



Kristiansand
kommune

Anskaffelse av prosjekthotell

Invitasjon til markedsdialog





Innhold

1. Invitasjon til dialog	3
2. Om Kristiansand kommune	3
2.1 Kommunens nåværende løsning	4
2.2 Systemlandskap	4
2.3 Kommunens behov	4
3. Tema og spørsmål	5
3.1 Funksjonalitet og brukervennlighet – demonstrasjon av løsning	5
3.2 Behov	6
3.3 IT, informasjonssikkerhet og personvern	7
4. Videre saksgang	8
5. Vedlegg: IT spesifikasjoner	9



1. Invitasjon til dialog

Kristiansand kommune planlegger å anskaffe et prosjekthotell i løpet av 2026, og ønsker i den forbindelse en dialog med markedet. Formålet med markedsdialogen er primært å få et innblikk i hvilke løsninger som finnes og hvordan de kan dekke kommunens behov for et helhetlig og effektivt prosjekthotell.

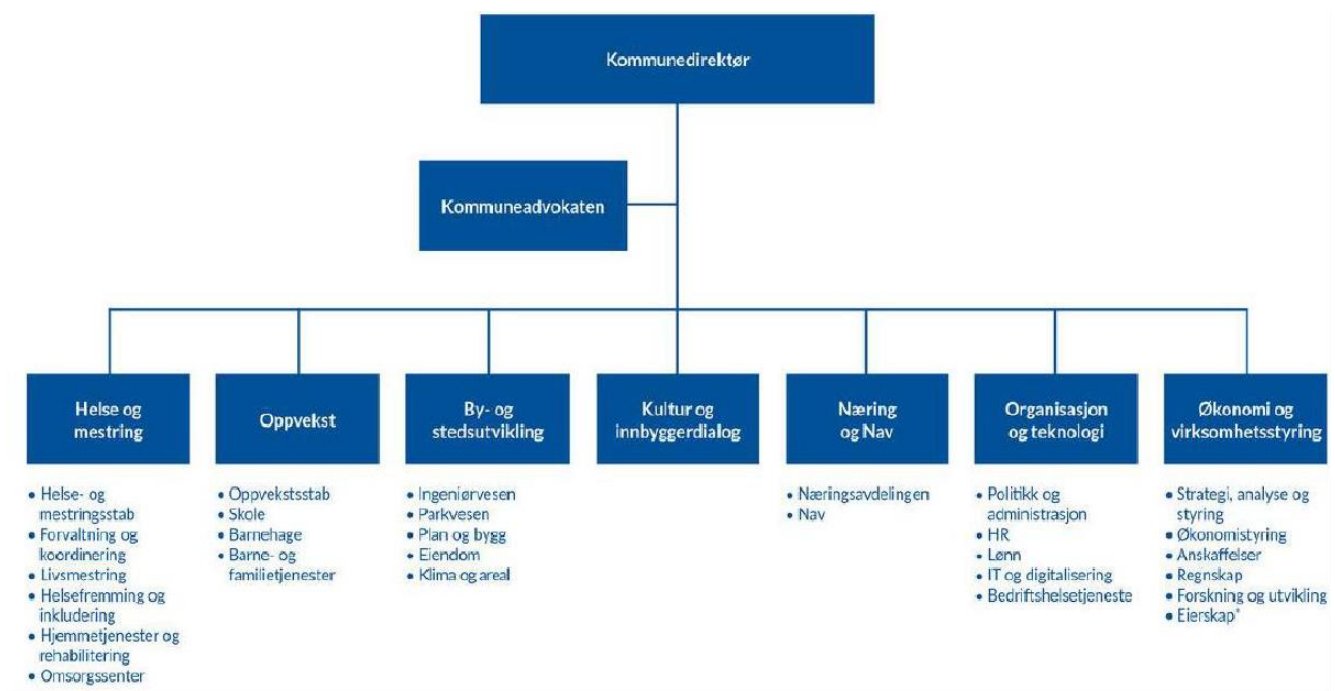
Vi vil gjerne også benytte anledningen til å presentere Kristiansand kommune og hvordan vi vil jobbe med og hvem som trenger prosjekthotellet. En slik presentasjon vil primært skje som en beskrivelse i dette dokumentet og ikke i selve dialogmøtene. Grunnen er at vi ønsker å spare tid og heller sette søkelys på det dere kan tilby.

