

Bilag til SSA-D

Bilag til Driftsavtalen

Statens standardavtale om levering driftstjenester til IT-løsninger

Innhold:

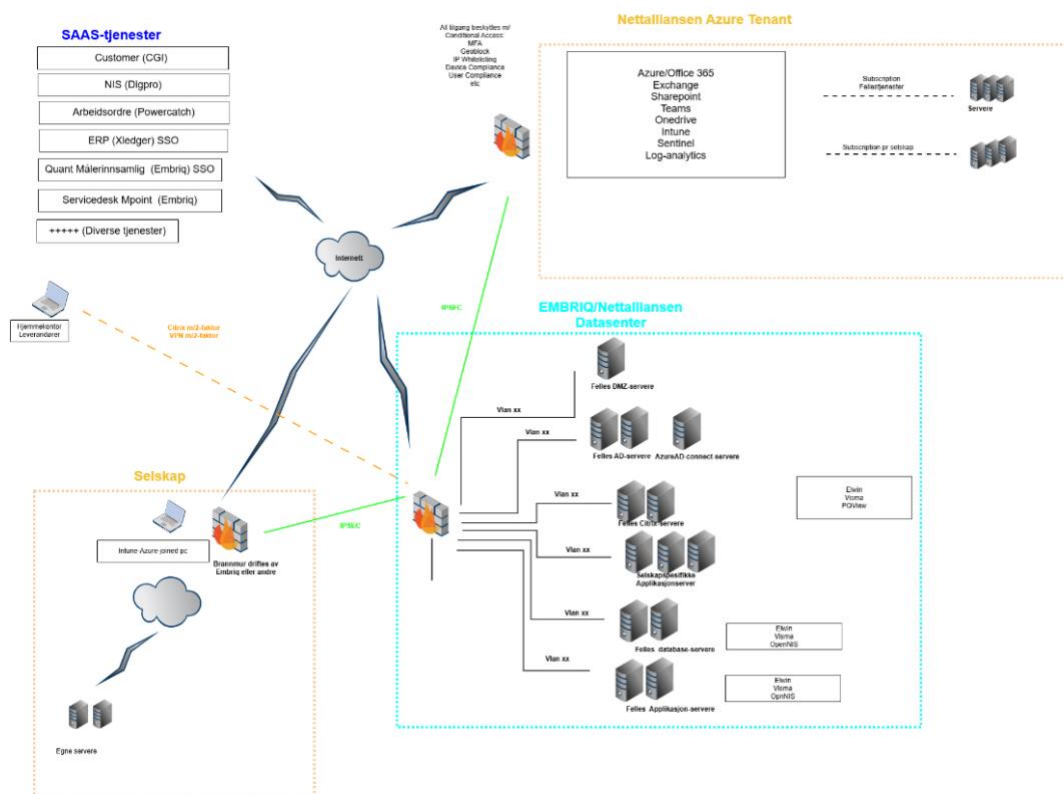
1. Avtalens punkt 1.1 Avtalens omfang.....	3
1.1. Dagens driftsmiljø og driftstjenester.....	3
1.2. Fremtidig driftsmiljø og driftstjenester.....	5
1.3. Gjennomføring av driftsovertakelsen	6
1.4. Kravspesifikasjon.....	7
2. Avtalens punkt 2.4.7 Planer og øvelser for beredskap og katastrofer.....	18
3. Avtalens punkt 2.4.9 Nye versjoner av programvare	18
4. Avtalens punkt 2.4.10 Livssyklusforvaltning – tidsmessighet.....	19
5. Avtalens punkt 2.5.1 Generelt om avslutning av Avtalen	19
6. Avtalens punkt 5.1.1 Leverandørens ansvar for leveransen - generelt	19
7. Avtalens punkt 7.1 Eksterne rettslige krav og tiltak generelt.....	20
8. Avtalens punkt 7.2.1 Generelt om informasjonssikkerhet.....	20
9. Avtalens punkt 7.2.2 Leverandørens plikt til å holde Kundens data atskilt.....	21
10. Avtalens punkt 8.3 Rettigheter til data	21

1. Avtalens punkt 1.1 Avtalens omfang

Dette punktet beskriver avtalens omfang: dagens driftsmiljø og driftstjenester, Kundens målilde for fremtidig driftsmiljø, hvordan driftsovertakelsen skal gjennomføres, og til slutt en tabell med Kundens nummererte krav til leveransen.

1.1. Dagens driftsmiljø og driftstjenester

Nettalliansen AS og Deltakende Selskap har siden 2017 kjøpt IT-driftstjenester fra dagens leverandør. Gjeldende driftsavtale utløper i februar 2027. Nedenfor oppsummeres omfanget av dagens drift og driftstjenester på et overordnet nivå, som bakgrunn for denne anskaffelsen. Teknisk beskrivelse av programvare, systemlandskap og arkitektur som skal driftes, fremgår av bilag 3.

