Principles of confidential operation of FINAS Finnish Accreditation Service

Leaflet 2

04.07.2024

Table of contents

1 Introduction

This leaflet describes the principles of confidential operation adopted by FINAS Finnish Accreditation Service. In its operations, FINAS takes into account Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR) and the Finnish Act on Information Management in Public Administration (906/2019), the latter of which includes information security obligations for public administration organisations. FINAS also observes the privacy policy and guidelines on information security and remote work of the Finnish Safety and Chemicals Agency (Tukes), the VAHTI guideline currently maintained by the Digital and Population Data Services Agency (DVV), and guidelines of the Finnish Transport and Communications Agency National Cyber Security Centre. In this context, “information materials” refer to documents and information stored in electronic and printed format 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(1)(4) of the aforementioned Regulation reiterates the principle referred to in ISO/IEC 17011:2017, according to which a national accreditation body shall have adequate arrangements to safeguard the confidentiality of 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, as amended). Among other provisions, the Act requires that the reasons for a decision shall be stated. Assessment activities by FINAS are subject to the Act on the Openness of Government Activities (621/1999, as amended). The starting point is that documents prepared by a public authority, such as accreditation decisions made by FINAS and the appendices thereto, are public and non-disclosable information is separately defined.

In assessing conformity, FINAS verifies the competence, reliability and effectiveness of the assessment object’s operations and highlights its strengths and weaknesses. The assessment covers aspects such as the accuracy and operational reliability of various measuring instruments, the competence of staff, working methods, practices and detailed quality assurance results. Such detailed information may be considered business or professional secrets to be kept secret under section 24, subsection 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. “Data protection legislation” specifically refers to Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR), the Finnish Data Protection Act

(1050/2018), other applicable data protection legislation and binding orders issued by data protection authorities. Applications, assessment reports and statements related to accreditation and assessments by FINAS contain information that must be considered confidential.

2 Disclosure of information to another authority

After having received a request for information, FINAS may disclose non-disclosable information to another authority, provided that the authority requesting the document has a statutory right to access said information, or the assessment object has consented to the disclosure of the information. This also applies to personal data. However, supervisory authorities should primarily request the information they need directly from the operator as part of their supervisory obligations.

3 Principles

Through European and international cooperation between accreditation bodies, FINAS has committed to harmonised procedures and principles. The international obligations are based on the principle that accreditation and related assessments are founded on confidentiality pursuant to Article 8(1)(4) of Regulation (EC) No 765/2008 of the European Parliament and of the Council and Section 8.1 of SFS-EN ISO/IEC 17011:2017. The principles of confidentiality that apply to FINAS also apply to FINAS' external assessors such as external lead assessors, technical assessors and technical specialists.

3.1 Principle I

Accreditation decisions and the appendices thereto are in the public domain.

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

In accreditation, it is crucial that FINAS receives information as comprehensively and openly as possible to assess compliance with the accreditation criteria. By safeguarding the confidentiality of accreditation reports related to its decisions, FINAS meets its international obligations. FINAS separately processes each received request for information. If FINAS were obligated to disclose its assessment reports in whole to any party requesting them, it would

lead to a risk of the assessment objects refraining from openly providing their information, in which case FINAS would not receive sufficient information for its assessment.

Each accreditation decision lists the procedures used by FINAS in the assessment and the criteria that the assessment object was found to meet. Grounds for the decision are provided in a summary report, which is a summary of the performed assessments and contains the sections of the assessment that are considered to be public:

- The organisation’s basic data
- Compliance or non-compliance with the assessment criteria
- The proposed accreditation decision

3.2 Principle II

Customers must to be able to trust that the staff of FINAS and the persons involved in assessments will process confidential information related to the customers’ business in a manner that will safeguard its 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 (e.g. verbal or visually obtained information). The non-disclosure obligation remains in force after the termination of the employment relationship or the end of the assignment. A customer's information will not be disclosed to an external assessor participating in the FINAS assessment until the assessor has signed the non-disclosure agreement and the customer has given its consent to the participation of this person in the assessment.

