MINISTRY OF FINANCE

Tiedonhallintalautakunta
Informationshanteringsnämnden

Handling of classified documents in cloud computing services

Board

Publications of the Ministry of Finance – 2022:7

Publications of the Ministry of Finance 2022:7

Handling of classified documents in cloud computing services

Ministry of Finance Helsinki 2022

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Publication sale

Online bookstore of the Finnish Government

vnjulkaisumyynti.fi

Publication distribution

Institutional Repository for the Government of Finland Valto

julkaisut.valtioneuvosto.fi

Ministry of Finance

ISBN pdf: 978-952-367-887-3
ISSN pdf: 1797-9714

Layout: Government Administration Department, Publications

Helsinki 2022

Description sheet
11 February 2022

Handling of classified documents in cloud computing services

Publications of the Ministry of Finance 2022:7		**Subject**	Board
Publisher	Ministry of Finance		
Group author	Information Management Board		
Language	English	**Pages**	30

Abstract

This recommendation of the Information Management Board on the handling of classified documents in cloud computing services supplements the previous recommendation on the handling of documents that are subject to security classification (Ministry of Finance 2021:5). These two recommendations offer guidance on how to meet the requirements of section 18 of the Act on Information Management in Public Administration (906/2019) and the Government Decree on Security Classification of Documents in Central Government (1101/2019). It is recommended that information management units select a cloud computing service based on use cases and on the information management and information security requirements specified for the classified information materials handled in the service. To manage the risks associated with cloud computing services, it is recommended that information management units use services or providers that have undergone facility security clearances under the Security Clearance Act or that have been granted a certificate of conformity with security requirements referred to in the provisions regarding information security assessment.

The Information Management Board approved the recommendation on 13 December 2021.

Keywords	Information Management Board, Information Management Act, recommendation, public sector ICT, boards, information security, public administration, classification, documents, information		
ISBN PDF	978-952-367-887-3	**ISSN PDF**	1797-9714
URN address	https://urn.fi/URN:ISBN:978-952-367-887-3		

Kuvailulehti
11.2.2022

Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa

Valtiovarainministeriön julkaisuja 2022:7		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	englanti	**Sivumäärä**	30

Tiivistelmä

Tämä tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa täydentää aiemmin annettua suositusta turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5). Nämä kaksi suositusta opastavat täyttämään julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 18 §:n ja asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun valtioneuvoston asetuksen (1101/2019) vaatimuksia. Tiedonhallintayksiköitä suositellaan valitsemaan pilvipalvelu siinä käsiteltävien turvallisuusluokiteltujen tietoaineistojen tiedonhallinta- ja tietoturvallisuusvaatimusten sekä käsittelyn käyttötapausten perusteella. Pilvipalveluihin liittyvien riskien hallitsemiseksi tiedonhallintayksiköitä suositellaan käyttämään sellaisia pilvipalveluita, joiden turvallisuus ja joiden tarjoajan turvallisuus on arvioitu turvallisuusselvityslain mukaan tehdyissä yritysturvallisuusselvityksissä, tai joille on myönnetty tietoturvallisuuden arviointitoimintaa koskevien säännösten mukainen turvallisuusvaatimustenmukaisuutta osoittava todistus.

Tiedonhallintalautakunta hyväksyi suosituksen 13.12.2021.

Asiasanat tiedonhallintalautakunta, tiedonhallintalaki, suositus, Julkisen hallinnon ICT, lautakunnat, tietoturva, julkinen hallinto, luokitukset, asiakirjat, tieto

ISBN PDF	978-952-367-887-3	**ISSN PDF**	1797-9714
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-887-3		

Presentationsblad
11.2.2022

Hantering av säkerhetsklassificerade handlingar i molntjänster

Finansministeriets publikationer 2022:7		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	engelska	**Sidantal**	30

Referat

Denna rekommendation från informationshanteringsnämnden om hantering av säkerhetsklassificerade handlingar i molntjänster kompletterar den tidigare rekommendationen om hantering av säkerhetsklassificerade handlingar (FM 2021:5). Dessa två rekommendationer hjälper att uppfylla kraven i 18 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019) och i statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019). Det rekommenderas att informationshanteringsenheterna väljer en molntjänst på basis av informationshanterings- och informationssäkerhetskraven samt användningsfallen i fråga om sådant säkerhetsklassificerat informationsmaterial som behandlas i tjänsten. För att hantera riskerna i anslutning till molntjänster rekommenderas det att informationshanteringsenheterna använder sådana molntjänster vars säkerhet och erbjudarens säkerhet har bedömts i säkerhetsutredningar av företag enligt säkerhetsutredningslagen, eller som beviljats ett intyg om överensstämmelse med säkerhetskraven enligt bestämmelserna om bedömning av informationssäkerhet.

Informationshanteringsnämnden godkände rekommendationen den 13 december 2021.

Nyckelord	informationshanteringsnämnden, informationshanteringslagen, rekommendation, den offentliga förvaltningens IKT, nämnderna, informationssäkerheten, den offentliga förvaltningen, klassificeringar, handlingar, information

ISBN PDF	978-952-367-887-3	**ISSN PDF**	1797-9714
URN-adress	https://urn.fi/URN:ISBN:978-952-367-887-3		

Table of contents

1 Introduction

This Recommendation of the Information Management Board on the processing of classified documents in cloud services was prepared by the Board's classified documents division appointed for a term running from 1 April 2020 to 31 December 2021. The division was chaired by Tuija Kuusisto, Senior Ministerial Adviser at the Ministry of Finance. The Information Management Board appointed the members of the division from among experts in the various information management entities. The draft Recommendation was made available for public comment via the Lausuntopalvelu public service for online consultation between 15 October and 15 November 2021.

