



Troms fylkeskommune
Romssa fylkkasuohkan
Tromssan fylkinkomuuni

Løsning for kundedialog, CRM og saksbehandling

Kravspesifikasjon



Innholdsfortegnelse

Definisjoner	2
Om oppdragsgiver	3
1. Formål.....	4
2. Overordnede krav.....	4
3. Microsoft 365-integrasjon	4
4. Omnikanal kommunikasjon.....	4
5. Saksbehandling og arbeidsflyt.....	4
6. Kategorisering og skjema.....	4
7. AI og automatisering	4
8. Kundehistorikk og CRM.....	4
9. Kunnskapsbase og selvbetjening	4
10. Integrasjoner	4
11. Rapportering og statistikk	5
12. Informasjonssikkerhet og personvern	5
13. Drift, forvaltning og vedlikehold (FDV)	5
14. Leverandørkrav	5
15. Tildelingskriterier.....	5
Vedlegg A – Detaljerte funksjonskrav	6
Vedlegg B krav til statistikk.....	8
Vedlegg C krav til kunnskapsbase.....	9
Vedlegg D krav til ivaretagelse av informasjonssikkerhet og personvern	10

Definisjoner

Oppdragsgiver: Troms fylkeskommune, som anskaffer og benytter løsningen eller tjenesten.

Leverandør: Virksomheten som leverer, drifter eller forvalter løsningen eller tjenesten på vegne av oppdragsgiver.

Bruker: Person som benytter løsningen eller tjenesten, for eksempel ansatte, innbyggere eller andre autoriserte brukere.

Kanaler: Kontaktpunkter der kunder kommuniserer med Svipper, mottar informasjon eller får kundeservice gjennom CRM- og kontaktsenterløsningen.

Kunde: Oppdragsgivers kunder eller sluttbrukere som løsningen eller tjenesten er utviklet for eller skal betjene.

Løsning: Systemet, tjenesten eller produktet som leverandøren skal levere.

Tjenesten: De funksjonene, tjenestene og eventuell drift/support som omfattes av avtalen.

Data: Informasjon som lagres, behandles eller overføres i løsningen.

Personopplysninger: Opplysninger som kan knyttes til en identifisert eller identifiserbar person.

Administrator: Person hos leverandør eller oppdragsgiver med utvidede rettigheter i løsningen.

Underleverandør: Tredjepart som leverandøren benytter for å levere hele eller deler av tjenesten.

Tilgjengelighet/oppetid: Hvor stor del av tiden tjenesten skal være tilgjengelig for bruk.

Om oppdragsgiver

Oppdragsgiver er Troms fylkeskommune, som har ansvaret for kollektivtrafikken i Troms fylke. Gjennom merkevaren Svipper tilbyr fylkeskommunen offentlig transport med buss, hurtigbåt og ferge, samt digitale tjenester for reiseplanlegging, billettkjøp og kundeinformasjon, og lovpålagt skoleskyss.

Svipper er det felles navnet på kollektiv- og mobilitetstilbudet i Troms, og skal gjøre det enklere for innbyggerne å finne fram til tjenester og informasjon på tvers av transportmidler. Målet er å gi reisende en enklere, mer sømløs og tilgjengelig reisehverdag.

Kollektivtilbudet i Troms er omfattende og viktig for hverdagsreiser i hele fylket. Hvert år gjennomføres rundt 21 millioner reiser med buss, hurtigbåt og ferge. Samtidig håndterer kundeservice cirka 25-30 000 kundeservicehendelser årlig knyttet til billetter, rutetilbud, reiseinformasjon og kundestøtte. Kundeservice håndterer også refusjoner, reisegarantier, plass- og setereservasjoner, avviksinformasjon og bestillingstransport.

1. Formål

Formålet med anskaffelsen er å etablere en skybasert løsning for kundedialog, CRM og saksbehandling knyttet til kollektiv- og mobilitetstilbudet i Troms.

2. Overordnede krav

Løsningen skal være en skybasert standardløsning (SaaS), støtte omnikanal kundedialog, CRM og saksbehandling, være skalerbar og kunne administreres av oppdragsgiver uten behov for utviklerbistand.

3. Microsoft 365-integrasjon

Løsningen skal kunne integreres med Outlook, Teams, Microsoft Entra ID (Azure AD) og Exchange Online.

4. Omnikanal kommunikasjon

Løsningen skal støtte mottak og håndtering av e-post, chat, nettskjema, sosiale medier, telefon og chatbot. Alle henvendelser skal samles i ett felles sakssystem med full historikk per kunde.

5. Saksbehandling og arbeidsflyt

Løsningen skal støtte opprettelse av saker fra alle kanaler, statusstyring, historikk, kategorisering, prioritering, automatisk ruting, interne notater, vedlegg og frist- og svartidshåndtering.