Matters related to the confidentiality of remote assessments have been taken into account in FINAS’s remote assessment principle.

Confidential processing of information by FINAS is ensured by verifying the information security of hardware and software, taking into account cloud services, and by means of personal diligence (e.g. updates, locking and monitoring of hardware, password protection, encryption of external hard drives or flash drives, ensuring the confidentiality of conversations, proper storage of electronic storage media, hard copies, etc.). The abovementioned aspects also apply to the persons involved in the assessment, i.e. external assessors need to ascertain the risks of cloud services in the management of confidential information, for example.

Taking photographs or screenshots during an assessment is not allowed. Also, it is not allowed to use on-line web applications, like Google translate, for translation of submitted material.

FINAS never requests documents containing patient information as the preliminary information, and no patient information that is possibly viewed during an assessment will be documented in any notes or assessment reports.

FINAS staff have received training on the appropriate processing of personal data. For more information about the processing of personal data, please see the privacy policies at https://www.finas.fi/Tietoa/Sivut/Tietosuoja.aspx (in Finnish). External assessors participating in FINAS assessments have been informed of the personal data processing principles. At FINAS, data is processed in various information systems. FINAS has concluded data processing agreements and non-disclosure agreements with its system suppliers, i.e. the suppliers are obligated to comply with data protection legislation and other regulations.

3.3 Principle III

Data transfers are confidential.

Confidential information materials are transferred using a secure connection (the FINAS extranet or secure email). This primarily applies to the transfer of confidential materials between FINAS and the customer and between FINAS and assessors. Confidential materials relating to an assessment include materials provided by the customer and the assessors' reports.

Customers may opt to submit information via an unsecure connection, as the customer is responsible for the transfer of data (Principle IV) and for the classification of the submitted materials as confidential. Regardless of the customer's policy in the matter, FINAS must safeguard the confidentiality of the customer's materials when forwarding them to third parties. FINAS is responsible for communicating its policies on the transfer and safeguarding of confidential information to the relevant parties. Customer must not send to FINAS security classified documents. With regarding to this customer must contact FINAS first.

3.4 Principle IV

Once information materials related to assessments are disclosed to the recipient, the rights and obligations related to processing and access will also be transferred to the recipient along with the data content.

The sender is responsible for the confidentiality of the data transfer.

In other words, materials submitted to FINAS by a customer do not become the responsibility of FINAS until after they have been received by FINAS.

Correspondingly, materials submitted by FINAS to parties such as technical assessors remain the responsibility of FINAS until received by the assessor.

3.5 Principle V

Destruction of confidential information.

When archiving documents related to its accreditation process, FINAS complies with its information management plan. In accordance with the information management plan, documents in the public domain and reports prepared during the assessment process are archived. Other materials related to the assessment process (such as materials requested before the assessment) will be destroyed at the end of the assessment process. The assessment team must also destroy the materials in their possession. The destruction must take place in a manner that safeguards the confidentiality of the materials. The materials must be permanently deleted from personal computers, also taking into account servers. The most secure way to destroy data on a flash drive is to physically destroy the flash drive. Secure methods for the destruction of hard copies include disposal in a confidential waste receptacle, shredding with shredder and incineration.

4 Validity

This leaflet will enter into force on 04.07.2024 and remains valid until further notice.

This leaflet supersedes Leaflet 2 issued on 13 May 2019 by FINAS Finnish Accreditation Service.

Director Katriina Luoma

Senior Specialist Annika Wickström

5 Changes from the previous version

04.07.2024

	Section	**Change**
1	Introduction	Non-disclosable information taken into account.
2	Disclosure of information to another authority	Procedure for requests for information taken into account.
3	Principles	Information that photographs and screen-shots must not be taken or medical records documented in notes or reports updated. Also, using on-line applications for translation is prohibited, Principle with security classified documents updated.