This Recommendation complements the earlier Recommendation on the handling of classified documents (Ministry of Finance 2021:8). These two Recommendations provide guidance on the fulfilment of the requirements under section 18 of the Act on Information Management in Public Administration (906/2019, "Information Management Act") and under the Government Decree on Security Classification of Documents in Central Government (1101/2019, "Security Classification Decree"). This Recommendation does not address other provisions limiting the use of cloud services such as data protection or provisions relating to classified materials under an international information security obligation.

Under the Information Management Act, the authorities operating in government agencies and public bodies, the courts of law and committees established to handle appeals shall security classify documents and make a security classification marking on them to indicate the information security measures to be complied with when processing the documents. The Recommendation on the handling of classified documents (Ministry of Finance 2021:8) sets out the following on the processing of classified documents in cloud services: "Documents at security classification level IV may be handled and stored in cloud services that are not estimated to be subject to the legislation-derived risks described at the start of chapter 7, provided that the authority has also taken into account all other protection needs and obligations associated with the handling of classified information. Documents at security classification level IV may be stored in other cloud services only in reliably encrypted format so that they cannot be decrypted in the said service during the lifecycle of the information. A part of an authority's classified information processing environment may thus be implemented by using cloud technology." These policies have been updated and clarified in this Recommendation.

This Recommendation describes the key pieces of legislation relating to the processing of classified documents in cloud services and the risk management procedure and risk management impact assessment in the protection of classified documents. It also describes the assessment of the reliability of the cloud services used in processing classified documents and the providers of these services as well as aspects to be taken into account in cloud service agreements.

2 Legislation and other guidance

The Recommendation on the processing of classified documents in cloud services is especially geared to experts in information management and processing, parties responsible for cloud services and technology procurement and development, and parties responsible for the protection of information. Cloud technology refers to the technological solutions on which the provision of cloud services is based. The Recommendation applies to the Information Management Act and the Security Classification Decree:

- **Act on Information Management in Public Administration (906/2019, Information Management Act).** The Information Management Act lays down provisions on matters including the data secure processing of datasets of authorities and the implementation of information security measures. The Act imposes legal obligations on information management entities and authorities in public administration as well as on private individuals, corporations and corporations subject to public law other than those serving as authorities when they exercise public authority. While the Information Management Act provides for a minimum level of information security measures, the information management entities are nonetheless given risk-based discretion in the implementation of the measures. Section 18 of the Information Management Act lays down provisions on the obligation of authorities operating in State agencies and institutions, the courts of law and committees established to handle appeals to security classify certain documents.
- **Government Decree on Security Classification of Documents in Central Government (1101/2019, Security Classification Decree).** The Decree lays down further provisions on the security classification of classified documents as referred to in the Information Management Act, the markings to be made in documents to be classified and the information security measures related to the handling of such documents.

This Recommendation does not apply to other legislation limiting the use of cloud services. The key pieces of legislation relating to the processing of classified documents in cloud services are:

- **Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union.** The key impact of the Regulation is that Member States cannot require non-personal data in electronic format to be stored or processed in a given geographic area or territory unless public security can be invoked as justification for such a requirement.

- **Act on the Openness of Government Activities (621/1999).** The Act on the Openness of Government Activities lays down provisions on matters including the principle of openness, disclosure of information held by the authorities, and secrecy. Under section 18 of the Information Management Act, a security classification marking shall be made on the documents defined in section 24, subsection 1, paragraphs 2, 5 or 7–11 of the Act on the Openness of Government Activities when the unauthorised disclosure or unauthorised use of the information contained in such documents can cause prejudice to matters including national security.

- **Act on the Assessment of the Information Security of Public Authorities' Information Systems and Telecommunications Arrangements (1406/2011, Assessment Act)**. *"In the assessment of the information security of their information systems and telecommunications arrangements, central government authorities may only use the procedure referred to in this Act or an inspection body to which the Finnish Communications Regulatory Authority"* (currently the Finnish Transport and Communications Agency, hereinafter Traficom) *"has granted accreditation under the **Act on Information Security Inspection Bodies (1405/2011, Inspection Body Act**)."*

- The purpose of the **Security Clearance Act (726/2014)** is "*to improve the opportunities to prevent activities that may cause prejudice to the security of the State, national defence, Finland's international relations, public safety or another comparable public interest or very significant private financial interest or security arrangements implemented in order to protect the interests referred to in the foregoing*". Under section 9, subsection 3 of the Security Clearance Act, Traficom "*as part of facility security clearance vetting shall prepare a report on the level of information security of information systems and telecommunications arrangements*".

In addition to this Recommendation, the reader is urged to review the other Recommendations of the Information Management Board as well as the policies and guidelines of the Ministry of Finance concerning cloud services (Ministry of Finance 2018:35, 2020:66, 2020:73, [in Finnish only]). In addition, Traficom's National Cyber Security Centre has issued Criteria to Assess the Information Security of Cloud Services (PiTuKri), Traficom publications 20/2020).

3 Risk management and impact assessment

Under section 13 of the Information Management Act, an information management entity shall determine the material risks to data processing and dimension the data security measures in accordance with the risk assessment. Risk management in information management entities is addressed at a general level in the Collection of recommendations on the application of certain information security regulations (VM 2021:65 [in Finnish only]).

When the use of cloud technology is considered in the processing of classified documents, for the purpose of enabling risk assessment, the information management entity must identify

- the classified datasets that are to be processed using cloud technology, and
- the information management and information security requirements applicable to the processing of these datasets, the use cases of the processing, and the related official processes.

In addition, the information management entity must assess the needs for using cloud technology. The use of cloud technology in the processing of classified documents may pursue aims such as cost-effectiveness, data storage needs, or utilisation of a given technology enabled by cloud technology, such as extensive analytics or artificial intelligence.

