FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Finanstilsynet 06.12.2021

Guidelines on outsourcing to cloud service providers

Stig Ulstein
Finanstilsynet

Agenda

Agenda

1. Guideline 1 – Cloud services and outsourcing
2. Guideline 2 – General principles of governance for cloud outsourcing
3. Guideline 3 – Update of the outsourcing written policy
4. Guideline 4 – Written notification to the supervisory authority
5. Guideline 5 – Documentation requirements
6. Guideline 6 – Pre-outsourcing analysis
7. Guideline 7 – Assessment of critical or important operational functions and activities
8. Guideline 8 – Risk assessment of cloud service provider
9. Guideline 9 – Due diligence on cloud service provider
10. Guideline 10 – Contractual requirements
11. Guideline 11 – Access and audit rights
12. Guideline 12 – Security of data and systems
13. Guideline 13 – Sub-outsourcing of critical or important operational functions or activities
14. Guideline 14 – Monitoring and oversight of cloud outsourcing arrangements
15. Guideline 15 – Termination rights and exit strategies
16. Guideline 16 – Supervision of cloud outsourcing arrangements by supervisory authorities

Guideline 1 – Cloud services and outsourcing

- The undertaking should establish whether an arrangement with a cloud service provider falls under the definition of outsourcing pursuant to the Solvency II Directive.

- Avtale om rett til bruk av programvare, plattform og/eller infrastruktur (IKT-systemer og -tjenester) som driftes av oppdragstaker på oppdragstakerens servere, anses som utkontraktering av foretakets IKT-virksomhet. Som eksempler på dette nevnes:
  - IaaS – (Infrastructure as a Service)
  - PaaS – (Platform as a Service)
  - SaaS – (Software as a Service)

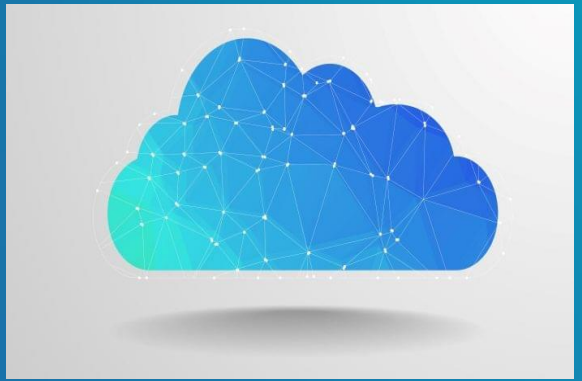
Bruk av IaaS, PaaS eller SaaS innebærer at foretaket også utkontrakterer driften, behandlingen og/eller oppbevaringen av data som registreres i forbindelse med bruken av slike programvarer og tjenester.

Guideline 2 – General principles of governance for cloud outsourcing

- Without prejudice to Article 274(3) of the Delegated Regulation, the undertaking's administrative, management or supervisory body ("AMSB") should ensure that any decision to outsource critical or important operational functions or activities to cloud service providers is based on a thorough risk assessment, including all relevant risks implied by the arrangement such as
  - information and communication technology ("ICT"),
  - business continuity,
  - legal and compliance,
  - concentration,
  - other operational risks,
  - and risks associated to the data migration and/or the implementation phase, where applicable.

Guideline 3 Update of the outsourcing written policy

- In case of outsourcing to cloud service providers the undertaking should update the written outsourcing policy



Guideline 4 - Written notification to the supervisory authority

- The written notification requirements set in Article 49(3) of the Solvency II Directive and further detailed by EIOPA Guidelines on System of Governance are applicable to all outsourcing of critical or important operational functions and activities to cloud service providers

- Finanstilsynsloven § 4 c med veiledning

Behandling og melding av IKT-utkontraktering

Behandling

Avtaler om utkontraktering av IKT-virksomhet og endringer i slike avtaler skal behandles av styret. Styret skal forelegges planer for utkontrakteringen, med risikovurdering, og en beskrivelse av hvordan foretaket skal sikre leveransen.

Melding

Meldeplikten gjelder avtaler om utkontraktering av virksomhet som er kritisk eller viktig for foretaket.

Krav til meldingen

a. navn og organisasjonsnummer på oppdragstaker
b. virksomheten/oppgavene som utkontrakteres
c. oppdragstaker driver virksomhet i Norge, i norsk selskap, i filial eller som grensekryssende virksomhet. (inkl land HK)
d. navn og organisasjonsnummer på oppdragstakers underleverandører for utførelse av oppgaven (inkl land)
e. avtalens oppstarts- og opphørsdato, herunder opplysninger om rullerende avtaleperiode
f. hvordan foretaket vil følge opp sitt ansvar for den utkontrakterte virksomheten, samt foretakets risikovurdering av utkontrakteringen
g. utkontrakteringsavtalen med vedlegg
h. styremøteprotokoll hvor det fremgår at styret har behandlet utkontrakteringsavtalen og risikovurdering av utkontraktering

Rundskriv: Veiledning om utkontraktering

Kapittel	Innhold
1	Innledning
2	Vurderinger som må gjennomføres før utkontraktering
3	Om utkontraktering
4	Begrensninger i hvilke oppgaver som kan utkontrakteres
5	Vurdering av oppdragstaker
6	Utkontrakteringsavtalen
7	Finanstilsynsloven § 4c
8	Risikostyring og internkontroll

Guideline 5 – Documentation requirements

- As part of its governance and risk management system, the undertaking should keep record of its cloud outsourcing arrangements, for example, in the form of a dedicated register kept updated over time.