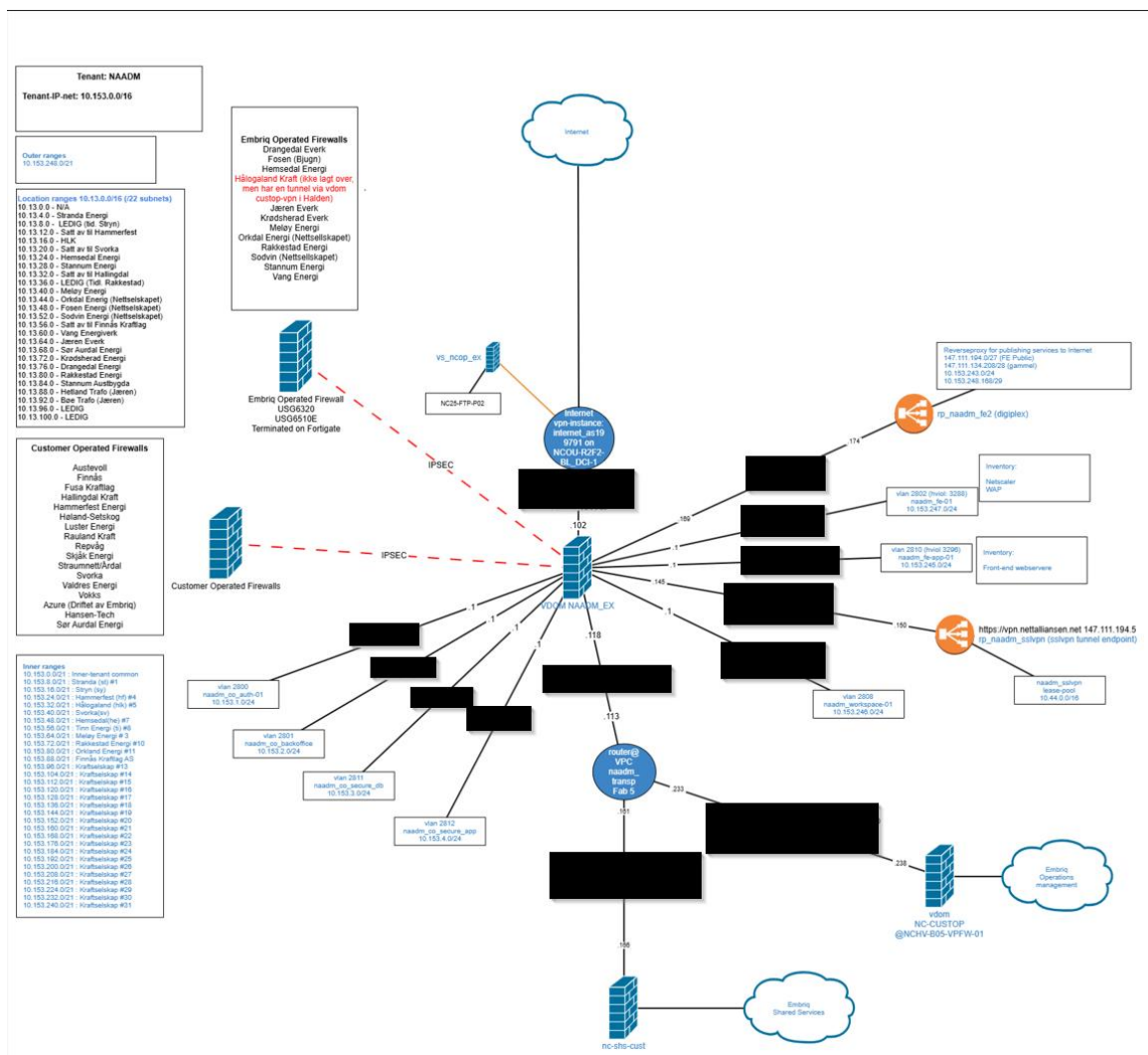


Figur 1: Forenklet arkitekturskisse av dagens driftsmiljø – brukertilgang til SaaS-tjenester, Nettalliansens Azure-tenant og Embriq/Nettalliansens datasenter (kilde: NA-Systemdokumentasjon, kap. 3 «Systembeskrivelse»).

- **Plattform og arbeidsflate:** Standard kontorstøtteplattform er Microsoft 365. Brukere opprettes i Nettalliansens lokale AD (NA-ADM) og synkroniseres til Nettalliansens Azure AD (NA-AAD).
- **Brukeradministrasjon og tilgangsstyring:** Bestilling av nye brukere, endringer og avslutning av brukerkonti (inkludert eksterne) skjer via bestillingsskjema i saksbehandlingsverktøyet Mpoint (ServiceNow), og krever godkjenning fra autorisert bestiller i det enkelte Deltakende Selskap. Tilganger styres via AD-grupper.
- **Autentisering og tilgangskontroll:** Passordpolicy krever i dag minimum 14 tegn, bytte

hver 90. dag og kompleksitetskrav. Multifaktorautentisering (MFA) håndheves gjennom Conditional Access, der kjente enheter/lokasjoner gir redusert friksjon mens ukjente lokasjoner (f.eks. hjemmekontor) krever MFA. Administrative tilganger beskyttes med Privileged Identity Management (PIM). Tilgang til on-premises-løsninger (Citrix/VPN) skjer via brannmur med topartsautentisering.

- **Servicedesk og support:** Leverandørens servicedesk har åpningstid 07:00–17:00 og mottar henvendelser via Mpoint, telefon og e-post. Feil kategoriseres med tilhørende responstider og eskaleringsrutiner, inkludert egen rutine for Major Incident. Nettalliansen sentralt og Deltakende Selskap har tilgang til dashbord med sakstatus og SLA-rapportering, samt en månedlig rapport med oppsummering av hendelser, lisensforbruk og planlagte aktiviteter.
- **Sikkerhetskopiering:** Det benyttes i dag tre backupløsninger: én for brukernes M365-data (Exchange, Teams, OneDrive, SharePoint), én for filer/servere on-premises (daglig snapshot, 90 dagers lagring) og én for SQL-servere (14 dagers lagring, med loggbackup flere ganger i døgnet).
- **Sikkerhet, logging og overvåkning:** Det mottas trusselvarsler fra KraftCERT og egen CTI/SOC-funksjon, med fortløpende sårbarhetshåndtering. Logger fra Office 365 (Exchange, SharePoint, Azure AD) lagres i 30 dager; loggingsnivå on-premises varierer noe mellom løsninger. Dagens leverandør er sertifisert iht. ISO 9001, ISO 14001, ISO 27001 og SOC 2.
- **Personvern og sletterutiner:** Ved avslutning av brukerforhold deaktiveres og flyttes brukeren til egen enhet for «sluttede brukere»; kontoer og tilhørende data (e-post, OneDrive, SharePoint) slettes normalt etter 30 dager. Data på fysiske disk destrueres av sertifiserte tredjeparter med utstedelse av slettesertifikat.
- **Nettverk og tredjepartsløsninger:** Dagens leverandør drifter WAN/LAN/WLAN og brannmur. Digitale verdikjeder omfatter blant annet løsninger for utskrift, «privilege elevation and delegation management» (PEDM) / patch management for tredjepartsprogramvare, og cloud backup.



Figur 2: Dagens nettverkstopologi, herunder soner, brannmurer, VLAN-oppsett og IP-adresseplan for NA-ADM (kilde: NA-Systemdokumentasjon, kap. 17 «Nettverk og prosesslogikk»).

- **Governance og samarbeid:** Det gjennomføres månedlige driftsmøter og brukerforum, kvartalsvise møter med Deltakende Selskap ved behov, og halvårlige møter på ledernivå mellom Nettalliansen AS og leverandøren.

Oppsummeringen ovenfor er på overordnet nivå. Leverandøren oppfordres til å gjøre seg kjent med bilag 3 for en detaljert forståelse av dagens driftsmiljø før tilbud utarbeides.