The information management entity must determine the material risks related to data processing in the manner described in chapters 3.1 and 3.2, taking into account the classified datasets that are to be processed using cloud technology and their information management and information security requirements as well as use cases and official processes, and dimension the data security measures accordingly. In addition, the information management entity must also perform the assessment of transformative impact referred to in section 5 of the Information Management Act in relation to data processing in the event of a change to the existing process for processing data. The assessment of transformative impact shall also take into account the measures and procedures relating to continuity management in exceptional situations material to the processing. Where the classified documents contain personal data, the information management entity shall assess the need for a separate data protection impact assessment.

3.1 Risk management relating to the processing of classified documents in cloud services

In services implemented with cloud technologies, the most significant risks and the measures required to manage them in respect of the processing of classified documents relate to the physical location of the classified information or the processors of that information, i.e. the cloud service provision model, deployment model and delivery model as well as the provider of the cloud service.

The processing of classified documents especially in cloud services provided from outside Finland involve several risks relating to global supply chains and actors. In terms of the risks to classified documents, cloud service provision models may be grouped into two main categories: cloud services provided from Finland and international cloud services. Based on an expert assessment, at present the provision models cannot be broken down in more detail to identify other international cloud service provision models based on e.g. geography.

The most common cloud service deployment models are private cloud, hybrid cloud and public cloud. The most common service delivery models are SaaS, PaaS, IaaS and CaaS. The risks related to service delivery models are addressed in the following guidelines: VM 2018:35, 2020:66 and Pitukri. The service provision, deployment and delivery models are described in further detail in Appendix 1, Terminology.

When planning to introduce a cloud service, attention must be paid not only to the security classification of individual documents but also to the wider whole to which the documents belong, as well as the security classification of that whole. Assessing this 'aggregate effect' is addressed in chapter 5.3 of the Recommendation on the handling of classified documents (Ministry of Finance 2021:8). In addition, the criticality of the cloud service and the classified information held in it must also be assessed from the viewpoints of continuity management and preparedness for exceptional circumstances. In many use cases and official processes, classified information must be accessible in all security situations, also during disruptions in normal circumstances and in exceptional circumstances. Consequently, the information cannot be allowed to be geographically located outside Finland – at least not exclusively.

In some special circumstances, the use of international cloud services may be necessary in the processing of classified information owing to the operational needs of the authorities. For example, the operational activities of an authority may involve saving lives in the event of a natural disaster striking abroad, in which case ordinary secure communications may not always be deployable with sufficient speed. In a situation of this kind, the secrecy and security classification period of classified information is very short, and classified

information is needed and may be disclosed e.g. for consideration by joint meetings of authorities from several countries.

When the processed classified datasets, their information management and information security requirements and use cases as well as official processes and needs for the use of cloud technology have been described, the information management entity must decide, on a risk basis and individually for each use case, which cloud service provision, deployment and delivery model may be used for processing which classified datasets. Risk-based decision-making means that the information management entity must assess the risks related to the cloud services provision, deployment and delivery models and to the service provider and implement the measures needed to manage these risks before any classified information is processed in the cloud services. In risk management, it is advisable for the information management entity to prepare reports and assessments of effective information management and information security compliance, or to make use of existing reports and assessments.

In designing and selecting information security measures relating to the use of cloud services, entities may rely not only on the Recommendations of the Information Management Board but also the more general guidelines designed to mitigate the impacts of risks to classified information, such as the Katakri 2020 Information Security Audit Tool for Authorities published by the National Security Authority of Finland and the Criteria to Assess the Information Security of Cloud Services (PiTuKri) published by the National Cyber Security Centre. Besides the general risks to classified information, the information management entity must take into account the specific risks relating to the classified datasets that it envisions to process in the cloud service under assessment and the processing of these in various use cases and official processes. Risk management procedures must be designed and implemented to manage specific risks. These procedures must be selected with attention to both information security measure implementation requirements and overall economic advantageousness.

The purpose of identifying and assessing risks to classified datasets and of implementing information security measures on a risk basis is to complement and clarify the minimum requirements for the protection of classified information laid down in legislation. Each identified risk must be assessed. When the assessment concludes that the residual risk is acceptable or that the risk has very low probability or impact in the use cases of classified data sets concerned or in official processes, the information management entity may waive a risk management procedure or security measure related to the risk.

An information management entity may also waive a risk management procedure or security measure when another such procedure or measure effectively prevents the impacts of the identified risk. Deficiencies identified in other security methods may be

complemented in certain cases by effective incident detection and response capabilities, for example. In addition, the impacts of many risks relating to information networks may be effectively prevented by e.g. isolating the entire data processing environment of a private cloud, including isolation of the physical terminal devices, and this may provide sufficient security. Risks relating to deficiencies in the processing of inputs to an application located in a cloud can be reduced by using a Web Application Firewall (WAF) to control access to the application interface. Risks relating to malware, for example, may be managed by validating input data at cloud service interfaces. However, an information management entity's decision to waive risk management/security measures on the basis of its risk assessment must never be allowed to lead to a situation where the key risks described below are ignored or the minimum requirements and necessary protective risk management measures to reduce their impacts are foregone.

3.2 Key risks to classified documents in cloud services

The specific risks to classified information may be divided into:

- legislation-derived risks,
- risks related to Foreign Ownership, Control or Influence (FOCI risks),
- risks related to the right to audit reserved by the authorities in control of the classified information, and
- risks related to the implementation security of individual technical security measures.

Typically, these risks are of greater significance in international cloud services than in ones provided from Finland. Legislation-derived risks are addressed in chapter 7 of the Recommendation on the handling of classified documents (Ministry of Finance 2021:8). FOCI risks are briefly discussed in the Ministry of Finance Guidelines for Security-Critical Procurements (VM 2019:7 [in Finnish only]).

