

Policy for utkontraktering

Dokumentet beskriver sentrale overordnede prinsipper knyttet til utkontraktering i SpareBank 1 SMN konsern

Innholdsansvarlig	Fagansvarlig Utkontraktering
Innholdseier	Konserndirektør Teknologi og Utvikling
Informasjonsklassifisering	Intern
Gjelder for	SpareBank 1 SMN konsern
Godkjenningsnivå	Styret
Sist godkjent	Velg dato
Sist revidert	29.01.2025
Krav om styregodkjenning i datterselskaper?	Ja

Innhold

1.	FORMÅL	3
2.	MÅLGRUPPE	3
3.	DEFINISJONER	3
4.	STYRENDE PRINSIPPER OG KRAV	3
5.	ORGANISERING OG ANSVAR	5
6.	FORVALTNING OG REVISJON AV POLICY	6
7.	HÅNDTERING AV AVVIK	6
8.	REFERANSER OG RELEVANTE KOBLINGER (KAN OPPDATERES UTEN NY GODKJENNING) FEIL! BOKMERKE ER IKKE DEFINERT.	

1. FORMÅL

Policy for utkontraktering angir rammebetingelser for all utkontraktering som SpareBank 1 SMN (SMN) foretar, herunder IT tjenester og avtaler om bruk av skytjenester.

Formålet med policyen er å angi overordnede prinsipper og føringer knyttet til utkontraktering og å understøtte styret og konsernledelsens krav til virksomhetsstyring i konsernet, i tillegg til å ivareta regulatoriske krav.

2. MÅLGRUPPE

Policy for utkontraktering i SMN gjelder for hele SMN konsernet, men særlig medarbeidere som er eier av eller forvalter utkontraktet virksomhet.

3. DEFINISJONER

Utkontraktering er å benytte oppdragstakere til å få utført arbeidsoppgaver, som alternativt kunne vært utført av virksomheten selv. Det er utkontraktering når SMN velger å la en annen juridisk enhet utføre arbeidsoppgaver på vegne av seg. Dette gjelder også for selskap i samme konsern eller konsernlignende grupper som oppdragstaker. Det må vurderes om en utkontraktering er «kritisk eller viktig» eller av betydning.

IKT Tjenester; betyr digitale og datatjenester levert gjennom IKT-systemer til en eller flere interne eller eksterne brukere på en kontinuerlig basis, inkludert maskinvare som en tjeneste og maskinvaretjenester som inkluderer levering av teknisk støtte via programvare- eller fastvareoppdateringer av maskinvareleverandøren, unntatt tradisjonelle analoge telefontjenester..

Skytjenester IT systemer eller programvare som tilbys av eksterne leverandører for behandling eller lagring av data.

Risikoeier er en person, eller en rolle som har ansvaret for å identifisere, evaluere, overvåke og håndtere en spesifikk risiko eller risikokategori, til eksempel en produkteier.

Due Diligence eller selskapsgjennomgang, er en arbeidsprosess og metode for å samle inn og analysere informasjon om et selskap ved utkontraktering. Prosessen brukes som et beslutningsgrunnlag for å avgjøre om et selskap er egnet som leverandør av utkontrakterte tjenester til konsernet.

For IKT tjenester er det sentralt å skille mellom de som er vanlige (av betydning) og IKT tjenester som er kritisk / viktige.

4. STYRENDE PRINSIPPER OG KRAV

Her angis forventninger og krav til styring av utkontraktering i SMN konsernet som er basert på Finanstilsynets veiledning for utkontraktering¹, EBA guidelines² og andre regulatoriske krav. Retningslinjene forventes fortsatt å bli gjeldende også etter innføring av DORA.

4.1 Overordnede prinsipper ved utkontraktering av virksomhet

- Konsernet og konsernselskapene er ansvarlig for alle tjenester, aktiviteter og ledelsesbeslutninger, samt regulatoriske forpliktelser, risiko og ansvar overfor kundene ved enhver utkontraktering.
- All utkontraktering skal ivareta de krav konsernet og konsernselskapene stiller seg selv gjennom styrende prinsipper og dokumentasjon gjennom hele utkontrakterings varighet. Dette inkluderer krav til informasjonssikkerhet, risikostyring, beredskapsplanverk og personvern.
- All utkontraktering skal registreres i en oversikt over konsernets utkontrakteringer, uavhengig av når avtalen ble inngått, med de krav som følger av forskrift om meldeplikt.
- Datterselskaper og må sikre at krav til risiko- og leverandørvurderinger er i henhold til regelverk og interne retningslinjer ivaretas, og gjennomføre dette i sitt rammeverk.

