
Bilag til SSA-D

Bilag til Driftsavtalen

Statens standardavtale om levering driftstjenester til IT-løsninger

Innhold:

Bilag 1: Kundens kravspesifikasjon	5
Avtalens punkt 1.1 Avtalens omfang.....	5
Bilag 1.1 Kravspesifikasjon for leveransen.....	8
Avtalens punkt 2.4.7 Planer og øvelser for beredskap og katastrofer	26
Avtalens punkt 2.4.9 Nye versjoner av programvare	27
Avtalens punkt 2.4.10 Livssyklusforvaltning – tidsmessighet.....	27
Avtalens punkt 2.5.1 Generelt om avslutning av Avtalen	28
Avtalens punkt 5.1.1 Leverandørens ansvar for leveransen – generelt	28
Avtalens punkt 7.1 Eksterne rettslige krav og tiltak generelt.....	29
Avtalens punkt 7.2.1 Generelt om informasjonssikkerhet	30
Avtalens punkt 7.2.2 Leverandørens plikt til å holde Kundens data atskilt.....	30
Avtalens punkt 8.3 Rettigheter til data	31
Bilag 2 – Leverandørens løsningsspesifikasjon	32
Avtalens punkt 1.1 – Avtalens omfang.....	32
Avtalens punkt 2.3.2.6 – Leverandørens overtakelse av Kundens infrastruktur – verifisering mv. 33	
Avtalens punkt 2.4.9 – Nye versjoner av programvare	33
Avtalens punkt 2.4.10 – Livssyklusforvaltning – tidsmessighet.....	33
Avtalens punkt 5.1.1 – Leverandørens ansvar for leveransen – generelt / standardvilkår	34
Avtalens punkt 5.1.2 – Kundens ansvar og medvirkning	34
Avtalens punkt 5.2.4 – Kundens ansvar for sine ressurser	35
Avtalens punkt 7.1 – Eksterne rettslige krav og tiltak generelt.....	35
Bilag 3: Beskrivelse av det som skal driftes	36
Avtalens punkt 1.1 Avtalens omfang.....	36
<i>Dagens driftsmiljø</i>	<i>36</i>
Bilag 4: Prosjekt- og fremdriftsplan for etableringsfasen	44
Bilag 5: Tjenestenivå og standardiserte kompensasjoner	48
Forholdet til Bilag 1.1	48
Avtalens punkt 2.3.2.4 – Samhandlingsplan og driftsspesifikasjon.....	49
Avtalens punkt 2.4.1 – Krav til tjenestenivå.....	50
Tilgjengelighet.....	50
Brukerstøtte og servicedesk	51
Sikkerhetshendelser	51
Backup og gjenoppretting	52

Avtalens punkt 2.4.2 – Uønskede hendelser	52
Avtalens punkt 2.4.5 – Rapportering	53
Avtalens punkt 9.5.4 – Økonomisk kompensasjon for brudd på avtalt tjenestnivå.....	54
KPI-er uten standardisert kompensasjon.....	54
Bilag 6: Administrative bestemmelser	56
Avtalens punkt 2.1 – Partenes representanter	56
Avtalens punkt 2.3.3.2 – Kundens tilrettelegging	57
Avtalens punkt 2.4.3 – Endringer i driftsmiljøet som initieres av Leverandøren	57
Avtalens punkt 2.4.6 – Dokumentasjon	58
Avtalens punkt 2.4.8 – Revisjon	59
Avtalens punkt 2.4.9 – Nye versjoner av programvare	60
Avtalens punkt 3.2 – Endringshåndtering.....	60
<i>A. Kundens endringsordre</i>	<i>60</i>
<i>B. Leverandørens håndtering av endringsordrer</i>	<i>60</i>
<i>C. Kundens aksept av Leverandørens utredning.....</i>	<i>61</i>
<i>D. Tvisteløsning.....</i>	<i>61</i>
Avtalens punkt 5.2.2 – Nøkkelpersonell.....	61
Avtalens punkt 5.3.1 – Leverandørens bruk av underleverandører	62
Avtalens punkt 5.3.2 – Kundens bruk av tredjepart	64
Avtalens punkt 5.6 – Møter.....	64
Avtalens punkt 5.7 – Lønns- og arbeidsvilkår.....	65
Avtalens punkt 5.8 – Taushetsplikt	65
Avtalens punkt 5.9 – Skriftlighet.....	65
Avtalens punkt 12.2 – Uavhengig ekspert.....	66
Bilag 7: Samlet pris og prisbestemmelser	67
Avtalens punkt 6.1 – Vederlag.....	67
Prisskjema	68
Etableringskostnad	68
Månedlig driftsvederlag	68
Tredjepartslisenser og standardtjenester	69
Timepriser	69
Opsjoner	70
Avtalens punkt 6.2 – Fakturering	72
Avtalens punkt 6.5.1 – Indeksregulering	73
Avtalens punkt 2.4.4 – Bestilling av tilleggstjenester / tjenestekatalog	73
Avtalens punkt 2.4.7 – Planer og øvelser for beredskap og katastrofer	73

Avtalens punkt 2.4.9 – Nye versjoner av programvare	74
Avtalens punkt 3.3 – Kostnader og øvrige konsekvenser av endringsordre.....	74
Avtalens punkt 4.2.1 – Avbestilling i etableringsfasen	74
Avtalens punkt 4.2.2 – Avbestilling i ordinær drift	74
Avtalens punkt 5.3.2 – Kundens bruk av tredjepart	74
Bilag 8: Endringer i den generelle avtaleteksten.....	75
Bilag 9: Endringer av leveransen etter avtaleinngåelsen	77
Bilag 10: Standard lisensvilkår for standardprogramvare og fri programvare	78
Avtalens punkt 5.1.1 – Leverandørens ansvar for leveransen – generelt	78
Fri programvare og åpen kildekode.....	79
Endringer i standardvilkår	79
Forholdet til øvrige bilag.....	79
Vedlegg til Bilag 10	79
Bilag 11: Databehandleravtale	81

Bilag 1: Kundens kravspesifikasjon

Avtalens punkt 1.1 Avtalens omfang

1. Innledning og formål

Direktoratet for mineralforvaltning med Bergmesteren for Svalbard (DMF) er statlig fagetat under Nærings- og fiskeridepartementet. DMF er avhengig av stabile, sikre og tilgjengelige IT-tjenester for å ivareta sitt samfunnsoppdrag.

Dette bilaget beskriver DMFs behov og krav til en helhetlig IT-driftsleveranse. Bilag 3 gir en nærmere beskrivelse av dagens IT-miljø, herunder brukere, klienter, lokasjoner, infrastruktur, skytjenester, applikasjoner, integrasjoner og utviklingsmiljø.

Leverandøren skal i Bilag 2 beskrive sin foreslåtte løsning, herunder eventuelle forutsetninger, avgrensninger og forhold som har betydning for etablering, drift, pris, sikkerhet eller tjenestenivå.

Leverandøren skal ved utforming av tilbudet legge til grunn opplysningene i Bilag 3, men samtidig ta høyde for at leveransen skal etableres som en fremtidsrettet, sikker og skalerbar driftstjeneste.

2. Overordnet anskaffelsesbehov

DMF skal anskaffe en helhetlig og fremtidsrobust IT-driftsleveranse som sikrer stabil, sikker og effektiv drift av DMFs IT-miljø og IT-tjenester. Leveransen skal samtidig gi fleksibilitet og kapasitet til videre digitalisering innenfor forutsigbare økonomiske og kontraktsmessige rammer.

IT-drift, sikkerhetsovervåking og drift av IT-utviklingsmiljø er kritiske tjenester for DMF. Leveransen skal derfor omfatte daglig driftstøtte, brukerstøtte, identitets- og tilgangsadministrasjon, drift av klienter og mobile enheter, nettverk, server- og skytjenester, applikasjonsdrift, backup og gjenoppretting, sikkerhetsovervåking, hendelseshåndtering, dokumentasjon, rapportering og kontinuerlig forbedring.

Leveransen omfatter også administrasjon av DMFs Microsoft Entra ID-tenant og relevante M365-tjenester. Leverandøren skal beskrive hvor og hvordan kundens data, metadata, logger, backup, sikkerhetsdata og administrasjonsdata behandles og lagres, herunder bruk av underleverandører og eventuelle skytjenester.

Kontrakten gjelder for perioden fra etablering og oppstart i 2026, med ordinær kontraktsperiode og opsjoner som angitt i konkurransegrunnlaget og SSA-D med bilag.

3. Mål for leveransen

Anskaffelsen skal gi DMF:

- lavere operasjonell risiko og høyere informasjonssikkerhet,
- stabil og dokumenterbar tilgjengelighet for sentrale IT-tjenester,
- effektiv brukerstøtte med høyt kunnskaps- og servicenivå,
- effektiv ressursbruk og frigjort intern kapasitet,
- forutsigbare og optimaliserte kostnader,
- fleksibel og skalerbar IT-plattform for fremtidige behov,
- helhetlig IT-drift og sikkerhet, inkludert SOC/MDR og incident response innenfor avtalens omfang.

Leveransen skal innrettes slik at DMF har nødvendig kontroll med egne data, dokumentasjon, tilgangsstyring, kostnader, sikkerhet og senere overgang til annen leverandør eller teknisk plattform.

4. Hovedområder i leveransen

Leverandøren skal ha et samlet ansvar for drift og koordinering av de tjenestene som inngår i avtalen. Dette omfatter blant annet:

- drift og administrasjon av identiteter og tilgangsstyring,
- drift og administrasjon av klienter, mobile enheter og relevante administrasjonsverktøy,
- drift og administrasjon av nettverk og tilhørende komponenter,
- drift og forvaltning av servermiljø, private cloud og relevante skytjenester,
- drift og forvaltning av Microsoft Entra ID og M365-tjenester,
- leveranse og administrasjon av avtalte basislisenser,
- brukerstøtte og servicedesk,
- sikkerhetsovervåking, sårbarhetsoppfølging og hendelsehåndtering,
- backup, gjenoppretting og disaster recovery,
- drift av utviklings-, test- og produksjonsmiljø for DMFs IT-utvikling,
- dokumentasjon, rapportering, samhandling og kontinuerlig forbedring,
- bistand ved etablering, overgang, endringer og avslutning av avtalen.

Leverandøren kan benytte underleverandører, men skal ha et samlet ansvar overfor DMF for leveransen, inkludert koordinering mot relevante tredjeparter.

5. Brukerstøtte

Leverandøren skal levere brukerstøtte som dekker DMFs behov for effektiv og sikker håndtering av brukershenvendelser. Brukerstøtten skal være tilgjengelig 24/7/365 og skal kunne håndtere henvendelser på norsk og engelsk.

Brukerstøtten skal som minimum dekke registrering, klassifisering, oppfølging og løsning av henvendelser knyttet til brukerens IT-miljø, herunder klient, mobil enhet, tilgang, programvare, fjernhjelp og relevante endringsforespørsler. Automatisering og KI kan benyttes som støtteverktøy, men brukerrettet håndtering, kvalitetssikring og beslutninger som påvirker brukerens tilgang, sikkerhet eller konfigurasjon skal være underlagt nødvendig menneskelig kontroll.

Nærmere krav til tilgjengelighet, svartid, responstid, løsnings tid, rapportering og eventuelle standardiserte kompensasjoner fremgår av Bilag 5.

6. Fleksibilitet, utvikling og ressursutnyttelse

Leveransen skal kunne tilpasses endringer i DMFs behov gjennom avtaleperioden. Dette omfatter blant annet skalerbar kapasitet for prosessering, lagring, backup, brukere, klienter og relevante skytjenester, samt samspill mellom private cloud, public/sovereign cloud og M365 der dette er avtalt.

Leverandøren skal bidra til god ressursutnyttelse gjennom transparent prismodell, rapportering av kostnadsutvikling, lisensoptimalisering, kapasitetsstyring og forslag til forbedringstiltak. Nærmere krav til priser, volumendringer, opsjoner, timebaserte tilleggstenester og fakturering fremgår av Bilag 7 og prisskjemaet.

7. Hva som inngår i anskaffelsen

Anskaffelsen omfatter helhetlig IT-drift og sikkerhet for de tjenestene som er beskrevet i dette bilaget og øvrige SSA-D-bilag. Dette omfatter blant annet:

- SOC/MDR og incident response innenfor avtalens omfang,
- administrerte identiteter, klienter, mobile enheter og nettverk,
- brukerstøtte 24/7/365,
- privat cloud/serverdrift, inkludert utviklingsmiljø,
- administrasjon av Entra ID og M365-tjenester,
- backup og gjenoppretting av avtalte tjenester og data,
- avtalte basislisenser og administrasjonsverktøy,
- dokumentasjon, rapportering og samhandling.

Alle tjenester som er nødvendige for å oppfylle må-kravene og avtalt tjenestenivå, skal være inkludert i faste eller enhetsbaserte priser, med mindre prisskjemaet uttrykkelig angir at ytelsen er en opsjon eller en timebasert tilleggsteneste.

8. Hva som ikke inngår i anskaffelsen

Følgende inngår ikke i anskaffelsen, med mindre annet uttrykkelig følger av kravspesifikasjonen, prisskjemaet eller senere endringsordre:

- utvikling av DMFs fagsystemer,
- kjøp og levering av brukerutstyr som PC-er, skjermer, IT-rekvisita og mobile enheter,
- leveranser som er dekket av statlige fellesavtaler, herunder programvarelisenser utover avtalte basislisenser, avhending/gjenbruk av IT-utstyr og mobiltelefoni.

Leverandøren skal likevel kunne samhandle med DMF og relevante tredjeparter om slike leveranser der dette er nødvendig for å levere avtalte driftstjenester.

9. Forbehold mot bruk av Kundens data

Uavhengig av SSA-D punkt 8.3 siste avsnitt kan Leverandøren ikke bruke Kundens data, metadata, logger, sikkerhetsdata, supportsaker, bruksmønstre, dokumentasjon eller andre data som skriver seg fra Kundens bruk av driftstjenesten – herunder aggregerte, statistiske eller anonymiserte avledninger av slike data – til analyse, produktutvikling, modelltrening, finjustering, forbedring av tjenester for andre kunder eller andre egne formål, uten Kundens uttrykkelige skriftlige forhåndsgodkjenning.

Bilag 1.1 Kravspesifikasjon for leveransen

Dette tabellen tar for seg krav til leveransen, samt det minimum av informasjon som skal besvares i «Bilag 2: Leverandørens løsningsspesifikasjon».

Alle krav skal som utgangspunkt inkluderes i månedsprisen i Bilag 7, tjenester som er beskrevet i Bilag 2 eller krav som ikke løses som en del av månedsprisen skal merkes som «Opsjon» eller «Faktureres pr. time». Priser på disse opsjonene og timesestimer for fakturerbare tjenester skal oppgis (suppleres) i Bilag 7.

Leverandøren bes tas utgangspunkt i at alle IT-relaterte tjenester som er omfattet av denne avtalen re- etableres og at dagens infrastruktur fases ut i sin helhet.

Kravtype:

M = Må-krav/minstekrav: skal oppfylles. Manglende oppfyllelse eller vesentlig avvik kan medføre avvisning.

B = Besvarelseskrav: leverandøren skal beskrive/redegjøre. Besvarelsen inngår i evalueringen og blir kontraktsinnhold, men kravet er ikke formulert som ett bestemt absolutt minstenivå.

O = Opsjon: leverandøren skal beskrive og prise opsjonen der dette er etterspurt. Opsjonen inngår ikke i basisleveransen med mindre den avropes.

A - Generelt

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
A1	Leverandøren skal levere standardiserte driftstjenester som samlet ivaretar DMFs brukere, klienter, lokal infrastruktur, skytjenester, sikkerhet og driftsplattform.	M	Beskriv hvordan kravet oppfylles.	Bilag 2

A2	Leverandøren skal beskrive sin standardleveranse og hvordan kundespesifikke tilpasninger håndteres innenfor denne.	B	Beskriv standardleveranse, tilpasningsmodell og eventuelle forutsetninger.	Bilag 2
A3	Leverandøren skal ha samlet ansvar for helheten i leveransen, inkludert koordinering av egne underleverandører og relevante tredjeparter innenfor avtalens omfang.	M	Beskriv ansvar, grensesnitt og koordineringsmodell.	Bilag 2 og Bilag 6
A4	Leverandøren skal redegjøre for hvordan kvaliteten i leveransen styres, måles og forbedres.	B	Beskriv kvalitetsstyring, metodeverk, målinger og oppfølging.	ISO 9001 eller tilsvarende dokumentasjon der relevant
A5	Leverandøren skal beskrive hvordan kontinuerlig forbedring og tjenesteutvikling drives, dokumenteres og kommuniseres til DMF.	B	Beskriv prosess, rapportering og forslag til forbedringstiltak.	Bilag 2 og Bilag 6
A6	Leverandøren skal beskrive hvordan det arbeides proaktivt med overvåking, hendelsesforebygging, rotårsaksanalyse og reduksjon av gjentakende feil.	B	Beskriv metoder, verktøy, prosess og rapportering.	Bilag 2 og Bilag 5
A7	Leverandøren skal oppgi hvilke støtteverktøy, portaler, driftsverktøy, sikkerhetsverktøy og standardprogramvare som inngår i leveransen.	B	List opp verktøy/programvare og angi om kostnad er inkludert i Bilag 7.	Bilag 2, Bilag 7 og Bilag 10
A8	Leverandøren skal beskrive hvordan kunstig intelligens, maskinlæring og automasjon benyttes i leveransen av IT-driftstjenester.	B	Beskriv bruksområder, datagrunnlag, menneskelig kontroll, logging og begrensninger.	DMFs KI-policy, Bilag 2 og Bilag 11 ved personopplysninger
A9	Leverandøren skal ikke benytte DMFs data, logger, metadata, dokumentasjon eller sikkerhetsinformasjon til trening, finjustering, modellforbedring eller produktutvikling uten skriftlig forhåndsgodkjenning fra DMF.	M	Bekreft etterlevelse og beskriv tekniske/organisatoriske tiltak.	DMFs KI-policy, Bilag 2 og Bilag 11

B – Dokumentasjon, innsyn og selvbetjening

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
B1	Leverandøren skal tilby portal eller webgrensesnitt for innsyn og selvbetjening for DMFs sluttbrukere og IT-personell.	M	Beskriv funksjonalitet, brukerroller, tilgangsstyring og språk.	Bilag 2

B2	Leverandøren skal beskrive hvordan dokumentasjon av DMFs IT-løsninger etableres, vedlikeholdes og tilgjengeliggjøres for DMF.	B	Beskriv dokumentasjonsstruktur, tilgang, oppdateringsrutiner og eierskap.	Bilag 2 og Bilag 6
B3	Leverandøren skal kommunisere helsestatus for avtalte tjenester til DMF.	M	Beskriv dashboard, varslings-, statusrapporter og historikk.	Bilag 2 og Bilag 5
B4	Leverandøren skal beskrive automasjon og selvbetjeningsmuligheter for administrasjon av DMFs IT-miljø.	B	Beskriv tilgjengelige selvbetjeningsprosesser, godkjenning og logging.	Bilag 2
B5	Dokumentasjon som er nødvendig for drift, sikkerhet, revisjon, beredskap og exit skal være tilgjengelig for DMF gjennom hele avtaleperioden.	M	Beskriv tilgang, format, oppdateringsansvar og eksportmuligheter.	Bilag 2, Bilag 6 og avslutningsbestemmelser
B6	Leverandørens digitale grensesnitt som gjøres tilgjengelig for DMFs brukere eller administratorer, herunder portal, selvbetjening, saksregistrering, statusvisning, kunnskapsbase og rapporteringsgrensesnitt, skal oppfylle gjeldende krav til universell utforming av IKT-løsninger så langt løsningen omfattes av regelverket.	M	Beskriv hvilke grensesnitt som omfattes, hvilket tilgjengelighetsnivå løsningen oppfyller, eventuelle kjente avvik og plan for retting.	Bilag 2

C – Brukerstøtte

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
C1	Leverandøren skal være SPOC for henvendelser fra DMFs brukere innenfor avtalens omfang.	M	Beskriv omfang, kanaler og grensesnitt mot DMF og tredjeparter.	Bilag 2 og Bilag 6
C2	Leverandørens servicedesk skal være tilgjengelig 24/7/365 og bemannet av mennesker.	M	Beskriv bemanning, åpningstid, lokasjon og eskaleringsmodell.	Bilag 2 og Bilag 5
C3	Automatisering og KI kan benyttes som støtte i servicedesk, men brukerrettet håndtering, kvalitetssikring og beslutninger som påvirker tilgang, sikkerhet eller konfigurering skal være underlagt nødvendig menneskelig kontroll.	M	Beskriv bruk av automasjon/KI, kontrollmekanismer og logging.	DMFs KI-policy og Bilag 2
C4	Leverandøren skal redegjøre for hvordan servicedesk har oppdatert	B	Beskriv kunnskapsbase, CMDB, dokumentasjon,	Bilag 2

	informasjon og innsikt i brukerens IT-miljø.		opplæring og oppdateringsrutiner.	
C5	Leverandøren skal beskrive arbeidsprosesser og verktøy for registrering, klassifisering, oppfølging og lukking av henvendelser.	B	Beskriv prosessflyt, saksverktøy, prioritering og rapportering.	Bilag 2 og Bilag 5
C6	Leverandøren skal kunne håndtere henvendelser på norsk og engelsk.	M	Beskriv språkkapasitet og eventuelle øvrige støttede språk.	Bilag 2
C7	Support skal kunne mottas via telefon, chat og saksregistrering.	M	Beskriv kanaler, tilgjengelighet og brukeropplevelse.	Bilag 2 og Bilag 5
C8	Ved telefon- og chathenvendelser skal support registrere sak på vegne av bruker dersom saken ikke løses direkte.	M	Beskriv rutine for saksopprettelse og videre oppfølging.	Bilag 2
C9	Leverandøren skal tilby sikker fjernhjelp/fjernstyring for PC-er og mobile enheter.	M	Beskriv løsning, autentisering, logging, samtykke og sporbarhet.	Bilag 2 og Bilag 6
C10	Brukere skal kunne registrere eller bestille endringsforespørsler knyttet til egen IT-profil, tilganger og programvare innenfor avtalte godkjenningsrutiner.	M	Beskriv prosess, godkjenning, roller og logging.	Bilag 2 og Bilag 6
C11	Endringer som gjelder primært mobilnummer, e-postadresse, privilegerte tilganger eller lokale administratorrettigheter skal godkjennes av DMFs autoriserte IT-kontakter.	M	Beskriv godkjenningsflyt og kontrolltiltak.	Bilag 2 og Bilag 6
C12	Leverandøren skal levere brukerstøtte og servicedesk i samsvar med tjenestenivå, responstider, rapportering og klassifisering som fremgår av Bilag 5.	M	Bekreft og beskriv hvordan servicedesk organiseres for å oppfylle Bilag 5.	Bilag 2 og Bilag 5
C13	Leverandøren skal beskrive hvordan saker mottas, registreres, klassifiseres, prioriteres, eskaleres og lukkes.	B	Beskriv saksflyt, saksverktøy, roller, eskalering og rapportering.	Bilag 2, Bilag 5 og Bilag 6