Authorities in control of classified information often reserve for themselves the right to audit all data processing environments where classified information under their control is processed. In respect of international classified information in particular, the term "data owner" is often used for such authorities, and sometimes also the term "data originator" in a similar sense. Audits often require physical and logical access to the site audited. Consequently, auditors often have the opportunity to also access the information processed at the site. In cloud services where the information of multiple authorities is processed, the structure of the data processing environment must enable audits to be carried out so that the different authorities in control of information do not gain access to each others' information in the context of their audit.

Both technical and administrative procedures may be put in place to reduce the risks related to the right to audit. Technical procedures are addressed in more detail in the Katakri 2020 Information Security Audit Tool for Authorities (section I-06), the Criteria to Assess the Information Security of Cloud Services (PiTuKri) (section JT-03) and also e.g. the Cloud Computing Compliance Controls Catalogue (C5) published by the German Federal Office for Information Security (BSI) (sections OPS-24 and COS-06). The most common administrative procedure is to require the authorities using a cloud service holding information from multiple authorities to undertake not to exercise the right of technical audit to the cloud service, instead relying on e.g. information provided through a facilities security clearance in accordance with the Security Clearances Act (726/2014). Chapter 4 discusses assessment of the reliability of the cloud service provider and the cloud service in more detail.

The implementation security aspects of technical protection measures are related to the provision, administration and management of cloud services and to data in transit. The information management entity must identify and assess the risks of subcontractor chains and subcontractors relating to the cloud service provision, deployment and delivery models as well as risks relating to the processing of classified information arising from the use of various technologies and the service along with the other services required for its provision. In encryption solutions, for example, attention must additionally be paid to risks relating to both data at rest and data in transit. The encryption solutions used to protect classified information must moreover be able to provide the information with protection throughout the period of its classification, taking into account the methods available to more sophisticated attackers.

Besides encryption solutions, it is also necessary to take account of the security of the processing of information and the associated risks e.g. in situations where data needs to be decrypted for the purpose of mathematical operations and other data analysis. The manners of use of cloud services may also entail risks that can sometimes be difficult to anticipate. The default configuration in anti-malware software installed on a terminal device, for example, may be such that it attempts to send to the software manufacturer's cloud service for analysis a hash of a file identified by the software as suspicious, metadata relating to such a file, for instance file name and timestamp, or even the file in its entirety.

When using cloud services, the technical protection requirements imposed in the Security Classification Decree to which particular attention must be paid are the obligations to roll out the obligations concerning need to obtain information and protection of classified information (section 8); protecting the handling of documents and information systems with security areas (section 10); obligation of separation from lower security level environments (section 11, subsection 1, paragraph 1); protection against general cyberattacks and guaranteeing protection throughout the lifecycle of the

information system (section 11, subsection 1, paragraph 2); implementing the principle of least privilege (section 11, subsection 1, paragraph 3); protecting the integrity of the information system (section 11, subsection 1, paragraph 4); the identification of users, equipment and information systems (section 11, subsection 1, paragraph 5); hardening policies (section 11, subsection 1, paragraph 6); and the adequate security of encryption solutions (section 11, subsection 1, paragraph 7).

Encryption solutions of adequate security are required especially when transferring classified information outside physical security areas or via a network of lower security level (section 12; also section 14 of the Information Management Act). A classified document which is no longer required shall be destroyed in such a way that re-creation and reconstruction of the information in whole or in part is prevented in a manner that is sufficiently reliable for the said security classification level (section 15). In addition, at security classification level III and higher, account shall be taken of electromagnetic emanations and sufficient protection against electronic intelligence gathering (section 11, subsection 2). Compliance with these requirements is addressed in more detail in the Information Management Board's Recommendation on the handling of classified documents (Ministry of Finance 2021:8).

3.3 Recommendations on the use of cloud services issued on the basis of a risk assessment

Information management entities are advised to select a cloud service on the basis of the information management and information security requirements applicable to the classified datasets processed in the service as well as the use cases of processing and the associated official processes. It is recommended that a risk assessment of cloud service use be carried out on a continual basis throughout the lifecycle of the service with particular attention to the risks relating to cloud services, addressed in chapters 3.1 and 3.2, and to the risks arising from the rapid advancement of technologies. It is recommended that the information management entity accept the residual risks by a written decision.

It is recommended that in the interests of managing the risks related to cloud services, only services and service providers assessed as reliable by the authorities be used. The reliability assessment of cloud services and cloud service providers is addressed in more detail in chapter 4. Where classified datasets are processed in international cloud services, it is moreover recommended that the classified datasets processed are limited and carefully selected on the basis of use cases and the associated official processes and also in such a manner that the datasets are amenable to transfer to the States to the jurisdiction of which the cloud service provider and its subcontractors are subject.

Generally speaking, classified documents may be construed to fall within the scope of Finland's national security. Processing in international cloud services is not recommended in respect of classified documents excluded from the scope of *Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union.* Ministry of Transport and Communications publication 2019:11 discusses interpretation of the scope of the Regulation. Location requirements imposed on the basis of national security and preparedness are excluded from the Regulation's scope and the obligations under the Regulation therefore do not apply to them.

International cooperation between States or information-sharing relating to international procurements, for example, may constitute grounds to process classified datasets in international cloud services assessed as reliable by the authorities. In such a case, the datasets shall be carefully limited and selected and based on a risk assessment in which the residual risks are deemed acceptable by the information management entity. For example, if a Finnish authority engages in cooperation with a Swedish authority, some of the national classified documents relating to such cooperation may be amenable to transfer for processing in a Swedish cloud service.