6. Kategorisering og skjema

Løsningen skal støtte hierarkisk kategorisering, logikkstyrte skjema, dynamiske felter og publisering av endringer i sanntid.

7. AI og automatisering

Løsningen skal støtte forslag til svar, automatisk kategorisering, oppsummering av dialoger, chatbot og automatisering av enkle henvendelser.

8. Kundehistorikk og CRM

Løsningen skal gi samlet oversikt over kundeinformasjon, tidligere dialog, saker og historikk på tvers av kanaler og fagområder.

9. Kunnskapsbase og selvbetjening

Løsningen skal støtte forhåndsdefinerte svarmaler og sentral administrasjon av disse. Løsningen skal støtte kunnskapsbase, selvbetjening og statussporing.

10. Integrasjoner

Løsningen skal tilby standard API-er og støtte integrasjon mot nettsider, mobilapplikasjoner, billettsystemer, økonomisystemer og analyseverktøy.

11. Rapportering og statistikk

Løsningen skal tilby statistikk og rapportering for kundeservice, saksbehandling og kanalbruk.

12. Informasjonssikkerhet og personvern

Løsningen skal være GDPR-kompatibel, støtte MFA, logging, revisjonsspor og datalagring innen EU/EØS.

Løsningen skal ha mulighet for å bestemme hvilke feltverdier i skjemaene som skal beskyttes ytterligere av GDPR, slik at de ikke vises på den automatiske genererte kvitteringen som sendes til e-post.

13. Drift, forvaltning og vedlikehold (FDV)

Tilbudet skal inkludere lisenskostnader, drift, vedlikehold, support, sikkerhetsoppdateringer og videreutvikling.

Leverandør skal oppgi årlig FDV-kostnad og utviklingsramme.

14. Leverandørkrav

Leverandør skal dokumentere erfaring fra tilsvarende leveranser, offentlig sektor eller omnikanal kundesenter.

15. Tildelingskriterier

- Funksjonalitet og løsningsbeskrivelse – 40 %
- Pris og totale FDV-kostnader – 30 %
- Implementering og gjennomføring – 15 %
- AI, innovasjon og videreutvikling – 10 %
- Miljø og bærekraft – 5 %

Vedlegg A – Detaljerte funksjonskrav

Løsningen skal støtte:

- håndtering av e-post, chat, skjema, nettside, sosiale medier og andre kanaler i samme løsning
- fleksibelt oppsett og administrasjon av innbokser, køer og filtergrupper
- automatisk ruting og delegasjon av saker basert på regler, kategori eller fagområde
- separate arbeidsflater for ulike fagområder
- deling av relevant informasjon på tvers av fagområder
- interne notater, kommentarer og diskusjoner på saker
- strukturert og sporbar saksbehandling med ett saksnummer gjennom hele dialogforløpet
- flere samtidige chatsamtaler per saksbehandler
- varslings ved nye meldinger eller svar i chat
- konfigurerbare åpningstider for chat med automatisk aktivering og deaktivering
- opprettelse og vedlikehold av digitale skjema uten behov for utviklerbistand
- publisering av endringer i skjema og chat-widget i sanntid
- logikkstyrte skjema og dynamiske felter
- fleksibel oppbygging av felter og gjenbruk av felter i skjema
- hierarkisk kategorisering, eksempelvis kategori, underkategori, årsak og konsekvens
- kobling mellom saker og hendelser i verdikjeden, eksempelvis avvik, kontrakt, linje, operatør, app og sanntidshendelser
- automatisk skille mellom interne og eksterne saker
- import og eksport av datasett i Excel- og CSV-format
- eksport og lagring av innsendte skjema som PDF-vedlegg i saken
- rollebasert tilgangsstyring og skjerming av sensitive felter i henhold til GDPR
- standard API-er og integrasjon mot tredjepartssystemer

Løsningen bør støtte:

- AI-basert kategorisering og ruting av saker
- automatisert opprettelse av filtergrupper og arbeidsflyter
- masseopprettelse av felter og skjemaelementer
- fleksibel administrasjon av chat-widget uten kodeendringer hos leverandør
- publisering av svarartikler og FAQ i chat-widget
- filtrering av svarartikler på språk, kategori og tema
- forbedret søkefunksjonalitet i chat og kunnskapsbase

- analyse av henvendelser og mønstre på tvers av datasett
- integrasjon mot eksterne mobilitets- og transportsystemer, eksempelvis Entur, WeCore og YouTravel

Vedlegg B krav til statistikk

Løsningen skal minimum kunne rapportere på:

- antall henvendelser
- kanalfordeling
- sakstyper og kategorier
- responstid og svartid
- behandlingstid
- SLA og fristbrudd
- restanser og åpne saker
- kundetilfredshet
- chatbotbruk og automatiseringsgrad
- volum per fagområde
- utvikling over tid