D – Overvåkning

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
D1	Leverandøren skal levere 24/7/365 overvåking av tilgjengelighet, ytelse, sikkerhet, kapasitetsutnyttelse, integrasjoner, dataflyter og sentrale avhengigheter for avtalte tjenester.	M	Beskriv omfang, verktøy, alarmgrenser og bemanning.	Bilag 2 og Bilag 5
D2	Leverandøren skal redegjøre for hvilke parametere som overvåkes og hvilken teknologi som benyttes.	B	Beskriv standardparametere, teknologier og eventuelle forutsetninger.	Bilag 2

D3	Leverandøren skal beskrive hvordan avvik i overvåkingen håndteres.	B	Beskriv varslingsløp, eskalering, rotårsaksanalyse og rapportering.	Bilag 2 og Bilag 5
D4	Leverandøren skal beskrive hvordan DMF og relevante tredjeparter involveres i hendelseshåndtering.	B	Beskriv samhandlingsmodell, varslingspunkter og ansvarsdeling.	Bilag 2 og Bilag 6
D5	Leverandøren skal beskrive hvilke hendelser som kan håndteres med automatiserte tiltak, eksempelvis restart av tjenester, skalering, failover, rekjøring av prosesser eller isolering av komponenter.	B	Beskriv tiltak, kontroll, logging og godkjenningsnivå.	Bilag 2 og DMFs KI-policy ved KI/automasjon
D6	Overvåkingsdata, hendelsesdata og rapportering skal kunne gjøres tilgjengelig for DMF i egnet format.	M	Beskriv innsyn, eksport og rapporteringsformat.	Bilag 2 og Bilag 5
D7	Leverandøren skal beskrive hvordan overvåking av tilgjengelighet, kapasitet, ytelse, sikkerhet og sentrale avhengigheter understøtter tjenestenivåene i Bilag 5.	B	Beskriv overvåkingspunkter, terskler, varslings, eskalering og rapportering.	Bilag 2 og Bilag 5

E – Lokalt nettverk

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
E1	Leverandøren skal ivareta nødvendige nettverkstjenester, inkludert overvåking, drift og vedlikehold av fysiske og virtuelle nettverk, samt tilgangsstyring til produksjonsnett og gjestenett.	M	Beskriv løsning, drift, ansvarsdeling og sikkerhetstiltak.	Bilag 2 og Bilag 3
E2	Leverandøren skal redegjøre for hvordan lokal nettverksinfrastruktur ivaretas.	B	Beskriv drift, vedlikehold, endringer, feilhåndtering og livssyklus.	Bilag 2
E3	Leverandøren skal beskrive herding av lokal nettverksinfrastruktur.	B	Beskriv baseline, konfigurasjonskontroll og sikkerhetstiltak.	NSM grunnprinsipper, ISO 27001/27002 eller tilsvarende
E4	Leverandøren skal dokumentere nettverkstopologi og holde dokumentasjonen oppdatert.	M	Beskriv dokumentasjonsform, tilgang og oppdateringsrutine.	Bilag 2 og Bilag 6
E5	Gjestenett skal være adskilt fra produksjonsnett og kun gi tilgang til internett.	M	Beskriv teknisk separasjon og kontrollmekanismer.	Bilag 2
E6	Leverandøren skal tilby testing av nettverkstilgang for produksjonsnett og gjestenett, herunder eksternt tilgang, intern tilgang og tilgang via mobilt kontor/VPN.	O	Beskriv testomfang, metode og pris.	Bilag 2 og Bilag 7

E7	Leverandøren skal beskrive hvordan redundans og tilgjengelighet for nettverkstjenester ivaretas på DMFs lokasjoner.	B	Beskriv redundansmodell, avhengigheter og eventuelle opsjoner.	Bilag 2, Bilag 5 og Bilag 7 ved opsjon
----	---	---	--	--

F – Sluttbrukerutstyr

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
F1	Leverandøren skal ha ansvar for administrasjon, drift, sikkerhetsovervåking og oppfølging av DMFs PC-klienter og mobile enheter innenfor avtalens omfang.	M	Beskriv prosess for innrulling, installasjon, oppdatering, feilretting og sikkerhet.	Bilag 2
F2	Leverandøren skal ikke ha ansvar for innkjøp av klientutstyr, men skal levere administrasjonsverktøy som forenkler registrering og onboarding for DMF.	M	Beskriv verktøy og grensesnitt mot DMFs anskaffelse av utstyr.	Bilag 2
F3	Leverandøren skal støtte registrering av Windows-klienter i Autopilot og innrulling av Apple-enheter i relevant administrasjonsløsning.	M	Beskriv prosess, forutsetninger og ansvarsdeling.	Bilag 2
F4	Leverandøren skal beskrive system for inventaroversikt over sluttbrukerutstyr.	B	Beskriv datagrunnlag, oppdatering, eksport og rapportering.	Bilag 2
F5	Leverandøren skal pakke og distribuere DMFs klientapplikasjoner, inkludert nye applikasjoner og nye versjoner i avtaleperioden.	M	Beskriv pakking, testing, utrulling, tilbakeføring og godkjenning.	Bilag 2 og Bilag 6
F6	Leverandøren skal redegjøre for hvordan helsestatus på enhetene måles og rapporteres.	B	Beskriv måleparametere, rapporter og proaktiv oppfølging.	Bilag 2 og Bilag 5
F7	Leverandøren skal redegjøre for hvordan data om enheter og klientapplikasjoner brukes i proaktiv feilretting.	B	Beskriv databruk, personvern vurdering og sikkerhetstiltak.	Bilag 2 og Bilag 11 ved personopplysninger
F8	Leverandøren skal beskrive herding og sikkerhetstiltak på klienter og mobile enheter.	B	Beskriv baseline, policy, patching, EDR/MDR og avvikshåndtering.	NSM grunnprinsipper, ISO 27001/27002 eller tilsvarende
F9	Leverandøren skal beskrive sin tjeneste for administrasjon og sikkerhet for mobile enheter, herunder iOS og Android.	B	Beskriv MDM/MAM, policy, sletting, logging og brukeropplevelse.	Bilag 2

G – Printere

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
----	-------------------------	------	--------------------------	----------------------------

G1	Leverandøren skal administrere DMFs printere innenfor avtalens omfang.	M	Beskriv drift, feilretting, grensesnitt mot printerleverandør og support.	Bilag 2
G2	Leverandøren skal i samarbeid med printerleverandør legge til rette for sikker utskriftsløsning via ID-kort eller tilsvarende.	M	Beskriv løsning, ansvarsdeling og sikkerhetstiltak.	Bilag 2 og Bilag 6
G3	Utskriftsdata og brukerdata skal sikres og ikke behandles utenfor avtalt administrert miljø med mindre dette er særskilt avtalt og dokumentert.	M	Beskriv behandlingssted, datatyper og tilgangsstyring.	Bilag 2 og Bilag 11 ved personopplysninger

H – MDR og operativ sikkerhet

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
H1	Leverandøren skal tilby MDR-tjeneste med Security Operations Center som ivaretar overvåking, deteksjon, analyse, respons og rapportering av sikkerhetshendelser 24/7/365.	M	Beskriv tjeneste, bemanning, teknologi, prosess og dekningsområde.	Bilag 2 og Bilag 5
H2	MDR/SOC-tjenesten skal være inkludert og integrert i basisleveransen, med mindre annet uttrykkelig fremgår av Bilag 7.	M	Bekreft og beskriv pris-/tjenesteplassering.	Bilag 7
H3	Leverandøren skal beskrive hvilke loggkilder som samles inn fra klienter, servere, nettverk, identitet, skyplattform, sikkerhetsteknologier og applikasjoner.	B	Beskriv loggkilder, retensjon, innsyn og begrensninger.	Bilag 2 og Bilag 11 ved personopplysninger
H4	Leverandøren skal beskrive rutiner for håndtering av sikkerhetshendelser, inkludert klassifisering, varsling, eskalering, isolering, tiltak, kommunikasjon, IRT-involvering og etterfølgende rapportering.	B	Beskriv prosess og frister.	Bilag 2 og Bilag 5
H5	Leverandøren skal beskrive playbooks eller standardiserte responsløp for phishing, kontokompromittering, skadevare, ransomware, lateral bevegelse og datalekkasjer.	B	Beskriv playbooks og tilpasning til DMF.	Bilag 2
H6	Leverandøren skal beskrive prosess for kontinuerlig sårbarhetsskanning, risikobasert prioritering, patching, kompensierende tiltak, rapportering og oppfølging av funn.	B	Beskriv frekvens, verktøy, roller og rapportering.	Bilag 2 og Bilag 5
H7	Leverandøren skal redegjøre for hvordan Zero Trust-prinsipper, nettverkssegmentering, least	B	Beskriv arkitektur og kontrolltiltak.	Bilag 2

	privilege, conditional access og privilegert tilgangsstyring benyttes for å redusere risiko.			
H8	Leverandøren skal håndtere sikkerhetshendelser i samsvar med responstider, eskaleringsrutiner og rapporteringskrav i Bilag 5.	M	Bekreft og beskriv hvordan SOC/MDR/IRT ivaretar disse kravene.	Bilag 2 og Bilag 5
H9	Leverandøren skal beskrive hvordan sikkerhetshendelser dokumenteres, rapporteres og følges opp med lærings- og forbedringstiltak.	B	Beskriv rapportering, etteranalyse, rotårsaksanalyse og tiltaksoppfølging.	Bilag 2, Bilag 5 og Bilag 6

I – Informasjonssikkerhet og personvern

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
I1	Leverandøren skal ha informasjonssikkerhet integrert i daglig drift av tjenestene.	M	Beskriv styring, kontroller og operativ etterlevelse.	Bilag 2
I2	Leverandøren skal kunne vise til sikkerhetsarkitektur som sikrer logiske og nettverksmessige barrierer og tilgang kun for autorisert personell.	M	Beskriv arkitektur, segmentering og tilgangsstyring.	Bilag 2
I3	Leverandøren skal inkludere nødvendige sikkerhetsteknologier for å beskytte DMFs brukere, enheter, tjenester og data innenfor avtalens omfang.	M	Beskriv teknologier og dekningsområde.	Bilag 2 og Bilag 7
I4	Leverandøren skal ha etablert styringssystem for informasjonssikkerhet som ivaretar styring, kontroll og kontinuerlig forbedring.	M	Beskriv ISMS.	ISO 27001-sertifikat eller likeverdig dokumentasjon
I5	Leverandøren skal ha etablerte informasjonssikkerhetskontroller basert på anerkjente rammeverk.	M	Beskriv rammeverk og kontrollstruktur.	ISO 27001/27002, NSM grunnprinsipper, NIST eller tilsvarende
I6	Leverandøren skal ha internkontrollsystem for informasjonssikkerhet og personvern som sikrer regelmessige risikovurderinger av tjenestene.	M	Beskriv risikostyring og internkontroll.	Bilag 2 og Bilag 11
I7	Leverandøren skal kunne fremlegge relevante revisjonsrapporter eller tilsvarende dokumentasjon som viser at sikkerhetskontroller fungerer og at avvik følges opp.	M	Beskriv tilgjengelig dokumentasjon og eventuelle begrensninger.	ISAE 3000/3402, SOC 2, ISO-revisjon eller tilsvarende
I8	Leverandøren skal overvåke, logge og håndtere sikkerhetshendelser 24/7/365.	M	Beskriv prosess, bemanning og rapportering.	Bilag 2 og Bilag 5

I9	Leverandøren skal beskrive sikkerhetsteknologiene som ligger til grunn for leveransen og hvilke som er inkludert i prisen.	B	Beskriv teknologier, lisensmodell og prisplassering.	Bilag 2 og Bilag 7
I10	Leverandøren skal ha dokumentert prosess for håndtering av sårbarheter i produkter og tjenester som leveres til DMF.	M	Beskriv prosess, frister og rapportering.	Bilag 2
I11	Leverandøren skal beskrive prosesser og kontroller som sikrer at DMFs IT-miljø sikkerhetsoppdateres fortløpende.	B	Beskriv patchregime, prioritering, testing og unntak.	Bilag 2 og Bilag 5
I12	Leverandørens egne utviklingsprosesser for komponenter som inngår i leveransen skal følge god praksis for sikker utvikling.	M	Beskriv prosess for sikker utvikling, tredjepartskomponenter og sårbarhetsoppfølging.	OWASP, ISO 27001/27002 eller tilsvarende
I13	Leverandøren skal inngå databehandleravtale med DMF der leverandøren behandler personopplysninger på vegne av DMF.	M	Bekreft og fyll ut/aksepter databehandleravtale.	Bilag 11
I14	Leverandøren skal beskrive hvordan behandlingssted, underleverandører, tilgangsstyring, logging og sletting ivaretas for personopplysninger.	B	Beskriv personvernmessige og tekniske tiltak.	Bilag 11
I15	Leverandøren skal kunne bistå DMF med etablering og vedlikehold av IKT-beredskapsplan.	O	Beskriv bistand og pris.	Bilag 7

J – Backup og disaster recovery

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
J1	Leverandøren skal levere en helhetlig backup- og gjenopprettingsstrategi som dekker systemer, data, konfigurasjoner, applikasjoner, identiteter og logger som inngår i leveransen.	M	Beskriv strategi, teknologi, omfang og begrensninger.	Bilag 2 og Bilag 5
J2	Leverandøren skal gjennomføre og dokumentere regelmessige tester av gjenoppretting, inkludert objektgjenoppretting, systemgjenoppretting og relevante katastrofescenarier.	M	Beskriv testfrekvens, metode og rapportering.	Bilag 5 og Bilag 6
J3	Leverandøren skal beskrive hvordan backup beskyttes mot sletting, kryptering eller kompromittering.	B	Beskriv immutability, isolerte kopier, tilgangskontroll og logging.	Bilag 2
J4	Leverandøren skal beskrive RTO- og RPO-nivåer for ulike tjenestetyper og hvordan disse måles og rapporteres.	B	Beskriv tjenestenivåer og måling.	Bilag 5

J5	Leverandøren skal bistå DMF med å gjennomføre sikkerhetsøvelser årlig og gjenopprettingsøvelser annet hvert år.	M	Beskriv plan, roller, omfang og rapportering.	Bilag 1, Bilag 5, Bilag 6 og Bilag 7
J6	Leverandøren skal legge til rette for off-site backup av virksomhetsdata lagret i leverandørens miljø til colocation i Norge eller tredjeparts backuptjeneste i Norge.	M	Beskriv løsning, grensesnitt, sikkerhet og kostnader.	Bilag 2 og Bilag 7
J7	Leverandøren skal som del av basisleveransen legge til rette for off-site backup av virksomhetsdata lagret i leverandørens miljø til colocation i Norge eller tredjeparts backuptjeneste i Norge. Kravet innebærer ikke at drift og administrasjon av Kundens dedikerte fysiske off-site backupservere i managed colocation inngår i basisleveransen. Slik drift og administrasjon prises som opsjon O001 i Bilag 7/prisskjemaet.	M	Beskriv løsning, grensesnitt, sikkerhet, ansvarsdeling og hvilke kostnader som inngår i basisleveransen og hvilke kostnader som eventuelt hører under opsjon O001	Bilag 2 og Bilag 7
J8	Leverandøren skal oppfylle krav til backupstatus, gjenopprettingstester, RTO/RPO og rapportering som fremgår av Bilag 5.	M	Bekreft og beskriv hvordan kravene oppfylles.	Bilag 2 og Bilag 5
J9	Leverandøren skal beskrive hvordan feil i backup, restore eller gjenopprettingsevne oppdages, varsles, prioriteres og lukkes.	B	Beskriv overvåking, eskalering, korrigerende tiltak og rapportering.	Bilag 2, Bilag 5 og Bilag 6

K – Infrastruktur som tjeneste - privat cloud/privat sovereign cloud

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
K1	Leverandøren skal levere eller tilby drift av nødvendig infrastrukturkapasitet fra datasentre i Norge eller EØS, i samsvar med krav til sikkerhet, personvern og datalagring.	M	Beskriv datasentre, tjenester og kapasitet.	Bilag 2
K2	Leverandøren skal beskrive hvordan løsningen understøtter krav til norsk/europeisk datalagring, tilgangskontroll og regulatorisk etterlevelse.	B	Beskriv tiltak, jurisdiksjon og eventuelle forbehold.	Bilag 2 og Bilag 11
K3	Leverandøren skal beskrive hvor DMFs data, metadata, logger, backup og administrasjonsdata lagres og behandles.	B	Angi behandlingssted, underleverandører og skytjenester.	Bilag 2 og Bilag 11
K4	Leverandøren skal redegjøre for relevante jurisdiksjoner for tjenesteleveransen, herunder eierskap,	B	Beskriv juridisk og operasjonell kontroll.	Bilag 2, Bilag 6 og Bilag 11

	driftspersonell, datasentre, support og underleverandører.			
K5	Infrastruktur, servere og produksjonsdata som er kritiske for leveransen skal være sikret med egnet redundans og disaster recovery-løsning.	M	Beskriv redundans, geo-redundans, RTO/RPO og unntak.	Bilag 2 og Bilag 5
K6	Leverandøren skal redegjøre for mekanismer som sikrer ytelsesnivåer for compute og storage.	B	Beskriv kapasitetsstyring, overvåking og skalering.	Bilag 2 og Bilag 5
K7	Leverandøren skal redegjøre for lagringsprofiler og ytelsesgrenser, herunder IOPS og throughput der dette er relevant.	B	Beskriv profiler og prismessige konsekvenser.	Bilag 2 og Bilag 7
K8	Leverandøren skal beskrive backuptjenesten for privat cloud/servermiljø.	B	Beskriv omfang, teknologi, retensjon og restore.	Bilag 2 og Bilag 5
K9	Leverandøren skal redegjøre for beskyttelsesmekanismer mot cryptolocker/ransomware.	B	Beskriv mekanismer og responsløp.	Bilag 2
K10	Leverandøren skal beskrive bruk av infrastruktur som kode eller tilsvarende mekanismer for standardisert, sporbar og kontrollerbar infrastrukturforvaltning.	B	Beskriv teknologi, endringskontroll og rollefordeling.	Bilag 2 og Bilag 6
K11	Leverandøren skal redegjøre for livssyklusforvaltning av serveroperativsystem, mellomvare og andre komponenter som er nødvendige for avtalt tjenestenivå.	B	Beskriv patching, oppgradering, utfasing og varsling.	Bilag 2 og Bilag 6
K12	Leverandøren skal levere sikker, overvåket og loggført fjernadministrasjon for drift og vedlikehold av tjenester i leverandørens driftsmiljø.	M	Beskriv løsning, tidsbegrenset tilgang, logging, tredjepartstilgang og godkjenning.	Bilag 2 og Bilag 6

L - Infrastruktur som tjeneste - public sovereign cloud

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
L1	Leverandøren skal kunne tilby administrert infrastruktur i public sovereign cloud i Norge som opsjon O002.	O	Beskriv tjenesten, behandlingssted, sikkerhetsmodell, ansvarsdeling og pris.	Bilag 2 og Bilag 7
L2	Leverandøren skal beskrive hvordan de kan bistå DMF med landing zone, policy, sikkerhetsbaseline og styring av public cloud-miljø.	O	Beskriv metode og avgrensning.	Bilag 2 og Bilag 7
L3	Leverandøren skal beskrive logging, overvåking, backup og sikring av data i public cloud-miljøer.	O	Beskriv løsning og prisforutsetninger.	Bilag 2, Bilag 5 og Bilag 7

L4	Leverandøren skal redegjøre for kostnadskontroll og FinOps for public cloud-tjenester.	O	Beskriv rapportering, budsjettering, varsling og optimalisering.	Bilag 2 og Bilag 7
L5	Leverandøren skal beskrive hvordan delt ansvarsmodell mellom DMF, leverandør og tredjeparter håndteres ved bruk av public cloud.	O	Beskriv roller, ansvar og endringsprosess.	Bilag 2 og Bilag 6

M - Applikasjonsdrift - dedikerte applikasjoner

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
M1	Leverandøren skal ha ansvar for daglig drift av DMFs avtalte applikasjonsportefølje, inkludert infrastruktur, dokumentasjon, overvåking og feilretting.	M	Beskriv omfang og ansvarsdeling.	Bilag 2 og Bilag 3
M2	Leverandøren skal utføre nødvendig koordinering med applikasjonsleverandører og utviklere for å sikre normal funksjon for applikasjonene.	M	Beskriv koordineringsmodell og avgrensning mot utvikling.	Bilag 2 og Bilag 6
M3	Leverandøren skal redegjøre for hvordan DMFs applikasjoner overvåkes.	B	Beskriv tekniske og funksjonelle overvåkingspunkter.	Bilag 2 og Bilag 5
M4	Leverandøren skal beskrive hvordan applikasjoner, integrasjoner og understøttende infrastruktur dokumenteres og vedlikeholdes.	B	Beskriv dokumentasjonsmodell og tilgang for DMF.	Bilag 2 og Bilag 6
M5	Leverandøren skal beskrive hvordan endringer utført av leverandøren, DMF eller tredjeparter gjennomføres på en sikker og sporbar måte.	B	Beskriv endringsprosess, fjernadministrasjon, logging og godkjenning.	Bilag 2 og Bilag 6
M6	Leverandøren skal beskrive hvordan forvaltning av relevante lisenser ivaretas.	B	Beskriv lisensoversikt, optimalisering og rapportering.	Bilag 2 og Bilag 7
M7	Leverandøren skal beskrive administrasjon og forvaltning av sertifikater.	B	Beskriv eierskap, varsling, fornyelse og hendelseshåndtering.	Bilag 2
M8	Leverandøren skal beskrive administrasjon og forvaltning av domener.	B	Beskriv roller, tilgang, endring og fornyelse.	Bilag 2
M9	Leverandøren skal beskrive ansvarsfordeling mellom leverandøren, DMF og tredjeparter, inkludert mellomvare og kjøretidskomponenter på applikasjonsplattformen.	B	Beskriv RACI eller tilsvarende ansvarsmodell.	Bilag 2 og Bilag 6