1.2. Fremtidig driftsmiljø og driftstjenester

Nettalliansen skal gjennom denne anskaffelsen transformere dagens driftsmiljø til en fremtidsrettet, sikker og brukervennlig driftsplattform for alle Deltakende Selskap. Følgende forhold er sentrale drivere for endringsbehovet:

- **Sikkerhetskrav og regulatorisk etterlevelse:** Forventede og innførte krav i NIS2-regelverket (risikostyring, hendelseshåndtering, varsling og sikkerhet i leverandørkjeden) samt videreført og styrket etterlevelse av personopplysningsloven/GDPR, stiller høyere krav til Leverandørens styringssystem for informasjonssikkerhet, logging/overvåkning og hendelseshåndtering enn i dagens avtale. For Deltakende Selskap som er omfattet av kraftforsyningsberedskapsforskriften, må løsningen også understøtte gjeldende beredskapskrav.
- **Brukervennlighet og moderne arbeidsflate:** Sluttbrukerne skal oppleve en enklere og

sikrere hverdag, blant annet gjennom passordløs autentisering (f.eks. FIDO2/Windows Hello for Business), redusert behov for manuelle bestillinger, og en felles, rollebasert portalløsning på tvers av Deltakende Selskap.

- **Standardisering med nødvendig isolasjon:** Plattformen skal standardiseres på tvers av Deltakende Selskap for å redusere kompleksitet og driftskostnader, samtidig som data og tilganger skal kunne isoleres per selskap der det er nødvendig.
- **Skalerbar og fleksibel infrastruktur:** Løsningen skal støtte hybrid bruk av private og offentlige skytjenester, med mekanismer for kostnadskontroll, kapasitetsstyring og fremtidig innovasjon, herunder styrt og transparent bruk av kunstig intelligens.
- **Kontinuerlig sikkerhetsforbedring:** Leverandøren skal bidra til at Nettalliansen til enhver tid har et oppdatert risikobilde, og kan dokumentere etterlevelse overfor tilsynsmyndigheter, revisorer og Kundens eksterne rådgiver for IT-sikkerhet.

Krav til driftsmiljø fremgår av kravtabellen nedenfor. Leverandørens forslag til løsning for å nå målbildet skal beskrives i bilag 2. Det oppfordres til tydelig besvarelse i forhold til eventuelle krav som vil kreve en transformasjon som det ikke anbefales å gjennomføre som del av driftsovertakelsen, men som vil bli implementert gjennom egne transformasjonsbølger i ordinær drift.

1.3. Gjennomføring av driftsovertakelsen

Gjennomføringen følger av Avtalens bestemmelser om etableringsfasen, samt eventuelle utfyllende bestemmelser i bilag 4 (prosjekt- og fremdriftsplan) og bilag 6 (samhandling). Gjennomføringen forutsetter et tett samarbeid mellom flere aktører, med følgende overordnede roller og ansvar:

- **Kunden (Nettalliansen AS):** har det overordnede styringsansvaret for anskaffelsen, og skal koordinere behov og beslutninger på tvers av Deltakende Selskap gjennom hele etableringsfasen.
- **Deltakende Selskap:** skal bidra med lokal tilrettelegging, informasjon om egne fagsystemer og arbeidsprosesser, samt delta i planlegging, pilotering og akseptansetesting av løsningen for eget selskap.
- **Eksisterende driftsleverandør:** skal, i den grad det følger av Kundens avtale med denne, bidra med nødvendig dokumentasjon, tilganger, konfigurasjonsdata og annen informasjon som er nødvendig for en forsvarlig og driftssikker overtakelse. Utstyr som eies av eksisterende driftsleverandør og leies ut til allianseselskaper «as-a-service» kan kjøpes ut etter nærmere avtale.
- **K Kundens eksterne rådgiver for IT-sikkerhet:** skal involveres av Leverandøren i planlegging og gjennomføring av sikkerhetsrelaterte aktiviteter, herunder gjennomgang av sikkerhetsarkitektur og gjennomføring av penetrasjonstesting før og etter idriftsettelse, samt ved vesentlige endringer i driftsmiljøet.
- **Leverandøren:** har det operative ansvaret for å planlegge og gjennomføre overtakelsen, herunder å samordne og koordinere arbeidet mellom de øvrige aktørene, jf. punkt «Avtalens punkt 5.1.1» nedenfor.

Overtakelsen skal gjennomføres uten vesentlig reduksjon i tjenestenivået for Deltakende Selskap. Migreringen skal gjennomføres trinnvis, selskap for selskap, etter en plan som er godkjent av Kunden, med klart definerte akseptanskriterier for hvert trinn. Etter fullført

driftsovertakelse går leveransen over i ordinær drift i henhold til Avtalens bestemmelser, med løpende oppfølging gjennom styrings- og driftsmøter som beskrevet i bilag 6. Nærmere krav til gjennomføringen er konkretisert i kravtabellen nedenfor, kategori «PRO – Organisering og prosjektorganisering».

1.4. Kravspesifikasjon

Tabellen nedenfor angir Kundens nummererte krav til leveransen. Kravene er inndelt i kategorier og prioritert som enten A-krav (bindende minstekrav), eller B-krav (krav som vektlegges positivt ved evalueringen, men som ikke er absolutte. Kravene i denne tabellen utfyller, og skal leses i sammenheng med, beskrivelsen i punkt 1.1–1.3 ovenfor og de øvrige punktene i dette bilag. Merk at ikke alle Deltakende Selskap benytter, eller kommer til å benytte, alle deler av IT driftsløsningen det her stilles krav til. De skal uansett ha mulighet til å tiltre alle tjenestene som omhandles.

Krav-ID benytter følgende prefiks per kategori: GEN = Generelle og overordnede krav, SIK = Sikkerhet, BER = Beredskap og kontinuitet, IAM = Identitets- og tilgangsstyring, PLA = Plattform og arbeidsflate, INF = Infrastruktur, servere og hybrid skyplattform, NET = Nettverk, BAK = Lagring, backup og gjenoppretting, DB = Database, INT = Integrasjoner, SUP = Drift, support og brukerstøtte, RAD = Rådgivning og kommunikasjon, PRO = Organisering og prosjektgjennomføring, KLI= Klima- og miljøhensyn.

