Outsourcing Policy

Utkontrakteringspolicy — Drop

Dokument-ID: UTKONTR-DROP-001 **Versjon:** 1.0 **Dato:** 12. februar 2026 **Eier:** ALAI Holding AS, org.nr. 932 516 136 **Klassifisering:** Intern **Regulatorisk grunnlag:** DORA (EU) 2022/2554 art. 28-30, Finanstilsynets retningslinjer for utkontraktering

---

1. Innledning

1.1 Formål

Denne policyen etablerer rammeverket for styring av utkontraktering og tredjepartsleverandører som understøtter Drop-tjenesten. Policyen sikrer at risikoen knyttet til utkontraktering identifiseres, vurderes og håndteres i samsvar med DORA og Finanstilsynets krav.

1.2 Virkeområde

Policyen gjelder for:

- Alle IKT-tjenester som er utkontraktert til tredjeparter
- Alle tredjepartsleverandører som har tilgang til Drop-systemer eller -data
- Internt utkontrakterte tjenester (innen konsern)
- Underleverandører til våre tredjepartsleverandører (kjede)

1.3 Regulatorisk bakgrunn

Regulering	Artikler	Beskrivelse
DORA (EU) 2022/2554	Art. 28	Generelle prinsipper for IKT-tredjepartsrisiko
DORA (EU) 2022/2554	Art. 29	Forhåndsvurdering av IKT-tredjepartsrisiko
DORA (EU) 2022/2554	Art. 30	Kontraktuelle krav
GDPR (EU) 2016/679	Art. 28	Databehandlere

Regulering	Artikler	Beskrivelse
PSD2 (EU) 2015/2366	Art. 19	Agenter og utkontraktering
Finanstilsynets rundskriv	—	Retningslinjer for utkontraktering
IKT-forskriften	—	Krav til IKT-drift

---

2. Prinsipper

2.1 Overordnede prinsipper

1. **Ledelsesansvar:** Styret og ledelsen har det overordnede ansvaret for all utkontraktering, jf. DORA art. 28(2). Utkontraktering fritar ikke selskapet fra regulatoriske forpliktelser.
2. **Risikostyring:** All utkontraktering vurderes gjennom vårt IKT-risikostyringsrammeverk.
3. **Proporsjonalitet:** Krav til leverandørstyring er proporsjonale med tjenestens kritikalitet.
4. **Konsentrasjonrisiko:** Vi vurderer og unngår uhensiktsmessig konsentrasjon hos enkeltleverandører.
5. **Exit-strategi:** Vi sikrer at vi kan avslutte eller overføre enhver utkontraktert tjeneste.

2.2 Hva som kan utkontrakteres

Følgende kan utkontrakteres med adekvat risikostyring:

- IKT-infrastruktur (hosting, lagring)
- Open Banking-tjenester (PSD2 PISP/AISP)
- Autentiseringstjenester (BankID)
- Kundeserviceteknologi
- Analysetjenester (anonymiserte data)

2.3 Hva som ikke kan utkontrakteres

Følgende kan ikke utkontrakteres:

- Overordnet risikostyring og compliance-overvåking
- Beslutninger om strategi og styring
- Overordnet ansvar for kundekontroll (KYC/AML)
- Regulatorisk rapportering (operasjonelt kan delegeres, ansvaret forblir)

---

3. Kritikalitetsklassifisering

3.1 Klassifiseringsmodell

Klasse	Beskrivelse	Kriterier	Eksempler
Kritisk	Bortfall medfører umiddelbar stans i kjernetjenester	Betalingsbehandling, autentisering, datalagring	Open Banking-leverandør, BankID, skyinfrastruktur, database
Viktig	Bortfall medfører vesentlig degradering	Kundeservice, rapportering, overvåking	Kundeserviceplattform, SIEM, analysetjenester
Standard	Bortfall medfører begrenset påvirkning	Støttefunksjoner, utviklingsverktøy	E-postleverandør, utviklingsmiljø, CI/CD

3.2 Kriterier for klassifisering

Klassifisering baseres på:

- **Konsekvens ved bortfall:** Påvirkning på kjernetjenester og brukere
- **Datatilgang:** Tilgang til personopplysninger eller finansielle data
- **Substituerbarhet:** Mulighet for rask erstatning
- **Regulatorisk relevans:** Tjenestens rolle i regulatorisk etterlevelse
- **Konsentrasjonsrisiko:** Avhengighet til enkelteleverandør