N - Applikasjonsdrift - SaaS

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
----	-------------------------	------	--------------------------	----------------------------

N1	Leverandøren skal sørge for sikker tilgang til DMFs SaaS-applikasjoner og ivareta relevante brukerkataloger og integrasjoner innenfor avtalens omfang.	M	Beskriv tilgangsstyring, SSO/MFA, brukerflyt og ansvarsdeling.	Bilag 2 og Bilag 3
N2	Leverandøren skal redegjøre for hvordan dokumentasjon, tilgangskontroll og livssyklus håndtering av SaaS-applikasjoner ivaretas.	B	Beskriv prosess, roller, avvikling og rapportering.	Bilag 2 og Bilag 6
N3	Leverandøren skal kunne samhandle med SaaS-leverandører der dette er nødvendig for drift, sikkerhet, feilsøking eller tilgangsstyring.	M	Beskriv grensesnitt og koordineringsansvar.	Bilag 2 og Bilag 6

O - Identitet og tilgangskontroll

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
O1	Leverandøren skal etablere og forvalte en enhetlig tjeneste for autentisering og tilgangskontroll på tvers av DMFs enheter, applikasjoner, filområder og skytjenester.	M	Beskriv løsning og ansvarsdeling.	Bilag 2
O2	Leverandøren skal drifte og forvalte DMFs Microsoft Entra ID-tenant og relevante M365-tjenester innenfor avtalens omfang.	M	Beskriv tjenesteomfang, sikkerhet og forutsetninger.	Bilag 2 og Bilag 3
O3	Leverandøren skal redegjøre for prosessen for opprettelse, endring og terminering av brukere og tilganger.	B	Beskriv prosess, roller, godkjenning og logging.	Bilag 2 og Bilag 6
O4	Leverandøren skal beskrive muligheter for automasjon og integrasjon av brukeroppsett mot HR-systemer eller andre kildesystemer.	B	Beskriv muligheter, forutsetninger og eventuelle opsjoner.	Bilag 2 og Bilag 7 ved opsjon
O5	Leverandøren skal beskrive løsning for privilegert tilgangsstyring, inkludert just-in-time-tilgang, godkjenning, MFA, rollebasert tilgang, logging, sesjonsopptak der relevant, tredjepartstilgang og periodisk tilgangsrevisjon.	B	Beskriv PAM-/tilgangsmodell og kontrolltiltak.	Bilag 2 og Bilag 6
O6	Leverandøren skal støtte tidsbegrenset, godkjent og loggført tilgang for DMFs IT-personell og relevante tredjeparter til servere og tjenester i leverandørens driftsmiljø.	M	Beskriv bestillingsflyt, godkjenning og logging.	Bilag 2 og Bilag 6

P - Kunstig intelligens og automasjon

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
P1	Leverandøren skal beskrive all bruk av KI, maskinlæring og automasjon som inngår i eller	B	Beskriv funksjoner, datatyper, behandlingssted, logging og menneskelig kontroll.	DMFs KI-policy og Bilag 2

	understøtter leveransen til DMF.			
P2	Leverandøren skal ikke ta i bruk nye KI-funksjoner som behandler DMFs data, logger, metadata, dokumentasjon, personopplysninger eller sikkerhetsinformasjon uten skriftlig forhåndsgodkjenning fra DMF.	M	Bekreft og beskriv endrings-/godkjenningsprosess.	DMFs KI-policy, Bilag 6 og Bilag 11
P3	Leverandøren skal beskrive hvordan tjenesten kan understøtte DMFs egen bruk av KI for DMFs applikasjoner på en sikker og kontrollert måte.	O	Beskriv mulige tjenester, forutsetninger og pris.	Bilag 2 og Bilag 7
P4	Leverandøren skal i tjenestekatalogen beskrive hvilke KI- og automasjonstjenester som kan leveres som tilleggstjenester.	O	Beskriv tjenestekatalog og pris.	Bilag 7
P5	Leverandøren skal beskrive hvordan KI-/automasjonsfunksjoner kan deaktiveres, begrenses eller konfigureres etter DMFs krav.	B	Beskriv styringsmuligheter og konsekvenser.	DMFs KI-policy og Bilag 2
P6	Leverandøren skal for alle KI-, maskinlærings- og automasjonsfunksjoner som inngår i leveransen eller tilbys som opsjon, redegjøre for relevant regulatorisk klassifisering og leverandørens vurdering av hvilke krav som kan få betydning for funksjonen i avtaleperioden.	B	Beskriv om funksjonen bygger på general-purpose AI-modell eller annen tredjepartsmodell, om funksjonen kan være underlagt særlige transparens-, risikostyrings- eller dokumentasjonskrav, leverandørens rolle, samt hvordan dokumentasjon, logging, risikostyring og menneskelig kontroll ivaretas.	DMFs KI-policy, Bilag 2 og Bilag 11 ved personopplysninger

Q - Utviklingsmiljø og analyse

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
Q1	Leverandøren skal levere og drifte utviklings-, test- og produksjonsmiljø for DMFs IT-utvikling.	M	Beskriv løsning, miljøseparasjon, drift og ansvar.	Bilag 2 og Bilag 3
Q2	Leverandøren skal tilby et Kubernetes-kompatibelt eller tilsvarende containerbasert kjøremiljø som dekker DMFs funksjonelle behov for provisjonering, skalering og avvikling av miljøer.	M	Beskriv plattform, brukergrensesnitt, CLI/API og avgrensninger.	Bilag 2

Q3	Leverandøren skal tilby innsikt i helsetilstand, ressursbruk og sikkerhetsstatus for DMFs utviklings-/containerbaserte miljøer.	M	Beskriv dashboard, logging, eksport og integrasjonsmuligheter.	Bilag 2 og Bilag 5
Q4	Leverandøren skal støtte integrasjon mot DMFs egne overvåkings- og utviklingsverktøy via åpne standarder der dette er relevant.	B	Beskriv støttede grensesnitt og forutsetninger.	Bilag 2
Q5	Leverandøren skal utføre løpende sårbarhetsskanning av container images, clustere og relevante komponenter, og gjøre funn tilgjengelige for DMF.	M	Beskriv frekvens, verktøy, kritikalitet og oppfølging.	Bilag 2 og Bilag 5
Q6	Leverandøren skal ikke ha ansvar for utvikling av DMFs fagsystemer, men skal legge til rette for sikker og stabil drift av miljøene der utvikling, test og produksjon skjer.	M	Bekreft ansvarsavgrensning.	Bilag 2 og Bilag 6

R - Etablering

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
R1	Leverandøren skal beskrive sin overordnede tilnærming til etablering av DMFs IT-tjenester, herunder reetablering, migrering, overgang og eventuell utfasing av dagens infrastruktur.	B	Beskriv metode, risiko, avhengigheter og forutsetninger.	Bilag 2 og Bilag 4
R2	Leverandøren skal etablere nødvendig støtteinfrastruktur for dokumentasjon, support, selvbetjening, overvåking, sikkerhet og rapportering.	M	Beskriv leveranser og milepæler.	Bilag 4
R3	Leverandøren skal beskrive steg, milepæler, avhengigheter, testopplegg og tidsplan for etableringsprosjektet.	M	Besvares i Bilag 4.	Bilag 4
R4	Leverandøren skal beskrive hvilke ressurser og hvilken medvirkning som kreves fra DMF og tredjeparter i etableringsfasen.	B	Beskriv roller, tidsbruk og forutsetninger.	Bilag 4 og Bilag 6
R5	Leverandøren skal beskrive test- og godkjenningsoopplegg før ordinær drift.	B	Beskriv testplan, akseptansekriterier og feilretting.	Bilag 4 og Bilag 5

S - Tjenestenivå, hendelsehåndtering og rapportering

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
S1	Leverandøren skal levere tjenestenivå for tilgjengelighet, brukerstøtte, hendelsehåndtering,	M	Bekreft at tjenestenivåene i Bilag 5 legges til grunn. Beskriv eventuelle tilbudte forbedringer.	Bilag 2 og Bilag 5

	sikkerhetshendelser, backup/gjenoppretting, rapportering og beredskapsøvelser i samsvar med Bilag 5.			
S2	Leverandøren skal beskrive hvordan tjenestenivåene i Bilag 5 måles, dokumenteres og rapporteres.	B	Beskriv målemetode, datagrunnlag, verktøy, rapporteringsformat og hvordan Kunden får innsyn i måldata.	Bilag 2 og Bilag 5
S3	Leverandøren skal beskrive hvordan avvik fra avtalt tjenestenivå håndteres, herunder klassifisering, eskalering, rotårsaksanalyse, korrigerende tiltak og rapportering til Kunden.	B	Beskriv prosess, roller, ansvar, eskalering og forbedringsarbeid.	Bilag 2, Bilag 5 og Bilag 6
S4	Leverandøren skal kunne håndtere uønskede hendelser etter klassifisering og frister fastsatt i Bilag 5.	M	Bekreft etterlevelse og beskriv hvordan hendelser registreres, prioriteres, eskaleres og lukkes.	Bilag 2 og Bilag 5
S5	Leverandøren skal beskrive hvordan kritiske og alvorlige sikkerhetshendelser håndteres, herunder varsling, eskalering, teknisk respons, kommunikasjon, rapportering og etterfølgende læring.	B	Beskriv prosess for håndtering av sikkerhetshendelser, inkludert samhandling mellom SOC/MDR/IRT, servicedesk, Kunden og relevante tredjeparter.	Bilag 2, Bilag 5 og Bilag 6
S6	Leverandøren skal beskrive hvordan backup, gjenoppretting og gjenopprettingstester måles og dokumenteres, herunder RTO/RPO der dette er relevant.	B	Beskriv backupstatus, restore-test, gjenopprettingsprosedyrer, rapportering og eventuelle begrensninger.	Bilag 2 og Bilag 5
S7	Leverandøren skal levere månedsrapportering i samsvar med Bilag 5. Rapporteringen skal gi Kunden grunnlag for å kontrollere tjenestenivå, sikkerhet, kapasitet, kostnader, hendelser og forbedringstiltak.	M	Bekreft og beskriv rapporteringsformat, innhold, datagrunnlag og leveringsmåte.	Bilag 2, Bilag 5 og Bilag 6
S8	Leverandøren skal gi Kunden tilgang til underliggende måldata, rapporter, logger eller eksportgrunnlag som er nødvendig for å kontrollere tjenestenivå, hendelsehåndtering og fakturagrunnlag.	M	Beskriv tilgang, format, begrensninger, sikkerhet og eventuell anonymisering.	Bilag 2, Bilag 5, Bilag 6 og Bilag 11
S9	Leverandøren skal beskrive eventuelle foreslåtte forbedringer eller supplerende KPI-er utover minimumskravene i Bilag 5.	B	Beskriv supplerende KPI-er, målemetode, verdi for Kunden og eventuell pris-/leveransekonsekvens.	Bilag 2 og Bilag 5

	Slike forslag kan ikke innebære lavere tjenestenivå enn kravene i Bilag 5.			
S10	Leverandøren skal akseptere at brudd på avtalte tjenestenivåer kan gi grunnlag for standardisert økonomisk kompensasjon etter Bilag 5.	M	Bekreft.	Bilag 5 og Bilag 7

T - Samhandling og governance

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
T1	Leverandøren skal være kontaktpunkt og koordinator mot relevante tredjeparter som har betydning for driftstjenesten.	M	Beskriv samhandling, rollefordeling og avgrensninger.	Bilag 2 og Bilag 6
T2	Leverandøren skal beskrive samhandlingsmodell mellom leverandøren og DMFs IT-administratorer.	B	Beskriv møtefora, roller, eskalering og arbeidsform.	Bilag 6
T3	Leverandøren skal fungere som proaktiv rådgiver innenfor avtalens omfang, herunder sikkerhet, drift, kostnadsutvikling, livssyklus, kapasitet og forbedring.	B	Beskriv rådgivningsmodell og rapportering.	Bilag 2 og Bilag 6
T4	Leverandøren skal delta i faste styrings- og driftsmøter etter nærmere regulering i Bilag 6.	M	Beskriv forslag til møte- og rapporteringsstruktur.	Bilag 6
T5	Leverandøren skal varsle DMF om forhold som kan påvirke sikkerhet, tjenestenivå, kostnad, behandlingssted, underleverandører eller regulatorisk etterlevelse.	M	Beskriv varslingsrutiner.	Bilag 6 og Bilag 11
T6	Leverandøren skal etablere og vedlikeholde samhandlingsplan og driftsspesifikasjon i samsvar med Bilag 5 og Bilag 6.	M	Beskriv hvordan dokumentene etableres, vedlikeholdes og godkjennes.	Bilag 2, Bilag 5 og Bilag 6
T7	Leverandøren skal beskrive hvordan månedsrapportering, driftsmøter, sikkerhetsmøter og forbedringstiltak knyttes sammen i kontraktsoppfølgingen.	B	Beskriv styringsmodell, møtefora, rapportering og tiltaksoppfølging.	Bilag 2, Bilag 5 og Bilag 6

U - Bærekraft

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
U1	Leverandøren skal beskrive sitt arbeid med bærekraft og miljøstyring som er relevant for leveransen.	B	Beskriv miljøstyring, tiltak og relevante sertifiseringer.	ISO 14001, Miljøfyrtårn eller tilsvarende

U2	Leverandøren skal beskrive hvordan miljøeffekt og bærekraftstiltak i leveransen evalueres og rapporteres til DMF.	B	Beskriv rapporteringsparametere og frekvens.	Bilag 2 og Bilag 6
U3	Leverandøren skal bidra til ressursoptimalisering i drift, herunder tiltak som kan redusere unødig forbruk av kapasitet, energi, lisenser og utstyr.	M	Beskriv tiltak og rapportering.	Bilag 2, Bilag 6 og Bilag 7
U4	Leverandøren skal beskrive hvordan levetidsforlengelse, gjenbruk og forsvarlig avhending ivaretas der leverandøren har oppgaver knyttet til utstyr eller komponenter.	B	Beskriv ansvarsdeling og rutiner.	Bilag 2 og Bilag 6

V - Kostnader

ID	Krav / besvarelsespunkt	Type	Leverandørens besvarelse	Dokumentasjon / henvisning
V1	Leverandøren skal beskrive prismodell for levering av IT-drift og infrastrukturtenester, herunder fastpris, enhetspris, brukerpris, volumpris og forbruksbaserte elementer.	B	Beskriv prismodell.	Bilag 7
V2	Leverandøren skal beskrive hvordan pris skaleres ved endringer i antall brukere, lokasjoner, enheter, kapasiteter eller tjenesteomfang.	B	Beskriv skaleringsmodell og terskler.	Bilag 7
V3	Leverandøren skal gi DMF løpende innsikt i skyforbruk, kostnadsdrivere, ressursutnyttelse, budsjettavvik og optimaliseringsmuligheter.	M	Beskriv rapportering, dashboard og varsling.	Bilag 2, Bilag 6 og Bilag 7
V4	Leverandøren skal tilby rapportering på forbruk, lisenskostnader og kostnadsutvikling, med eksportmulighet til Excel, Power BI eller tilsvarende.	M	Beskriv rapporteringsformat og frekvens.	Bilag 2 og Bilag 7
V5	Leverandøren skal oppgi et komplett kostnadsbilde for etablering og månedlig drift av alle tjenester. Kostnadene skal inkludere nødvendig støtteinfrastruktur og tilhørende lisensiering for drift, overvåking og administrasjon.	M	Besvares i prisskjema.	Bilag 7
V6	Leverandøren skal spesifisere eventuelle kostnader som ikke er inkludert i faste kostnader, og prise disse som opsjon eller timebasert tilleggstjeneste.	M	Besvares i prisskjema.	Bilag 7
V7	Leverandøren skal beskrive faktureringsvilkår, betalingsplan,	M	Besvares i Bilag 7.	Bilag 7

	prisregulering og håndtering av tredjepartslisenser.			
V8	Leverandøren skal kunne håndtere e-faktura og sende faktura i elektronisk format som DMF kan motta, uten kostnad for DMF.	M	Bekreft løsning.	Bilag 7
V9	Alle tjenester som er nødvendige for å oppfylle må-kravene og avtalt tjenestenivå skal være inkludert i faste eller enhetsbaserte priser, med mindre prisskjemaet uttrykkelig angir at ytelsen er en opsjon eller timebasert tilleggstjeneste.	M	Bekreft og vis hvor eventuelle unntak er priset.	Bilag 7/prisskjema
V10	Leverandøren skal ikke kunne kreve særskilt vederlag for ytelser som er nødvendige for å oppfylle kravene i Bilag 1, Bilag 5, Bilag 6 og Bilag 11, med mindre dette klart fremgår av Bilag 7.	M	Bekreft.	Bilag 7
V11	Leverandøren skal beskrive hvordan beregningsgrunnlag for standardisert økonomisk kompensasjon etter Bilag 5 kan identifiseres i faktura og prisskjema.	B	Beskriv hvordan månedlig fast driftsvederlag, tredjepartslisenser og forbruksbaserte kostnader skilles i fakturering og rapportering.	Bilag 7

Avtalens punkt 2.4.7 Planer og øvelser for beredskap og katastrofer

Leverandøren skal ha dokumenterte beredskaps- og katastrofeplaner for de tjenestene som omfattes av avtalen. Planene skal dekke håndtering av alvorlige driftsavbrudd, sikkerhetshendelser, tap av tilgjengelighet, datatap, kompromittering av identiteter, svikt i kritiske integrasjoner og behov for gjenoppretting av tjenester og data.

Leverandøren skal årlig, i samarbeid med Kunden, utarbeide en øvingsplan for IT-beredskap og gjenoppretting. Øvingsplanen skal være risikobasert og tilpasses Kundens kritiske tjenester, tjenestenivåkrav og sikkerhetsbehov.

Leverandøren skal som del av det faste vederlaget planlegge, gjennomføre og dokumentere minst én sikkerhets- eller beredskapsøvelse per år. Øvelsen kan gjennomføres som table-top, simulert øvelse eller teknisk øvelse, avhengig av formål og risiko.

Annet hvert år skal det i tillegg gjennomføres en utvidet gjenoppsettøvelse. Øvelsen skal teste gjenoppsett av utvalgte kritiske tjenester, data eller konfigurasjoner, herunder validering av backup, gjenoppsettstid og datatap der dette er relevant. Øvelsen skal så langt det er praktisk og sikkerhetsmessig forsvarlig gjennomføres i et produksjonsnært test- eller beredskapsmiljø.

Øvelsene skal som minimum kunne omfatte relevante scenarioer knyttet til:

- ransomware, skadevare, phishing eller kontokompromittering,
- alvorlig tjenestenedetid eller svikt hos kritisk underleverandør,
- tap av data eller behov for gjenoppretting,
- svikt i integrasjoner eller sentrale driftskomponenter,
- hendelser som krever samhandling mellom Kunden, Leverandøren og relevante tredjeparter.

Etter hver øvelse skal Leverandøren utarbeide en kort evalueringsrapport. Rapporten skal minimum beskrive gjennomføring, måloppnåelse, avvik, læringspunkter og anbefalte forbedringstiltak. Rapporten skal foreligge senest 30 kalenderdager etter gjennomført øvelse.

Identifiserte forbedringstiltak skal følges opp i avtalens ordinære styrings- og forbedringsarbeid. Tiltak som krever endring av leveransen, håndteres etter avtalens regler om endringshåndtering.

Nærmere krav til tjenestenivå, måling av RTO/RPO, rapportering og standardiserte kompensasjoner fremgår av Bilag 5. Eventuelle øvelser, tester eller beredskapsbistand utover det som uttrykkelig inngår i fast vederlag, prises etter Bilag 7.

Avtalens punkt 2.4.9 Nye versjoner av programvare

Nye versjoner, programrettelser, sikkerhetsoppdateringer og øvrige endringer i programvare som benyttes for å levere driftstjenesten, skal håndteres etter Leverandørens etablerte og dokumenterte oppgraderingsløp, med mindre annet følger av avtalen, Bilag 2, Bilag 5 eller Bilag 6.

Sikkerhetsoppdateringer og kritiske feilrettinger skal prioriteres og driftsettes uten ugrunnet opphold, basert på risiko, kritikalitet og behov for testing. Leverandøren skal kunne dokumentere hvordan sårbarheter vurderes, prioriteres, testes, implementeres og eventuelt kompenseres for dersom umiddelbar oppdatering ikke er mulig.

Endringer som kan påvirke Kundens bruk av tjenestene, informasjonssikkerhet, personvern, integrasjoner, kostnader eller tjenestenivå, skal varsles og håndteres i samsvar med Bilag 6 og avtalens regler om endringshåndtering.

Driftssetting av ordinære programrettelser, sikkerhetsoppdateringer og nye versjoner som er nødvendige for å opprettholde avtalt tjenestenivå og sikkerhet, inngår i det faste vederlaget, med mindre annet uttrykkelig fremgår av Bilag 7.

Avtalens punkt 2.4.10 Livssyklusforvaltning – tidsmessighet

Leverandøren har ansvar for livssyklusforvaltning av de tjenester, plattformer, komponenter, verktøy, standardprogramvare og øvrige ytelser som Leverandøren benytter eller leverer som del av driftstjenesten, i den utstrekning dette er nødvendig for å opprettholde avtalt tjenestenivå, sikkerhet og kontraktsmessig funksjonalitet.

Leverandøren skal løpende følge opp end-of-life, end-of-support, sikkerhetsrisiko, teknisk gjeld, kapasitetsbehov og behov for oppgradering eller utskifting av komponenter som inngår i leveransen. Leverandøren skal varsle Kunden i rimelig tid om forhold som kan påvirke drift, sikkerhet, kostnader, tjenestenivå eller videreutvikling.