Rapportering skal kunne filtreres på:

- tidsperiode
- kanal
- fagområde
- sakstype
- team og saksbehandler

Løsningen skal støtte:

- eksport av data
- dashboards
- sanntidsoversikt
- automatiske rapporter
- rollebasert tilgang til rapportering

Løsningen bør støtte:

- Power BI-integrasjon
- analyse av trender og mønstre
- AI-basert innsikt
- visualisering av kundereiser og kanalbruk
- analyse av chatbot og selvbetjening
- analyse av årsaker til henvendelser
- prediksjon av volum og belastning

Vedlegg C krav til kunnskapsbase

Kunnskapsbasen skal bidra til å redusere personavhengighet i organisasjonen ved å samle og tilgjengeliggjøre relevant informasjon på ett sted.

Oppbygging, vedlikehold og administrasjon av kunnskapsbasen skal kunne utføres direkte i systemet uten behov for eksterne verktøy.

Løsningen skal:

- støtte strukturering og organisering av informasjon gjennom kategorisering, tagging, filtrering og andre relevante funksjoner
- gjøre det mulig for brukere å søke opp og hente ut nødvendig informasjon på en enkel og effektiv måte
- legge til rette for at ulike faggrupper kan arbeide selvstendig med egne fagområder, samtidig som det støtter samarbeid på tvers av faggrupper
- kunne skille mellom intern og ekstern informasjon med egne tilgangs- og publiseringsnivåer
- støtte publisering av ekstern informasjon gjennom utgående kanaler, som for eksempel avviksmeldinger, standardiserte maler og annen relevant informasjon
- ha integrasjonsmuligheter mot chat-løsninger, sosiale medier og virksomhetens nettsider
- muliggjøre automatisk eller forenklet distribusjon av informasjon fra kunnskapsbasen til eksterne kanaler

Vedlegg D krav til ivaretagelse av informasjonssikkerhet og personvern

Leverandøren og leverandørens ansatte skal ha taushetsplikt om informasjon de får tilgang til gjennom kontraktsforholdet.

Dersom leverandøren skal behandle personopplysninger på vegne av oppdragsgiver, skal det inngås databehandleravtale.

Dersom leverandøren skal benytte oppdragsgivers IKT-systemer eller IKT-ressurser, skal gjeldende IKT-reglement og sikkerhetskrav følges.

Databehandleravtale

Når en leverandør behandler personopplysninger på vegne av fylkeskommunen, skal det i tillegg etableres en databehandleravtale for å sikre at behandlingen skjer i tråd med personvernregelverket. Det skal brukes standardiserte maler, enten malen til DFØ eller Datatilsynet.

Tilstrekkelige garantier

Leverandøren skal, dersom det er aktuelt å behandle personopplysninger på vegne av oppdragsgiver, opptre som databehandler i henhold til personopplysningsloven og personvernforordningen (GDPR).

Leverandøren skal kunne dokumentere at det er etablert tilstrekkelige tekniske og organisatoriske tiltak for å sikre at behandlingen av personopplysninger skjer i samsvar med gjeldende regelverk.

Som dokumentasjon kan leverandøren for eksempel vise til:

- sertifisert styringssystem for informasjonssikkerhet (ISO 27001),
- styringssystem for informasjonssikkerhet og personvern (ISO 27701), eller
- annen relevant dokumentasjon som demonstrerer etterlevelse av kravene i personopplysningsloven og GDPR.

Sikkerhetsrevisjon

Oppdragsgiver skal ha rett til å gjennomføre sikkerhetsrevisjon av leverandøren og den leverte løsningen i avtaleperioden.

Sikkerhetsrevisjon kan blant annet omfatte:

- penetrasjonstesting,
- sårbarhetsskanning, og
- kontroll av leverandørens etterlevelse av krav til informasjonssikkerhet.

Leverandøren skal legge til rette for slike revisjoner og bidra med nødvendig dokumentasjon og tilgang innen rimelig tid.

Risikostyring

Leverandøren skal ha etablerte prosesser for løpende identifisering, vurdering og håndtering av sårbarheter og sikkerhetsrisiko i tjenesten og tilhørende systemer.

Leverandøren skal dokumentere hvordan sikkerhetsarbeidet følges opp, herunder rutiner for risikovurdering, hendelseshåndtering og oppdatering av sikkerhetstiltak.

Leverandøren bør være åpen om egne sikkerhetspraksiser og regelmessig rapportere til oppdragsgiver om sikkerhetsstatus, avvik og sikkerhetshendelser som kan påvirke tjenesten eller oppdragsgivers data.