4 Assessment of the reliability of cloud services used in the processing of classified documents and cloud service providers

Legislative basis for assessment of reliability

Section 26, subsection 3 of the Act on the Openness of Government Activities reads: *An authority requesting executive assistance or the performance of a task on commission by it or otherwise on its behalf may grant access to a secret document, if such access is indispensable for the assistance or the performance of the task. For such tasks, access to secret information may be granted also if the removal of the secret information is obviously not feasible owing to its large volume or for any other comparable reason. The authority shall ensure in advance that the arrangements for the secrecy and the protection of the information are appropriate*." Under section 6 of the Security Classification Decree, "*a central government authority shall ensure in advance that the protection of a classified document is duly organised if the authority grants access to a classified document to a party other than a central government authority*". This means that access to classified information may not be granted to a cloud service provider, either, before the information management entity has ascertained the reliability of the provider and ensured that the provider will process the information in compliance with the Information Management Act and the Security Classification Decree.

It should moreover be noted that under section 8, subsection 1 of the Security Classification Decree, "*the right to handle a classified document may be granted only to persons who, due to their work duties or a need connected to attending to other duties of central government authorities, need to obtain information on a document or otherwise to handle it and who have been informed of the instructions and procedures related to the protection of classified information and who are aware of the obligations related to the handling of documents*". This means that access to classified information may not be granted to a cloud service provider, either, before the information management entity has ascertained the rights to process the classified datasets that are to be processed in the cloud service and ensured that the persons processing such datasets are familiar with the instructions and procedures related to the protection of classified information and the obligations related to its processing.

Facility security clearance vetting in assessing the reliability of cloud services provided from Finland

A possible procedure, compliant with legislation, for assessing the reliability of a cloud service provider is facility security clearance vetting, as provided in the Security Clearance Act, of a cloud service that is now or will be provided from Finland, and of its provider. Facility security clearance vetting assesses the reliability of responsible individuals in the enterprise, its level of data security, and its ability to discharge its commitments. Under section 9 of the Security Clearance Act, Traficom "*as part of a facility security clearance shall prepare a report on the level of information security of information systems and telecommunications arrangements*". As a rule, a certificate of facility security clearance remains valid for five years while the period of validity for the associated clearance of information systems and telecommunications arrangements is three years. The facility security clearance vetting process is described in more detail on the website of the Finnish Security Intelligence Service.

Certificate of conformity as provided in the Assessment Act in assessing the reliability of cloud services provided from Finland

The reliability of a cloud service and its provider may also be assessed by means of assessments under the Assessment Act. The processing requirements for information at each security classification level are used in these assessments. The scope of application of the Assessment Act is limited to assessing the information security of the information systems and telecommunications arrangements of the authorities. The Inspection Body Act applies to "*traders and entities providing service tasks to public administration which, upon commission, assess the level of information security (information security inspection body) and which desire the approval of the Finnish Communications Regulatory Authority* [currently Traficom] *for their operations*" and to the inspection body accreditation procedure. Information security refers to ensuring confidentiality, availability and integrity.

Under section 4 of the Assessment Act, the conformity assessment of the information system or telecommunications arrangement of an authority shall be performed upon commission which, besides an authority, may also be given by a party which procures on account of the authority, provides the authority with data processing or telecommunications services, or performs service tasks relating to the organisation of the aforementioned services. Under the Assessment Act, the assessment may be performed by Traficom or an accredited inspection body within its approved competence area. To date, no inspection body has been accredited to assess systems at the highest security classification levels (II and I), and consequently assessments of these may only be performed by Traficom, which is also accredited to perform assessments of information systems or telecommunications arrangements at security levels IV and III. Traficom may issue a certificate of conformity as provided in the Assessment Act for an information

system or telecommunications arrangement. As a rule, such a certificate remains valid for a period of three years. The assessment procedure under the Assessment Act is described in more detail on the website of the Finnish Transport and Communication Agency Traficom's National Cyber Security Centre [in Finnish only].

Recommendations on assessing the reliability of cloud services provided from Finland

Information management entities are advised to use cloud services whose security and the security of the provider of which has been assessed by means of facility security clearance vetting conducted in accordance with the Security Clearance Act or which have been granted the certificate of security conformity referred to in the Assessment Act. It is recommended that the party which commissions the assessment conclude the agreement on the assessment with Traficom in a way that allows the provider of the cloud service subject to assessment to report that the assessment has been conducted. The results of an assessment may be shared with information management entities requesting these only with the consent of the party which commissioned the assessment.

An information management entity may also seek to independently assess the reliability of cloud service providers or cloud services. The challenge here lies in the fact that information management entities typically do not possess sufficient information to perform a risk assessment and therefore lack the capabilities to conduct a reliable, in-depth assessment. In-depth assessment also calls for specialised expertise which not all information management entities possess – nor do they need to. Legislation moreover does not permit all information management entities to gain access to all sources of information used in facility security clearance vetting. Some cloud service providers may also decline to disclose details about their service to all information management entities. An information management entity may find it challenging to conduct a credible assessment of the reliability of cloud services or their providers in the processing of classified information when in its assessment of compliance with statutory requirements, the entity must rely only on evidence such as the cloud services providers' self-assessments, commercial certificates, and agreements, for example.

Assessing the reliability of international cloud services by means of international facility security clearance vetting

Finland has concluded General Security Agreements with several countries and international organisations. The purpose of the General Security Agreements is "*to protect the classified information owned by States and international organisations that the parties exchange directly between themselves or between public or private legal entities or individuals under their jurisdiction*". (Industrial Security Manual, 2011).