Kristiansand kommune inviterer derfor interesserte leverandører til digitale (Teams) 1:1-møter fortrinnsvis 15. og 18. juni 2026. Det settes av 1 til 2 timer per leverandør.

Potensielle leverandører bes om å sende påmelding på e-post Thomas.Tverbakk.Bjorgve@kristiansand.kommune.no før 05.06.2026. Oppdragsgiver vil kontakte påmeldte leverandører fortløpende for å avtale tidspunkt.

2. Om Kristiansand kommune

Kristiansand kommune har ca. 9500 ansatte, og er organisert i følgende tjenesteområder:





Det er i første rekke By- og stedsutvikling som har meldt behov for et skybaser prosjekthotell. Hotellet skal dekke alle faser av bygge- og anleggsprosjekter, med tanke på byggeledelse og kvalitetssikring, herunder både store og små, nybygg og rehabilitering. Prosjekthotellet er tenkt som et verktøy for å håndtere kommunikasjon og dokumentasjon med god oversikt over all prosjektinformasjon gjennom hele byggets levetid.

2.1 Kommunens nåværende løsning

Kristiansand kommune har i dag ikke en fullgod løsning for prosjekthotell og benytter i dag Teams for disse oppgavene. Det er manuell arkivering i Public 360 for arkivverdig materiale og manuell overføring av dokumenter til gjeldende konkurransegjennomførings (KGV)- og kontraktsadministrasjonsverktøy (KAV), som for tiden er *Merzell*.

2.2 Systemlandskap

Prosjekthotellet må ha mulighet for å kunne innlemmes sammen med andre systemer via API løsninger. Nedenfor er en forenklet oversikt over systemer som er i bruk i dag. Det er arkivsystem og KGV/KAV (konkurranse)-verktøy som vil være prioritert.

- Arkivsystem (Public360)
- KGV/KAV (Merzell)

2.3 Kommunens behov

Kristiansand kommune har behov for et helhetlig IT-system som støtter god styring, internkontroll og kvalitet i prosjektleveransene. Kommunen trenger en løsning som sikrer at prosjektmedlemmer, interne og eksterne, til enhver tid kan arbeide på grunnlag av siste oppdaterte dokumenter, samt til enhver tid ha kontroll over hva som er utført og hva som gjenstår avhengig av hvor i prosjektet en befinner seg. Det er videre behov for å kunne registrere og følge opp endringer, spørsmål og avklaringer på en brukervennlig måte – uavhengig av om prosjektmedarbeider jobber ved kontorarbeidsplasser eller ute i felten. Det er også ønskelig med et system for å følge opp framdrift, for eksempel i form av milepælssjekklistor/sjekk om oppgaver er utført eller ikke.

Kommunen har behov for en løsning som er ferdigutviklet (*hylleware*), driftsstabil og i aktiv bruk hos sammenlignbare oppdragsgivere.



3. Tema og spørsmål

Nedenfor følger en oversikt over temaer, behov og krav Kristiansand kommune ønsker tilbakemelding på som en del av markedsdialogen.

Temaene i **punkt 3.1** ønskes demonstrert i 1:1-møtene. Det settes av 40 minutter til dette.

3.1 Funksjonalitet og brukervennlighet – demonstrasjon av løsning

Kristiansand kommune ønsker gjennom demoene å få et inntrykk av hvordan en løsning kan fungere i praktisk bruk for ulike roller i et prosjekt (prosjekterende, øverste prosjektledelse, utførende, ledere og administratorer).

Vi ønsker særlig å se hvordan systemet støtter:

