UDKAST

Ejerstrategi

Vedrørende [Navn] A/S

KØBENHAVN
KALVEBOD BRYGGE 32
DK-1560 KØBENHAVN V

AARHUS
EUROPAPLADS 8
DK-8000 AARHUS C

NUUK
ISSORTARFIMMUT 7
GL-3900 NUUK

T +45 33 15 20 10
@ MAIL@POULSCHMITH.DK
W WWW.POULSCHMITH.DK

CVR: 64 95 28 11
SÅDAN HÅNDTERER VI DINE PERSONOPLYSNINGER
POULSCHMITH.DK/PERSONOPLYSNINGER

1. INDLEDNING

1.1 Denne ejerstrategi fastlægger de overordnede mål, rammer og principper for ejerkommunernes (herefter "Kommunernes") ejerskab af [Navn] A/S (herefter "Selskabet").

1.2 Strategien skal:

1. tydeliggøre Kommunernes forventninger til Selskabets formål, opgaveløsning og udvikling,
2. sikre sammenhæng mellem Selskabets virksomhed og Kommunernes mål, herunder de mål og ambitioner, der følger af aftalen om kommunernes økonomi for 2026 på it-området, herunder navnlig styrket cybersikkerhed samt forbedret rekrutteringsgrundlag, øget omkostningseffektivitet og udnyttelse af økonomiske skalafordele i Kommunernes it-drift og
3. danne grundlag for en klar og professionel ejerstyring.

1.3 Ejerstrategien supplerer, men erstatter ikke, Selskabets vedtægter, ejeraftale, aftaler indgået mellem Kommunerne og Selskabet samt gældende lovgivning.

2. EJERKREDS OG EJERROLLE

2.1 Selskabet er etableret som et fælleskommunalt redskab til at styrke kvalitet, robusthed og omkostningseffektivitet i Kommunernes it-drift og relaterede ydelser.

2.2 Kommunerne ønsker, at Selskabet:

- understøtter Kommunernes fælles interesser og mål på it-området og
- agerer langsigtet, stabilt og økonomisk ansvarligt.

3. STRATEGISKE MÅL OG PEJLEMÆRKER

3.1 Kommunerne opstiller følgende overordnede strategiske mål for Selskabets virksomhed:

1. Styrket cybersikkerhed

Selskabet skal bidrage til, at Kommunerne opnår et højt og dokumenterbart niveau for cybersikkerhed, herunder ved følgende:

- implementering og løbende vedligeholdelse af relevante sikkerhedsstandarder og -kontroller, med udgangspunkt i regelmæssigt opdateret risikoanalyser
- etablering af fælles sikkerhedsarkitektur, sikkerhedsoperationer (SOC) og beredskab på tværs af Kommunerne i samarbejdet og
- systematisk uddannelse og træning af it-personale og øvrige medarbejdere.

Bestyrelsen skal fastsætte konkrete mål og nøgletal for cybersikkerhed, herunder modenhedsniveau, hændelsesrespons og efterlevelse af standarder.

Bestyrelsen skal i øvrigt understøtte Kommunernes efterlevelse af forpligtelserne i NIS2-loven[1] ud over at sikre Selskabets egen efterlevelse af NIS2-loven, hvis Selskabet er et selvstændigt NIS2-pligtsubjekt.

2. Forbedret rekrutterings- og kompetencegrundlag

Selskabet skal være en attraktiv arbejdsplads, der kan tiltrække, udvikle og fastholde specialiserede it- og sikkerhedsprofiler, som det kan være vanskeligt for den enkelte Kommune at rekruttere og fastholde alene. Selskabet skal:

- udvikle og vedligeholde en samlet kompetencestrategi, særligt for cybersikkerhed, cloud, arkitektur og drift,
- sørge for fælles kompetenceudviklingsforløb og faglige miljøer for medarbejdere og
- understøtte talentudvikling og karriereveje for medarbejdere.

3. Øget omkostningseffektivitet og skalafordele

Selskabet skal inden for rammerne af EU's statsstøtteregler bidrage til at reducere de samlede omkostninger ved Kommunernes it-drift på lang sigt og samtidig skabe bedre kvalitet og robusthed. Dette omfatter blandt andet følgende:

- konsolidering af infrastruktur og standardisering af løsninger, hvor det er økonomisk og driftsmæssigt fordelagtigt og
- udnyttelse af fælles indkøb og forhandlingskraft.