Avslutning av avtale

Ved avslutning av avtalen skal leverandøren bistå oppdragsgiver med en ordnet avvikling og overgang til annen løsning eller leverandør.

Leverandøren skal legge til rette for at oppdragsgivers data kan overføres til oppdragsgiver eller til tredjepart utpekt av oppdragsgiver, i et strukturert og alminnelig brukt format.

Oppdragsgiver skal beholde eierskapet til alle data som er lagret eller behandlet i tjenesten gjennom hele avtaleperioden og etter avtalens opphør, frem til data er overført og/eller slettet i henhold til oppdragsgivers instruksjoner.

Leverandøren skal, etter oppdragsgivers anmodning, dokumentere at data er slettet fra leverandørens systemer og eventuelle underleverandørers systemer, med mindre lagring er påkrevd etter lov eller forskrift.

Beskyttelse av data under overføring

All data som overføres via nettverk skal sikres mot uautorisert tilgang, endring og avlytting. Dette gjelder både data som overføres til og fra tjenesten, data som overføres internt i tjenesten, og data som utveksles med eksterne tjenester eller integrasjoner.

Leverandøren skal benytte anerkjente og oppdaterte sikkerhetsmekanismer for kryptering og sikker kommunikasjon ved overføring av data.

Beskyttelse av datasenter

Leverandøren skal sikre at datasentre og tilhørende infrastruktur er beskyttet mot uautorisert tilgang, tyveri, skade, tap og driftsavbrudd.

Leverandøren skal ha etablerte fysiske og tekniske sikkerhetstiltak som bidrar til å sikre kontinuerlig og stabil drift av tjenesten.

Beskytte lagret informasjon

Leverandøren skal definere, velge, dimensjonere og implementere egnede kryptografiske mekanismer, inkludert tilstrekkelig nøkkeladministrasjon, for å sikre sikker drift av tjenestene. Dette gjelder både data lagret i tjenesten og data som overføres via nettverk.

Leverandøren skal sikre at det finnes pålitelige rutiner for sikkerhetskopiering og gjenoppretting for å beskytte data mot tap, skade eller utilgjengelighet.

Separasjon mellom kunder

Leverandøren skal sikre at oppdragsgivers tjenester og data er logisk og/eller fysisk separert fra andre kunders tjenester og data hos leverandøren.

Backup

Leverandøren skal sørge for tilfredsstillende sikkerhetskopiering av data, slik at data kan gjenopprettes raskt og effektivt ved behov.

Sletting av data

Leverandøren skal kunne dokumentere rutiner og metoder for sikker sletting av data.

Leverandøren skal sikre at slettede data ikke kan gjenopprettes, rekonstrueres eller komme på avveie etter sletting.

Tilgjengelighet

Tjenesten skal ha høy tilgjengelighet og være tilgjengelig for oppdragsgiver når tjenesten er nødvendig for virksomheten.

Leverandøren skal kunne dokumentere garantert oppetid for tjenesten, inkludert eventuelle servicenivåavtaler (SLA).

Leverandøren skal på forespørsel kunne dokumentere historisk oppetid og tilgjengelighet for tjenesten.

Endringshåndtering

Leverandøren skal ha prosess for å håndtere endringer for å sikre at endringer som kan påvirke sikkerheten identifiseres og håndteres, og at uautoriserte endringer kan oppdages.

Sporbarhet

Leverandøren skal sikre at alle relevante handlinger utført av leverandøren logges.

Loggene skal være beskyttet mot manipulering, endring og uautorisert tilgang.

Oppdragsgiver skal på forespørsel gis tilgang til relevante logger.

Tilgangskontroll/autentisering

Løsningen skal ha tilgangskontroll som sikrer at brukere kun får tilgang til informasjon og funksjoner de er autorisert for.

Autentisering basert utelukkende på brukernavn og passord anses ikke som tilstrekkelig. Løsningen skal støtte sterk autentisering, herunder multifaktorautentisering (MFA).

Dersom det er relevant for tjenesten, skal leverandøren tilby verktøy for administrasjon av oppdragsgivers brukere og tilganger.

Løsningen skal ha støtte for integrasjon med eksterne identitetstilbydere, herunder Microsoft Entra ID eller tilsvarende løsninger.

Sikkerhetsovervåking

Leverandøren skal ha tilstrekkelig sikkerhetsovervåking av tjenesten, rutiner for varsling ved sikkerhetshendelser og evne til å håndtere sikkerhetshendelser raskt og effektivt.

Leverandøren skal på forespørsel gi oppdragsgiver tilgang til relevante revisjonsrapporter for vurdering av sikkerhetsovervåking, tilgangsstyring for leverandørens administratorer samt prosedyrer og rutiner for varsling og hendelseshåndtering.

Sikkerhetslogger skal gjøres tilgjengelig for oppdragsgiver på forespørsel.