- Internsjekk (*prosjektmedlemmer kan gi innspill til dokumenter*)
- Saks- og kommunikasjonssystem
- System for endringskontroll
- Revisjonshåndtering
- Modellvisning og kollisjonssjekk (BIM) – for eksempel i forhold til AutoCAD, NovaPoint
- Opprettelse og bruk av sjekklister, herunder fasesjekklister, eventuelt andre sjekklister
- Tilgangsstyring per dokument, per mappe, grupper mm
- God søkefunksjon på tvers av all metadata, evt. bruk av KI og også søk på innhold i dokumentene
- Hvilke metadata som er lagret per dokument og muligheter for egendefinert utvidelse.
Dette særlig med tanke på dokumenter som skal til offentlig arkiv (P360) og som kanskje skal være «Unntatt offentlighet», eller andre scenarier. Hvordan håndteres dette ift. revisjoner.
- Utsending og publisering av dokumenter og endringer, og styring av hyppighet (mail)
- Standardisering/ dokumentmaler
- Dokumenteierskap – lagres og eies for evig
- Overføring av dokumenter til annet system i framtiden (dette med tanke på bytte av prosjekthotell)
- Systemet må ha mulighet for å bygge egen mappestruktur.
- Systemet må ha mulighet for å opprette «MAL-Prosjekt», og som inneholder dokumenter og sjekklister
- Det skal være enkelt å ha opp flere dokumenter samtidig og manøvrere mellom mapper og filer
- Mulighet for uttrekk av rapporter, statistikk og oversikter (sammenlignbare data)
- Eventuell fremtidig KI-assistent for intern bruk

Demonstrasjonen skal vise funksjonalitet som allerede eksisterer i dagens løsning, uten behov for nyutvikling. Det vil også være mulig å diskutere nye løsninger som er under utvikling.



Som en avsluttende refleksjon av demonstrasjonen, ber vi leverandørene gi en generell betraktning av hva oppdragsgivere bør tenke på ved utforming av konkurransegrunnlag for denne type anskaffelser, herunder Prismodell - dette for å kunne sammenligne priser på likt nivå.

3.2 Behov

- A) **Eksterne brukere: Det er viktig at eksterne uten IT-bruker i** Kristiansand kommune skal kunne være fullverdige medlemmer i prosjektteamene og få tildelt rett brukertilgang. Hvordan håndteres dette?
- B) **Dokumentflyt:** Hvordan støtter løsningen vitale elementer ved dokumenthåndtering som listet over?
- C) **Interne og eksterne må ha tilgang på ulike nivå.** Beskriv hvordan systemet håndterer dette.
- D) **Roller og rettigheter:** Nødvendig å kunne tildele ulike rettigheter avhengig av roller. Beskriv hvordan systemet håndterer
- E) **Opprette og følge egne saker/ case:** Beskriv hvordan systemet håndterer dette
- F) **Implementering og migrering:** Kan leverandøren si noe om forventet tidsløp for implementering for en kommune av vår størrelse, erfaring med migrering fra andre systemer, hvordan dokumenter, prosesser, metadata og historikk etableres og kan videreføres til et eventuelt nytt system. Kan dere vise til konkrete implementeringer hos sammenlignbare kunder, inkludert eventuelle overganger fra andre prosjekthotell?
- G) **Videreutvikling:** Hvordan planlegger dere å videreutvikle løsningen de neste 3-5 årene, og hvilke større endringer eller satsingsområder ser dere for dere innen denne perioden?
- H) **Kunstig intelligens:** Hvordan benytter dere kunstig intelligens i dagens løsning, og hvilke konkrete planer har dere for videre utvikling av KI-basert funksjonalitet? Hva er deres overordnede KI-strategi fremover; hvordan skal KI skape merverdi for brukere av deres løsning de neste 3-5 årene? Hvordan sikrer dere at eventuell KI-bruk er i tråd med gjeldende regelverk, personvern og etikk?
- I) **Kundebase og erfaring:** Hvem er deres primære kunder i dag, og hvilken erfaring har dere med større, offentlige virksomheter?
- J) **Dashboards:** hvordan støtter løsningen deres standardiserte Dashboards og muligheten for å konfigurere tilpassede Dashboards?
- K) **Organisering av leveranse og kundestøtte:** Hvordan er dere organisert når det gjelder drift, support og utvikling? Hvordan sikrer dere effektiv og



forutsigbar oppfølging av kundene – både i implementering og drift?