Leverandøren skal minst årlig gi Kunden en oversikt over relevante livssyklusforhold, identifiserte risikoer og anbefalte tiltak. Tiltak som ligger innenfor avtalens omfang og er nødvendige for å opprettholde avtalt tjenestenivå og sikkerhet, inngår i vederlaget. Tiltak som innebærer endring av leveransen, håndteres etter avtalens regler om endringshåndtering.

Avtalens punkt 2.5.1 Generelt om avslutning av Avtalen

Leverandøren skal løpende vedlikeholde dokumentasjon og informasjon som er nødvendig for at Kunden kan forberede, gjennomføre og kontrollere overgang til ny leverandør, ny teknisk plattform eller egen drift.

Som minimum skal Leverandøren kunne utlevere oppdatert informasjon om:

- tjenestearkitektur og systemlandskap,
- konfigurasjoner, avhengigheter og integrasjoner,
- brukere, roller, tilganger og privilegerte kontoer,
- driftsrutiner, beredskapsrutiner og gjenopprettingsrutiner,
- oversikt over data, metadata, logger og backup,
- lisenser, standardprogramvare og underleverandører,
- kjente feil, risikoer, teknisk gjeld og åpne forbedringstiltak,
- eksportformater og fremgangsmåte for uttrekk av Kundens data.

Dokumentasjonen skal holdes oppdatert gjennom avtaleperioden og gjøres tilgjengelig for Kunden ved forespørsel. Ved avslutning av avtalen skal Leverandøren bistå med overføring av relevant dokumentasjon, data, konfigurasjoner og nødvendig kunnskap i samsvar med avslutningsplanen.

Leverandørens bistand ved avslutning prises etter Bilag 7, med mindre bistanden allerede inngår i fast vederlag eller følger av Leverandørens alminnelige plikt til å vedlikeholde og utlevere dokumentasjon.

Avtalens punkt 5.1.1 Leverandørens ansvar for leveransen – generelt

Leverandøren har et samlet ansvar for leveransen overfor Kunden, uavhengig av om hele eller deler av leveransen utføres av underleverandører.

Leverandøren skal sørge for nødvendig samordning og koordinering mellom egne ressurser, underleverandører og relevante tredjeparter som har betydning for driftstjenesten. Dette omfatter blant annet samhandling med applikasjonsleverandører, skyleverandører, nettverksleverandører, sikkerhetsleverandører og andre leverandører Kunden benytter.

Leverandøren skal levere tjenestene i samsvar med anerkjent god praksis for IT-drift, informasjonssikkerhet, personvern, beredskap og tjenestestyling. Leverandøren skal ha etablerte styringssystemer og prosesser som understøtter kravene i Bilag 1, Bilag 5, Bilag 6, Bilag 7 og Bilag 11.

Avtalens punkt 7.1 Eksterne rettslige krav og tiltak generelt

Leverandøren skal levere tjenestene i samsvar med de lover, forskrifter, pålegg og offentlige krav som gjelder for leveransen og for Kundens bruk av tjenestene.

Leverandøren skal særlig ivareta relevante krav knyttet til informasjonssikkerhet, personvern, konfidensialitet, logging, tilgangsstyring, datalagring, beredskap, sikkerhetsoppdatering, underleverandørstyring og revisjon.

Leverandøren skal varsle Kunden uten ugrunnet opphold dersom Leverandøren blir kjent med forhold som kan påvirke Kundens etterlevelse av rettslige krav, sikkerhetskrav, personvernkrav eller krav fra offentlig myndighet.

Dersom nye eller endrede rettslige krav får betydning for leveransen, skal Leverandøren redegjøre for konsekvensene og foreslå nødvendige tiltak. Eventuelle endringer i leveransen håndteres etter avtalens regler om endringshåndtering.

Avtalens punkt 7.2.1 Generelt om informasjonssikkerhet

Leverandøren skal ivareta informasjonssikkerheten i leveransen gjennom egnede tekniske, organisatoriske og fysiske tiltak. Tiltakene skal være risikobaserte og stå i forhold til tjenestenes kritikalitet, trusselbilde, datatyper og Kundens behov.

Leverandøren skal som minimum ivareta:

- sikker identitets- og tilgangsstyring,
- logging, overvåking og sporbarhet,
- sikker konfigurasjon og herding,
- sårbarhetsstyring og sikkerhetsoppdatering,
- hendelsehåndtering og varsling,
- beskyttelse mot skadevare, kontokompromittering og uautorisert tilgang,
- sikker fjernadministrasjon,
- sikker bruk av underleverandører,
- dokumentasjon og revisjonsspor.

Leverandøren skal kunne dokumentere sitt styringsystem for informasjonssikkerhet og relevante kontroller. Dokumentasjonen kan bestå av sertifiseringer, revisjonsrapporter, kontrollbeskrivelser eller annen likeverdig dokumentasjon.

Avtalens punkt 7.2.2 Leverandørens plikt til å holde Kundens data atskilt

Leverandøren skal sikre at Kundens data, metadata, logger, backup, konfigurasjoner og administrasjonsdata holdes logisk adskilt fra andre kunders data og fra Leverandørens egne data.

Tilgang til Kundens data skal begrenses til autorisert personell med tjenstlig behov. Tilganger skal være rollebaserte, tidsbegrensede der dette er relevant, og underlagt logging og periodisk kontroll.

Leverandøren skal ikke bruke Kundens data, metadata, logger, dokumentasjon, sikkerhetsinformasjon eller personopplysninger til egne formål, analyse, produktutvikling, modelltrening, finjustering av KI-modeller eller forbedring av tjenester for andre kunder uten Kundens uttrykkelige skriftlige forhåndsgodkjenning.

Leverandøren skal beskrive i Bilag 2 og Bilag 11 hvordan atskillelse, tilgangsstyring, logging, behandlingssted, underleverandører og sletting ivaretas.

Avtalens punkt 8.3 Rettigheter til data

Kunden beholder alle rettigheter til egne data, metadata, dokumentasjon, konfigurasjoner, logger og øvrig informasjon som behandles eller etableres som ledd i leveransen, med mindre annet uttrykkelig følger av avtalen.

Leverandøren skal ikke disponere over Kundens data til andre formål enn det som er nødvendig for å levere avtalte tjenester. Leverandøren skal ikke gjøre tilbakeholdsrett gjeldende i Kundens data, dokumentasjon eller informasjon som er nødvendig for drift, revisjon, beredskap eller avslutning av avtalen.

Kunden skal kunne få utlevert egne data og relevant dokumentasjon i dokumenterte, alminnelig brukte og maskinlesbare formater. Leverandøren skal beskrive format, fremgangsmåte, frister og eventuelle tekniske forutsetninger for uttrekk og overføring.

Leverandøren skal medvirke til testing av datauttrekk og overføring der dette er nødvendig for revisjon, beredskap, leverandørbytte, avslutning av avtalen eller annen lovlig bruk. Nærmere pris for bistand utover det som inngår i fast vederlag, fremgår av Bilag 7.

Ved avtalens opphør skal Leverandøren tilbakelevere, overføre, slette eller destruere Kundens data i samsvar med Kundens instruksjer, avtalen og databehandleravtalen.

Bilag 2 – Leverandørens løsningsspesifikasjon

Bilaget skal fylles ut av Leverandøren.

Leverandøren skal i dette bilaget beskrive den tilbudte løsningen og hvordan leveransen oppfyller Kundens behov og krav i Bilag 1 og Bilag 1.1. Beskrivelsen skal være konkret, etterprøvbar og tilpasset den tilbudte leveransen til Kunden.

Leverandøren skal besvare alle krav og besvarelespunkter i Bilag 1.1. Besvarelsen skal struktureres med henvisning til krav-ID. Der Leverandøren viser til dette Bilag 2, skal det fremgå tydelig hvilket krav eller besvarelespunkt teksten gjelder.

Leverandøren skal særlig merke seg følgende:

- **M-krav** skal bekreftes oppfylt. Dersom Leverandøren ikke oppfyller et M-krav, eller oppfyller det med avvik, forutsetninger eller begrensninger, skal dette komme frem klart og uttrykkelig i teksten.
- **B-besvareleskrav** skal besvares med en konkret redegjørelse for tilbudt løsning, metode, organisering, verktøy, ansvar, risiko og eventuelle forutsetninger.
- **O-opsjoner** skal beskrives der dette er etterspurt, og prises i Bilag 7/prisskjema dersom opsjonen skal kunne benyttes av Kunden.
- Forutsetninger, avgrensninger eller standardvilkår som kan påvirke leveransen, pris, ansvar, sikkerhet, personvern, tjenestenivå eller Kundens rettigheter, skal fremgå tydelig. Slike forhold kan bli vurdert som avvik eller forbehold dersom de ikke er i samsvar med konkurransegrunnlaget eller avtalen.

Generelle produktark, markedsmateriell eller standardbeskrivelser kan legges ved, men erstatter ikke Leverandørens konkrete besvarelse i Bilag 1.1 og Bilag 2.

Avtalens punkt 1.1 – Avtalens omfang

Leverandøren skal beskrive den samlede løsningen som tilbys for levering av driftstjenesten.

Beskrivelsen skal minimum omfatte:

- overordnet løsningsarkitektur,
- tjenestemodell og leveransemodell,
- organisering av leveransen,
- ansvarsdeling mellom Leverandøren, Kunden, underleverandører og tredjeparter,
- hvilke tjenester, plattformer, verktøy, lisenser og standardprogramvare som inngår,
- hvilke deler av leveransen som leveres som standardtjeneste, kundespesifikk tjeneste, opsjon eller tilleggstjeneste,
- hvordan løsningen oppfyller kravene i Bilag 1 og Bilag 1.1,
- eventuelle avgrensninger, forutsetninger eller avhengigheter.

Leverandøren skal beskrive løsningen på en måte som gjør det mulig for Kunden å vurdere sammenhengen mellom krav, tilbudt løsning, tjenestenivå og pris.

Avtalens punkt 2.3.2.6 – Leverandørens overtakelse av Kundens infrastruktur – verifisering mv.

Leverandøren skal beskrive hvilke forutsetninger som ligger til grunn for løsningsspesifikasjonen, etableringsplanen og prisingen.

Beskrivelsen skal minimum omfatte:

- hvilke opplysninger i Bilag 3 og øvrige konkurransedokumenter Leverandøren har lagt til grunn,
- behov for verifisering før eller under etableringsfasen,
- forhold som kan påvirke etablering, migrering, drift, sikkerhet, tjenestenivå eller pris,
- forutsetninger om Kundens medvirkning,
- forutsetninger om eksisterende leverandør, tredjeparter, tilganger, dokumentasjon og teknisk tilstand,
- hvordan avvik mellom opplyst og faktisk tilstand skal håndteres.

Forutsetninger som kan innebære avvik fra konkurransegrunnlaget eller avtalen, skal fremgå klart og uttrykkelig.

Avtalens punkt 2.4.9 – Nye versjoner av programvare

Leverandøren skal beskrive anbefalt oppdaterings- og livssyklusløp for programvare, plattformer, sikkerhetskomponenter, operativsystem, klienter, servere, nettverk, skytjenester og øvrige komponenter som inngår i leveransen.

Beskrivelsen skal minimum omfatte:

- ordinær oppdateringstakt,
- håndtering av sikkerhetsoppdateringer og kritiske sårbarheter,
- testing før produksjonssetting,
- varsling til Kunden,
- håndtering av endringer som kan påvirke tjenestenivå, sikkerhet, personvern, integrasjoner eller pris,
- håndtering av unntak og kompenserende tiltak.

Avtalens punkt 2.4.10 – Livssyklusforvaltning – tidsmessighet

Leverandøren skal beskrive hvordan livssyklusforvaltning ivaretas for utstyr, programvare, standardtjenester, skytjenester, lisenser, sikkerhetskomponenter og andre ytelser som er nødvendige for å opprettholde avtalt tjenestenivå og sikkerhet.

Dersom Leverandøren ikke påtar seg totalansvar for livssyklusforvaltning av enkelte komponenter eller tjenester, skal dette fremgå klart og uttrykkelig, med angivelse av:

- hvilke komponenter eller tjenester dette gjelder,
- hvem som har ansvar,

- hvilke konsekvenser dette har for drift, sikkerhet, tjenestenivå, pris og exit,
- hvordan Kunden varsles om end-of-life, end-of-support, teknisk gjeld og behov for tiltak.

Avtalens punkt 5.1.1 – Leverandørens ansvar for leveransen – generelt / standardvilkår

Leverandøren skal beskrive hvordan det samlede ansvaret for leveransen ivaretas, inkludert ansvar for underleverandører og koordinering mot relevante tredjeparter.

Eventuell standardprogramvare, standardtjenester, skytjenester eller tredjepartsleveranser som inngår i leveransen og som leveres under standard lisensvilkår eller standard avtalevilkår, skal spesifiseres her.

For hver slik leveranse skal Leverandøren minimum oppgi:

- navn på produkt/tjeneste,
- produsent/underleverandør,
- formål i leveransen,
- hvilke data som behandles,
- behandlingssted der dette er relevant,
- om vilkårene påvirker Kundens rettigheter, sikkerhet, personvern, revisjonsmulighet, exit eller pris,
- henvisning til lisensvilkår eller standardvilkår vedlagt i Bilag 10.

Lisensvilkår eller standardvilkår som ikke er uttrykkelig angitt her og vedlagt i Bilag 10, kan ikke gjøres gjeldende overfor Kunden.

Avtalens punkt 5.1.2 – Kundens ansvar og medvirkning

Leverandøren skal beskrive hvilken medvirkning som kreves fra Kunden for å etablere og levere driftstjenesten.

Beskrivelsen skal minimum omfatte:

- nødvendige roller hos Kunden,
- forventet tidsbruk og tilgjengelighet,
- beslutninger og godkjenninger Kunden må gi,
- tilganger, dokumentasjon og informasjon Kunden må stille til rådighet,
- medvirkning fra eksisterende leverandør og andre tredjeparter,
- konsekvenser dersom nødvendig medvirkning ikke gis.

Krav til Kundens medvirkning skal være realistiske, konkrete og tilpasset Kundens organisasjon og størrelse.

Avtalens punkt 5.2.4 – Kundens ansvar for sine ressurser

Leverandøren skal beskrive eventuelle særskilte kompetansekrav som Kundens ressurser må ha for at leveransen skal kunne etableres og forvaltes som forutsatt.

Beskrivelsen skal skille mellom:

- kompetanse som kreves i etableringsfasen,
- kompetanse som kreves i ordinær drift,
- kompetanse som kreves for sikkerhets- og beredskapsarbeid,
- kompetanse som kreves ved exit eller overgang til ny leverandør.

Dersom Leverandøren forutsetter at Kunden har bestemte roller, sertifiseringer, administratorrettigheter eller teknisk kompetanse, skal dette beskrives uttrykkelig.

Avtalens punkt 7.1 – Eksterne rettslige krav og tiltak generelt

Leverandøren skal beskrive hvordan rettslige, regulatoriske og partsspesifikke krav som er angitt i Bilag 1, Bilag 11 og øvrige konkurransedokumenter ivaretas gjennom den tilbudte løsningen.

Beskrivelsen skal minimum omfatte hvordan Leverandøren ivaretar krav til:

- informasjonssikkerhet,
- personvern og databehandlerforpliktelser,
- behandlingssted og bruk av underleverandører,
- logging, sporbarhet og revisjon,
- tilgangsstyring og privilegerte tilganger,
- beredskap og hendelsehåndtering,
- datalagring, datauttrekk og sletting,
- bruk av kunstig intelligens, maskinlæring og automasjon,
- klima- og miljøkrav der dette er relevant for leveransen.

Leverandøren skal beskrive eventuelle forhold ved løsningen som kan ha betydning for Kundens etterlevelse av rettslige krav, herunder bruk av standardtjenester, skytjenester, underleverandører eller behandling av data utenfor Norge.

Leverandøren skal i tillegg beskrive hvordan leverandøren overvåker, vurderer og implementerer endringer i relevant regelverk, myndighetskrav, standarder og bransjekrav som kan påvirke leveransen i avtaleperioden, herunder krav til cybersikkerhet, skytjenester, KI, data, personvern, standardprogramvare, underleverandører og leverandørkjeder.

Beskrivelsen skal minst omfatte ansvar, prosess, varslingsrutiner til Kunden, konsekvensvurdering, foreslåtte tiltak og håndtering av tiltak som krever endring av leveransen.

Bilag 3: Beskrivelse av det som skal driftes

Avtalens punkt 1.1 Avtalens omfang

Bilag 3: Beskrivelse av det som skal driftes

Bilaget er fylt ut av Kunden og beskriver dagens IT-miljø hos DMF. Formålet med bilaget er å gi leverandørene et faktagrunnlag for å forstå omfang, kompleksitet, eksisterende arkitektur, lokasjoner, tjenester, systemlandskap, klienter, servere, skytjenester, integrasjoner og øvrige forhold som har betydning for driftstjenesten.

Opplysningene i bilaget beskriver dagens situasjon og kjente planlagte endringer per juni 2026, med mindre annet er uttrykkelig angitt. Tall for brukere, klienter, mobile enheter, servere, lisenser, lagring, applikasjoner og øvrige kapasiteter må anses som estimater og kan endres i avtaleperioden.

Produktnavn, tjenestenavn og leverandørnavn som fremgår av bilaget beskriver dagens miljø og innebærer ikke i seg selv krav om at samme produkter, tjenester eller leverandører skal videreføres i ny leveranse, med mindre dette uttrykkelig følger av Bilag 1, Bilag 1.1, Bilag 5 eller Bilag 7.

Krav til fremtidig leveranse følger av Bilag 1 og Bilag 1.1. Leverandørens løsning skal beskrives i Bilag 2. Tjenestenivå følger av Bilag 5, og priser og prisforutsetninger følger av Bilag 7.

Dagens driftsmiljø

Overordnet beskrivelse:

DMF har hovedkontor i Trondheim (HK), kontor i Longyearbyen på Svalbard (LS) og et prosessanlegg på Løkken Verk (LV).

IT-miljøet består overordnet av følgende komponenter per juni 2026:

- 2 administrerte nettverk + 1 adm. nettverk under «onboarding» på LV
- Ca 90 PC-klienter (82 aktive p.t.)
- Ca 80 «fysiske» brukere (75 aktive p.t.)
- 14 servere i privat sky (Oslo/Stavanger), hvorav 7 utviklingsservere (OpenShift).
- Public sky: Microsoft Entra ID Tenant, M365 i Sovereign Cloud Norway
- SaaS-tjenester (primærtjenester): P360 Online, DFØ: Lønn, HR og økonomi/regnskap, Juridiske (Lovdata Pro og Gyllendal Rettsdata), ArcGIS Basic (Online)

Antall fysiske brukere pr brukersted:

- HK – 80 stk
- LS – 2 (varierer fra 0-4 stk i over året) – Ikke fast bemannet p.t.
- LV – 2 (varierer fra 0-2 stk i over året) – Ikke fast bemannet.

Hjemmekontor: Alle brukere har mulighet til å benytte hjemmekontor. Tilgang utenfor administrert kontornettverk skjer via automatisk VPN eller tilsvarende sikker tilgangsløsning.

Tjenester per brukersted

Hovedkontor i Trondheim: Ladebekken 50, 7066 Trondheim

- Administrert nettverk: Kablet, WiFi (jobbnettverk og gjestenettverk)
- Betinget tilgang (Conditional Access) til jobbnettverket (kablet/WiFi).
- Pålogging: Sertifikatbasert (aut. pålogging for adm. klienter)
- Linje: 200 Mbit symmetrisk. Det er ikke etablert linjeredundans p.t. Eventuelle krav til redundans i ny leveranse fremgår av Bilag 1 og Bilag 1.1.
- WiFi: Cisco (2,4 og 5 GHz), 14 aksesspunkt.
- Kablet: Ca 100 punkt (1 pr kontorplass/møterom/printerrom)
- Administrerte MFP (printere): 2 stk (KM)
- Møterom: 7 stk
 - o 1 kombinert allmøte/kantine med 3 projektorer og lydanlegg m/2 trådløse mikrofoner: Kapasitet Ca 80 personer
 - o 3 store møterom (10-16 pers.), VC: Logitech MeetUp + LCD-skjerm (65-90")
 - o 3 små møterom (4-6 pers.), VC: Logitech MeetUp + LCD-skjerm (65-90")
- Stillerom: 4 stk (1-2 pers.)
 - o VC: Logitech e925 og LCD (ca 50")

Kontoret på Svalbard er p.t. lokalisert i Bergmesterboligen. DMF planlegger å flytte tilbake til sentrum i avtaleperioden og samlokalisere med NFD, tidligst i 2027. Leverandøren må derfor ta høyde for at lokasjon, linje, nettverksoppsett og utstyr ved Svalbard-kontoret kan bli endret i avtaleperioden. Eventuelle endringer håndteres etter avtalens endringsbestemmelser.