3.3 Register over utkontrakterte tjenester

Vi vedlikeholder et oppdatert register over alle utkontrakterte IKT-tjenester, jf. DORA art. 28(3), som minimum inneholder:

- Leverandørens navn, organisasjonsnummer og kontaktinformasjon
- Tjenestebeskrivelse
- Kritikalitetsklasse
- Dato for avtaleinngåelse og utløp
- Databehandlerstatus (ja/nei)
- Land der tjenesten utføres
- Underleverandører
- Dato for siste risikovurdering

---

4. Due diligence — DORA art. 29

4.1 Forhåndsvurdering

Før inngåelse av avtale om utkontraktering gjennomføres due diligence proporsjonalt med tjenestens kritikalitet:

Kritiske tjenester — utvidet due diligence

Område	Vurdering
Finansiell stabilitet	Kredittvurdering, årsregnskap, eierstruktur
Teknisk kompetanse	Referanser, sertifiseringer, teknisk arkitektur
Sikkerhet	Sikkerhetssertifiseringer (ISO 27001, SOC 2), penetrasjonstester
Regulatorisk samsvar	Relevante lisenser, tilsynsstatus, DORA-beredskap
Operasjonell resiliens	BCP/DR-kapasitet, SLA-historikk, hendelseshistorikk
Personvern	GDPR-samsvar, databehandleravtale, TIA ved tredjeland
Konsentrasjonrisiko	Leverandørens markedsandel, avhengigheter
Underleverandører	Oversikt og vurdering av kritiske underleverandører
Exit-mulighet	Dataportabilitet, overgangsperiode, migrasjonsplan

Viktige tjenester — standard due diligence

- Teknisk kompetanse og referanser
- Sikkerhetssertifiseringer
- GDPR-samsvar og databehandleravtale
- SLA-betingelser
- Exit-klausuler

Standard tjenester — forenklet due diligence

- Grunnleggende selskapsinfo
- Relevante sertifiseringer
- GDPR-samsvar der relevant
- Kontraktvilkår

4.2 Risikovurdering

Due diligence resulterer i en risikovurdering som dokumenterer:

- Identifiserte risikoer per kategori
- Risikonivå (lav, middels, høy, kritisk)
- Anbefalte mitigerende tiltak

- Gjenværende risiko
- Anbefaling (godkjent, godkjent med betingelser, avvist)

4.3 Godkjenning

Kritikalitet	Godkjenner
Kritisk	Styret
Viktig	Daglig leder
Standard	CISO

---

5. Kontraktuelle krav — DORA art. 30

5.1 Obligatoriske kontraktbestemmelser

Alle avtaler om utkontraktering av IKT-tjenester skal inneholde følgende, jf. DORA art. 30:

5.1.1 Tjenestebeskrivelse

- Detaljert beskrivelse av tjenesten
- Tjenestenivå (SLA) med målbare kriterier
- Rapporteringsforpliktelser

5.1.2 Sikkerhet

- Sikkerhetskrav i henhold til vår IKT-sikkerhetspolicy
- Hendelsesrapportering — varsling til oss uten ugrunnet opphold, senest innen 24 timer
- Sårbarhetshåndtering og patchkrav
- Krypteringskrav

5.1.3 Databehandling

- Databehandleravtale iht. GDPR artikkel 28 (for alle leverandører som behandler personopplysninger)
- Datalokalitet (EØS-krav)
- Sletting/tilbakelevering ved avtalens opphør
- Forbud mot sekundærbruk av data

5.1.4 Tilsyn og revisjon

- Vår rett til revisjon og inspeksjon, jf. DORA art. 30(3)(e)
- Finanstilsynets rett til tilgang og informasjon

- Samarbeid med tredjepartsrevisorer
- Rett til on-site inspeksjon ved kritiske tjenester

5.1.5 Underleverandører

- Forhåndsgodkjenning av kritiske underleverandører
- Varsling ved endring av underleverandører
- Samme kontraktuelle krav videreføres i kjeden
- Rett til å motsette seg bruk av spesifikke underleverandører

5.1.6 Kontinuitet og exit

- Leverandørens forpliktelser ved egen konkurs eller opphør
- Overgangsperiode ved oppsigelse (minimum tilstrekkelig for migrasjon)
- Bistand ved overføring til ny leverandør
- Dataportabilitet og -tilbakelevering
- Videreføring av tjeneste under overgangsperiode