Guideline 5 – Documentation requirements

(jf., forskrift om meldeplikt ved utkontraktering)

- Foretakets oversikt inkluderer følgende opplysninger:
  a. navn og organisasjonsnummer på oppdragstaker
  b. virksomheten/oppgavene som utkontrakteres
  c. oppdragstaker driver virksomhet i Norge, i norsk selskap, i filial eller som grensekryssende virksomhet. Dersom oppdragstaker er etablert i utlandet skal det også opplyses hvilket land foretakets hovedkontor er etablert i
  d. navn og organisasjonsnummer på underleverandører som oppdragstaker bruker ved utførelse av oppgaver på vegne av foretaket. Dersom underleverandør er etablert i utlandet bes det opplyst hvilket land
  e. avtalens oppstarts- og opphørsdato, herunder opplysninger om rullerende avtaleperiode
  f. hvordan foretaket vil følge opp sitt ansvar for den utkontrakterte virksomheten, samt foretakets risikovurdering av utkontrakteringen

Guideline 6 – Pre-outsourcing analysis

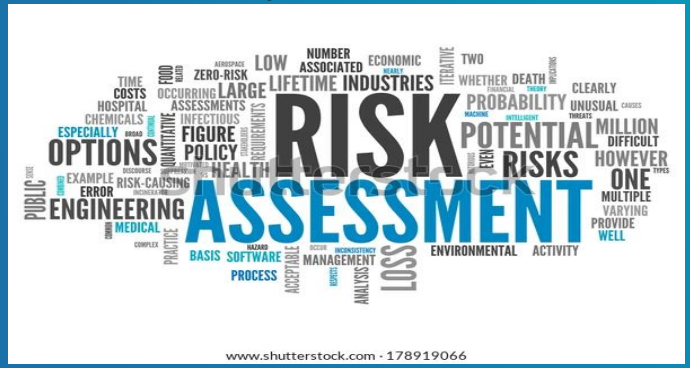
- Before entering into any arrangement with cloud service providers, the undertaking should:
  a) assess if the cloud outsourcing arrangement concerns a critical or important operational function or activity in accordance with Guideline 7;
  b) identify and assess all relevant risks of the cloud outsourcing arrangement in accordance with Guideline 8;
  c) undertake appropriate due diligence on the prospective cloud service provider in accordance with Guideline 9;
  d) identify and assess conflicts of interest that the outsourcing may cause in line with the requirements set out in Article 274(3)(b) of the Delegated Regulation.

Guideline 7 – Assessment of critical or important operational functions and activities

- Prior to entering into any outsourcing arrangement with cloud service providers, the undertaking should assess if the cloud outsourcing arrangement relates to an operational function or activity that is critical or important.
- Perform Business Impact Analysis

Guideline 8 – Risk assessment of cloud service provider

- In general, the undertaking should adopt an approach proportionate to the nature, scale and complexity of the risks inherent in the services outsourced to cloud service providers. This includes, assessing the potential impact of any cloud outsourcing, in particular, on their operational and reputational risks

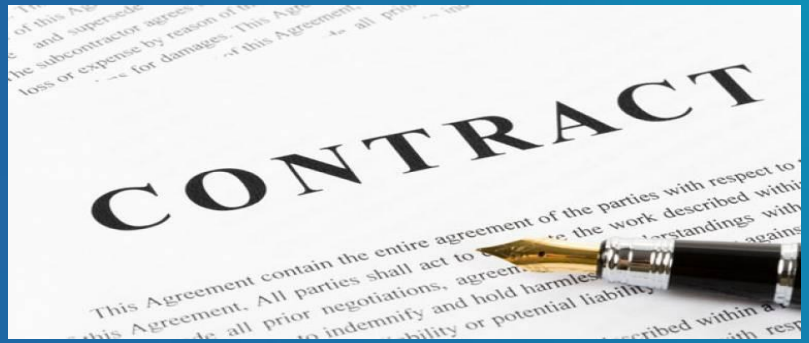


Guideline 9 – Due diligence on cloud service provider

- The undertaking should ensure in its selection and assessment process that the cloud service provider is suitable according to the criteria defined by its written outsourcing policy.

Guideline 10 – Contractual requirements

- The respective rights and obligations of the undertaking and of the cloud service provider should be clearly allocated and set out in a written agreement.



Guideline 11 – Access and audit rights

- The cloud outsourcing agreement should not limit the undertaking's effective exercise of access and audit rights as well as control options on cloud services in order to fulfil its regulatory obligations.

Guideline 12 – Security of data and systems

- The undertaking should ensure that cloud service providers comply with European and national regulations as well as appropriate ICT security standards.

Guideline 13 – Sub-outsourcing of critical or important operational functions or activities

- If sub-outsourcing of critical or important operational functions (or a part thereof) is permitted, the cloud outsourcing agreement between the undertaking and the cloud service provider should be back-to-back agreements

Guideline 14 – Monitoring and oversight of cloud outsourcing arrangements

- The undertaking should monitor, on a regular basis, the performance of activities, the security measures and the adherence to agreed service level by their cloud service providers on a risk based approach.

Guideline 15 – Termination rights and exit strategies

- In case of cloud outsourcing of critical or important operational functions or activities, within the cloud outsourcing agreement the undertaking should have a clearly defined exit strategy clause ensuring that it is able to terminate the arrangement, where necessary

Guideline 16 – Supervision of cloud outsourcing arrangements by supervisory authorities

- The supervisory authorities should perform the analysis of the impacts arising from undertakings' cloud outsourcing arrangements as part of their supervisory review process

Spørsmål?

FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY