

## FINAS Finnish Accreditation Service principles of confidential conduct

FINAS Finnish Accreditation Service

Helsinki 2019

## Content

Introduction	3
Disclose of information to other authorities	3
Principles	4
General .....	4
Principle I .....	4
Principle II .....	4
Principle III.....	5
Principle IV.....	5
Principle V.....	6
Entry into force	7

## Introduction

This information release describes the principles of confidential conduct of Finnish Accreditation Service (FINAS). FINAS observes the EU General Data Protection Regulation 2016/679 (GDPR) in its operations. In its operations and operating instructions, FINAS also observes the Finnish Safety and Chemicals Agency Tukes privacy policy and guidelines on information security and remote work, as well as the Ministry of Finance VAHTI guideline on the implementation of Government Decree (681/2010) on information security in central government. In this context, data material refers to documents and information stored in electronic and printed forms and on other data media.

Regulations on accreditation at the Community level were first set out in Regulation (EC) No 765/2008 of the European Parliament and of the Council. Article 8(4) of the aforementioned Regulation reiterates the principle referred to in standard SFS-EN ISO/IEC 17011:2017, according to which a national accreditation body shall have adequate arrangements to safeguard the confidentiality of the information obtained.

The operations of FINAS are comparable to actions taken by authorities, and decisions issued by FINAS are considered administrative decisions. In its operations, FINAS must comply with the Administrative Procedure Act (434/2003 and amendments). Among other provisions, the Act requires that FINAS must present grounds for its decisions. Assessment activities by FINAS are subject to the Act on the Openness of Government Activities (621/1999 and amendments). The starting point is that official documents, such as applications received by FINAS and accreditation decisions and their appendices, are in the public domain.

In assessing, FINAS verifies the competence, reliability and effectiveness of operations and evaluates the strengths and weaknesses of the subject of assessment. The assessment covers aspects such as the accuracy and operational reliability of various measuring instruments, professional competence of personnel, working methods, established practices, and the detailed results of quality assurance. These types of detailed information may be considered business or professional secrets to be kept secret under Section 24(1), paragraphs 17 and 20 of the Act on the Openness of Government Activities. In addition, provisions on the safeguarding of personal data under data protection legislation apply. The detailed definition of data protection legislation comprises: EU General Data Protection Regulation (2016/679), Finnish Data Protection Act (1050/2018), other applicable data protection legislation, and binding orders issued by data protection authorities. Assessment reports and statements related to accreditation and assessment by FINAS contain confidential information. These documents are not fully public.

## Disclose of information to other authorities

FINAS may disclose secret information to other authorities, provided that the authority requesting the document has a statutory right to access said information, or the subject of the assessment has consented to the disclosure. This also applies to personal data.

## Principles

### General

In European and international cooperation between accreditation bodies, FINAS is committed to following harmonised standards and principles. These international obligations are based on the principle that accreditation and its related assessments are founded on confidentiality (EU Regulation 765/2008 Article 8(1)(4) and standard SFS-EN ISO/IEC 17011:2017, section 8.1).

### Principle I

**Accreditation decisions and their appendices are public.**

**Documents and information received from the customer for the purpose of assessment and during the assessment process as well as reports prepared on the assessment are confidential.**

In order to assess competence and meet the criteria of accreditation, it is crucial that FINAS receives information for its accreditation as comprehensively and openly as possible. By safeguarding the confidentiality of accreditation reports related to its decisions, FINAS fulfils its European and international requirements. FINAS processes each request for information on a case-by-case basis. Where FINAS to be obligated to disclose its assessment reports to any party requesting them, this could cause the subjects of assessment to refrain from openly providing their information. In this event, FINAS would be unable to obtain sufficient information to use for its assessment, thus negating the purpose of the accreditation system.

The decision lists the standards used by FINAS in the assessment and the criteria that the subject of the assessment is found to meet. The grounds for the decision are given in a summary report. The summary report provides an overview of the conducted assessments, and contains those sections of the assessments considered to be in the public domain:

- basic details on the organisation, such as a general description of the organisation and its operation in view of the assessment criteria.
- a general description of the personnel's competence and level of expertise.
- a general description of the management system and the organisation, functionality and procedures of operations.
- central elements of the assessment of operations, based on which the assessment criteria are met or not met.