- Administrert nettverk: Kablet, WiFi (jobbnettverk og gjestenettverk)
- Betinget tilgang (Conditional Access) til jobbnettverket (kablet/WiFi).
- Pålogging: Sertifikatbasert (aut. pålogging for adm. klienter)
- Linje: Telenor Internett Aksess Bedrift, 10 Mbit – m/redundans (fallback: mobilt bredbånd 4G/5G)
- WiFi: Cisco (2,4 og 5 GHz), 1 aksesspunkt.
- Kablet: 3 punkt p.t. (kontorplass/møterom/printer)
- Administrerte MFP (printere): 1 stk (Canon)
- Møterom: 1 stk, kapasitet 12 personer
 - o VC: Logitech e925 + LCD-skjerm ca 75"

Serverefunksjoner i privat sky:

Name	Applications	Asset type	Platform	Region	OS	CPU	Memory	Environment
YO-X-D-1	Azure Backup Vault (yo.cust.xcv.net), Entra Password Protection (yo.cust.xcv.net), Intility Active Directory (yo.cust.xcv.net)	Domain Controller	InCloud	Oslo	Windows Server 2022	2	8	Prod
YO-X-D-2	Azure Backup Vault (yo.cust.xcv.net), Entra Password Protection (yo.cust.xcv.net), Intility Active Directory (yo.cust.xcv.net)	Domain Controller	InCloud	Oslo	Windows Server 2022	2	8	Prod
YO-X-S-1	Intility File Server	Virtual Machine	InCloud	Oslo	Windows Server 2022	2	4	Prod
YO-X-S-2	Entra ID Connect, Entra Password Protection (yo.cust.xcv.net), Intility Bridge	Virtual Machine	InCloud	Oslo	Windows Server 2022	2	6	Prod
YO-X-S-3	ASVA Dirsync, Azure Automation	Virtual Machine	InCloud	Oslo	Windows Server 2022	2	4	Prod
YO-X-S-4	InCloud Connect (GPO Mgmt)	Virtual Machine	InCloud	Oslo	Windows Server 2022	2	4	Prod
YO-X-S-5	MSSQL-Server: EQS, Ayfie Locator, Public 360 (arkivert)	Virtual Machine	InCloud	Oslo	Windows Server 2022	4	24	Prod
YO-X-S-9	Ayfie Locator	Virtual Machine	InCloud	Oslo	Windows Server 2025	12	48	Prod
YO-X-S-10	EQS Kvalitetssystem	Virtual Machine	InCloud	Oslo	Windows Server 2022	2	8	Prod
YO-X-S-11	OpenShift 4 (YO Test)	Openshift AppNode	InCloud	Oslo	Red Hat Enterprise Linux 8	2	16	Test/QA
YO-X-S-12	OpenShift 4 (YO Test)	Openshift AppNode	InCloud	Oslo	Red Hat Enterprise Linux 8	2	16	Test/QA
YO-X-S-13	OpenShift 4 (YO Prod - Availability Set)	Openshift AppNode	InCloud	Oslo	Red Hat Enterprise Linux 8	4	24	Prod
YO-X-S-14	OpenShift 4 (YO Prod - Availability Set)	Openshift AppNode	InCloud	Oslo	Red Hat Enterprise Linux 8	4	24	Prod
YO-X-S-15	eInnsyn	Virtual Machine	InCloud	Oslo	Windows Server 2022	2	4	Prod
YO-X-S-16	OpenShift Infra Nodes (YO - Availability Set)	Openshift AppNode	InCloud	Oslo	Red Hat Enterprise Linux 8	4	16	Prod
YO-X-S-17	OpenShift Infra Nodes (YO - Availability Set)	Openshift AppNode	InCloud	Oslo	Red Hat Enterprise Linux 8	4	24	Prod
YO-X-S-18	(OpenShift Infra Nodes (YO - Availability Set)?)	Openshift AppNode	InCloud	Oslo	Red Hat Enterprise Linux 8	4	24	Unknown

Lagringskapasitet servere:

Samlet lagringsbehov i privat cloud per juni 2026:

Production			
HL105	Production Storage	per 100 GB	90,0
HL109	Backup Storage	per 100 GB	131,0
HL132	Elasticsearch Storage High Performance	per 20 GB	6,0
HL127	Disk Profile Upgrade 5 000 IOPS	per disk	4,0

Filserverkapasitet utgjør i dag om lag 7 TB produksjonslagring med rask tilgang. Øvrig lagring består i hovedsak av serverdisker. DMF har i tillegg data med lavere krav til hyppig tilgang, anslagsvis 2–3 TB per juni 2026. Behovet for slik lagring kan endre seg i avtaleperioden, blant annet som følge av digitalisering av papirarkiv og økt bruk av SharePoint/Teams. Eventuelle endringer i lagringsbehov, lagringsprofiler eller flytting av data håndteres innenfor avtalens ordinære bestemmelser om kapasitetsendringer, pris og endringshåndtering.

PC-klienter:

PC-klienter: 80+ stk. Lenovo ThinkPad T14/L14 eller tilsv. m/Windows Ent/Pro v11. 2 stk MacBook Air M2/M3 til uttesting (kun 1 i aktiv testing p.t.). Alle PC-klienter er administrert i Intune.

Antall maskiner 82 + 0 i dag	Windows 81	Mac 1
Produsentgaranti 32.9% innenfor garanti	Maskinvare 2 Leverandører 12 Modeller	Operativsystem 3 Ulike systemer

Mobiler:

Vi skiller mellom «Jobbmobiler» (eies av DMF og benyttes kun til jobb) og «Kombinert mobiler» (eid av DMF/bruker og benyttes som kombinert jobb- og privat mobil).

Alle mobiler er administrerte i Intune og har tilgang til DMF-data dersom de tilfredsstiller policy (krav til oppdatert OS m.m.).

Jobbmobiler (alle Apple iPhone) er registrert i ABM med Business Apple-ID, og er fullt administrert («fully managed»). Kun godkjente apper i MS Firmaportal kan installeres av bruker utover obligatoriske/preinstallerte apper.

Kombinertmobiler er delvis administrerte; dvs. jobb + privat profil. Kun apper fra MS Firmaportal har tilgang til DMF-data (jobbprofil).

Antall mobiler 68 + 0 i dag	Android 18	iOS 50
Innrullingsrate ⓘ 86.67% av enhetene →	Aktiv Compliance Rate ⓘ ✓ 100% av enhetene	Maskinvare 3 Leverandører 34 Modeller →

Applikasjoner: Intune Firmaportal

Totalt 97 applikasjoner	Nye de siste 30 dagene 1 applikasjoner →	Oppdatert de siste 30 dagene 17 applikasjoner →
Windows 54 applikasjoner →	Mac 0 Mac →	Mobil 23 iOS 20 Android →

SaaS-applikasjon: (de viktigste)

- P360 Online (Tieto): Arkivtjenester
- DFØ: Lønn og økonomitjenester
- Juridiske: Lovdata Pro og Rettsdata (Gyldendal)
- ArcGIS Basic (Online)
- Plandisc (Visma)
- Decisions (meetingdecisions.com)
- Canva (Canva)

Andre programvarelisenser: (utover MS-applikasjoner i M365)

- 2 stk Adobe Creative Cloud
- 3 stk Stata (statistikkprogram)
- 12 stk ArcGIS Pro

Administrerte printere (MFP):

Printere

Oversikt over printere og printerkøer

Printere 3 + 0 i dag	Printerkøer 3 unike køer	Tilkoblet 3 printere er tilkoblet	Frakoblet 0 printere er frakoblet	
Printere	Printerkøer			
Hurtigsøk	Filter	3 resultater	Eksporter Kolonner 10 rader	
Printer	Firma	Lokasjon	Serienummer	Status
> Canon IR-ADV C3525 III	DIRMIN - Direktoratet for mineralforvaltning med Bergmesteren for Svalbard	DIRMIN Avdelingskontor	2GE25806	Online
> Konica Minolta bizhub C558	DIRMIN - Direktoratet for mineralforvaltning med Bergmesteren for Svalbard	DIRMIN - Direktoratet for mineralforvaltning med Bergmesteren for Svalbard - Trondheim Hovedkontor	A79K021010165	Online
> Konica Minolta bizhub C558	DIRMIN - Direktoratet for mineralforvaltning med Bergmesteren for Svalbard	DIRMIN - Direktoratet for mineralforvaltning med Bergmesteren for Svalbard - Trondheim Hovedkontor	A79K021010173	Online

Beskrivelse av dagens IT-utviklingsmiljø:

DMF har i dag en portefølje av tjenester som er utviklet med innleide IT-konsulenter og interne ressurser. Disse omfatter:

- Hjemmeside med datadeling og kartløsninger.
- Integrasjonspunkt for innsendinger av skjema utviklet i Altinn 3.
- Interne fagsystem/registreringsløsninger.
- Dataplattform med sammenstilling av data fra interne og eksterne datakilder.

DMF har i dag selv ansvar for videreutvikling av funksjonalitet, feilretting og overvåkning av tjenestene som utvikles, mens leverandøren står for all drift av infrastrukturen.

Dagens driftsløsning for IT-utvikling består av følgende kjernekomponenter:

- Kubernetes
 - o Navnerom Test: 2 noder (2 CPU / 16 RAM hver).
 - o Navnerom Prod: 3 noder (4 CPU / 24 RAM hver).
 - o Plattform i dag: *OpenShift*.
- Kildekodehåndtering, bygg og pipeline.
 - o Plattform i dag: *GitLab CI/CD*.
- Utrulling til Kubernetes basert på konfigurasjon fra kildekode.
 - o Plattform i dag: *ArgoCD*.
- Administrasjon av hemmeligheter og tilgjengeliggjøring i Kubernetes.
 - o Plattform i dag: *HashiCorp Vault med Vault Operator*.
- Logging og feilsøk.
 - o Plattform i dag: *Elasticsearch*.

DMF benytter ikke plattformspesifikk funksjonalitet, og ny leverandør kan foreslå alternative plattformer for å tilfredsstille de funksjonelle krav IT-utvikling har til sitt driftsmiljø.

Administrerte identiteter og lisenser: (per 2026-06-22)

Platform services

Artikkel	Navn	Antall
P110	24/7/365 End-to-end responsibility & support	75
P137	End-User Application Management	75
P113	Managed Identity & Access Platform	75
P103	Managed Resource Account	32
P115	Managed Security & Compliance Platform	75
P130	Managed Shared Calendar	8
P131	Managed Shared Mailbox	19
P106	Privileged Access User	7

Microsoft 365 CSP

Artikkel	Navn	Antall
SD844	Exchange Online (Plan 1) (Commercial, Monthly Billing, Monthly Duration)	4
SD651	Microsoft 365 Business Premium (Commercial, Monthly Billing, Annual Duration)	76
SD6555	Microsoft Defender Suite for Microsoft 365 Business Premium (Commercial, Monthly Billing, Annual Duration)	71
SD412	Office 365 E1 (Commercial, Monthly Billing, Annual Duration)	1
SD649	Power Automate Premium (Commercial, Monthly Billing, Annual Duration)	1
SD462	Power BI Pro (Commercial, Monthly Billing, Annual Duration)	5

Mailbox

Artikkel	Navn	Antall
P508	Exchange Online Email	106

Licenses

Artikkel	Navn	Antall
P683	Intility 365 Manager Compliance Center User	75
P610	Managed Defender for Endpoint Clients	75
P674	Managed Defender for Identity	71
P667	Managed Defender for Office 365	75
P121	Managed Microsoft 365 Enterprise	75
P725	Managed Risky User	71

Application options

Artikkel	Navn	Antall
P135	Intility Multi-Factor Authentication CA	77
VPN	Intility Remote Access via VPN	74

Application handled

Artikkel	Navn	Antall
P660	Managed Dynatrace User Access	2
P562	Managed GitLab	3
P188	Mobile VPN	1

Annet

Artikkel	Navn	Antall
	Deaktiverte brukere (siste 12 mnd)	8

Bilag 4: Prosjekt- og fremdriftsplan for etableringsfasen

Bilaget fylles ut av Leverandøren basert på Kundens overordnede føringer i dette bilaget, Bilag 1, Bilag 2, Bilag 3, Bilag 5, Bilag 6 og Bilag 7.

Leverandøren skal i tilbudet beskrive en realistisk og forpliktende plan for etablering av driftstjenesten. Planen skal vise hvordan Leverandøren vil gjennomføre overgang fra dagens driftsmodell til ny driftstjeneste med lav risiko for driftsavbrudd, sikkerhetshendelser, tap av data, mangelfull brukerstøtte eller mangelfull kontroll med tilganger og dokumentasjon.

Planen skal minimum beskrive:

- hovedaktiviteter og milepæler,
- fremdrift frem til oppstartsdag,
- organisering, roller og ansvar,
- behov for medvirkning fra Kunden, eksisterende leverandør og tredjeparter,
- verifisering av dagens miljø,
- migrering, etablering og overtakelse av tjenester,
- etablering av servicedesk, overvåking, SOC/MDR/IRT, backup og rapportering,
- test før oppstartsdag,
- plan for oppstartsperiode og godkjenningsperiode,
- risikoer, avhengigheter og risikoreduserende tiltak.

Leverandøren skal beskrive eventuelle forutsetninger for fremdriftsplanen. Forutsetninger som kan påvirke pris, fremdrift, risiko, sikkerhet, tjenestenivå eller Kundens medvirkning, skal fremgå klart.

Overordnet fremdriftsplan for etablering av driftstjenesten

Leverandøren skal fylle ut overordnet fremdriftsplan for etableringsfasen.

Fremdriftsplanen skal minimum angi:

- tidspunkt for kontraktsignering,
- oppstart av etableringsfasen,
- planleggingsfase,
- verifisering av dagens miljø,
- etablering av nødvendige drifts-, support-, sikkerhets- og rapporteringsfunksjoner,
- eventuell migrering eller reetablering av tjenester,
- test før oppstartsdag,
- oppstartsperiode,
- oppstartsdag for ordinær drift,
- godkjenningsperiode,

- leveringsdag.

Planlagt oppstartsdag for ordinær drift er [01.10.2026].

Dersom Leverandøren mener at planlagt oppstartsdag ikke kan nås, skal dette fremgå tydelig av tilbudet, med begrunnelse og forslag til alternativ fremdriftsplan.

Avtalens punkt 2.3.1.2 – Delleveranser

Leverandøren skal beskrive om etableringen foreslås gjennomført som én samlet leveranse eller som delleveranser.

Dersom Leverandøren foreslår delleveranser, skal beskrivelsen minimum omfatte:

- hvilke tjenester eller områder hver delleveranse omfatter,
- rekkefølge og avhengigheter mellom delleveransene,
- planlagt tidspunkt for test og eventuell idriftsettelse av hver delleveranse,
- hvordan allerede idriftsatte delleveranser skal kontrolleres ved senere delleveranser,
- hvordan samlet ytelse, stabilitet, sikkerhet og kapasitet skal testes før ordinær drift,
- hvilke konsekvenser delleveransene har for Kundens medvirkning, risiko og ressursbruk.

Delleveranser kan bare tas i bruk dersom dette er forsvarlig ut fra drift, sikkerhet, personvern, brukerstøtte og Kundens behov for sammenhengende tjenesteleveranse.

Med mindre annet uttrykkelig avtales, skal det gjennomføres samlet test før oppstartsdag og samlet godkjenningssperiode for driftstjenesten.

Dersom Leverandøren foreslår at én eller flere delleveranser skal unntas fra samlet testing, skal dette begrunnes særskilt.

Avtalens punkt 2.3.2.3 – Testplaner

Leverandøren skal utarbeide testplan for driftstjenesten før oppstartsdag. Testplanen skal forelegges Kunden for godkjenning senest 4 uker før planlagt oppstart av test, med mindre annet er avtalt skriftlig.

Testplanen skal minimum dekke:

- identitets- og tilgangsstyring, herunder Entra ID, MFA, privilegerte tilganger og godkjenningsflyt,
- M365-tjenester og relevante administrasjonsfunksjoner,
- klientadministrasjon, Intune, Autopilot og mobiladministrasjon,
- nettverk, VPN/fjerntilgang og sentrale lokasjonstjenester,
- server- og privat sky-tjenester,
- utviklings-, test- og produksjonsmiljø,
- backup, restore og verifikasjon av gjenoppretting,
- servicedesk, saksflyt, eskalering og rapportering,
- SOC/MDR/IRT, sikkerhetsovervåking og hendelsesvarsling,

- dokumentasjon, driftsrutiner og rapporteringsoppsett.

Testplanen skal angi testaktiviteter, akseptansekriterier, testdata, roller, ansvar, forventet medvirkning fra Kunden og håndtering av feil.

Kunden skal ha rett til å delta i utarbeidelse og gjennomføring av testene.

Dersom Leverandøren mener at enkelte testområder ikke er relevante, skal dette begrunnes.

Avtalens punkt 2.3.2.6 – Leverandørens overtakelse av Kundens infrastruktur – verifisering

Leverandøren skal i etableringsfasen gjennomføre nødvendig verifisering av Kundens eksisterende driftsmiljø basert på opplysningene i Bilag 3 og øvrige konkurransedokumenter.

Verifiseringen skal minimum omfatte relevante forhold knyttet til:

- brukere, klienter og mobile enheter,
- Entra ID, M365, Intune og administrasjonsoppsett,
- nettverk, lokasjoner og fjerntilgang,
- servere, privat sky, lagring og backup,
- utviklingsmiljø og integrasjoner,
- SaaS-tjenester og tredjeparter,
- dokumentasjon, tilganger og driftsrutiner,
- sikkerhetsoppsett, logging og overvåking.

Leverandøren skal beskrive tidspunkt, metode, behov for tilgang og behov for medvirkning fra Kunden, eksisterende leverandør og tredjeparter.

Eventuelle avvik mellom opplyst og faktisk tilstand som kan ha betydning for leveransen, skal varsles uten ugrunnet opphold og håndteres etter avtalens regler om endringshåndtering.

Leverandøren skal ikke legge til grunn forutsetninger som avviker fra konkurransegrunnlaget eller avtalen uten at dette fremgår klart og uttrykkelig av tilbudet.

Avtalens punkt 2.3.6.1 – Godkjenningsperiodens varighet

Godkjenningsperioden er 2 måneder fra oppstartsdag, jf. SSA-D punkt 2.3.6.1.

Dersom det benyttes delleranser, skal Leverandøren beskrive hvordan godkjenningsperioden skal gjennomføres for den enkelte delleranse og for den samlede driftstjenesten.

Samlet godkjenning av driftstjenesten skal som minimum omfatte kontroll av:

- stabilitet,
- kapasitet,
- sikkerhet,
- brukerstøtte,
- backup og gjenoppretting,
- dokumentasjon,

- rapportering,
- samhandling,
- håndtering av uønskede hendelser.

Godkjenningsperioden reduserer ikke Leverandørens ansvar for at driftstjenesten oppfyller avtalte krav etter leveringsdag.

Avtalens punkt 2.3.6.4 – Håndtering av feil

Feil som avdekkes i test, oppstartsperiode eller godkjenningsperiode skal registreres, prioriteres og følges opp av Leverandøren.

Kritiske og alvorlige feil skal håndteres uten ugrunnet opphold og i samsvar med avtalte frister og prioriteringer i Bilag 5.

Øvrige feil skal rettes innen utgangen av godkjenningsperioden, med mindre Kunden skriftlig aksepterer annen rettefrist.

Feil som påvirker sikkerhet, tilgangsstyring, backup/gjenoppretting, servicedesk, overvåking, rapportering eller Kundens evne til å bruke driftstjenesten, skal vurderes særskilt ved Kundens godkjenning av driftstjenesten.

Leverandøren skal føre feil- og avvikslogg i godkjenningsperioden. Kunden skal ha innsyn i loggen.

Avtalens punkt 4.1 – Varighet

Avtalen trer i kraft ved signering.

Avtalen omfatter en etableringsfase frem til oppstartsdag for ordinær drift. Planlagt oppstartsdag for ordinær drift er [01.10.2026].

Ordinær kontraktsperiode er 4 år regnet fra oppstartsdag for ordinær drift.

Kunden har opsjon på forlengelse av avtalen i ytterligere 2 + 2 år, samlet maksimal ordinær avtaleperiode 8 år fra oppstartsdag for ordinær drift.

Opsjon på forlengelse utløses ensidig av Kunden ved skriftlig varsel til Leverandøren senest [6] måneder før utløpet av gjeldende avtaleperiode.

Avtalens bestemmelser om midlertidig forlengelse gjelder i tillegg.

Avtalens punkt 9.5.3.1 – Når det foreligger grunnlag for dagbot

Dagbot gjelder ved forsinkelse i forhold til avtalt oppstartsdag for ordinær drift og ved forsinkelse i forhold til leveringsdag dersom forsinkelsen skyldes Leverandørens forhold.

Det knyttes ikke særskilt dagbot til andre milepæler, med mindre dette uttrykkelig fremgår av endelig prosjekt- og fremdriftsplan.

Forsinkelse i delmilepæler som påvirker oppstartsdag eller leveringsdag, inngår i vurderingen av forsinkelse knyttet til oppstartsdag eller leveringsdag.

Avtalens punkt 9.5.3.2 – Beregning av dagboten

SSA-Ds standardbestemmelser om beregning av dagbot gjelder.

Andre dagbotsatser, annet beregningsgrunnlag eller annen maksimalbegrensning er ikke avtalt.

Bilag 5: Tjenestenivå og standardiserte kompensasjoner

Bilaget fylles ut av Kunden. Leverandøren kan i tilbudet foreslå høyere tjenestenivåer eller supplerende KPI-er, men kan ikke tilby lavere tjenestenivå enn minimumskravene som følger av dette bilaget, med mindre dette er angitt som et uttrykkelig avvik.

Dette bilaget fastsetter tjenestenivå, måling, rapportering og standardiserte kompensasjoner for utvalgte deler av driftstjenesten. Tjenestenivåene bygger på kravene i Bilag 1 og Bilag 1.1, og skal ikke forstås som en selvstendig utvidelse av leveransens omfang.

Dersom et tjenestenivå gjelder et bestemt krav eller tjenesteområde i Bilag 1.1, er dette angitt med henvisning til kravområde eller krav-ID. Leverandøren skal i Bilag 2 beskrive hvordan tjenestenivåene oppfylles, måles, dokumenteres og rapporteres.

For standardtjenester og SaaS-tjenester levert av tredjeparter, herunder Microsoft 365, DFØ, P360 Online og tilsvarende tjenester, har Leverandøren ansvar for overvåking, oppfølging, koordinering, varsling, feilsøking og rapportering innenfor sitt ansvarsområde. Leverandøren er ikke ansvarlig for tjenestenivåbrudd som utelukkende skyldes forhold hos slik tredjepart, forutsatt at Leverandøren kan dokumentere at Leverandøren har ivaretatt sine egne plikter etter avtalen.

Planlagt vedlikehold regnes ikke som nedetid dersom vedlikeholdet er varslet og gjennomført i samsvar med Bilag 6, samhandlingsplanen og avtalte endringsrutiner. Kritiske sikkerhetsoppdateringer og tiltak som er nødvendige for å avverge alvorlig sikkerhetsrisiko, kan gjennomføres som hasteendring. Kunden skal i slike tilfeller varsles så raskt som praktisk mulig.

SSA-D legger opp til at krav til tjenestenivå, håndtering av uønskede hendelser, rapportering og standardisert kompensasjon reguleres i Bilag 5, mens kravene til selve leveransen angis i Bilag 1 og leverandørens løsning i Bilag 2.