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
GEN– Generelle og overordnede krav			
GEN-01	Norsk språk i kommunikasjon	Leverandøren skal benytte norsk språk i all muntlig og skriftlig kommunikasjon med sluttbruker, med mindre annet er avtalt for enkelte fagmiljøer.	A
GEN-02	Geografisk lokalisering av data og leveranse	Leverandøren skal lagre all data innenfor EU/EØS, og utføre hele leveransen (inkludert bruk av underleverandører) innenfor EU/EØS eller NATO-medlemsland.	A
GEN-03	Etterlevelse av lovkrav for databehandling	Leverandøren skal lagre og behandle data i henhold til gjeldende EU- og norsk lovgivning, inkludert GDPR, digitalsikkerhetsoven og kraftberedskapsforskriften, samt fremtidige krav som innføres i avtaleperioden. Leverandøren skal i hele avtaleperioden etterleve relevante lover, forskrifter, direktiver, standarder og bransjekrav, og dokumentere hvilke krav som følges.	A

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
GEN-04	Underleverandører - samme krav som hovedleverandør	Leverandøren skal ha fullt ansvar for hele leveransen, også der deler utføres av underleverandører. Underleverandører skal oppfylle de samme krav til sikkerhet, dokumentasjon, kvalitet og etterlevelse av regelverk som stilles til Leverandøren, og Nettalliansen skal ha oversikt over hvilke underleverandører som benyttes og til hvilke deler av leveransen.	A
GEN-05	Exit og overgang ved kontraktsslutt	Leverandøren skal legge til rette for en strukturert og planlagt overgang ved avslutning av avtalen eller ved overføring av deler av leveransen til ny leverandør. Dette omfatter at Leverandøren, uten unødig forsinkelse, gjør tilgjengelig all relevant dokumentasjon, konfigurasjon, data og logger, og bidrar til nødvendig kunnskapsoverføring, uten at dette går på bekostning av drift, sikkerhet eller tilgjengelighet i overgangsperioden. Kunden/Deltakende Selskap skal ved avtaleoppør ha rett, men ikke plikt, til å kjøpe utstyr som inngår i tjenesten til en pris tilsvarende utstyrets restverdi beregnet lineært over fem (5) år, dog aldri høyere enn markedsverdien for tilsvarende brukt utstyr på kjøpstidspunktet.	A
SIK– Sikkerhet			
SIK-01	Styringssystem, risikostyring og revisjon	Leverandøren skal ha et styringssystem for informasjonssikkerhet (ISMS) i tråd med ISO 27000-serien eller tilsvarende, arbeide systematisk med risikostyring, og selv gjennomføre løpende sikkerhetsrevisjoner, sårbarhetsskanning og sikkerhetstesting av leveransen.	A
SIK-02	Styringssystem, risikostyring og revisjon	Leverandøren skal gi Nettalliansen, NVE eller tredjepart utpekt av Kunden full rett til å gjennomføre egen revisjon av sikkerhetsløsninger, prosedyrer, logger og dokumentasjon, med tilhørende innsyn. Leverandørens kostnader til slik bistand dekkes av Kunden, såfremt det ikke avdekkes avvik i forbindels med revisjonen.	A

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
SIK-03	Styringssystem, risikostyring og revisjon	Leverandøren skal ha en dokumentert policy for sikkerhetsoppdatering (patching) av alle komponenter i leveransen, med risikovurdering, varsling ved planlagte oppdateringer og mulighet for reversering ved behov.	A
SIK-04	Isolasjon av data mellom selskaper, roller og sikkerhetssoner	Leverandøren skal sikre full isolasjon av data mellom deltakende selskaper, roller og sikkerhetssoner. Dette skal ivaretas gjennom logisk og nettverksmessig segmentering, samt tilgangskontroll med prinsippet om minste privilegium.	A
SIK-05	Kryptering av data og kommunikasjon	Alle data som håndteres i plattformen skal være kryptert både i ro og i transitt ved bruk av moderne og anerkjente kryptografiske standarder. Leverandøren skal dokumentere sin løsning for nøkkelhåndtering.	A
SIK-06	Logging, sikkerhetsovervåkning og etterlevelse av sikkerhetsstandarter	Leverandøren skal etablere IDS/IPS, helhetlig logging og kontinuerlig sikkerhetsovervåkning av alle relevante komponenter fra klient til plattform, med automatisk deteksjon, varsling og dokumentert hendelseshåndtering. Nettalliansen skal ved forespørsel gis innsyn i tilgangsløgger. Leverandøren skal kontinuerlig implementere beste praksis innen IKT-sikkerhet og etterleve NSMs grunnprinsipper for IKT-sikkerhet, og oppdatere tiltak i takt med trussel- og regelverksbildet. Ved sikkerhetshendelser skal Leverandøren varsle Nettalliansen uten ugrunnet opphold og med tilstrekkelig informasjon til at Nettalliansen kan ivareta egen varslingsplikt overfor relevante myndigheter, herunder NVE og KraftCERT.	A
SIK-07	Fysisk og logisk sikring av datasentre	Leverandøren skal dokumentere fysisk og logisk sikring av alle datasentre, inkludert adgangskontroll, overvåkning, bakgrunnssjekk av personell, driftssikkerhet og kontroll med fysisk tilgang.	A

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
SIK-08	Sikker sletting av data	Leverandøren skal kunne slette alle data, inkludert replikerte data og backup-data, innen avtalt tidsramme etter forespørsel fra Kunden. Det skal foreligge dokumenterte rutiner og sporbarhet på sletting.	A
SIK-09	AVS / endepunktbeskyttelse	Leverandøren skal levere og forvalte en løsning for beskyttelse av endepunkter (klienter og øvrige relevante enheter) som sikrer effektiv beskyttelse mot skadelig programvare, uautoriserte endringer og kjente trusler, samt støtte sentral administrasjon, oppdatering og overvåkning.	A
SIK-10	Bruk av kunstig intelligens i leveransen	Leverandøren skal sikre at eventuell bruk av kunstig intelligens eller automatiserte beslutnings- og analyseverktøy i leveransen er transparent, dokumentert og i samsvar med gjeldende krav til informasjonssikkerhet, personvern og databehandleransvar, og ikke tas i bruk uten avklaring og godkjenning fra Kunden.	A
SIK-11	Kritikalitetsklassifisering og differensierte krav til tilgjengelighet og gjenoppretting	Leverandøren skal, i samarbeid med Nettalliansen, bidra til å klassifisere systemer og tjenester etter kritikalitet (f.eks. samfunnskritisk, forretningskritisk, øvrig), og tilpasse krav til tilgjengelighet, responstid og gjenopprettingstid (RTO/RPO) differensiert etter denne klassifiseringen, med særlig høye krav til de mest kritiske systemene.	A
BER– Beredskap og kontinuitet			
BER-01	Beredskap og krisehåndteringsevne	Leverandøren skal ha beredskaps- og katastrofeplaner for leveransen og bidra til Nettalliansens egne beredskapsøvelser. Nettalliansen skal ha tilgang på kritisk personell og kompetanse hos Leverandøren i ekstraordinære situasjoner, med definert reaksjonstid.	A
IAM– Identitets- og tilgangsstyring			