International information security obligations refers to the provisions of the General Security Agreements concluded by Finland for the protection of classified information. Provisions on the responsibilities under the General Security Agreements are laid down in the Act on international information security obligations (588/2004). Under section 4 of the Act, in the implementation of international information security obligations, the Ministry for Foreign Affairs acts as the National Security Authority (NSA) and Traficom as the Designated Security Authority (DSA) referred to in the Act in matters concerning the information security of information systems and telecommunications arrangements. Other Designated Security Authorities in Finland are the Ministry of Defence, the Defence Command and the Finnish Security Intelligence Service, which "*act as experts for the National Security Authority in matters concerning personnel security, corporate security and premises security*". Classified information is defined as "*such secret documents and materials as well as the information available in these and documents and materials produced on the basis of these which have been classified in accordance with the international information security obligation*".

A General Security Agreement between two States does not oblige the commercial actors in the States party to the Agreement to implement the obligations under the Agreement. The obligations under a General Security Agreement are made to apply to commercial actors by means of the Facility Security Clearance (FSC) procedure referred to in the international information security obligations. As a rule, this procedure is available when processing classified documents at security classification level III / CONFIDENTIAL and higher.

Recommendations relating to the assessment of the reliability of international cloud service providers

It is recommended that the Facility Security Clearance procedure referred to in the international information security obligations be utilised whenever possible when assessing the reliability of international cloud services and their providers. Consequently, it is recommended that when classified documents are to be processed in international cloud services, the information management entity should contact the NSA in advance and

- determine the situation vis-à-vis General Security Agreements between Finland and the States having jurisdiction over the cloud services provider and its subcontractors, and
- determine the status of FSC relating to the General Security Agreements for the cloud services provider, and
- in cooperation with the NSA, assess whether the international information security obligations under any eventual General Security Agreements are fulfilled in using the said cloud service, and
- consult the NSA as to whether transfer of the information to the cloud service provider is feasible.

5 Service agreements relating to cloud services used in processing classified documents

When cloud services are used in the processing of classified documents, the secure processing of information is ensured on the basis of the assessment of the reliability of cloud services and their providers described in chapter 4 and the agreements concluded between the information management entity and the cloud service provider and the integrator, if any. Agreements must cater for aspects including the States in which the information is to processed. Attention must be paid to country-specific legislation, aspects including the coverage of subcontractor chains (whether all subcontractors and any support arrangements of the service are covered) and the manner in which the service provider proves a sufficient level of security, for example by means of inspection reports and audits.

The information management entity must ensure that the service agreement fulfils the requirements relating to the processing of classified information. A more comprehensive discussion of information security aspects in agreements may be found in the Information Management Board's Collection of recommendations on the application of certain information security regulations (VM 2021:65 [in Finnish only]). Moreover, it must be ascertained, on a risk basis and no later than during the term of the agreement, that the service provider complies with the information security obligations under the agreement.

Assessment of any subcontractor chain associated with the provision of the cloud service is typically included in the assessments of information systems and telecommunications arrangements described in chapter 4. Where no such assessment procedure has been applied, it is important for the information management entity to determine the entire contractual chain and establish which subcontractors may possibly be involved in the processing of the entity's information as well as the geographical location of such subcontractors. In many cases, the information management entities will not have a direct contractual relationship with the cloud service provider and instead, the use of the cloud services will be based on a longer contractual chain involving multiple actors. In such a case, the information management entity typically acquires the cloud service via an integrator and the first link in the contractual chain is the ICT service agreement or other agreement between the information management entity and the integrator. The

contractual chain between integrator and cloud service provider may further include an intermediary that brokers and operates solutions from different cloud services or a reseller with which the integrator has concluded a purchase agreement. In this case, the third link in the contractual chain is the agreement between the intermediary or reseller and the cloud service provider. Additionally, it should be noted that cloud service providers may use any number of subcontractors that take part in the provision of the services and their delivery to the end-user information management entity. These subcontractors may be based in more than one country, which increases the volume of legislation that must be reviewed. In such a case, it is of particular importance to determine any legislation-derived risks. Any requirements imposed by the processing and transfer of personal data must also be taken into account.

The in-use management of cloud services underscores the monitoring and supervision of contractual changes as well as supervision of the security of the cloud service and the management of access rights and administration. It is recommended that information management entities use a cloud service provider that has been assessed to comply with information security requirements in accordance with the Security Clearance Act or the Assessment Act, and which is also responsible for configuration as a service.

It is recommended that the cloud service provider be required to notify well in advance of any significant changes to the service or the agreements. It is advisable to require immediate notification of any information security incidents and notification of any other significant events in the cloud service provision environment on a monthly basis. Notification of an overview of security should also be requested at regular intervals, for example on a quarterly basis. While some cloud service providers supply tools for reviewing reports, in many cases these do not extend to information on the system's internal security or the full picture arising from the use of more than one cloud service component. It is recommended that the information management entity see to it that the monitoring of the security of the cloud service used in the processing of classified documents (detection, response and analysis) has been ensured e.g. by means of a Security Operations Centre (SOC) independent of the cloud service provider.

Under section 13 of the Information Management Act, "*an information management entity shall monitor the state of the data security of its operating environment and ensure the data security of its datasets and information systems over their entire lifecycle*". In other words, the information management entity is obliged to ensure the information security of classified documents and the information systems in which they are processed, cloud services included, over their entire lifecycle. Cloud services are in constant flux. They are characterised by rapid advancements on a wide front, which necessitates ongoing monitoring and supervision of agreements as well as change management. All changes increase the risk of the service, its provider or a new feature in the service becoming

non-compliant with the agreement or requirements. These also result in the risk of change of control risks being realised. Additionally, it should be noted that it may be impossible to ensure lifecycle-long information security with cloud service providers that in their agreements reserve the right unilaterally to change the terms and conditions of the agreement.