5.1.7 Oppsigelse

- Gjensidig oppsigelsesrett med rimelig varsel
- Rett til umiddelbar oppsigelse ved vesentlig mislighold
- Rett til oppsigelse dersom leverandøren ikke oppfyller regulatoriske krav
- Rett til oppsigelse ved endringer som vesentlig påvirker risikoprofilen

5.2 Tilleggskrav for kritiske tjenester

For kritiske tjenester kreves i tillegg:

- Detaljert BCP/DR-plan med testforpliktelse
- Dedikerte sikkerhetskontakter og eskaleringsprosedyrer
- Kvartalsvise ytelsesrapporter
- Årlig uavhengig sikkerhetsrevisjon (eller deling av SOC 2-rapport)
- Minimumsgaranti for tilgjengelighet (99,9% eller høyere)
- Penalty-klausuler ved gjentatte SLA-brudd

---

6. Løpende overvåking

6.1 Overvåkingsrammeverk

Kritikalitet	Frekvens for gjennomgang	Revisjon	SLA-rapportering

Kritisk	Kvartalsvis	Årlig	Månedlig
Viktig	Halvårlig	Hvert 2. år	Kvartalsvis
Standard	Årlig	Ved behov	Halvårlig

6.2 Løpende vurdering

For alle utkontrakterte tjenester overvåkes:

- SLA-etterlevelse og tjenestekvalitet
- Sikkerhetshendelser og sårbarhetsstatus
- Regulatorisk etterlevelse
- Finansiell stabilitet (for kritiske leverandører)
- Endringer i underleverandørkjeden
- Endringer i risikoprofil

6.3 Hendelseshåndtering

Ved hendelser hos leverandør:

1. Leverandør varsler oss iht. avtalt prosedyre
2. Vi vurderer konsekvens for Drop-tjenesten
3. Vi aktiverer interne prosedyrer ved behov (se `hendelseshaandtering.md`)
4. Vi rapporterer til Finanstilsynet ved vesentlig IKT-hendelse
5. Hendelsen dokumenteres og følges opp

6.4 Leverandørmøter

Kritikalitet	Frekvens	Agenda
Kritisk	Kvartalsvis (min.)	SLA-gjennomgang, sikkerhetsoppdatering, roadmap, hendelser
Viktig	Halvårlig	SLA-gjennomgang, sikkerhetsoppdatering
Standard	Årlig	Generell gjennomgang

---

7. Exit-strategi

7.1 Prinsipper

For alle utkontrakterte tjenester av klasse Kritisk og Viktig skal det foreligge en dokumentert exit-strategi. Exit-strategien sikrer at tjenesten kan overføres til alternativ leverandør eller tas tilbake internt uten uakseptabel forstyrrelse.

7.2 Exit-plan per kritisk tjeneste

Hver exit-plan inneholder:

- **Trigger-hendelser:** Scenarioer som utløser exit (oppsigelse, mislighold, konkurs, regulatorisk pålegg)
- **Alternativ leverandør:** Identifisert og prekvalifisert alternativ
- **Migrasjonsprosedyre:** Steg-for-steg-plan for overføring
- **Tidsramme:** Estimert tid for komplett migrasjon
- **Ressursbehov:** Personell, teknologi, budsjett
- **Dataoverføring:** Prosedyre for sikker overføring/sletting av data
- **Testprosedyre:** Verifisering av tjenestekvalitet hos ny leverandør
- **Kommunikasjon:** Plan for informasjon til brukere og myndigheter

7.3 Spesifikke exit-strategier

Open Banking-leverandør (Kritisk)

- Sekundær leverandør identifisert og API-integrert (varm standby)
- Switchover testbar innen 4 timer
- Full migrasjon innen 30 dager
- Data: Transaksjonshistorikk overføres eller gjenopprettes fra egen database

Skyinfrastruktur (Kritisk)

- Infrastruktur-som-kode (IaC) sikrer reproduserbarhet
- Sekundær region hos alternativ leverandør prekonfigurert
- Database-replikering til alternativ plattform
- Full migrasjon innen 14 dager

BankID (Kritisk)

- Ingen realistisk alternativ autentiseringsløsning i Norge
- Exit-strategi: Degradert modus med midlertidig autentisering i begrenset periode
- Avhengigheten aksepteres som nasjonal infrastrukturrisiko