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
IAM-01	Identitets- og tilgangsstyring (AD/Entra ID og SSO)	Leverandøren skal etablere og forvalte en sentral identitets- og tilgangsstyringsløsning basert på Microsoft Active Directory/Entra ID eller tilsvarende, som autoritativ kilde for brukere, grupper og roller, med støtte for full brukerlivssyklus og rolle- og selskapsbasert tilgangsstyring. Plattformen skal støtte Single Sign-On for alle integrerte systemer, inkludert O365, fagsystemer og SaaS-løsninger hvor dette støttes og Nettalliansen ønsker det. Ved autentisering skal det benyttes phishing resistant MFA, for eksempel passkeys.	A
IAM-02	Livssyklushåndtering av brukerkontoer	Deltakende selskaper skal kunne registrere og bestille opprettelse av nye brukerkontoer innen avtalt tidsramme, og Leverandøren skal kunne stenge brukerkontoer umiddelbart etter melding fra deltakende selskap, med dokumentasjon av både opprettelse og stenging.	A
PLA– Plattform og arbeidsflate			
PLA-01	Office 365 som standard kontorstøtteplattform	Leverandøren skal levere og drifte Office 365 som standard kontorstøtteplattform for alle deltakende selskaper, inkludert full integrasjon med plattformen, fagsystemer og identitetsstyring. Løsningen skal støtte bruk av siste tilgjengelige versjon av O365-applikasjoner. Leverandøren skal til enhver tid sørge for riktig lisensiering av Office 365.	A
PLA-02	Plattformtilgjengelighet fra godkjente lokasjoner	Plattformen skal være tilgjengelig fra hvilken som helst innrullert enhet og godkjente nettverk.	A
PLA-03	Enhetlig portal med rollebasert tilgang og kontinuerlig forbedring	Sluttbrukerne skal kunne møte et felles åpningsbilde/portal, likt på tvers av deltakende selskaper, som gir rollebasert og personalisert tilgang til applikasjoner og tjenester ut fra brukerens tilhørighet. Alle deltakende selskaper skal kunne ha en enhetlig brukeropplevelse basert på en standardisert plattform, samtidig som selskapenes egne systemer og informasjon kan isoleres (multi-tenant). Leverandøren skal ha etablerte prosesser for kontinuerlig, brukerorientert videreutvikling av portalen.	A

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
PLA-04	Tilgang fra flere enheter/operativsystem og god ytelse	Alle portalbaserte tjenester skal kunne brukes fra PC/Mac, nettbrett og mobil, på tvers av kjente operativsystemer (Windows, MacOS, iOS, Android), og med akseptabel svartid i henhold til SLA slik at sluttbrukere kan navigere mellom systemer uten ventetid som påvirker arbeidsflyten.	A
PLA-05	Samhandling og tilgang til fagsystemer via portal	Løsningen skal støtte moderne samhandlingsfunksjoner som videomøter, chat, tale og enkel fildeling internt og på tvers av selskaper, og brukerne skal kunne nå egne lokale fagsystemer (som KIS, NIS, ERP) direkte fra arbeidsflaten uten separate innlogginger.	A
PLA-06	Klient, maskinvare og utskriftstjenester	Leverandøren skal drifte og forvalte Nettalliansen-enheter (PC, Mac, VDI, nettbrett, mobil, skrivere/scannere mm).	A
INF– Infrastruktur, servere og hybrid skyplattform			
INF-01	Plattformarkitektur, skalerbarhet og fremtidig teknologistøtte	Leverandøren skal levere en standardisert, skalerbar plattformarkitektur for alle deltakende selskaper som muliggjør skalerbar ASP-drift av fagsystemer uten ytelsesforringelse, og som kan støtte fremtidige AI-tjenester gjennom standard API-tilkobling, datahåndtering og sikkerhetsmekanismer.	A
INF-02	Hybrid sky- og serverdrift, kostnads- og kapasitetsstyring	Leverandøren skal drifte fysiske og virtuelle servere på private og offentlige skytjenester som en helhetlig hybrid infrastruktur, med mekanismer for helhetlig kostnadskontroll samt kapasitets- og ytelsesoptimalisering.	A
INF-03	Drift av lokale servere	Leverandøren skal kunne drifte lokale servere, frem til de eventuelt kan fases ut eller migreres til felles plattform.	A
NET– Nettverk			
NET-01	Drift og forvaltning av WAN, LAN og WLAN	Leverandøren skal tilby drift og forvaltning av WAN (inkl. internettskess for alle lokasjoner), LAN, VLAN og WLAN hos deltakende selskaper, inkludert konfigurasjon, sikkerhetsoppsett, overvåking og feilretting.	A

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
NET-02	Nettverksarkitektur, overvåkning og ytelse	Leverandøren skal ivareta nødvendige nettverkstjenester og etablere nettverkstopologi etter beste praksis, hvor skalerbarhet, redundans, lastbalansering og dokumentasjon ivaretas og løsningen støtter hybrid infrastruktur, samt overvåke og følge opp nettverksytelse og -tilgjengelighet med tilhørende feilidentifisering og varsling.	A
NET-03	Brannmur, nettverkssikkerhet og beredskap	Leverandøren skal drifte og forvalte brannmurer og ivareta nettverkssikkerhet og -beredskap, herunder varsel- og hendelseshåndtering samt responstid ved kritiske feil.	A
NET-04	Sikker fjernaksess	Leverandøren skal levere en sikker løsning for fjernaksess til systemer og infrastruktur, basert på gjeldende anbefalinger fra NSM, med multifaktorautentisering, personlige (ikke delte) brukerkontoer, tilgang etter prinsippet om minste privilegium, og tidsbegrenset og behovsstyrt tilgang for eksterne brukere. All fjernaksess skal være sporbar, inkludert identitet, tidspunkt og kilde, og løsningen skal understøtte de vanligste klientplattformene. ved Autentisering skal det benyttes phishing resistant MFA, for eksempel passkeys.	A
NET-05	Nettverk og fjernaksess til OT-/SCADA-miljøer	For deltakende selskaper med OT-/SCADA-miljøer skal Leverandøren kunne drifte og sikre tilknyttede nettverkskomponenter og fjernsessløsninger, med fysisk og logisk adskillelse fra øvrig IT-infrastruktur. Leverandørens ansvar skal kunne avgrenses til nettverk, perimeter og fjernaksess, uten ansvar for drift av selve OT-/SCADA-systemene eller tilhørende applikasjoner, og Leverandøren skal bidra til nødvendig kompetanseoverføring slik at det enkelte selskap selv kan ivareta drift og gjenoppretting av eget OT-miljø ved behov.	A
BAK– Lagring, backup og gjenoppretting			