Forholdet til Bilag 1.1

Tjenestenivåene i dette bilaget er knyttet til følgende hovedområder i Bilag 1.1:

Tjenestenivåområde	Forankring i Bilag 1.1	Oppfølging i Bilag 5
Brukerstøtte og servicedesk	Kravområde om brukerstøtte	Tilgjengelighet, første respons, saksregistrering, løsningstid og rapportering
Overvåking og hendeshåndtering	Kravområde om overvåking og uønskede hendelser	Varsling, responstid, klassifisering, eskalering og rapportering
SOC/MDR/IRT og sikkerhetshendelser	Kravområde om MDR, operativ sikkerhet og informasjonssikkerhet	Responstid, eskalering, hendelsesrapportering og forbedringstiltak
Backup og gjenoppretting	Kravområde om backup, disaster recovery og beredskap	Backupstatus, restore-test, RTO/RPO, gjenopprettingsøvelser og rapportering

Tilgjengelighet for driftstjenester	Kravområde om infrastruktur, identitet, nettverk, privat sky og tjenestenivå	Oppetid, måling og unntak
Rapportering og styring	Kravområde om rapportering, samhandling, governance og kostnadsstyring	Månedrapport, måledata, avvik og forbedringstiltak
Beredskap og øvelser	Kravområde om beredskap, sikkerhetsøvelser og gjenoppretting	Øvingsplan, gjennomføring, evalueringsrapport og oppfølging

Dersom det er motstrid mellom Bilag 1.1 og dette bilaget om hvilke tjenester som inngår i leveransen, gjelder Bilag 1.1 for leveransens omfang. Dette bilaget regulerer hvordan avtalte tjenester skal måles, følges opp og eventuelt kompenseres ved brudd på avtalt tjenestenivå.

Avtalens punkt 2.3.2.4 – Samhandlingsplan og driftsspesifikasjon

Leverandøren skal utarbeide samhandlingsplan og driftsspesifikasjon i etableringsfasen. Samhandlingsplanen og driftsspesifikasjonen skal foreligge senest ved oppstart av godkjenningsperioden.

Samhandlingsplanen skal minimum beskrive:

- roller, ansvar og kontaktpunkter hos Kunden og Leverandøren,
- eskaleringslinjer for ordinære saker, kritiske hendelser og sikkerhetshendelser,
- rutiner for mottak, registrering, klassifisering, prioritering og lukking av saker,
- rutiner for varsling av driftsavvik, sikkerhetshendelser og planlagt vedlikehold,
- rutiner for endringshåndtering,
- rutiner for samhandling med Kundens tredjeparter,
- møteplan, rapporteringsrutiner og beslutningspunkter,
- rutiner for beredskap, gjenoppretting og krisehåndtering.

Driftsspesifikasjonen skal minimum beskrive:

- hvilke tjenester og komponenter som inngår i driftstjenesten,
- teknisk arkitektur og sentrale avhengigheter,
- tjenestekatalog og ansvarsdeling,
- overvåkingsoppsett og varslingsgrenser,
- backup- og gjenopprettingsoppsett,
- sikkerhetsfunksjoner, logging og hendelsehåndtering,
- driftsrutiner, kjente begrensninger og forutsetninger,
- dokumentasjon som er nødvendig for drift, sikkerhet, revisjon, beredskap og exit.

Samhandlingsplan og driftsspesifikasjon skal holdes oppdatert gjennom hele avtaleperioden. Vesentlige endringer skal behandles etter avtalens regler om endringshåndtering.

Administrative forhold som møtefrekvens, bemyndigede representanter, varslingsrutiner og endringsprosess reguleres nærmere i Bilag 6.

Avtalens punkt 2.4.1 – Krav til tjenestenivå

Leverandøren skal levere driftstjenesten i samsvar med tjenestenivåene nedenfor. Måling skjer per kalendermåned dersom ikke annet er angitt.

Tilgjengelighet måles slik:

$$\text{Oppetid (\%)} = (\text{totaltid} - \text{ikke-planlagt nedetid}) / \text{totaltid} \times 100$$

Planlagt og godkjent vedlikehold regnes ikke som ikke-planlagt nedetid.

Leverandøren skal i Bilag 2 beskrive hvordan tilgjengelighet måles, hvilke komponenter som inngår i målingene, hvilke avgrensninger som gjelder, og hvordan Kunden får innsyn i målegrunnlaget.

Tilgjengelighet

Tjenesteområde	Minimum tjenestenivå	Måleperioder	Forankring i Bilag 1.1	Kommentar
Kritiske nettverks- og sikkerhetskomponenter under Leverandørens ansvar	99,9 %	Per måned	Nettverk, sikkerhet, overvåking	Gjelder komponenter innenfor Leverandørens kontroll
Server- og privat sky-tjenester under Leverandørens ansvar	99,9 %	Per måned	Privat sky, serverdrift, infrastruktur	Gjelder avtalte produksjonstjenester
Identitets- og tilgangstjenester under Leverandørens ansvar	99,9 %	Per måned	Identitet og tilgangskontroll	Gjelder drift og forvaltning innenfor Leverandørens ansvarsområde
Overvåking og sikkerhetsovervåking/SOC-funksjon	99,9 %	Per måned	MDR/SOC/IRT, overvåking	Gjelder tilgjengelighet for overvåkings- og varslingsfunksjon
Serviceportal og saksregistrering	99,5 %	Per måned	Brukerstøtte og selvbetjening	Gjelder bruker- og kundegrensesnitt
Backupplattform under Leverandørens ansvar	99,7 %	Per måned	Backup og disaster recovery	Gjelder evne til å gjennomføre avtalte backupjobber og restoreprosesser

Tilgjengelighetskravene gjelder bare for de deler av tjenesten som er under Leverandørens ansvar og kontroll. Dersom avvik skyldes tredjepartstjeneste, Kundens forhold eller annen årsak utenfor Leverandørens kontroll, skal Leverandøren likevel dokumentere hendelsen, følge opp tredjepart og rapportere status til Kunden.

Brukerstøtte og servicedesk

Leverandøren skal levere servicedesk og brukerstøtte 24/7/365 for tjenester som inngår i driftstjenesten.

Henvendelsestype	Første respons	Mål for løsning / videre håndtering	Forankring i Bilag 1.1	Kommentar
Kritisk hendelse	5 minutter	Løpende arbeid til tjenesten er gjenopprettet eller stabilisert	Brukerstøtte, hendelseshåndtering	Gjelder hendelser med vesentlig påvirkning på drift, sikkerhet eller mange brukere
Alvorlig hendelse	30 minutter	Plan for løsning innen 4 timer	Brukerstøtte, hendelseshåndtering	Gjelder vesentlig funksjonstap eller påvirkning på flere brukere
Mindre alvorlig hendelse	4 timer	Løsning eller plan innen 3 virkedager	Brukerstøtte	Gjelder ordinære feil og avvik
Ordinær bestilling / service request	1 virkedag	Etter avtalt bestillingsflyt	Brukerstøtte, identitet, tilgang	Gjelder tilgangsbestillinger, programvare, brukerendringer mv.
Telefon/chat	80 % besvart innen 2 minutter	Sak opprettes dersom saken ikke løses direkte	Brukerstøtte	Måles månedlig som KPI

Leverandøren skal registrere alle henvendelser i saksverktøy. Dersom en henvendelse mottas via telefon eller chat og ikke løses ved første kontakt, skal Leverandøren opprette supportsak for videre oppfølging.

For henvendelser som gjelder endring av brukerens IT-profil, tilganger, programvare eller lokale administratorrettigheter, skal Leverandøren følge avtalte godkjenningrutiner i Bilag 1.1, Bilag 2 og Bilag 6.

Sikkerhetshendelser

Leverandøren skal håndtere sikkerhetshendelser i samsvar med kravene til MDR/SOC/IRT, informasjonssikkerhet og hendelseshåndtering i Bilag 1.1.

Hendelsestype	Første respons	Eskalering / tiltak	Rapportering	Forankring i Bilag 1.1
Kritisk sikkerhetshendelse	5 minutter	Umiddelbar eskalering og iverksetting av nødvendige tiltak	Foreløpig rapport snarest og senest innen 24 timer	MDR/SOC/IRT, informasjonssikkerhet
Alvorlig sikkerhetshendelse	30 minutter	Eskalering til avtalt kontaktpunkt	Foreløpig rapport senest innen 2 virkedager	MDR/SOC/IRT, informasjonssikkerhet

Mindre alvorlig sikkerhetshendelse	4 timer	Håndteres etter ordinær sikkerhetsprosess	Inngår i månedsrapport	MDR/SOC/IRT, informasjonssikkerhet
------------------------------------	---------	---	------------------------	------------------------------------

Kritisk sikkerhetshendelse omfatter blant annet mistanke om ransomware, pågående kompromittering, uautorisert privilegert tilgang, alvorlig kontokompromittering, datalekkasje, vesentlig svikt i sentrale sikkerhetsfunksjoner eller annen hendelse med høy risiko for Kundens data, drift eller omdømme.

Leverandøren skal i Bilag 2 beskrive hvordan SOC/MDR/IRT-funksjonen ivaretar deteksjon, analyse, varsling, eskalering, respons, kommunikasjon og etterfølgende rapportering.

Backup og gjenoppretting

Leverandøren skal levere backup og gjenoppretting i samsvar med kravene i Bilag 1.1 og den løsningen som er beskrevet i Bilag 2.

Område	Minimum tjenestenivå	Forankring i Bilag 1.1	Kommentar
Backup av avtalte systemer og data	Daglig eller etter avtalt frekvens	Backup og disaster recovery	Omfang og frekvens spesifiseres i Bilag 2
Backup-jobber	Minst 98 % vellykket gjennomføring per måned	Backup og disaster recovery	Feilede jobber skal følges opp uten ugrunnet opphold
Test av objekt-/filgjenoppretting	Minst årlig	Backup, beredskap	Kan inngå i ordinær beredskapsøvelse
Utvidet gjenopprettingsøvelse	Annet hvert år	Backup, beredskap	Skal teste utvalgte kritiske tjenester, data eller konfigurasjoner
RTO/RPO	Skal beskrives per tjenestekategori	Backup, tjenestenivå	Endelige nivåer fremgår av driftsspesifikasjon/Bilag 5

Leverandøren skal dokumentere at backup og gjenoppretting fungerer. Feil eller mangler som kan påvirke Kundens evne til å gjenopprette tjenester eller data, skal varsles uten ugrunnet opphold.

RTO/RPO skal beskrives av Leverandøren i Bilag 2 for relevante tjenestekategorier. Dersom Kunden fastsetter konkrete RTO/RPO-nivåer i Bilag 1.1 eller dette bilaget, gjelder disse som minimumskrav.

Avtalens punkt 2.4.2 – Uønskede hendelser

Uønskede hendelser skal klassifiseres etter alvorlighetsgrad. Klassifiseringen skal benyttes ved prioritering, respons, rapportering og eventuell økonomisk kompensasjon.

Nivå	Kategori	Beskrivelse
A	Kritisk	Hele eller vesentlige deler av driftstjenesten er utilgjengelig, eller det foreligger alvorlig sikkerhetshendelse, betydelig datatap, vesentlig svikt i identitet/tilgang eller annen hendelse med kritisk påvirkning på Kundens virksomhet

B	Alvorlig	Kritiske funksjoner virker ikke eller fungerer vesentlig dårligere enn avtalt, flere brukere er berørt, eller det foreligger sikkerhetshendelse med forhøyet risiko
C	Mindre alvorlig	Ikke-kritiske funksjoner virker ikke, enkeltbrukere eller begrensede brukergrupper er berørt, eller tjenesten har redusert kvalitet uten vesentlig virksomhetspåvirkning
D	Service request / bestilling	Ordinær bestilling, endringsforespørsel, tilgangsforespørsel eller annen henvendelse som ikke er feil eller hendelse

Hendelser skal registreres, prioriteres og følges opp i Leverandørens saksverktøy. Tidspunkt for måling av respons starter når hendelsen er meldt til Leverandøren eller registrert i Leverandørens overvåking.

Leverandøren skal varsle Kunden uten ugrunnet opphold ved kritiske og alvorlige hendelser. Ved kritiske hendelser skal Leverandøren gi løpende statusoppdateringer til Kunden frem til hendelsen er stabilisert eller løst.

Ved uenighet om klassifisering skal Kundens klassifisering legges til grunn inntil partene eventuelt blir enige om annet. Leverandøren kan i ettertid dokumentere at klassifiseringen bør endres.

Avtalens punkt 2.4.5 – Rapportering

Leverandøren skal rapportere månedlig til Kunden om driftstjenesten. Måned rapport skal leveres senest 5 virkedager etter utløpet av måneden.

Måned rapporten skal minimum inneholde:

- oppnådd tjenestenivå per tjenesteområde,
- oversikt over uønskede hendelser og klassifisering,
- brudd på tjenestenivå og årsaksanalyse,
- sikkerhetshendelser og relevante sikkerhetsobservasjoner,
- status for backup, restore og gjenopprettingstester,
- patching, sårbarheter og risikoreduserende tiltak,
- endringer gjennomført i driftsmiljøet,
- kapasitet, ytelse og ressursutnyttelse,
- lisens- og kostnadsutvikling der dette er relevant,
- status for åpne avvik, problem management og forbedringstiltak,
- eventuelle forhold som bør eskaleres til Kundens styringsnivå.

Leverandøren skal i tillegg delta i faste drifts- og styringsmøter i samsvar med Bilag 6.

Leverandøren skal kunne gi Kunden innsyn i underliggende måledata, logger, rapporter eller eksportgrunnlag som er nødvendig for å kontrollere tjenestenivå og fakturagrunnlag.

Avtalens punkt 9.5.4 – Økonomisk kompensasjon for brudd på avtalt tjenestenivå

Ved brudd på avtalt tjenestenivå kan Kunden kreve standardisert økonomisk kompensasjon etter tabellen nedenfor.

Kompensasjon beregnes av månedlig fast driftsvederlag ekskl. merverdiavgift for den berørte tjenesten. Dersom det ikke er mulig å skille ut vederlaget for den berørte tjenesten, beregnes kompensasjonen av samlet månedlig fast driftsvederlag, ekskludert tredjepartslisenser og rene forbruksbaserte kostnader.

Brudd	Standardisert kompensasjon
Tilgjengelighet under avtalt nivå for kritisk tjenesteområde	2 % av månedlig beregningsgrunnlag per påbegynte 0,1 prosentpoeng under avtalt nivå, begrenset til 10 % per måned
Manglende første respons på kritisk hendelse	1 % per hendelse
Manglende første respons på kritisk sikkerhetshendelse	2 % per hendelse
Manglende eller vesentlig forsinket oppfølging av backupfeil med betydning for gjenopprettingsevne	2 % per måned forholdet består
Manglende gjennomføring av avtalt årlig beredskaps-/sikkerhetsøvelse	2 % per uteblitt øvelse
Manglende gjennomføring av avtalt utvidet gjenopprettingsøvelse annet hvert år	3 % per uteblitt øvelse
Måned rapport levert mer enn 5 virkedager for sent	0,5 % per rapport
Måned rapport levert mer enn 10 virkedager for sent	1 % per rapport

Samlet standardisert økonomisk kompensasjon er begrenset til 15 % av månedlig fast driftsvederlag per måned.

Dersom samme forhold gir grunnlag for flere kompensasjoner, skal Kunden bare kunne kreve den høyeste kompensasjonen for samme hendelse eller samme underliggende årsak, med mindre det foreligger separate og uavhengige brudd.

Standardisert økonomisk kompensasjon er ikke til hinder for at Kunden gjør gjeldende andre misligholdsbeføyelser etter avtalen dersom vilkårene for dette er oppfylt.

KPI-er uten standardisert kompensasjon

Følgende KPI-er skal rapporteres, men gir ikke i seg selv grunnlag for standardisert økonomisk kompensasjon med mindre annet uttrykkelig følger av dette bilaget:

- totalkostnad per bruker,
- kostnad per ny bruker,
- kapasitetsutnyttelse,
- lisensutnyttelse,
- antall gjentakende feil,

- brukeropplevelse/brukertilfredshet,
- andel saker løst ved første kontakt,
- miljø- og ressursparametere,
- gjennomførte forbedringstiltak.

Disse KPI-ene brukes til styring, forbedringsarbeid og kontraktsoppfølging.

Bilag 6: Administrative bestemmelser

Administrative bestemmelser og andre opplysninger relevant for Partenes forhold. Bilaget fylles ut av Leverandøren basert på Kundens overordnede føringer i dette bilaget, Bilag 1, Bilag 2, Bilag 3, Bilag 5, Bilag 7 og Bilag 11.

Bilaget regulerer administrative forhold knyttet til gjennomføring og oppfølging av avtalen, herunder representanter, medvirkning, endringshåndtering, dokumentasjon, revisjon, underleverandører, tredjeparter, møter, varsling og skriftlig kommunikasjon.

Leverandøren skal i tilbudet fylle ut de deler av bilaget som etter sin art skal beskrive Leverandørens organisering, roller, rutiner, underleverandører, verktøy og administrative prosesser. Leverandørens utfylling skal være konkret og tilpasset leveransen til Kunden.

Avtalens punkt 2.1 – Partenes representanter

Partene skal oppnevne bemyndigede representanter for avtalen. Bemyndiget representant skal ha nødvendig fullmakt til å opptre på vegne av Parten i saker som gjelder den løpende gjennomføringen av avtalen, herunder godkjenning av planer, oppfølging av tjenestenivå, endringer, avvik, rapportering og eskalering.

Hos Kunden:

Rolle	Navn	Kontaktinformasjon	Myndighet / ansvar
Bemyndiget representant	[Fylles ut av Kunden]	[Fylles ut av Kunden]	Overordnet kontraktsoppfølging og godkjenning av endringer
Operativ IT-kontakt	[Fylles ut av Kunden]	[Fylles ut av Kunden]	Løpende operativ samhandling
Sikkerhetskontakt	[Fylles ut av Kunden]	[Fylles ut av Kunden]	Sikkerhetshendelser, sikkerhetskrav og beredskap
Personvernkontakt	[Fylles ut av Kunden]	[Fylles ut av Kunden]	Personvern og databehandleravtale

Hos Leverandøren:

Rolle	Navn	Kontaktinformasjon	Myndighet / ansvar
Bemyndiget representant	[Fylles ut av Leverandøren]	[Fylles ut av Leverandøren]	Overordnet kontraktsoppfølging og godkjenning av endringer
Leveranseansvarlig / Service Manager	[Fylles ut av Leverandøren]	[Fylles ut av Leverandøren]	Løpende leveranseoppfølging
Teknisk ansvarlig	[Fylles ut av Leverandøren]	[Fylles ut av Leverandøren]	Teknisk arkitektur, drift og endringer
Sikkerhetsansvarlig / SOC-kontakt	[Fylles ut av Leverandøren]	[Fylles ut av Leverandøren]	Sikkerhetshendelser, SOC/MDR/IRT og sikkerhetsrapportering
Etableringsansvarlig / prosjektleder	[Fylles ut av Leverandøren]	[Fylles ut av Leverandøren]	Etableringsfasen og overgang til ordinær drift
Personvernkontakt	[Fylles ut av Leverandøren]	[Fylles ut av Leverandøren]	Personvern og databehandlerforpliktelser

Utskifting av bemyndiget representant, leveranseansvarlig, teknisk ansvarlig eller sikkerhetsansvarlig skal varsles skriftlig senest 20 virkedager før utskiftingen, med mindre utskiftingen skyldes forhold Leverandøren ikke med rimelighet kunne forutse. Ny ressurs skal ha minst tilsvarende kompetanse og tilgjengelighet.

Avtalens punkt 2.3.3.2 – Kundens tilrettelegging

Kunden skal legge til rette for at Leverandøren får tilgang til nødvendig informasjon, dokumentasjon og kompetanse for å etablere og levere driftstjenesten.

Kundens medvirkning omfatter blant annet:

- tilgang til relevant dokumentasjon om dagens IT-miljø,
- tilgang til nødvendige kontaktpersoner hos Kunden,
- nødvendig bistand til avklaringer om eksisterende tjenester, systemer og integrasjoner,
- bistand til å innhente informasjon fra eksisterende driftsleverandør og relevante tredjeparter,
- tilgang til nødvendige systemer og miljøer i etableringsfasen, i den grad dette er sikkerhetsmessig forsvarlig,
- beslutninger og godkjenninger innenfor avtalte frister,
- deltakelse i test, godkjenning, møter og øvelser etter avtalt plan.

Leverandøren skal i Bilag 2 og Bilag 4 beskrive hvilken medvirkning som kreves fra Kunden i etableringsfasen og i ordinær drift. Krav til Kundens medvirkning skal være konkrete, realistiske og tilpasset Kundens størrelse og organisasjon.

Dersom Leverandøren mener manglende medvirkning fra Kunden påvirker fremdrift, pris, risiko, sikkerhet eller tjenestenivå, skal Leverandøren varsle Kunden uten ugrunnet opphold.

Avtalens punkt 2.4.3 – Endringer i driftsmiljøet som initieres av Leverandøren

Leverandøren skal varsle Kunden om endringer i driftsmiljøet som kan påvirke Kundens bruk av driftstjenesten, informasjonssikkerhet, personvern, behandlingssted, underleverandører, kostnader, tjenestenivå, integrasjoner, dokumentasjon eller Kundens mulighet til å gjennomføre revisjon eller exit.

Leverandørinitierte endringer skal klassifiseres slik:

Type endring	Beskrivelse	Varsling / godkjenning
Standard endring	Lavrisikoendring som er forhåndsdefinert, testet og ikke påvirker Kundens bruk, sikkerhet, personvern, pris eller tjenestenivå vesentlig	Kan gjennomføres etter avtalt rutine og inngå i periodisk rapportering
Normal endring	Endring som kan påvirke tjenester, brukere, integrasjoner,	Skal varsles Kunden på forhånd og håndteres etter samhandlingsplan/endringsrutine

	dokumentasjon, sikkerhet eller tjenestenivå	
Vesentlig endring	Endring som kan påvirke pris, behandlingssted, underleverandører, sikkerhetsnivå, personvern, kritiske tjenester, arkitektur, exit eller vesentlige deler av leveransen	Krever skriftlig forhåndsgodkjenning fra Kunden
Hasteendring	Endring som er nødvendig for å avverge eller begrense alvorlig driftsavvik, sikkerhetsrisiko eller sårbarhet	Kan gjennomføres uten forhåndsgodkjenning dersom det er nødvendig, men Kunden skal varsles så raskt som praktisk mulig

Følgende endringer krever alltid skriftlig forhåndsgodkjenning fra Kunden:

- endring av behandlingssted for Kundens data, metadata, logger eller backup,
- ny eller endret underleverandør som har betydning for leveransen,
- vesentlig endring i sikkerhetsarkitektur eller tilgangsstyring,
- innføring av ny KI-, maskinlærings- eller automasjonsfunksjonalitet som behandler Kundens data, metadata, logger, dokumentasjon, sikkerhetsinformasjon eller personopplysninger,
- endring som kan svekke Kundens mulighet til innsyn, revisjon, dokumentasjon, datauttrekk eller exit,
- endring som kan medføre økte kostnader for Kunden.