¹ Finanstilsynets rundskriv 7/21 «Veiledning om utkontraktering»

² EBA Guidelines on outsourcing arrangement» September 2019

- Det må foreligge tilstrekkelige ressurser til å forvalte og følge opp utkontraktinger samt sikre kontinuitet dersom utkontrakterte oppgaver må flyttes eller tas tilbake.
- Konsernets beredskapsplaner skal omfatte utkontraktert virksomhet. Beredskapsplanen skal sikre at virksomheten drives i samsvar med plikter som følger av lov, og avtaler dersom det oppstår uønskede hendelser, og planer for å håndtere kriser. Planverket skal også inkludere kontinuitetsplan ved terminering av avtale.

4.2 Virksomhet som kan utkontrakteres

SMN kan kun utkontraktere tjenester som anses forsvarlig å utkontraktere som betyr:

- Forbud mot utkontrakting av kjerneoppgaver knyttet til konsesjonsbelagt virksomhet
- Aktiviteter som utgjør en nødvendig og integrert del av konsesjonsbelagt virksomhet, skal ikke utkontrakteres.
- Virksomheten må være forsvarlig å utkontraktere basert på en konkret vurdering av risiko for selskapet og konsernet.
- Utkontrakting må ikke stride med konsernets eller konsernselskapenes strategi.

4.3 Risikovurdering ved utkontrakting

Før avtale om utkontrakting inngås, må det sikres en due diligence av leverandør og gjennomføres risikovurdering³ av system og av leverandør, som må dokumenters, men også bygge på et proporsjonalitetsprinsipp. Proporsjonalitetsprinsippet betyr at det skal tas hensyn til foretakets størrelse og risikoprofil, samt arten, omfanget og kompleksiteten i foretakets tjenester, aktiviteter og drift⁴.

4.4 Metode for fastsetting av kritikalitet

Kartlegging av IKT tjeneste som støtter «kritisk eller viktige funksjoner» er viktig i arbeidet med implementeringen av DORA. For at en funksjon skal være kritisk eller viktig, må en svikt i leveransen ha vesentlig («material») påvirkning på et av følgende alternativ:

- Den økonomiske ytelsen til finansinstitusjonen
- Kvaliteten på dens tjenester og aktiviteter
- Dens evne til å overholde regulatoriske forpliktelser

4.5 Skriftlig utkontrakteringsavtale

Det skal foreligge en skriftlig avtale ved utkontrakting. Avtalen sikrer at utkontraktert virksomhet til enhver tid drives i samsvar med gjeldende regelverk og internt rammeverk. Ved bruk av Sparebank1 Utvikling sine standard avtalemaler og -vedlegg sikrer man at kravene til utkontrakteringsavtalen ivaretas. Der dette ikke er mulig, eller må gjøres avvik, må det sikres at avtalen inneholder minimumskrav i henhold til gjeldende regelverk og SpareBank 1 SMN sine retningslinjer. En skriftlig avtale sikrer kontroll av risikovurderingen og forvaltning av avtalen. I tillegg muliggjør den rett til innsyn, kontroll og revisjon av den utkontrakterte virksomhet for SpareBank 1 SMN og tilsynsmyndigheten.

4.6 Samlet oversikt over avtaler om utkontrakting

SpareBank 1 SMN skal til enhver tid ha oversikt over avtaler om utkontrakting som er i henhold til regelverket for utkontrakting. Oversikten skal omfatte alle avtaler som innebærer utkontrakting av virksomhet, herunder også avtaler som ikke er meldepliktige til Finanstilsynet.

4.7 Krav til meldeplikt til Finanstilsynet og styrebehandling

³ Se policy og standard for operasjonell risiko, i tillegg til EBA guidelines punkt 12 flg.

⁴ Forordning om digital operasjonell motstandsdyktighet i finanssektoren (DORA) - Finanstilsynet.no

SpareBank 1 SMN konsernet må påse at den lovregulerte meldeplikten til Finanstilsynet overholdes. Selskap i konsernet som omfattes av finanstilsynsloven⁵ skal melde fra til Finanstilsynet ved inngåelse av nye avtaler om utkontraktering som er «viktig eller kritisk» for konsernet. Tilsvarende gjelder ved senere endring i eksisterende avtaler om utkontraktering, herunder endring i kritikalitet og bytte av oppdragstaker/leverandør gitt at endringen medfører at avtaleforholdet vurderes som «viktig eller kritisk» for konsernet. Endringsavtaler skal lagres sammen med hovedavtalen.

Melding til Finanstilsynet skal sendes minst 60 dager før iverksettelsen av avtalen, ved endring, eller ved bytte av oppdragstaker/leverandør og må innfri de krav som følger av forskrift om meldeplikt⁶ ved utkontraktering av virksomhet.