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
BAK-01	Lagringsområder per selskap, avdeling og bruker	Plattformen skal støtte dedikerte og strukturerte lagringsområder per bruker, per avdeling, per selskap og på konsernnivå, med rolle- og selskapsbasert tilgangsstyring som muliggjør både kontrollert samhandling og nødvendig isolasjon mellom deltakende selskaper.	A
BAK-02	Lagringstjenester - nivå og rapportering	Leverandøren skal håndtere lagring for alle relevante tjenester som tilbys, med definerte nivåer for integritet og ytelse i tråd med avtalt SLA.	A
BAK-03	Backup, gjenoppretting og validering	Leverandøren skal etablere og forvalte en helhetlig backup- og gjenopprettingsløsning for plattform, applikasjoner og data, med regelmessig backup, dokumenterte rutiner og pålitelig restore, inkludert "immutable" backup. Leverandøren skal håndtere gjenoppretting av data der dette er relevant, herunder legge til rette for at sluttbrukere/systemeiere selv kan initiere gjenoppretting av enkeltelementer, og skal tilby tjeneste for løpende validering av at backup faktisk er gjenopprettbar.	A
DB– Database			
DB-01	Databasedrift, forvaltning og rådgivning	Leverandøren er ansvarlig for databaseadministrasjon og drift for databaser på private og offentlige skytjenester, herunder installasjon, versjonskontroll, oppgradering/patching, feilhåndtering og optimalisering, og skal rådgi Nettalliansen om blant annet teknologivalg, lisensiering, migrering og datamodellering.	A
INT– Integrasjoner			
INT-01	Åpen integrasjonstilrettelegging i plattform	Plattformen skal tilrettelegge for integrasjon mot alle relevante 3.-parts fagsystemer og SaaS-tjenester via åpne API-er, mellomvare eller SaaS-integrasjon, uten vendorspesifikke begrensninger.	B
INT-02	Unngå låste, proprietære integrasjoner	Leverandøren skal unngå integrasjoner som krever proprietære protokoller, spesiallisenser eller bindinger som gjør det vanskelig å bytte leverandør i fremtiden.	B

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
INT-03	Integrasjon mot ASP-drevne fagsystemer og terminalmiljø	Leverandøren skal sikre at fagsystemer som krever drift i ASP-miljø kan integreres uten proprietære løsninger eller lisensmessige/tekniske begrensninger, og skal legge til rette for at lokale klienter (PC/MAC, mobil, nettbrett) kan samhandle med applikasjoner i datasenter/terminalmiljø uten ekstra installasjonskrav eller redusert brukeropplevelse.	A
INT-04	Integrasjonsrammeverk, vedlikehold og overvåkning	Leverandøren skal tilby et standardisert rammeverk for integrasjoner (f.eks. API-gateway, webservices, meldingsbus) slik at nye integrasjoner kan etableres uten særskilt utvikling, tilrettelegge for at 3.parts-leverandører kan vedlikeholde sine integrasjoner uten driftsstopp, og tilby overvåkning av integrasjoner med logg, status og varsling ved feil.	B
SUP– Drift, support og brukerstøtte			
SUP-01	SPOC og linjedelt brukerstøtte, inkl. tilgjengelighet	Leverandøren skal tilby et Single Point of Contact (SPOC) som håndterer alle henvendelser og er kundens eneste kontaktpunkt, med 1., 2. og 3. linje brukerstøtte. Leverandøren skal tilby full support innenfor ordinær arbeidstid, online brukerstøtte mellom kl. 07.00 og 17.00 på hverdager, samt 24/7 brukerstøtte (f.eks. vakttelefon) for enkelte kritiske tjenester.	A
SUP-02	Fysisk og fjernbasert support samt varsling/eskalering	Leverandøren skal tilby fjernsupport, og fysisk support på lokasjon ved behov, for alle deltakende selskaper, og skal etablere rutiner for varsling og eskalering ved driftsavvik, inkludert kritiske hendelser.	A
SUP-03	Dashboard for drift og support	Leverandøren skal levere et dashboard som viser alle saker, SLA-er, status, logger og kommunikasjon mellom kunde og leverandør. I tillegg skal Leverandøren levere periodisk (minimum kvartalsvis) sammenstilt rapportering som gir Nettalliansen samlet oversikt over sikkerhetsstatus, hendelser, endringer, patching, kapasitet og tilgjengelighet.	A

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
SUP-04	Tjenestekatalog samt rolle- og ansvarsbeskrivelse	Leverandøren skal tilby en standardisert tjenestekatalog som beskriver alle tjenester i leveransen (priser, tjenestenivåer, avgrensninger) og implementere ITSM-prosesser og -verktøy der det er hensiktsmessig, samt beskrive alle roller og ansvar i driftssamarbeidet, inkludert SPOC, superbrukere og driftsansvarlige mm.	A
RAD– Rådgivning og kommunikasjon			
RAD-01	Proaktiv rådgivning og tilgang til kompetanse	Leverandøren skal være en proaktiv driftspartner på strategisk, taktisk og operativt nivå, tilpasse oppgraderinger til utviklingstakten i Nettalliansens systemportefølje, og ha rutiner som sikrer at Nettalliansen får tilgang på nødvendig kompetanse og ressurser i Leverandørens organisasjon ved behov.	A
RAD-02	Kunnskapsutveksling og kommunikasjon mellom partene	Leverandøren skal sørge for kunnskapsutveksling med Nettalliansen for hele leveransen, og sikre god informasjonsflyt mellom partene.	A
PRO– Organisering og prosjektgjennomføring (etableringsfasen)			
PRO-01	Prosjektorganisering og gjennomføringsmodell	Leverandøren skal etablere en prosjektorganisasjon med tydelig definerte roller og ansvar for etableringsprosjektet (prosjektleder, tekniske ressurser, sikkerhetsansvarlig, migrasjonsansvarlig), og beskrive sin metodikk for gjennomføring, inkludert prosjektstruktur, faser, styringsmodell og beslutningspunkter.	A
PRO-02	Fremdrifts- og utrullingsplan med milepæler	Leverandøren skal utarbeide en oversikt over hovedmilepæler med godkjenningskriterier, en detaljert fremdriftsplan som viser avhengigheter, ressursbruk og rekkefølge, samt en konkret plan for utrulling av grunnpakken til hvert deltakende selskap, inkludert lokal avhengighetskartlegging, migrasjonsaktiviteter og akseptansekriterier.	A

