the e-mail messages.

The delivery of new messages to Mr. Researcher's inbox was prevented on 20 March, 2010, and an automatic reply message was set to instruct senders to send messages related to the symposium to the address zz.symposium2010@aalto.fi.

On the above-specified grounds, Mr. Researcher's e-mail messages were retrieved, under Section 19 of the Act on the Protection of Privacy in Working Life on 21 March, 2010, to ascertain whether he has received or sent messages containing information crucial to the YY department. A report of the retrieval is attached as Appendix 1.

In conjunction with the message retrieval, it was discovered that Mr. Researcher's inbox contains messages that need to be opened. Consequently, Mr. Researcher's e-mail messages were opened, under Section 20 of the Act on the Protection of Privacy in Working Life, on 22 and 23 March, 2010. A report of the opening is attached as Appendix 2.

City, 23 March 2010	Paula Professor	
	Andy Assistant	Daisy Infosecofficer
	Arnold Administrator	Mary Mailmanager

Appendices	1. Report of retrieving messages belonging to the employer 2. Report of opening a message belonging to the employer
Distribution	Registry office, Ronald Researcher