- L) **Universell utforming:** Hvordan oppfyller systemet krav til universell utforming av ikt-systemer?
- M) **Bruk på ulike digitale flater:** Ansatte i mange tjenesteområder jobber primært på nettbrett eller mobil. Beskriv kort hvordan løsningen fungerer på tvers av ulike enheter, samt hvordan grensesnittet er tilpasset (responsivt) for å sikre god brukervennlighet.
- N) **Innspill til konkurransestrategi:** Eventuelle anbefalinger fra leverandøren til hvordan kommunen legger opp konkurransen.
- O) **Diskusjon av prismodell ønskes.**
- P) **Autentisering og eksterne brukere**
 - Løsningen skal støtte sikker pålogging for både interne og eksterne brukere. For interne brukere er det ønskelig med Single Sign-On (SSO) via Microsoft Entra ID.
 - **For eksterne prosjektdeltakere** ønsker oppdragsgiver innspill til hvordan sikker autentisering og identitetsforvaltning kan løses, herunder håndtering av tilgangsstyring, brukeradministrasjon og livssyklus for brukere.
 - Det bes om at leverandørene beskriver anbefalt løsning og beste praksis for sikker og skalerbar håndtering av eksterne brukere.

3.3 IT, informasjonssikkerhet og personvern

Kristiansand kommune ønsker en god og åpen dialog med leverandørene om forventninger og krav knyttet til IT og informasjonssikkerhet.

Informasjonssikkerhet og personvern

Leverandøren bes beskrive hvordan løsningen ivaretar krav til informasjonssikkerhet og personvern, herunder:

1. Hvordan de grunnleggende prinsippene (konfidensialitet, integritet og tilgjengelighet) for behandling av personopplysninger ivaretas
2. Hvordan data lagres og behandles, inkludert bruk av eventuelle underleverandører
3. Om det er gjennomført ROS-analyse/DPIA for løsningen, og om denne kan deles
4. Hvilke risikoer som er identifisert, og hvilke tiltak som er planlagt eller iverksatt

Vedlagt ligger kommunens dokument «*IT-krav for generell anskaffelse av nytt fagsystem pr13mai26*». Dette er kommunens IT- og sikkerhetsspesifikasjon for anskaffelse av nye løsninger. Vi ønsker å sjekke med dere om kravene er for strenge



eller om dere oppfyller dem. I denne delen av dialogen setter vi pris på at leverandørene stiller med personer med tilstrekkelig teknisk kompetanse som kan svare på spørsmål om temaene i listen under.

4. Videre saksgang

Kommunen vil behandle innspillene fra markedsdialogen og vil så snart som det er mulig lyse ut en konkurranse. Man vil i selve konkurransen formidle når implementering starter og når løsningen må være i drift.



5. Vedlegg: IT spesifikasjoner

Krav nr	Spesifikasjonsbeskrivelse
XX.1	Løsningen skal støtte Single Sign-On (SSO) mot Microsoft Entra ID via enten SAML eller OIDC. Leverandøren skal bekrefte oppfyllelse og beskrive implementasjonen.
XX.2	All brukerautentisering skal skje via Oppdragsgivers Entra ID og støtte Oppdragsgivers bruk av Conditional Access Policies. Leverandøren skal bekrefte dette og beskrive hvordan støtten er implementert.
XX.3	Løsningen skal ha offline eller immutable backup tilgjengelig fra leveransedato. Leverandøren skal beskrive hvordan kravet oppfylles, inkludert teknisk sikring mot endring og sletting.
XX.4	Alle API-er skal ha mulighet for rolle- og tilgangsstyring (RBAC). Leverandøren skal bekrefte oppfyllelse og beskrive funksjonaliteten.
XX.5	Systemet skal til enhver tid oppfylle og være oppdatert i henhold til alle gjeldende lovpålagte krav knyttet til drift og sikkerhet. Leverandøren skal bekrefte rutiner for etterlevelse.
XX.6	Tjenesten skal leveres som en skybasert SaaS-tjeneste der brukeren benytter Oppdragsgivers standard nettleser. Leverandøren skal bekrefte dette.
XX.7	Løsningen skal benytte kryptering av data både i hvile (at-rest) og under overføring (in-transit). Leverandøren skal beskrive rutiner for oppbevaring og rotasjon av krypteringsnøkler.
XX.8	Oppdragsgivers data skal være logisk eller fysisk separert fra andre kunders data. Leverandøren skal beskrive implementasjonen (tekst og skisse) og legge ved dokumentasjon som penetrasjonstester som bekrefter kundeskilte.
XX.9	Leverandøren bes beskrive datasenter som benyttes til primærdrift og redundans, og bekrefte at alle data lagres innenfor EU/EØS. Dersom andre skytjenester enn AWS eller Azure benyttes, skal eierforhold, sertifiseringer, sikkerhetsløsninger og redundans beskrives utførlig.
XX.10	Leverandøren bes beskrive løsningens skyarkitektur (Private/Public/Hybrid) og tenant-modell (Single/Semi/Multi). Ved semi-tenant modell skal det redegjøres for separasjon mellom felles applikasjonsservere og separate databaser.