Inngåelse av nye eller endring i eksisterende meldepliktige utkontrakteringer skal styrebehandles løpende. Utkontrakteringer som vurderes til å ikke være «viktig eller kritisk», men vurderes å være «av betydning» for konsernet, skal etter IKT-forskriften § 2, 4 ledd, behandles av styret. Slike utkontrakteringer kan styrebehandles etterskuddsvis, halvårlig av styret.

4.8 Oppfølging av utkontraktert virksomhet

Utkontraktert virksomhet skal innlemmes i selskapets rammeverk for risikostyring og internkontroll på samme måte som annen virksomhet. Dette betyr at:

- Det må være tilstrekkelig ressurser til å forvalte og følge opp utkontraktering og sikre kontinuitet om utkontrakterte oppgaver må flyttes eller tas tilbake.
- Det må foreligge et risikobasert regime for regelmessig oppfølging og rapportering for å sikre kontinuerlig kontroll med den utkontrakterte virksomheten og pålagt varsling til myndigheter. Dokumentasjon for gjennomført oppfølging skal lagres, også der det ikke er gjort funn som foranlediger oppfølgingstiltak.
- Det må utarbeides en ny oppdatert risikovurdering av tjenesten og / eller leverandør ved vesentlig endring i utkontraktert tjeneste eller ved leverandørendring, herunder finansielle, strukturelle eller endring i eierskap. Tilsvarende må det foretas oppdaterte vurderinger ved endringer i regulatoriske krav eller ved vesentlige endringer i konsernets eller selskapenes styrende prinsipper som omfatter den utkontrakterte tjenesten.

5. ORGANISERING OG ANSVAR

Styret har det overordnede ansvar for at SMN etterlever utkontrakteringsregleverket.

Styret skal:

- Fastsetter prinsipper og overordnet strategi for iverksetting av, kontroll og overvåking av utkontraktering.
- Fastsetter metoden som er bestemmende for hvilke IKT-tjenester som understøtter kritiske eller viktige funksjoner.
- Påser at det er en klar tildeling av internt ansvar for godkjenning, forvaltning, kontroll og dokumentasjon med hensyn til utkontraktering.
- Styrebehandle utkontrakteringer i tråd med kravene til meldeplikt og styrebehandling
- Vedta policy for utkontraktering

Konsernsjef har det øverste ansvaret for at regelverket og interne retningslinjer knyttet til utkontraktering etterleves. Konsernsjef skal:

- Påse at avtaler som utformes ved utkontraktering ivaretar kvalitet, rett til oppsigelse, uinnskrenket tilgang, inspeksjon eller revisjon og tilfredsstillende relevante lov – og forskriftskrav.
- Påse at aktuelle nye og endrede utkontrakteringsavtaler meldes til Finanstilsynet i tråd med gjeldende forskrift om meldeplikt.

⁵ Gjelder ikke selskaper som er unntatt fra meldeplikt i henhold til forskrift om unntak fra meldeplikt

⁶ Forskrift om meldeplikt ved utkontraktering av virksomhet mv - Lovdata

- Påse at foretaket har tilstrekkelig gjenværende kompetanse til å følge opp den utkontrakterte tjenesten og leverandøren.
- Iverksette nødvendige tiltak dersom tilstrekkelig leveranse skulle utebli eller utkontrakteringsforholdet ikke fungerer i samsvar med inngåtte avtaler.

Konsernsjef har delegert sine oppgaver for virksomheten til Konserndirektør Teknologi og Utvikling i rollen som strategisk utkontrakteringsansvarlig.

Øvrige Konserndirektører og Administrerende direktører har ansvar for utkontraktering, og er eier av avtaler innenfor sitt område. Som avtaleier har man et operasjonelt ansvar for oppfølging av leverandører og forvaltning av avtaler.

Konserndirektører og Administrerende direktører kan delegere det operasjonelle ansvaret.

6. FORVALTNING OG REVISJON AV POLICY

Policyen skal revideres ved behov og godkjennes av styret ved endringer. Policyen skal uansett godkjennes av styret hvert tredje år.

7. HÅNDTERING AV AVVIK

Avvik fra prinsipper og krav i denne policy skal betraktes som en uønsket hendelse og registreres som et brudd på regler og retningslinjer etter konsernselskapets rutine for oppfølging av avvik⁷.

8. ENDRINGSLOGG

Nedenfor vises logg over når policy er endret og/eller revidert, i tillegg til godkjent av styret.

Status	Versjon	Dato
Policy godkjent i konsernets styre	1.0	
Revisjon under arbeid	1.9	November 2023
Oppdatert policy fremsendt for godkjenning i styret	1.99	6.12.2023
Policy godkjent i konsernets styre	2.0	14.12.2023
Oppdatert policy fremsendt for godkjenning i styret	2.99	11.2.2025
Policy godkjent i konsernets styre	3.0	11.2.2025

⁷ Hendelsesregistrering i Betr