[1] Lov nr. 434 af 6. maj 2025 – Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

Selskabet skal årligt dokumentere udviklingen i aftalte nøgletal der kan vedrøre enheds-omkostninger, sikkerhed, kvalitet og tilgængelighed for centrale it-ydelser.

4. Kvalitet, stabilitet og brugertilfredshed

Selskabet skal levere stabil drift og høj servicekvalitet. Selskabet skal til brug herfor sikre, at der fastsættes:

- servicemål og SLA'er for centrale ydelser (f.eks. oppetid, svartider, fejlrettelse m.v.) og
- klare procedurer for håndtering af fejl, afbrydelser og større hændelser.

4. STYRING OG GOVERNANCE

4.1 Kommunerne udøver deres ejerstyring gennem følgende:

- Selskabets vedtægter og Kommunernes ejeraftale,
- denne ejerstrategi,
- generalforsamlinger, hvor Selskabets årsrapport, strategi og andre centrale forhold behandles,
- udpegning af bestyrelsesmedlemmerne i Selskabet samt
- ved løbende rapportering til Kommunerne fra Selskabets bestyrelse.

5. ØKONOMI

5.1 Selskabet har ikke et erhvervsøkonomisk formål.

5.2 I det omfang Selskabet udøver økonomisk aktivitet omfattet af EU's statsstøtteregler, skal bestyrelsen sikre, at det sker i overensstemmelse med EU's statsstøtteregler. Dette kan efter omstændighederne kræve en opdeling af aktiviteter i henholdsvis økonomiske aktiviteter og ikke-økonomiske aktiviteter og en regnskabsmæssig adskillelse af disse to typer aktiviteter.

5.3 Bestyrelsen skal i øvrigt sikre, at Selskabets priser og betalingsmodeller er gennemsigtige, saglige og objektive.

6. RISIKOSTYRING

6.1 Generelt

6.1.1 Selskabet skal have en samlet og systematisk tilgang til risikostyring, særligt med fokus på:

- cybersikkerheds- og driftsrisici
- leverandør- og kontraktrisici
- økonomiske og finansielle risici, herunder investeringsniveau og likviditet
- overholdelse af databeskyttelsesregler og øvrig relevant regulering.

6.1.2 Bestyrelsen skal mindst én gang årligt godkende en samlet risikorapport og risikoprofil for Selskabet og sikre passende kontroller og beredskabsplaner.

6.2 Cybersikkerhed som særskilt fokusområde

6.2.1 Cybersikkerhed er et strategisk kerneområde for Selskabet. Kommunerne forventer, at Selskabet:

- arbejder efter anerkendte standarder og frameworks for informationssikkerhed,
- har en tydelig governance for informationssikkerhed, herunder udpegning af CISO eller tilsvarende funktion,
- etablerer og vedligeholder processer relateret til sikkerhedshændelser, inkl. rapportering til relevante myndigheder og Kommunerne og
- sikrer, at it-systemer og -infrastruktur understøtter Kommunernes lovpligtige krav til sikkerhed og databeskyttelse.

7. ORGANISATION, KOMPETENCER OG REKRUTTERING

7.1 Selskabet skal opbygges og udvikles som en professionel, innovativ og attraktiv arbejdsplads. Kommunerne forventer, at Selskabet:

- arbejder strategisk med rekruttering og fastholdelse af nøglekompetencer,
- prioriterer efteruddannelse og certificeringer inden for især cybersikkerhed, cloud, netværk, arkitektur og projektledelse,
- understøtter et stærkt fagligt miljø og
- har fokus på ordentlige arbejdsvilkår, trivsel og et godt arbejdsmiljø.

7.2 Der bør udvikles en flerårig kompetence- og rekrutteringsplan, som årligt forelægges og drøftes i bestyrelsen.

8. REVISION AF EJERSTRATEGIEN

8.1 Ejerstrategien revurderes mindst hvert fjerde år eller når væsentlige ændringer i rammebetingelser, lovgivning, teknologi eller Kommunernes behov tilsiger det.

8.2 Ændringer i ejerstrategien skal godkendes af Kommunerne med [2/3 eller 3/4 flertal].