Leverandøren skal føre endringslogg for alle endringer som har betydning for driftstjenesten. Kunden skal ha innsyn i endringsloggen.

Avtalens punkt 2.4.6 – Dokumentasjon

Leverandøren skal etablere, vedlikeholde og gjøre tilgjengelig dokumentasjon som er nødvendig for drift, sikkerhet, revisjon, beredskap, tjenestenivåoppfølging, endringshåndtering og avslutning av avtalen.

Dokumentasjonen skal som minimum omfatte:

- tjenestebeskrivelse og tjenestekatalog,
- samhandlingsplan og driftsspesifikasjon,
- overordnet arkitektur og systemlandskap,
- nettverks- og integrasjonsoversikter,
- oversikt over servere, klienter, mobile enheter og administrasjonsverktøy innenfor avtalens omfang,
- konfigurasjonsoversikter og sentrale driftsrutiner,
- oversikt over tilganger, roller, privilegerte brukere og tilgangsprosesser,
- backup- og gjenopprettingsrutiner,
- beredskaps- og katastrofeplaner for driftstjenesten,
- oversikt over sikkerhetstiltak, logging, overvåking og hendelseshåndtering,
- oversikt over underleverandører, standardtjenester og behandlingssteder,
- lisens- og tjenesteoversikter der Leverandøren administrerer slike på vegne av Kunden,
- endringslogg, avviksllogg og dokumentasjon av gjennomførte forbedringstiltak,

- dokumentasjon som er nødvendig for datauttrekk, overføring til ny leverandør og exit.

Dokumentasjonen skal være oppdatert, lesbar og tilgjengelig for Kunden gjennom avtaleperioden. Dokumentasjon som er nødvendig for sikkerhet, beredskap, revisjon eller exit, skal kunne utleveres i alminnelig brukte og maskinlesbare formater.

Leverandøren skal i Bilag 2 beskrive hvilke dokumentasjonsverktøy og formater som benyttes, hvordan dokumentasjonen vedlikeholdes, og hvordan Kunden får tilgang.

Avtalens punkt 2.4.8 – Revisjon

Kunden har rett til å gjennomføre revisjon og verifikasjon av at Leverandøren oppfyller avtalte forpliktelser. Revisjon kan omfatte drift, informasjonssikkerhet, personvern, beredskap, underleverandørstyring, dokumentasjon, tjenestenivå, logging, tilgangsstyring, backup/gjenoppretting og etterlevelse av relevante krav i avtalen.

Ordinær revisjon kan gjennomføres én gang per kalenderår. Kunden skal varsle Leverandøren skriftlig med rimelig frist, normalt minst 20 virkedager før revisjon.

I tillegg kan Kunden gjennomføre eller kreve særskilt revisjon dersom:

- det foreligger alvorlig sikkerhetshendelse,
- det foreligger vesentlig eller gjentatt brudd på avtalen,
- offentlig myndighet, tilsyn eller overordnet departement krever eller forventer dokumentasjon,
- det er nødvendig for å kontrollere etterlevelse av personvernregelverk, sikkerhetskrav eller databehandleravtale,
- det foreligger vesentlig endring i leveransen, underleverandører, behandlingssted eller sikkerhetsoppsett.

Leverandøren skal legge til rette for revisjon og gi Kunden tilgang til nødvendig dokumentasjon, rapporter, revisjonsuttalelser, kontrollbeskrivelser og annet relevant grunnlag. Kunden kan benytte ekstern revisor eller rådgiver, forutsatt at denne ikke er direkte konkurrent av Leverandøren og er underlagt nødvendig taushetsplikt.

Leverandøren skal sikre at avtaler med underleverandører som har betydning for leveransen, gir Leverandøren og Kunden tilstrekkelig mulighet til å verifisere etterlevelse av krav som gjelder driftstjenesten.

Leverandørens avtaler med tredjeparter som har betydning for levering av driftstjenesten skal angis her eller i vedlegg til dette bilaget:

Underleverandør / tredjepart	Tjenesteområde	Behandlingssted / leveransested	Behandler personopplysninger?	Betydning for leveransen	Standardvilkår i Bilag 10?
[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]	[Ja/Nei]	[Fylles ut]	[Ja/Nei]

Avtalens punkt 2.4.9 – Nye versjoner av programvare

Leverandøren skal ha dokumenterte prosedyrer for testing, godkjenning og idriftsettelse av nye versjoner, programrettelser, sikkerhetsoppdateringer og endringer i programvare og plattformer som benyttes for å levere driftstjenesten.

Prosedyrene skal minimum beskrive:

- hvordan oppdateringer identifiseres og risikovurderes,
- hvordan sikkerhetsoppdateringer prioriteres,
- hvordan testing gjennomføres før produksjonssetting,
- hvordan Kunden varsles om endringer som kan påvirke bruk, sikkerhet, personvern, integrasjoner, tjenestenivå eller kostnader,
- hvordan tilbakeføring eller kompenserende tiltak håndteres,
- hvordan endringer dokumenteres i endringslogg og driftsspesifikasjon.

Kritiske sikkerhetsoppdateringer skal håndteres uten ugrunnet opphold. Dersom en kritisk sikkerhetsoppdatering ikke kan implementeres umiddelbart, skal Leverandøren dokumentere årsaken og beskrive kompenserende tiltak.

Avtalens punkt 3.2 – Endringshåndtering

A. Kundens endringsordre

Dersom Kunden ønsker å endre leveransen, skal Kunden utarbeide en skriftlig endringsordre. Endringsordren skal beskrive Kundens behov for endringen og eventuelle ønskede frister.

Endringsordre kan gis ved bruk av Kundens eller Leverandørens avtalte samhandlings-/saksverktøy, forutsatt at endringen kan dokumenteres skriftlig og godkjennes av bemyndiget representant.

Endringsordre skal som minimum inneholde:

- beskrivelse av ønsket endring,
- bakgrunn og formål,
- ønsket virkningstidspunkt,
- eventuelle krav til testing, dokumentasjon og godkjenning,
- eventuell foreløpig vurdering av risiko, sikkerhet, personvern, kostnad eller tjenestenivå.

B. Leverandørens håndtering av endringsordrer

Leverandøren skal beskrive sin rutine for håndtering av endringsordrer, herunder verktøy for registrering, oppfølging og rapportering av endringsordrer.

Med mindre annet er avtalt i det enkelte tilfellet, skal Leverandøren innen 10 virkedager fra mottak av endringsordre utrede aktuelle risiko- og endringskonsekvenser og gi et prisestimat.

Utredningen skal som minimum omfatte:

- a) beskrivelse av endringen,
- b) beskrivelse av arbeidet som må gjøres for å levere endringen,
- c) virkning på leveransen,
- d) virkning på tidsplaner,
- e) virkning på vederlag, herunder etableringskostnad, løpende kostnad, lisenskostnad, forbrukspris og eventuell reduksjon i kostnad,
- f) tidsplan for gjennomføring av endringen,
- g) virkning på tjenestenivå, rapportering og standardisert kompensasjon,
- h) virkning på informasjonssikkerhet, personvern, beredskap og behandlingssted,
- i) virkning på ansvarsfordeling mellom Kunden, Leverandøren, underleverandører og tredjeparter,
- j) behov for test og eventuell godkjenning av endringen,
- k) behov for oppdatering av dokumentasjon, driftsspesifikasjon, samhandlingsplan, prisskjema eller øvrige bilag.

Leverandøren skal ikke iverksette endringen før Kunden har godkjent endringen skriftlig, med mindre det gjelder hasteendring som er nødvendig for å avverge alvorlig driftsavvik eller sikkerhetsrisiko.

C. Kundens aksept av Leverandørens utredning

Dersom Kunden aksepterer Leverandørens beskrivelse av endringen, pris og øvrige konsekvenser, skal Kunden gi Leverandøren skriftlig beskjed om at Kunden ønsker endringen utført.

Leverandøren skal iverksette endringen i henhold til de frister og vilkår som fremgår av endringsordren eller endringsavtalen. Leverandøren skal orientere Kunden når endringen er utført.

Endringsordren skal føres i endringslogg og inntas i Bilag 9.

D. Tvisteløsning

Uenighet om konsekvensene av en endring håndteres etter avtalens punkt 3.4 og 3.5.

Partene skal søke å avklare uenigheter på lavest mulig nivå og uten unødvendig opphold. Dersom uenigheten ikke løses operativt, skal saken eskaleres til Partenes bemyndigede representanter.

Det avtales ikke særskilt uavhengig ekspert ved avtaleinngåelsen, med mindre dette fremgår av punktet om Avtalens punkt 12.2 nedenfor.

Avtalens punkt 5.2.2 – Nøkkelpersonell

Leverandøren skal angi nøkkelpersonell for leveransen. Nøkkelpersonell skal ha sentrale roller i etablering, drift, sikkerhet, tjenesteoppfølging eller kontraktsstyring.

Leverandørens nøkkelpersonell:

Rolle	Navn	Kompetanse / erfaring	Tilgjengelighet for Kunden	Erstattes bare etter godkjenning?
Leveranseansvarlig / Service Manager	[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]	Ja
Etableringsleder / prosjektleder	[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]	Ja
Teknisk arkitekt / løsningsansvarlig	[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]	Ja
Sikkerhetsansvarlig / SOC-ansvarlig	[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]	Ja
Personvern- /etterlevelseskontakt	[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]	Ja

Utskifting av nøkkelpersonell skal godkjennes av Kunden på forhånd. Godkjenning kan ikke nektes uten saklig grunn. Ny ressurs skal ha minst tilsvarende kompetanse og tilgjengelighet.

Avtalens punkt 5.3.1 – Leverandørens bruk av underleverandører

Leverandørens godkjente underleverandører skal angis i tabellen nedenfor.

Underleverandør	Organisasjonsnummer / land	Tjenesteområdene	Rolle i leveransen	Behandler personopplysninger?	Behandlingssted	Kritisk for leveransen?	Sanksjons-/restriksjonskontroll gjennomført?	Vurdert for menneskerettigheter/anstendige arbeidsforhold?
[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]	[Fylles ut]	[Ja/Nei]	[Fylles ut]	[Ja/Nei]	[Ja/Nei]	[Ja/Nei]

Leverandøren skal kunne dokumentere at sentrale og kritiske underleverandører er vurdert opp mot sanksjoner, restriktive tiltak, behandlingssted, informasjonssikkerhet, personvern og relevante risikoområder for menneskerettigheter og anstendige arbeidsforhold.

For underleverandører som er kritiske for leveransen, skal Leverandøren kunne redegjøre for hvilke kontroller som er gjennomført og hvordan eventuelle funn eller risikoer følges opp.

Leverandøren kan ikke skifte ut underleverandører som medvirker direkte til levering av driftstjenesten uten Kundens skriftlige forhåndssamtykke, med mindre annet er uttrykkelig avtalt.

Leverandøren skal varsle Kunden skriftlig om ønsket endring av underleverandør. Varslet skal beskrive:

- hvilken underleverandør som ønskes lagt til, skiftet ut eller fjernet,
- hvilke tjenester underleverandøren skal levere,

- om underleverandøren vil behandle Kundens data eller personopplysninger,
- behandlingssted og eventuelle overføringer utenfor Norge/EU/EØS,
- betydning for sikkerhet, personvern, tjenestenivå, pris, revisjon og exit.

Endring av underleverandør som behandler personopplysninger, skal i tillegg håndteres etter Bilag 11.

Avtalens punkt 5.3.2 – Kundens bruk av tredjepart

Kunden kan benytte tredjeparter i forbindelse med sine oppgaver under avtalen, herunder fagsystemleverandører, SaaS-leverandører, sikkerhetsleverandører, konsulenter, revisorer og andre rådgivere.

Kjente tredjeparter ved avtaleinngåelsen:

Tredjepart	Tjenesteområde	Kontaktpunkt	Betydning for leveransen
Eksisterende driftsleverandør	Overgang / etablering	[Fylles ut av Kunden]	Overlevering, dokumentasjon og avklaringer
P360 Online / arkivleverandør	Arkiv og dokumentforvaltning	[Fylles ut av Kunden]	Tilgang, integrasjoner og feilsøking
DFØ	Lønn, HR, økonomi og regnskap	[Fylles ut av Kunden]	SaaS-tjenester og tilgangsstyring
Microsoft / CSP	M365, Entra ID og lisenser	[Fylles ut av Kunden/Leverandøren]	Skytjenester, lisenser og drift
Andre fagsystemleverandører	Fagsystemer og integrasjoner	[Fylles ut]	Drift, feilsøking og endringer

Leverandøren skal samarbeide med Kundens tredjeparter der dette er nødvendig for å levere driftstjenesten. Eventuelt vederlag for samarbeid som ligger utenfor avtalt leveranse, skal fremgå av Bilag 7 eller avtales som endring.

Avtalens punkt 5.6 – Møter

Partene skal gjennomføre faste møter for oppfølging av leveransen.

Møte	Frekvens	Deltakere	Formål
Operativt driftsmøte	Månedlig	Operative kontaktpersoner	Drift, hendelser, avvik, kapasitet, saker og forbedringstiltak
Sikkerhetsmøte	Kvartalsvis eller ved behov	Sikkerhetskontakt, SOC/MDR/IRT, relevante IT-ressurser	Sikkerhetsstatus, sårbarheter, hendelser, risikoreduserende tiltak
Kontrakts-/styringsmøte	Kvartalsvis	Bemyndigede representanter og leveranseansvarlig	Tjenestenivå, økonomi, risiko, forbedringer, endringer og eskaleringer
Etableringsmøter	Etter avtalt prosjektplan	Prosjektressurser	Etablering, test, overgang og fremdrift
Beredskaps-/øvelsesmøte	Årlig eller etter øvingsplan	Relevante roller	Planlegging og evaluering av øvelser

Leverandøren skal forberede agenda og relevant dokumentasjon til møtene. Referat skal utarbeides og gjøres tilgjengelig for Partene. Aksjoner, frister og ansvarlige skal følges opp i senere møter.

Møter kan gjennomføres digitalt med mindre Partene blir enige om annet.

Avtalens punkt 5.7 – Lønns- og arbeidsvilkår

Leverandøren skal på forespørsel dokumentere etterlevelse av krav til lønns- og arbeidsvilkår i samsvar med avtalen.

Dokumentasjon kan omfatte egenerklæring, oversikt over relevante tariffavtaler, arbeidsavtaler, lønns slipper, timelister eller annen dokumentasjon som er egnet til å verifisere etterlevelse. Dokumentasjon kan kreves for Leverandøren og relevante underleverandører.

Det avtales ikke høyere dagbot for brudd på dokumentasjonsplikten enn det som følger av avtalens punkt 5.7.2, med mindre annet uttrykkelig avtales her:

[Eventuell annen dagbot fylles ut av Kunden]

Avtalens punkt 5.8 – Taushetsplikt

SSA-Ds standardbestemmelse om taushetsplikt gjelder.

For informasjon som gjelder sikkerhetsarkitektur, sårbarheter, sikkerhetshendelser, tilgangsmodeller, beredskapsplaner, logger, revisjonsfunn, personopplysninger, forretningssensitiv informasjon eller opplysninger underlagt lovbestemt taushetsplikt, gjelder taushetsplikten så lenge informasjonen har beskyttelsesbehov eller så lenge dette følger av lov, forskrift eller avtale.

Leverandøren skal sikre at ansatte, innleide, underleverandører og andre som får tilgang til taushetsbelagt informasjon, er bundet av tilsvarende taushetsplikt.

Avtalens punkt 5.9 – Skriftlighet

Varsler, krav og andre meddelelser etter avtalen skal gis skriftlig.

Følgende kommunikasjonskanaler kan benyttes:

Type kommunikasjon	Kanal	Kommentar
Formelle kontraktsvarsler	E-post til bemyndiget representant / avtalt kontraktsadresse	Gjelder endringer, mislighold, krav, opsjoner, avbestilling og andre formelle varsler
Operative saker	Avtalt saks- /samhandlingsverktøy	Gjelder supportsaker, endringer, avvik, hendelser og bestillinger
Kritiske hendelser og sikkerhetshendelser	Telefon og e-post / avtalt beredskapskanal	Skal registreres skriftlig i etterkant
Rapportering	Avtalt portal, e-post eller samhandlingsverktøy	Gjelder månedsrapporter, sikkerhetsrapporter og driftsrapporter

Muntlige beskjeder ved kritiske hendelser skal dokumenteres skriftlig så snart som praktisk mulig.

Avtalens punkt 12.2 – Uavhengig ekspert

Det oppnevnes ikke uavhengig ekspert ved avtaleinngåelsen.

Dersom det oppstår tvist der Partene ønsker å benytte uavhengig ekspert, kan Partene avtale dette særskilt på tvistetidspunktet. Ekspertens mandat, kompetanse, habilitet, frist, kostnadsdeling og om uttalelsen skal være bindende eller rådgivende, skal i så fall avtales skriftlig.

Bilag 7: Samlet pris og prisbestemmelser

Alle priser og nærmere betingelser for det vederlaget Kunden skal betale for Leverandørens ytelser, fremgår av dette bilaget og tilhørende prisskjema i Excel.

Prisskjemaet utgjør en del av Bilag 7. Dersom det er motstrid mellom dette bilaget og prisskjemaet, gjelder dette bilaget for prisbestemmelser, betalingsvilkår og tolkningsregler. Prisskjemaet gjelder for konkrete priser, enhetspriser, evalueringspris, opsjoner, timepriser og prisposter.

Alle priser skal oppgis i norske kroner eksklusive merverdiavgift. Prisene skal inkludere toll, avgifter, gebyrer, administrasjonskostnader og øvrige kostnader som er nødvendige for å levere ytelsene, med mindre annet uttrykkelig fremgår av dette bilaget eller prisskjemaet.

Avtalens punkt 6.1 – Vederlag

Leverandørens vederlag består av følgende priselementer:

- etableringskostnad,
- faste og enhetsbaserte månedlige driftsvederlag,
- tredjepartslisenser og standardtjenester,
- opsjoner,
- timepriser for uttrykkelig bestilte tilleggstjenester,
- eventuelle forbruksbaserte priselementer som fremgår av prisskjemaet.

Leverandøren skal fylle ut prisskjemaet i samsvar med instruksene i Excel-filen. Leverandøren skal ikke endre forhåndsutfylte mengder, formler, struktur eller evalueringsmodell, med mindre Kunden uttrykkelig åpner for dette.

Alle tjenester som er nødvendige for å oppfylle kravene i konkurransegrunnlaget, Bilag 1, Bilag 1.1, Bilag 5, Bilag 6 og Bilag 11, skal være inkludert i fast eller enhetsbasert vederlag, med mindre prisskjemaet uttrykkelig angir at ytelsen er en opsjon eller en timebasert tilleggstjeneste.

Leverandøren kan ikke kreve særskilt vederlag for ytelser som er nødvendige for å oppfylle må-kravene eller avtalt tjenestenivå, med mindre dette klart fremgår av tilbudet og er priset i prisskjemaet.

Dette gjelder blant annet:

- servicedesk og brukerstøtte innenfor avtalt omfang,
- SOC/MDR/IRT innenfor avtalt omfang,
- sikkerhetsoppdatering og patching,
- M365/Entra ID-drift innenfor avtalt omfang,
- klientadministrasjon,
- nettverksdrift,
- server- og privat sky-drift,
- backup og gjenoppretting innenfor avtalt omfang,
- dokumentasjon,

- rapportering,
- normal koordinering med Kundens tredjeparter,
- deltakelse i avtalte drifts-, sikkerhets- og styringsmøter.

Dersom Leverandøren mener at en ytelse ikke er inkludert i fast eller enhetsbasert vederlag, skal dette fremgå klart av prisskjemaet og Leverandørens tilbud.

Prisskjema

Leverandøren skal prise leveransen i vedlagte prisskjema.

Prisskjemaet består av følgende faner:

Fane	Innhold
Instruks	Utfyllingsinstruks og prislogikk
Prisposter	Etablering, månedlige driftsposter, lisenser og løpende tjenester
Opsjoner	Opsjoner og evalueringsvolum
Timepriser	Timepriser og evalueringsvolum for tilleggstjenester
Evaluering	Automatisk beregning av samlet evalueringspris og kontrollsum

Samlet evalueringspris beregnes slik:

Etableringskostnad + obligatorisk månedlig vederlag × 48 måneder + evalueringssum timepriser + evalueringssum opsjoner.

Evalueringsvolumer for timepriser og opsjoner er kun fastsatt for å gjøre tilbudene sammenlignbare. De innebærer ingen kjøpsplikt for Kunden.

Etableringskostnad

Etableringskostnaden skal omfatte alle kostnader knyttet til etablering, overgang, migrering, verifisering, test, dokumentasjon, oppstart og bistand frem til ordinær drift er etablert i samsvar med avtalen.

Etableringskostnaden inngår én gang i evalueringsprisen.

Etableringskostnaden faktureres slik, med mindre annet avtales:

- 50 % ved oppstartsday for ordinær drift,
- 50 % etter godkjent godkjenningsperiode.

Dersom etableringen ikke godkjennes som følge av forhold Leverandøren svarer for, kan Kunden holde tilbake betaling til forholdet er rettet.

Månedlig driftsvederlag

Månedlig driftsvederlag faktureres etterskuddsvis per måned fra oppstartsday for ordinær drift.

Månedlig driftsvederlag skal omfatte alle avtalte faste og enhetsbaserte tjenester som inngår i driftstjenesten, med mindre annet uttrykkelig fremgår av prisskjemaet.

Ved endringer i antall brukere, enheter, lisenser, kapasiteter eller andre volumdrivere, justeres vederlaget i samsvar med enhetsprisene i prisskjemaet. Slike volumendringer innenfor avtalens rammer regnes ikke som endring etter SSA-D kapittel 3, med mindre endringen også innebærer endring i leveransens art, ansvar, tjenestenivå eller tekniske løsning.