7.4 Testing av exit-strategi

- Tabletop-gjennomgang årlig for kritiske leverandører
- Teknisk exit-test (failover) halvårlig for leverandører med varm standby

- Dokumentasjon av testresultater og forbedringspunkter

---

8. Finanstilsynet — varsling og rapportering

8.1 Varsling

I henhold til Finanstilsynets retningslinjer og DORA varsles Finanstilsynet:

- **Før inngåelse:** Av avtaler om utkontraktering av kritiske IKT-tjenester
- **Ved vesentlige endringer:** I eksisterende avtaler for kritiske tjenester
- **Ved hendelser:** Hos leverandører som påvirker vår tjenesteleveranse vesentlig

8.2 Informasjon til Finanstilsynet

Varsling inneholder:

- Leverandørens identitet
- Tjenestens art og kritikalitet
- Risikovurdering
- Kontraktuelle beskyttelser
- Exit-strategi
- Konsekvenser for tjenesteleveranse

8.3 Register tilgjengelig for tilsyn

Vi opprettholder et oppdatert register over all utkontraktering som gjøres tilgjengelig for Finanstilsynet på forespørsel, jf. DORA art. 28(3).

---

9. Konsentrasjonsrisiko — DORA art. 29(2)

9.1 Vurdering

Vi vurderer regelmessig konsentrasjonsrisiko, inkludert:

- Avhengighet til enkelteleverandører for kritiske tjenester
- Geografisk konsentrasjon (alle tjenester i samme region/land)
- Teknologisk konsentrasjon (alle tjenester på samme plattform)
- Sektorkonsentrasjon (leverandørers avhengighet av samme bransje)

9.2 Mitigering

- Sekundære leverandører for kritiske tjenester
- Geografisk diversifisering av infrastruktur (flere regioner/soner)
- Unngå kritisk avhengighet til én enkelt skyplattform der mulig
- Regelmessig vurdering av leverandørmarkedet

---

10. Internkontroll

10.1 Roller og ansvar

Rolle	Ansvar
Styret	Godkjenning av policy og kritiske avtaler
Daglig leder	Overordnet ansvar for utkontraktering, godkjenning av viktige avtaler
CISO	Sikkerhetsvurdering, due diligence, løpende overvåking
Compliance-ansvarlig	Regulatorisk samsvar, Finanstilsynet-rapportering
Innkjøpsansvarlig	Kontraktshåndtering, leverandørkontakt
Driftsteam	Operasjonell oppfølging, SLA-overvåking

10.2 Første linje — operasjonell styring

- Daglig overvåking av tjenestekvalitet
- Oppfølging av SLA-etterlevelse
- Kontaktpunkt mot leverandør

10.3 Andre linje — kontroll og risikostyring

- Periodisk risikovurdering
- Due diligence-gjennomføring
- Policy-etterlevelse

10.4 Tredje linje — uavhengig kontroll

- Årlig gjennomgang av utkontrakteringspolicyen
- Stikkprøvekontroll av leverandøravtaler
- Rapportering til styret

---

11. Revisjon og oppdatering

11.1 Gjennomgang

- **Årlig:** Full gjennomgang av policyen
- **Ved nye kritiske avtaler:** Vurdering av behov for policyendringer
- **Ved regulatoriske endringer:** Oppdatering iht. nye krav
- **Etter hendelser:** Revisjon basert på hendelser hos leverandører

11.2 Versjonshistorikk

Versjon	Dato	Endring	Godkjent av
1.0	12.02.2026	Opprinnelig dokument	_____

Vedlegg

Vedlegg A: Register over utkontrakterte tjenester

Separat dokument — vedlikeholdes av CISO.

Vedlegg B: Mal for due diligence-rapport

Separat dokument — tilgjengelig ved forespørsel.

Vedlegg C: Mal for exit-plan

Separat dokument — tilgjengelig ved forespørsel.

Vedlegg D: Sjekkliste for kontraktskrav (DORA art. 30)

Separat dokument — brukes ved alle nye avtaler.

Denne utkontrakteringspolicyen er eid av CISO og godkjent av styret i ALAI Holding AS.

Revision #5
Created 2026-02-18 08:44:36 UTC by John
Updated 2026-05-25 07:24:15 UTC by John