When an information management entity lacks the expertise to monitor developments in the services of cloud service providers and the changes ensuing from such development, it is advisable to use services acquired through a trusted service provider. The recommendation is, whenever possible, to use cloud services established to be compliant with security requirements and provided from Finland so as to enable management of the risks associated with international cloud services over the entire lifecycle of classified documents. An option worthy of consideration is to use cloud services acquired through Hansel or the Government ICT Centre Valtori that have been assessed to be compliant with the security requirements imposed by the authorities.

An information management entity may discontinue the use of cloud services when the service's lifecycle ends, when it no longer has a need for the service or when the service is restored for provision from Finland or otherwise transferred to another provider. Over the entire the lifecycle of the cloud service, starting from the relevant procurement and planning, the information management entity must cater and prepare for the possibility of unsubscribing from the service or changing service provider. Discontinuing the use of a cloud service is addressed in a separate Recommendation of the Information Management Board.

6 Recommendations in brief

Information management entities are recommended to select their cloud service on the basis of the information management and information security requirements for the classified datasets processed in the service as well as the use cases of processing and the associated official processes. It is recommended that the risks of using cloud services are subject to ongoing assessment over the entire lifecycle of the service, taking into account in particular the risks associated with cloud services discussed in chapter 3 as well the risks arising from rapid advances in technologies. It is recommended that the information management entity accept the residual risks by a written decision.

In order to manage the risks related to cloud services, information management entities are advised to use services where the security of the services and their provider has been assessed by means of facility security clearance vetting conducted in accordance with the Security Clearance Act or which have been granted a certificate of security conformity in accordance with the provisions on assessment of information security. It is recommended that the party which commissions the assessment conclude the agreement on the assessment with Traficom in a way that allows the provider of the cloud service subject to assessment to report that the assessment has been conducted.

Where classified datasets are processed in international cloud services, it is moreover recommended that the classified datasets are limited and carefully selected on the basis of use cases and the associated official processes and also in such a manner that the datasets are amenable to transfer to the States to the jurisdiction of which the cloud service provider and its subcontractors are subject. It is recommended that the Facility Security Clearance procedure referred to in the international information security obligations be utilised whenever possible, in the manner described in chapter 4, when assessing the reliability of international cloud services and their providers.

It is recommended that over the entire the lifecycle of the cloud services, starting from the relevant planning, purchase and contracts, the information management entity cater and prepare for the possibility of unsubscribing from the service or changing service provider. Ongoing monitoring of changes in technologies and contracts is recommended.

7 References

Ministry for Foreign Affairs, National Security Authority (NSA) 2020. Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje [Guideline for handling international classified information]. https://um.fi/turvallisuusluokitellun-tiedon-kasittelyohje

Ministry for Foreign Affairs, National Security Authority (NSA) 2015. Industrial Security Manual. https://um.fi/documents/35732/48132/industrial_security_manual/37116023-0471-2beb-7a8a-f7905dda94ba?t=1525647189259

Ministry of Finance 2018:35. Julkisen hallinnon pilvipalvelulinjaukset [Guidelines for Public Sector on Data Communications Services]. http://urn.fi/URN:ISBN:978-952-251-982-5

Ministry of Finance 2020:66. Tuottavuutta pilvipalveluilla. Ohje julkisen hallinnon pilvipalvelujen hyödyntämiseen [Productivity through cloud services. Guidelines for making use of cloud services in the public sector]. http://urn.fi/URN:ISBN:978-952-367-327-4

Ministry of Finance 2020:73. Pilvipalvelujen soveltamisohje – Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon tiedonhallintayksiköille [Guidelines on using cloud services: Practical guidelines for public sector organisations on making use of cloud services]. http://urn.fi/URN:ISBN:978-952-367-503-2

Information Management Board (Ministry of Finance 2021:8). Recommendation on the handling of classified documents. http://urn.fi/URN:ISBN:978-952-367-512-4

Information Management Board (Ministry of Finance 2021:65): Suositus tiettyjen tietoturvallisuussäännösten soveltamisesta [Collection of recommendations on the application of certain information security regulations]. http://urn.fi/URN:ISBN:978-952-367-897-2

Ministry of Transport and Communications (2019:11) Muiden kuin henkilötietojen vapaan liikkuvuuden esteet Suomessa [Obstacles to the mobility of non-personal data in Finland]. http://urn.fi/URN:ISBN:978-952-243-571-2

Finnish Transport and Communications Agency Traficom National Cyber Security Centre 2020:20. Criteria to Assess the Information Security of Cloud Services (PiTuKri). https://www.traficom.fi/sites/default/files/media/file/PiTuKri_v1__english.pdf

APPENDIX 1. Terminology

Term	Definition
Document	For the purposes of this Recommendation, document means a document as provided in section 5, subsection 1 of the Act on the Openness of Government Activities (621/1999), i.e. a written or visual presentation stored on a platform, regardless of the nature of the platform, for example a decision, memorandum, notice, list, photograph, drawing or chart. Document furthermore also means a message relating to a given topic or subject-matter and consisting of signs which, by virtue of the use to which they are put, are meant to be taken as a whole, but are decipherable only by means of a computer, an audio or video recorder or some other technical device. Consequently, the information stored in the databases of cloud services or in other storage media may also constitute documents.
Information	For the purposes of this Recommendation, information means the same as document.
Dataset	For the purposes of this Recommendation, dataset has the meaning defined in section 2 of the Act on Information Management in Public Administration (906/2019), i.e. an information entity composed of documents and other corresponding information related to a specific task or service of the authorities.
Information system	For the purposes of this Recommendation, information system means an information system as provided in section 2 of the Act on Information Management in Public Administration (906/2019), i.e. an overall arrangement comprising data processing equipment, software and other data processing. Information systems include e.g. cloud services of various kinds and terminal devices used to run software.
Cloud service	There are numerous definitions for a cloud service. For the purposes of this Recommendation, cloud service means, as provided in the NIS Directive[1], "a digital service that allow access to a scalable and elastic pool of shareable computing resources". Cloud service further means "data processing capacity or service that is accessible over network, and which is provided applying a model of shared, scalable and flexible resources and automated to be partially provided on a self-service basis" (PiTuKri). The term cloud technology often refers to the same as the above references to definitions of cloud service. In many cases, cloud service only refers to services provided by international suppliers by leveraging cloud technology.
Cloud technology	For the purposes of this Recommendation, cloud technology means the technological solutions on which the provision of cloud services is based.