Tredjepartslisenser og standardtjenester

Tredjepartslisenser og standardtjenester skal fremgå av prisskjemaet og eventuelt Bilag 10.

Leverandøren skal angi om prisen er:

- direkte tredjepartskostnad,
- tredjepartskostnad med administrasjon inkludert i annen prispost,
- tredjepartskostnad med særskilt administrasjonspåslag,
- del av fast driftsvederlag.

Eventuelle administrasjonspåslag, rabatter, marginer eller gebyrer skal fremgå klart. Skjulte påslag kan ikke kreves dekket.

Dersom rettighetshaver eller produsent endrer prisene for tredjepartslisenser eller standardtjenester, kan Leverandøren justere prisen tilsvarende den dokumenterte endringen. Leverandøren skal varsle Kunden skriftlig senest 30 dager før endringen får virkning, så langt Leverandøren selv har mottatt varsel i tide.

Leverandøren skal dokumentere prisendringen fra rettighetshaver eller produsent. Kunden skal ikke belastes høyere prisøkning enn den dokumenterte økningen, med mindre særskilt administrasjonspåslag er uttrykkelig avtalt i prisskjemaet.

Timepriser

Timepriser gjelder bare for uttrykkelig bestilte tilleggstjenester som ikke inngår i fast eller enhetsbasert vederlag.

Timeprisene kan ikke benyttes for ytelser som er nødvendige for å oppfylle må-kravene, avtalt tjenestenivå eller Leverandørens ordinære ansvar etter avtalen, med mindre dette uttrykkelig fremgår av Bilag 7 eller er avtalt som endring.

Timebasert arbeid skal forhåndsgodkjennes skriftlig av Kunden. Leverandøren skal oppgi estimert timeforbruk før arbeidet påbegynnes. Faktura for timebasert arbeid skal spesifisere dato, ressurskategori, aktivitet, timeantall og relevant bestilling/endringsordre.

Evalueringsvolumene i prisskjemaet er kun brukt for evaluering og innebærer ingen kjøpsplikt.

Opsjoner

Opsjoner fremgår av prisskjemaets opsjonsfane.

Kunden har rett, men ikke plikt, til å bestille opsjoner. Opsjoner kan bare tas i bruk etter skriftlig bestilling fra Kunden.

Opsjoner skal leveres til prisene og betingelsene som fremgår av prisskjemaet, med mindre partene avtaler annet innenfor anskaffelsesregelverkets rammer.

Uttak av opsjoner skal skje innenfor kontraktens maksimale økonomiske ramme.

Følgende opsjoner er beskrevet for prising:

Beskrivelse av opsjonene:

O001 - Drift og adm. av offsite backupservere (managed colocation i Norge)

Omfang: Administrert nettverk, linje (100 Mbit), backupservere: 3x2U HP Server (LHR/StoreOnce), lisenser.

Leverandøren leverer nettverkskomponenter til administrert nettverk.

Leverandøren skal tilby drift av Kundens off-site backupmiljø bestående av tre (3) fysiske servere plassert i colocation-anlegg i Norge. Backupløsningen skal ivareta DMF sine virksomhetskritiske data, ikke gjenoppretting (recovery) av driftsmiljø (VM-er, servere m.m.).

Leverandøren skal etablere og drifte et administrert nettverksmiljø for backupserverne, inkludert LAN-infrastruktur, ruting, brannmurfunksjonalitet og nødvendig nettverkssikkerhet. Løsningen skal være fysisk og logisk adskilt fra ordinær produksjonsinfrastruktur og tilrettelagt for sikker lagring og gjenoppretting av sikkerhetskopier.

Leverandøren skal etablere integrasjon mot Kundens Entra ID for autentisering og tilgangsstyring. Tilgang til backupmiljøet skal baseres på dedikerte sikkerhetsgrupper og prinsippet om minste privilegium (Zero trust).

Leverandøren skal ivareta:

- Drift, overvåkning og vedlikehold av nettverks- og serverinfrastruktur.
- Tilgangskontroll basert på Entra ID og rollebasert tilgangsstyring (RBAC).
- Multifaktorautentisering (MFA) for alle administrative tilganger.
- Sikkerhetslogging og overvåkning av brukeraktiviteter og administrative handlinger.
- Nettverkssegmentering og nødvendig beskyttelse mot uautorisert tilgang.
- Oppdatering og vedlikehold av operativsystem og infrastrukturkomponenter.
- Dokumenterte prosedyrer for tilgangsstyring, endringshåndtering og hendelseshåndtering.

Krav til fjernadministrasjon

Leverandøren skal tilby sikker fjernadministrasjon av backupmiljøet gjennom dedikert administrativ tilgangsløsning (f.eks. Remote Desktop Services, bastion-/jumpserver eller tilsvarende). Tilgang skal kunne bestilles, godkjennes og tildeles etter dokumenterte rutiner, og all administrativ tilgang skal autentiseres mot Kundens Entra ID, beskyttes med MFA og loggføres for revisjonsformål.

Krav til lokasjon

Colocation-anlegg, backupservere og tilhørende administrasjonsinfrastruktur skal være lokalisert i Norge.

O002 - Administrert infrastruktur i public, sovereign cloud i Norge

Omfang: Compute, 2 stk servere med 4xCPU, 2xGPU, 24GB RAM, 0.5 TB SSD.

Drift av compute-kapasitet i offentlig sky

Leverandøren skal tilby mulighet for kjøp og drift av separat compute-kapasitet i offentlig sky (Microsoft Azure, AWS eller tilsvarende), uavhengig av leverandørens private skyplattform.

Løsningen skal være integrert med Kundens Entra ID-tenant slik at brukere, administratorer og tjenester kan autentiseres ved bruk av samme identitet og etablerte sikkerhetsmekanismer som benyttes for Kundens M365-plattform og private skyinfrastruktur.

Leverandøren skal etablere, drifte og vedlikeholde nødvendig sikkerhets- og styringsrammeverk i offentlig sky, herunder:

- Integrasjon mot Kundens Entra ID for autentisering og autorisasjon (Single Sign-On).
- Implementering av rollebasert tilgangsstyring (RBAC) basert på prinsippet om minste privilegium.
- Etablering og forvaltning av sikkerhetspolicyer, guardrails og governance-regler tilsvarende eller bedre enn de som benyttes i privat sky.
- Sentralisert logging, overvåkning og hendelsehåndtering integrert med Kundens øvrige drifts- og sikkerhetsløsninger.
- Aktivisering og forvaltning av multifaktorautentisering (MFA), Conditional Access og øvrige identitetsbaserte sikkerhetsmekanismer fra Entra ID.
- Sikker nettverkssegmentering, brannmurregler og kontroll av trafikk mellom privat sky, offentlig sky og eksterne nettverk.
- Kontinuerlig sårbarhetshåndtering, sikkerhetsoppdateringer og operativsystemvedlikehold for virtuelle maskiner og tilhørende tjenester.
- Beskyttelse av data under overføring og lagring ved bruk av anerkjente krypteringsmekanismer.
- Etablering av sikkerhetskopiering og gjenoppretting i henhold til avtalte krav til tilgjengelighet og beredskap.
- Løpende kostnads- og kapasitetsstyring for å sikre effektiv ressursutnyttelse i offentlig sky.

Særskilt krav til identitetsforvaltning

Kundens Entra ID skal være autoritativ kilde for identiteter, grupper og tilgangsstyring både i privat sky og offentlig sky. Leverandøren skal sikre at identiteter, sikkerhetspolicyer og tilgangskontroller kan forvaltes sentralt og konsistent på tvers av miljøene.

Særskilt krav til lokasjon

For Microsoft-løsninger skal compute-kapasitet kunne leveres fra Microsoft Azure-regioner i Norge. For alternative skyleverandører skal leverandøren dokumentere hvor compute-kapasitet og tilhørende data lagres og behandles, samt hvordan krav til suverenitet, informasjonssikkerhet og etterlevelse ivaretas.

O003 - KI- og automasjonstjenester i privat, sovereign sky

Oppdragsgiver skal kunne avrope en sikker og skalerbar plattform for kunstig intelligens, avansert dataanalyse og automasjon, levert fra privat eller sovereign cloud innenfor Norge eller EU/EØS. Plattformen skal støtte flere språkmodeller og KI-teknologier, herunder generativ KI, dokumentanalyse, semantisk søk, kunnskapsagenter og analyse av strukturerte og ustrukturerte data. Løsningen skal kunne benyttes til blant annet analyse av store dokumentmengder, regnskaps- og økonomidata, geologiske rapporter, saksbehandling og beslutningsstøtte. Oppdragsgiver skal ha full kontroll over data, modeller og tilgangsstyring. Plattformen skal være intuitiv å bruke og legge til rette for at virksomheten selv kan utvikle, konfigurere og forvalte egne KI-agenter og automatiserte arbeidsprosesser gjennom lavkode-/ingenkodeverktøy (low-code/no-code).

Avtalens punkt 6.2 – Fakturering

Betaling skjer etter faktura med 30 dagers betalingsfrist.

Faktura skal sendes elektronisk i godkjent standardformat. Leverandøren bærer selv kostnader knyttet til elektronisk faktura.

Faktura skal være tilstrekkelig spesifisert til at Kunden kan kontrollere fakturagrunnlaget mot avtalen, prisskjemaet, bestillinger, endringsordrer og godkjente volum.

Faktura for månedlig drift skal minimum spesifisere:

- fast månedlig driftsvederlag,
- bruker-/enhetsbaserte priser,
- tredjepartslisenser,
- forbruksbaserte priselementer,
- opsjoner som er bestilt,
- eventuelle timebaserte tilleggstjenester,
- eventuelle prisreguleringer,
- kreditnotaer eller fradrag,

- eventuell standardisert økonomisk kompensasjon etter Bilag 5.

Kunden kan holde tilbake omtvistet del av faktura dersom fakturaen ikke er i samsvar med avtalen eller ikke er tilstrekkelig dokumentert.

Avtalens punkt 6.5.1 – Indeksregulering

Tjenestepriiser og timepriser kan reguleres én gang per år i samsvar med Statistisk sentralbyrås konsumprisindeks, hovedindeksen, med mindre annet fremgår av prisskjemaet.

Prisregulering kan første gang skje tidligst 12 måneder etter oppstartsdag for ordinær drift.

Leverandøren skal varsle Kunden skriftlig senest 60 dager før reguleringen får virkning. Varslet skal dokumentere beregningen.

Prisregulering gjelder ikke etableringskostnaden.

Tredjepartslisenser og standardtjenester reguleres etter bestemmelsen om tredjepartslisenser ovenfor.

Forbruksbaserte tjenester faktureres etter faktisk forbruk og avtalte enhetspriser. Leverandøren skal gi Kunden løpende innsikt i forbruk, kostnadsutvikling og relevante optimaliseringstiltak.

Avtalens punkt 2.4.4 – Bestilling av tilleggstjenester / tjenestekatalog

Leverandørens tjenestekatalog skal fremgå av prisskjemaet, Bilag 2 eller vedlegg til Bilag 7.

Tilleggstjenester kan bare leveres etter skriftlig bestilling fra Kunden. Bestillingen skal angi om tjenesten prises etter fastpris, enhetspris eller timepris.

Tilleggstjenester skal ikke benyttes til å prise ytelser som etter avtalen inngår i fast eller enhetsbasert vederlag.

Avtalens punkt 2.4.7 – Planer og øvelser for beredskap og katastrofer

Årlig sikkerhets-/beredskapsøvelse og utvidet gjenopprettingsøvelse annet hvert år inngår i fast vederlag, med mindre annet uttrykkelig fremgår av prisskjemaet.

Øvelser, tester eller bistand utover dette kan faktureres etter avtalte timepriser eller særskilt opsjonspris, forutsatt at Kunden har bestilt dette skriftlig.

Leverandøren kan ikke kreve særskilt vederlag for øvelsesaktiviteter som er nødvendige for å oppfylle minimumskravene i Bilag 1, Bilag 1.1 eller Bilag 5.

Avtalens punkt 2.4.9 – Nye versjoner av programvare

Driftssetting av ordinære programrevisjoner, sikkerhetsoppdateringer, programrettelser og feilrettingsutgaver som er nødvendige for å opprettholde avtalt tjenestenivå, sikkerhet og kontraktsmessig funksjonalitet, inngår i det løpende driftsvederlaget.

Større versjonsløft, teknologiskifte, migrering eller endringer som går utover Leverandørens ordinære ansvar for drift, sikkerhet og livssyklusforvaltning, håndteres etter avtalens regler om endringshåndtering dersom endringen ikke allerede er inkludert i avtalt vederlag.

Avtalens punkt 3.3 – Kostnader og øvrige konsekvenser av endringsordre

Leverandørens konsekvensutredning ved endringsordre skal som utgangspunkt prises etter avtalte timepriser, med mindre annet avtales skriftlig.

Kort innledende vurdering av om en forespørsel er en endring eller ligger innenfor eksisterende avtale, inngår i ordinær kontraktsoppfølging.

Dersom Leverandøren mener at utarbeidelse av konsekvensutredning vil kreve vesentlig arbeid, skal Kunden godkjenne estimert omfang før arbeidet påbegynnes.

Endringsarbeid prises etter relevante timepriser, enhetspriser eller fastpriser i prisskjemaet. Dersom relevant pris ikke fremgår av prisskjemaet, skal Leverandørens tilbud reflektere det generelle prisnivået i avtalen.

Avtalens punkt 4.2.1 – Avbestilling i etableringsfasen

SSA-Ds standardbestemmelser om avbestilling i etableringsfasen gjelder.

Det er ikke avtalt særskilt avbestillingsvederlag utover det som følger av SSA-D, med mindre annet uttrykkelig fremgår av prisskjemaet eller skriftlig avtale mellom partene.

Avtalens punkt 4.2.2 – Avbestilling i ordinær drift

SSA-Ds standardbestemmelser om avbestilling i ordinær drift gjelder.

Det er ikke avtalt særskilt avbestillingsvederlag utover det som følger av SSA-D, med mindre annet uttrykkelig fremgår av prisskjemaet eller skriftlig avtale mellom partene.

Ved delvis avbestilling skal vederlaget reduseres i samsvar med relevante enhetspriser i prisskjemaet, så langt dette er praktisk og kontraktsmessig mulig.

Avtalens punkt 5.3.2 – Kundens bruk av tredjepart

Normal samhandling med Kundens tredjeparter som er nødvendig for å levere driftstjenesten, inngår i fast eller enhetsbasert vederlag.

Dette omfatter blant annet ordinær koordinering, feilsøking, informasjonsutveksling, møter og oppfølging mot relevante fagsystemleverandører, SaaS-leverandører, skyleverandører, sikkerhetsleverandører og eksisterende eller ny driftsleverandør innenfor avtalens omfang.

Bistand som går utover normal samhandling, kan faktureres etter avtalte timepriser dersom Kunden har bestilt bistanden skriftlig.

Reise- og diettkostnader dekkes bare dersom dette er skriftlig forhåndsgodkjent av Kunden. Godkjente reise- og diettkostnader dekkes etter statens gjeldende satser. Reisetid faktureres ikke, med mindre dette er særskilt avtalt skriftlig.

Bilag 8: Endringer i den generelle avtaleteksten

Endringer til den generelle avtaleteksten skal samles i dette bilaget, med mindre den generelle avtaleteksten uttrykkelig henviser slike endringer eller presiseringer til et annet bilag.

Ved avtaleinngåelsen er det ikke avtalt endringer i den generelle avtaleteksten.

Den generelle avtaleteksten gjelder uendret. Presiseringer, utfyllende reguleringer og kundespesifikke krav som er inntatt i de øvrige bilagene, skal ikke anses som endringer i den generelle avtaleteksten når den generelle avtaleteksten selv åpner for at slike forhold reguleres i bilagene.

Dette gjelder særlig reguleringer i:

- Bilag 1 Kundens behovsbeskrivelse og kravspesifikasjon,
- Bilag 2 Leverandørens løsningsspesifikasjon,
- Bilag 5 Tjenestenivå og standardiserte kompensasjoner,
- Bilag 6 Administrative bestemmelser,
- Bilag 7 Samlet pris og prisbestemmelser,
- Bilag 11 Databehandleravtale.

Leverandøren skal ikke fylle ut Bilag 8 med endringer, avvik eller forbehold til den generelle avtaleteksten.

Eventuelle avvik, forbehold eller forslag til endringer i avtalen ved tilbudsinnlevering skal fremgå klart av tilbudet og kan medføre avvisning.

Punkt i avtalen	Erstattes med
Ingen	Det er ikke avtalt endringer i den generelle avtaleteksten.

Bilag 9: Endringer av leveransen etter avtaleinngåelsen

Endringer som gjøres etter avtalens inngåelse skal føres inn her, jf. avtalens punkt 3.2.

Eksempel på endringskatalog:

Endringsnr.	Beskrivelse	Ikraftsettelsesdato	Arkivreferanse

Bilag 10: Standard lisensvilkår for standardprogramvare og fri programvare

Dette bilaget skal inneholde eller henwise til standard lisensvilkår, standardvilkår og vilkår for fri programvare/åpen kildekode som inngår i leveransen, og som Leverandøren mener skal gjelde for Kundens bruk av slike produkter eller tjenester.

Bilaget skal fylles ut av Leverandøren.

Standardvilkår, lisensvilkår eller vilkår for fri programvare som ikke er uttrykkelig angitt i Bilag 2 og inntatt eller henvist til i dette bilaget, kan ikke gjøres gjeldende overfor Kunden.

Avtalens punkt 5.1.1 – Leverandørens ansvar for leveransen – generelt

Dersom standardprogramvare, standardtjenester, skytjenester, sikkerhetsverktøy, administrasjonsverktøy eller fri programvare/åpen kildekode inngår i leveransen og må leveres under standard lisensvilkår eller standard avtalevilkår, skal dette være uttrykkelig angitt i Bilag 2.

For hver standardleveranse skal Leverandøren fylle ut tabellen nedenfor:

Produkt/tjeneste	Produsent/rettighetshaver	Formål i leveransen	Type vilkår	Behandlingssted / leveranssted der relevant	Behandler personopplysninger?	Påvirkning er sikkerhet, revisjon, datauttrekk eller exit?	Vedlagt/lenke til vilkår
[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]	Standard lisensvilkår / standard tjenestevilkår / fri programvare	[Fylles ut]	[Ja/Nei]	[Ja/Nei – beskriv kort]	[Vedlegg/URL/versjon]

Leverandøren skal sikre at vilkårene som inntas eller henvises til i dette bilaget, er de vilkårene som faktisk gjelder for Kundens bruk av produktet eller tjenesten på avtaletidspunktet.

Dersom vilkårene finnes elektronisk, skal Leverandøren oppgi stabil lenke, versjonsnummer eller dato for vilkårene. Kunden kan kreve at kopi av vilkårene vedlegges som fil dersom lenke ikke gir tilstrekkelig notoritet.

Fri programvare og åpen kildekode

Leverandøren skal opplyse om fri programvare og åpen kildekode som inngår i leveransen der dette kan ha betydning for Kundens bruk, sikkerhet, rettigheter, videre drift, revisjon eller exit.

Leverandøren skal særlig opplyse om komponenter med lisensvilkår som kan innebære krav om tilgjengeliggjøring av kildekode, videreformidling av lisensvilkår, merking, attribusjon eller andre forpliktelser for Kunden.

For fri programvare/åpen kildekode skal Leverandøren som minimum oppgi:

Komponent	Lisens	Bruksområde i leveransen	Versjon	Eventuelle forpliktelser for Kunden	Dokumentasjon/henvisning
[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]	[Fylles ut]	[Fylles ut]	[Fylles ut]

Dersom Leverandøren benytter Software Bill of Materials (SBOM) eller tilsvarende oversikt, kan slik oversikt vedlegges eller gjøres tilgjengelig som del av dokumentasjonen.

Endringer i standardvilkår

Leverandøren skal varsle Kunden dersom standardvilkår, lisensvilkår eller vilkår for fri programvare/åpen kildekode endres på en måte som kan påvirke Kundens rettigheter, kostnader, sikkerhet, personvern, revisjonsmulighet, datatilgang, behandlingssted, exit eller bruk av leveransen.

Endringer som påvirker leveransen, håndteres etter avtalens regler om endringshåndtering.

Forholdet til øvrige bilag

Pris for standardprogramvare, standardtjenester og lisenser skal fremgå av Bilag 7/prisskjemaet.

Personvern, behandlingssted og bruk av underdatabehandlere skal fremgå av Bilag 11 der standardprogramvaren eller standardtjenesten innebærer behandling av personopplysninger.

Underleverandører og tredjeparter som har betydning for levering av driftstjenesten, skal fremgå av Bilag 6.

Vedlegg til Bilag 10

Leverandøren skal legge ved eller henvise til følgende vilkår:

Nr.	Produkt/tjeneste/komponent	Dokument/lenke	Versjon/dato
1	[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]
2	[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]
3	[Fylles ut av Leverandøren]	[Fylles ut]	[Fylles ut]

Bilag 11: Databehandleravtale

Databehandleravtale inngås som del av avtalen.

Databehandleravtalen består av:

- Databehandleravtale – generell avtaletekst, versjon 01.2020
- Bilag A – Opplysninger om behandlingen
- Bilag B – Betingelser for Databehandlerens bruk av Underdatabehandlere
- Bilag C – Instruks vedrørende behandling av personopplysninger
- Bilag D – Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen

Databehandleravtalen gjelder for all behandling av personopplysninger som Leverandøren utfører på vegne av Kunden som ledd i levering av driftstjenestene etter SSA-D med bilag.

Leverandøren skal i tilbudet fylle ut de deler av Databehandleravtalens bilag som skal fylles ut av Databehandler, herunder opplysninger om underdatabehandlere, behandlingssteder, kontaktpunkter, standardtjenester, sikkerhetstiltak og eventuelle forutsetninger.

Leverandøren skal ikke gjøre endringer i Databehandleravtalens generelle avtaletekst. Eventuelle avvik, forbehold eller forslag til endringer i Databehandleravtalen kan medføre avvisning av tilbudet.

Ved motstrid mellom Hovedavtalen og Databehandleravtalen har Databehandleravtalen forrang for forhold som spesifikt gjelder behandling av personopplysninger.