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
PRO-03	Endringsstyring og risikorapportering	Leverandøren skal etablere strukturert endringsstyring (Change Management) og avviksprosesser for etableringsprosjektet, og skal rapportere fremdrift, status og risiko regelmessig til Nettalliansen, inkludert estimerte konsekvenser, tiltak og oppdatert risikobilde.	A
PRO-04	Opplæring/brukerdokumentasjon	Leverandøren skal tilby nødvendig opplæring/brukerdokumentasjon for relevante roller hos Nettalliansen i forbindelse med etablering av løsningen, vesentlige endringer og innføring av nye tjenester som påvirker bruk eller drift.	A
KLI – Klima- og miljøhensyn			
KLI-01	Datasenterets energieffektivitet (PUE)	Alt datasenterutstyr og all infrastruktur som benyttes til å levere IT-driftstjenestene under denne avtalen, skal driftes i et datasenter med en årlig gjennomsnittlig Power Usage Effectiveness (PUE) på maksimalt 1,3 under normal drift.	B
KLI-02	100 % fornybar energi	All elektrisk energi som forbrukes av servere, lagringsenheter, nettverksutstyr og tilhørende kjøleinfrastruktur for å levere den tilbudte tjenesten, skal være dekket av 100 % fornybar energi .	B
KLI-03	Miljøkrav til nyinnkjøpt maskinvare	Dersom det kjøpes inn nye fysiske servere, lagringsenheter eller nettverkskomponenter spesifikt for å etablere eller drifte oppdragsgivers miljø, skal dette utstyret oppfylle kravene til TCO Certified (siste gjeldende generasjon for Enterprise-produkter), EU Ecolabel eller tilsvarende anerkjent miljømerking. Utstyret skal ha en garantert tilgjengelighet på reservedeler og support i minimum 5 år fra innkjøpsdato.	B

Krav-ID	Kort beskrivelse av krav	Krav	Prioritet
KLI-04	Sirkulær avhending og ombruk (Take-back)	Leverandøren skal ha et etablert system for sikker utfasing og sirkulær håndtering av utrangert IT-utstyr som benyttes i tjenesten. Ved utskiftning eller avslutning av avtalen skal utstyret håndteres etter følgende avfallshierarki: 1. Sikker datasletting og klargjøring for ombruk/videresalg , 2. Dersom ombruk ikke er teknisk mulig, skal utstyret materialgjenvinnes hos en godkjent avfallsaktør. Deponering eller forbrenning av elektronisk avfall (EE-avfall) er ikke tillatt.	B

2. Avtalens punkt 2.4.7 Planer og øvelser for beredskap og katastrofer

Med mindre annet fremgår nedenfor, gjelder Avtalens ordinære bestemmelser om beredskaps- og katastrofeøvelser i punkt 2.4.7, herunder at Leverandøren skal gjennomføre egne øvelser minst én gang per år, og bistå ved inntil én av Kundens øvelser per år.

I tillegg gjelder følgende for denne Avtalen:

- Leverandøren skal koordinere gjennomføring og tidspunkt for øvelser med Kunden og berørte Deltakende Selskap gjennom samhandlingsplanen, slik at øvelser i minst mulig grad kolliderer med kritiske driftsperioder hos det enkelte selskap.
- For Deltakende Selskap som er omfattet av kraftforsyningsberedskapsforskriften, skal Leverandøren, i den grad det er relevant for driftstjenesten, kunne bidra inn i disse selskapenes lovpålagte beredskapsøvelser.
- Evalueringsrapport fra Leverandørens egne øvelser skal, i tillegg til å gjøres tilgjengelig på forespørsel, oversendes Kunden sentralt innen fristen i Avtalens punkt 2.4.7, med eventuelle forbedringstiltak som berører driftstjenesten.

3. Avtalens punkt 2.4.9 Nye versjoner av programvare

Med mindre annet fremgår nedenfor, følger nye versjoner av programvare (herunder programrettelser) Leverandørens alminnelige oppgraderingsløp, jf. Avtalens punkt 2.4.9.

- Oppgraderinger som berører felles plattformkomponenter (f.eks. Microsoft 365, portal, identitetsløsning), og som kan påvirke flere Deltakende Selskap samtidig, skal varsles Kunden i god tid og koordineres gjennom avtalt endringsvindu i samhandlingsplanen.
- Leverandøren skal, så langt det er praktisk mulig, teste oppgraderinger i eget test-/pilotmiljø før idriftsettelse i produksjon.
- Sikkerhetsoppdateringer skal, i tråd med Avtalens punkt 2.4.9, driftsettes uten unødig opphold, uavhengig av ordinært endringsvindu, med etterfølgende varslings til Kunden.

4. Avtalens punkt 2.4.10 Livssyklusforvaltning – tidsmessighet

Leverandøren skal ha totalansvar for livssyklusforvaltning av utstyr, programvare og andre ytelser som er nødvendig for å opprettholde avtalt tjenestenivå, i tråd med Avtalens punkt 2.4.10.

- Leverandøren skal årlig, eller ved vesentlige endringer, fremlegge en oppdatert livssyklusplan for Kunden som viser status og forventet utløp av support («end of life»/«end of support») for sentrale komponenter i driftsmiljøet, samt forslag til tiltak i god tid før utløp.
- Livssyklusplanen skal, i etableringsfasen, også vise hvordan komponenter som fases ut i forbindelse med overgangen til fremtidig driftsmiljø, jf. punkt 1.2, håndteres.

5. Avtalens punkt 2.5.1 Generelt om avslutning av Avtalen

I tillegg til Leverandørens generelle bistandsplikt ved avslutning av Avtalen, jf. Avtalens punkt 2.5.1, skal Leverandøren som et minimum levere følgende informasjon i forbindelse med forberedelse til inngåelse av ny driftsavtale:

- Fullstendig og oppdatert teknisk dokumentasjon av driftsmiljøet, herunder arkitektur, konfigurasjon, integrasjoner og avhengigheter.
- Oversikt over alle tilganger, brukerkontoer, roller og grupper i identitets- og tilgangsstyringsløsningen.
- Eksport av Kundens data i strukturert, maskinlesbart format med bevarte metadata, jf. punkt «Avtalens punkt 8.3 Rettigheter til data» nedenfor.
- Oversikt over avtaler med underleverandører og tredjeparter som er nødvendige for videre drift.
- Dokumentert status på alle åpne saker, avvik og planlagte aktiviteter.