### Principle II

**Customers need to be able to trust that FINAS personnel and persons involved in assessments will process confidential customer information in a manner that safeguards their confidentiality.**

All external assessors involved in assessments by FINAS must sign a non-disclosure agreement. The non-disclosure obligation applies to both written and unrecorded information (such as verbal or visually obtained information). The non-disclosure obligation continues after the end of the employment relationship or commission for as long as the information remains secret. Customers' information may

not be disclosed to external assessors before a non-disclosure agreement has been signed and the customer has consented to the participation of the individual in question in the assessment.

In safeguarding confidential information from access by outsiders, FINAS employs technical measures such as computer lock screens, password protections and hard drive encryption. Computers and mobile devices may not be left unattended, and external storage media, printed copies and other data media must be appropriately stored. Confidential information must be safeguarded when engaging in conversations over the phone or in public spaces. The above obligations apply also to individuals participating in assessments.

FINAS personnel have received training on the appropriate processing of personal data, and further information on processing personal data is provided in the privacy policies (<https://tukes.fi/en/about-us/data-protection-at-tukes>). At FINAS, data are processed in various information systems. FINAS has concluded data processing agreements and non-disclosure agreements with its system suppliers, and its suppliers are obligated to comply with data protection legislation and other provisions.

### Principle III

**After data material related to assessments has been disclosed to the recipient, the rights and obligations related to processing and access are transferred to the recipient along with the data content.**

The sender is responsible for the confidentiality of data transfer.

In other words, data material submitted to FINAS by a customer is under the responsibility of FINAS only after they have been received.

Correspondingly, data material provided by FINAS to parties such as technical assessors remains the responsibility of FINAS until the material has been received by the recipient.

### Principle IV

**Transfer of confidential data material.**

Data material in electronic format:

Confidential data material in electronic format is transferred via a secure connection (FINAS Extranet) or by secure email. This primarily concerns confidential material communicated between FINAS and customers and FINAS and assessors, such as background material provided by customers for the assessment, reports by assessors, and other confidential material related to the assessment.

Customers may choose to submit information by an unsecure connection as the customer is responsible for the transfer of data (principle III) and for classifying the confidentiality of the submitted material. Regardless of the customer's policy in the matter, FINAS must safeguard the confidentiality of the customer's material when forwarding it to third parties. FINAS is responsible for communicating its policies on the transfer and safeguarding of confidential information to the relevant parties.

Data material in printed format, external storage media, etc.

Confidential data material in printed format or by external storage media is sent by postal item. FINAS will send the postal item by registered letter or courier. Customers are also recommended to follow this procedure. Confidential information transferred by external storage media (USB flash drive, external hard drive, etc.) must always be encrypted and accessible only with a password. Even if the information in question is not confidential, external storage media should still be encrypted to ensure that they cannot be infected with malware or spyware during transfer.

## Principle V

### **Destruction of confidential information.**

In archiving documents related to its accreditation process, FINAS complies with the archiving principle. In accordance with the Information Management Plan, documents in the public domain and reports prepared in the assessment process are archived. Other data material related to the assessment process is either destroyed after the process has ended (such as assessment material requested prior to an assessment visit) or retained until the end of the following accreditation period (such as information submitted to FINAS on measures taken to rectify non-conformities) in accordance with the Information Management Plan. Persons not part of the assessment unit must also destroy any material in their possession. Data material must be destroyed in a way that safeguards its confidentiality. The most secure way to destroy data material in electronic format is to physically destroy the storage medium, such as the USB flash drive. Secure methods for the destruction of printed materials include disposal by a confidential waste receptacle, shredding or incineration.

## Entry into force

**This leaflet shall come into force 13.5.2019, and it shall be valid until further notice.**

**This leaflet replaces the TP11 issued by FINAS Finnish Accreditation Service, 18.5.2015.**

**Director**

**Risto Suominen**

**Lead Assessor**

**Annika Wickström**