XX.11	Leverandøren bes legge ved en tekstlig beskrivelse og grafisk skisse av nettverksflyt og sikkerhetsarkitektur. Skissen skal inkludere relevante komponenter, IP-adresser og porter.
XX.12	Oppdragsgiver bør ha fullt eierskap til alle egne data og ha fri tilgang til disse. Leverandøren skal beskrive metoder for ekstrahering og spesifisere eventuelle begrensninger for tilgang (f.eks. hva som ikke er tilgjengelig via API eller begrensninger på nedlasting).
XX.13	Leverandøren skal oppgi og dokumentere støtte for både IPv4 og IPv6.
XX.14	Leverandøren bes beskrive hvordan flaskehalser overvåkes og håndteres, inkludert rutiner for ytelsestesting og om det foreligger kontinuerlig overvåking og utbedring 24/7.
XX.15	Løsningen bør støtte en hendelsesbasert arkitektur der endringer genererer hendelser som eksterne systemer kan abonnere på eller agere på. Leverandøren skal beskrive støtten.
XX.16	Løsningen bør ha integrasjon mellom moduler slik at felles registre benyttes på tvers og dobbeltregistrering unngås. Leverandøren skal beskrive eventuelle begrensninger.
XX.17	Dersom KI benyttes, bes leverandøren beskrive forvaltning av datatilgang, lagringssted for mellomlagring og sletterutiner. Det skal bekreftes at data ikke benyttes til trening av modeller utenfor systemet.
XX.18	Leverandøren bes oppgi hvilken type applikasjon som tilbys (tradisjonell app, webapp eller progressiv webapp).
XX.19	Identitet Leverandøren bes beskrive metoder for provisjonering av brukere og tilganger, herunder støtte for API, fileksport og SCIM 2.0.
XX.20	Leverandøren bes beskrive identitetsattributter som kan benyttes som anker ved provisjonering (uforanderlig ID) og gi anbefalinger som tåler endring av navn eller e-post. Eventuelle begrensninger skal oppgis.
XX.21	Løsningen bes støtte eksterne identitetsløsninger og flerfaktorautentisering for eksterne brukere (f.eks. ID-porten eller HelseID). Leverandøren skal beskrive støtten.
XX.22	Integrasjoner Løsningen bes kunne utveksle data via standardiserte, maskinlesbare grensesnitt (API) og vanlige filformater. Leverandøren skal beskrive støttede formater for både automatisk og manuell utveksling, samt innebygget sikkerhet (kryptering og nøkkelhåndtering).
XX.23	Leverandøren bes beskrive eventuelle nødvendige tredjepartsløsninger (f.eks. M365, Adobe) og spesifisere minimum lisensnivå og nødvendige komponenter for full funksjonalitet.
XX.24	Løsningen bes støtte filtrerte spørringer og praktisere dataminimering ved kun å returnere informasjon som er nødvendig og relevant for den spesifikke forespørselen.