Listen ovenfor er ikke uttømmende, jf. Avtalens punkt 2.5.1 tredje ledd.

6. Avtalens punkt 5.1.1 Leverandørens ansvar for leveransen - generelt

Leverandøren skal, som et minimum, dokumentere etterlevelse av lover, forskrifter og forordninger som kravsatt i kravtabellen i punkt 1.4, kategori «GEN – Generelle krav»: Leverandøren skal videre ha ansvaret for å samordne, styre og koordinere arbeidet mellom de ulike aktørene som har betydning for driftstjenesten. Dette omfatter blant annet:

- Deltakende Selskaps egne fagsystemleverandører og lokale IT-ressurser, i den grad disse har grensesnitt mot driftstjenesten.
- Eksisterende driftsleverandør i overtakelsesperioden, jf. punkt 1.3.

- Underleverandører og tredjepartsleverandører som benyttes av Leverandøren for å levere driftstjenesten (f.eks. sky- og programvareleverandører).
- Kundens eksterne rådgiver for IT-sikkerhet, i forbindelse med sikkerhetsrelaterte aktiviteter som revisjon og penetrasjonstesting.

Leverandøren har ansvaret for å opprette/ajourholde systemdokumentasjon gjennom hele avtaleperioden, og skal fylle ut en første versjon av «Bilag 1, Vedlegg 1 – Systemdokumentasjon IT Drift» så langt det er mulig, som del av sitt tilbud.

7. Avtalens punkt 7.1 Eksterne rettslige krav og tiltak generelt

Kunden har identifisert følgende rettslige og partsspesifikke krav som særlig relevante for inngåelse og gjennomføring av Avtalen. Leverandøren skal beskrive i bilag 2 hvordan disse ivaretas gjennom sin løsning:

- Personopplysningsloven og personvernforordningen (GDPR), herunder krav til lovlig behandlingsgrunnlag, databehandleravtale og eventuell overføring av personopplysninger ut av EU/EØS.
- Regelverket om digital sikkerhet i viktige og essensielle virksomheter (NIS2), herunder krav til risikostyring, hendelseshåndtering, varsling av sikkerhetshendelser og sikkerhet i leverandørkjeden, i den grad dette gjelder for leveransen og/eller for Deltakende Selskap.
- Kraftforsyningsberedskapsforskriften og relatert regelverk
- NSMs grunnprinsipper for IKT-sikkerhet.
- Eventuelt sektorspesifikt regelverk som gjelder for det enkelte Deltakende Selskap, og som Leverandøren gjøres kjent med i etableringsfasen.

Kravene ovenfor er utdypet i kravtabellen i punkt 1.4, særlig i kategoriene «SIK – Sikkerhet» og «BER – Beredskap og kontinuitet».

8. Avtalens punkt 7.2.1 Generelt om informasjonssikkerhet

I tillegg til Avtalens generelle bestemmelser om informasjonssikkerhet, jf. Avtalens punkt 7.2.1, har Kunden følgende nærmere krav til hvordan informasjonssikkerheten skal ivaretas fra Leverandørens side:

- Leverandøren skal legge Zero Trust-prinsipper og NSMs grunnprinsipper for IKT-sikkerhet til grunn for sikkerhetsarkitekturen.
- Leverandøren skal etablere sentralisert logging og sikkerhetsovervåkning på tvers av tjenester og plattform, med varsling ved avvik og sikkerhetshendelser.
- Leverandøren skal ha dokumenterte og testede rutiner for hendelseshåndtering, inkludert klassifisering, eskalering og varsling ved sikkerhetshendelser (herunder eventuell varslingsplikt etter NIS2 og personvernregelverket).

- Kunden og Kundens eksterne rådgiver for IT-sikkerhet skal ha rett til innsyn i relevante sikkerhetslogger, og til å gjennomføre penetrasjonstesting og andre sikkerhetsvurderinger av løsningen.

Ytterligere krav til informasjonssikkerhet fremgår av kravtabellen i punkt 1.4, kategori «SIK – Sikkerhet».

9. Avtalens punkt 7.2.2 Leverandørens plikt til å holde Kundens data atskilt

I tillegg til Avtalens generelle bestemmelse om atskillelse av Kundens data fra andre kunders data, jf. Avtalens punkt 7.2.2, har Kunden følgende nærmere krav:

- Data og tilganger skal, der det er relevant, også kunne isoleres logisk mellom de enkelte Deltakende Selskap, slik at hvert selskap kun har tilgang til egne data, med mindre samhandling på tvers av selskapene er eksplisitt avtalt eller ønsket av det enkelte selskap.
- Isolasjon skal ivaretas gjennom en kombinasjon av fysisk, logisk og nettverksmessig segmentering, samt tilgangskontroll basert på prinsippet om minste privilegium.

10. Avtalens punkt 8.3 Rettigheter til data

I tillegg til Avtalens generelle bestemmelser om rettigheter til data, jf. Avtalens punkt 8.3, har Kunden følgende nærmere krav:

- Data skal, både ved avtalens opphør og på forespørsel i avtaleperioden, kunne eksporteres i strukturert, maskinlesbart og allment tilgjengelig format (f.eks. CSV eller JSON for strukturerte data, og bransjestandardformat for e-post/dokumenter), med opprinnelige strukturer og metadata intakt.
- Leverandøren skal, på Kundens forespørsel, kunne demonstrere/teste uthenting av data i løpet av avtaleperioden, og ikke bare ved avtalens opphør.
- Med mindre annet er skriftlig avtalt, skal Leverandøren slette alle egne kopier av Kundens data, inkludert i backup, innen den frist Kunden fastsetter i denne bestemmelsen (forslagsvis 30 dager) etter Avtalens opphør, med mindre lovpålagt lagringsplikt tilsier lengre lagring.
- Leverandøren skal ikke benytte Kundens data, herunder anonymiserte eller aggregerte data, til trening av kunstig intelligens/maskinlæringsmodeller eller til andre egne formål, uten Kundens uttrykkelige, skriftlige samtykke.