[1] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

Term	Definition
Cloud service provider	For the purposes of this Recommendation, cloud service provider means an actor that provides a service having IaaS, PaaS or SaaS as its delivery model or another service based on cloud technology.
Cloud platform provider	For the purposes of this Recommendation, cloud platform provider means the actor which provides the cloud service consisting of infrastructure capacity, performance, telecommunications and ancillary services, if any. The services may be selected and possibly also configured by the client and the application provider.
Service provider	For the purposes of this Recommendation, service provider means an actor which provides a service provided for the cloud platform. The service may comprise virtual servers, applications or systems built on top of the cloud platform's capacity and solutions. Service providers often have administrator rights to the system itself and to the application. Service providers and application providers may have their own subcontractors. Service providers may also hold the role of integrator.
Integrator	For the purposes of this Recommendation, integrator means an actor which procures services on behalf of the client from both cloud platform providers and service providers and which is often contractually responsible for the security and compatibility of the services.
Information management entity	Under section 2 of the Information Management Act, information management entity means an authority whose task is to arrange information management in accordance with the requirements of that Act.
Client	An information management entity subscribes for the service directly from the cloud service provider or employs a service provider or integrator to assist in the acquisition and specification of the service. A central purchasing body such as Hansel may also act as the client.
IaaS (Infrastructure as a Service)	Cloud service delivery model: In the IaaS model, the entire infrastructure related to providing services is acquired from the cloud service provider.
PaaS (Platform as a Service)	Cloud service delivery model: In the PaaS model, services are provided through an existing software platform.
SaaS (Software as a Service)	Cloud service delivery model: In the SaaS model, the service provider provides the services as a whole.
CaaS (Containers as a Service)	Cloud service delivery model: In the CaaS model, the cloud service client may upload, organise, run, scale and otherwise manage software containers, applications and clusters. Software containers are software that may be migrated from one location to another without any need for adaptation. A software container may be migrated from a dedicated data centre to a cloud service, for example.

Term	Definition
Private cloud	Cloud service deployment model: Private cloud generally refers to service provided for exclusive use by a single information management entity. The service may be operated from the data centre of either the service provider and/or the information management entity. A typical strength of a private cloud is reliable isolation of the physical and logical level of the cloud service infrastructure and information processed in it from other data processing environments, information management entities and external parties. Typically, a private cloud can provide services of a higher security level compared with the other deployment models.
Public cloud	Cloud service deployment model: Public cloud generally means a service that is publicly available for open use by anyone. The service is practically always provided from the service provider's data centres. In a public cloud, the cloud service infrastructure and information processed in it involve a larger attack surface than a private cloud through other users or external parties, for example.
Hybrid cloud	Cloud service deployment model: Hybrid cloud generally refers to a service that combines a private and public cloud into a single service configuration. For instance, a private cloud on the organisation's own data centre may be supplemented with services from a public cloud. The security level achieved typically depends on the type of information that may travel from the private cloud into the public cloud and on the implementation of security measures at the interface of the cloud platforms.
Cloud service provided from Finland	Cloud service provision model: For the purposes of this Recommendation, cloud service provided from Finland means a service where the information and capacity are located in the territory of Finland and the service provision and administration takes place in Finland.
International cloud service	Cloud service provision model: For the purposes of this Recommendation, international cloud service means a service where the information and capacity are located or the provision or administration of the service takes place outside Finland. For example, a cloud service whose data centre is located in Finland but the administration of which takes place from another country subject to its legislation shall be construed as an international cloud service.
Change in control	Change in control refers to a change in the party exercising control in the enterprise providing a cloud service or its subcontractors, for example the right to appoint or dismiss the majority of the members of the enterprise's board of directors or otherwise effectively control the enterprise.

APPENDIX 2. Examples of duties of actors

Examples of the in-service management duties of each actor in a cloud service are described below.

Duties of the information management entity

- Responsible for the lifecycle protection of classified information in the cloud service and for the entry into and removal of information from the service.
- Defines the permitted use of the cloud service.
- Responsible for supervision and risk management.
- Responsible for the security of the supply chain relative to the requirements for the processing of classified information.
- Responsible for management and control of overall security.
- Monitors the aggregation of data.

Duties of the integrator

- Implements, supervises and reports on technical controls in the cloud service.
- Monitors any impending changes to the cloud services.
- Keeps systems and protections up to date.
- Contractually responsible for the security of its own supply chains relative to requirements on the processing of classified information.
- Contractually responsible for management and guidance of overall security.
- Role of monitoring and supervision
  - May be outsourced to a third party (SOC)
  - Incident detection and management

Duties of the service provider/application provider

- Change management
- Administration and verification of access rights
- Monitoring the use of the service
- Risk assessment maintenance
- Monitors any impending changes to the cloud services.
- Keeps systems and protections up to date.
- Contractually responsible for the security of its own supply chains relative to requirements on the processing of classified information.

MINISTRY
OF FINANCE

MINISTRY OF FINANCE
Snellmaninkatu 1 A
PO BOX 28, 00023 GOVERNMENT
Tel. +358 295 160 01
financeministry.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-887-3 (pdf)

February 2022