	Leverandøren bes beskrive hvordan dette er ivaretatt i API-ene.
XX.25	Leverandøren bes beskrive omfanget av data som er tilgjengelig via API og bekrefte at det tilbys oppdatert dokumentasjon (f.eks. Swagger) som inkluderer endepunkter, parametre, forespørsels- og svarformater.
XX.26	Leverandøren bes beskrive hvordan integrasjoner overvåkes og bekrefte om Oppdragsgiver kan motta varsling ved utfall.
XX.27	Leverandøren bes bekrefte og dokumentere at det tilbys oppdatert teknisk dokumentasjon for API-er i formater som Swagger eller Redoc.
XX.28	Alle API-er bes støtte moderne sikkerhetsmekanismer, herunder OAuth 2.0/OIDC med klientlegitimasjon (M2M). Det skal være støtte for forsterket sikkerhet via klientsertifikat og/eller IP-allowlisting. Leverandøren bes beskrive implementasjonen.
XX.29	Alle tilgjengelige API-er skal stilles til disposisjon for Oppdragsgiver uten ekstra kostnad. Leverandøren bes bekrefte dette.
XX.30	Løsningen bør tilrettelegge for uthenting av data til ekstern datasjøl (f.eks. Microsoft Fabric) via batch-eksport, datafeed eller direkte integrasjon. Data skal leveres i strukturerte formater som støtter moderne analyseverktøy og KI. Leverandøren bes beskrive mekanismer, sikkerhet og eventuelle begrensninger.
XX.31	Leverandøren bes beskrive prosedyrer for etablering, endring og forvaltning av integrasjoner, inkludert ansvarsfordeling mellom parter og rutiner for feilretting.
XX.32	Leverandøren bes beskrive rutiner for sikkerhetskopiering (backup), herunder oppbevaringstider og definerte mål for RPO (Recovery Point Objective) og RTO (Recovery Time Objective).
XX.33	Leverandøren bes oppgi om det gjennomføres årlig penetrasjonstesting av interne eller eksterne aktører, og bekrefte om Oppdragsgiver kan få innsyn i sammendrag av testresultatene.
XX.34	Leverandøren bes beskrive løsningens loggingsmekanismer, inkludert hvilke aktiviteter som logges, oppbevaringstid og hvilke logger Oppdragsgiver har tilgang til.
XX.35	Leverandøren bes beskrive hvordan løsningen er beskyttet mot DoS- og DDoS-angrep.
XX.36	All utgående e-post fra løsningen skal sikres ved bruk av TLS, SPF, DKIM og DMARC. Leverandøren bes bekrefte etterlevelse.
XX.37	Leverandøren bes oppgi antall og roller for ansatte som har tilgang til Oppdragsgivers data, og beskrive bruk av PIM (Privileged Identity Management). Det skal oppgis om kunden kan få innsyn i logger som viser leverandørens aksess til data.
XX.38	Leverandøren bes legge ved en tekstlig og grafisk skisse av sikkerhetsarkitekturen og beskrive ytterligere sikkerhetstiltak eller sertifiseringer som gir merverdi utover standardkravene.



XX.39	Leverandøren bes bekrefte og beskrive muligheten for å levere en komplett sikkerhetskopi av databasen til Oppdragsgiver, enten regelmessig eller på forespørsel.
XX.40	Leverandøren bes beskrive rutiner ved opphør av avtale, inkludert sikker sletting av data og prosedyrer for overføring til ny leverandør.
XX.41	Leverandøren bes beskrive hvordan flaskehalser overvåkes og utbedres (automatisk/manuelt), inkludert responstider for utbedring ved hendelser 24/7.
XX.42	Leverandøren bes beskrive hvilke tekniske logger Oppdragsgiver har tilgang til, loggenes innhold og metoder for tilkobling.
XX.43	Løsningen bør inkludere regelmessig ytelsesrapportering med statistikk over responstider, belastningstester og avvik fra standarder. Leverandøren skal beskrive rapportenes innhold.
XX.44	Ved alvorlige driftsavvik skal leverandøren levere en rapport med årsaksanalyse (RCA), oversikt over hendelsesforløp, iverksatte tiltak og plan for å forebygge gjentakelse. Leverandøren skal bekrefte rutinen.
XX.45	Leverandøren bes oppgi SLA (Service Level Agreement) for oppetid basert på 24/7 bruk av løsningen.
XX.46	Klienter Eventuelle mobilapplikasjoner som kreves skal være tilgjengelige via offisielle kanaler som Apple App Store og Google Play.
XX.47	Leverandøren bes beskrive eventuelle behov for bruk av sertifikater eller tokens for tilgang til løsningen.
XX.48	Leverandøren bes beskrive støttede klientplattformer og redegjøre for eventuelle begrensninger knyttet til funksjonalitet, respons, skalering eller brukervennlighet.
XX.49	Leverandøren bes beskrive løsningens offline-funksjonalitet, herunder teknisk plattform (App/PWA), lokal mellomlagring, sletterutiner, kryptering, tilgangsstyring og synkroniseringsmekanismer.