

SSA-L-2018

**Bilag til avtale om løpende tjenestekjøp over internett**

Statens standardavtaler for IT-anskaffelser

bilag til SSA-L - versjon 2018

FOR 004 – 2020 Anskaffelse av FIT verktøy



Bilag til SSA-L – Avtale om løpende tjenestekjøp over internett– versjon 2018

Innhold:

[Bilag 1: Kundens kravspesifikasjon 3](#_Toc507588406)

[Bilag 2: Leverandørens beskrivelse av tjenesten 11](#_Toc507588407)

[Bilag 3: Plan for etableringsfasen 13](#_Toc507588409)

[Bilag 4: Tjenestenivå med standardiserte kompensasjoner 15](#_Toc507588410)

[Bilag 5: Administrative bestemmelser 16](#_Toc507588411)

[Bilag 6: Samlet pris og prisbestemmelser 18](#_Toc507588412)

[Bilag 7: Endringer i den generelle avtaleteksten 21](#_Toc507588413)

[Bilag 8: Endringer av tjenesten etter avtaleinngåelsen 22](#_Toc507588414)

[Bilag 9: Vilkår for Kundens tilgang og bruk av tredjepartsleveranser 23](#_Toc507588415)

# Bilag 1: Kundens kravspesifikasjon

## Avtalens punkt 1.1 Avtalens omfang

# Lisenser: FIT - Feedbackinformert behandling/tjenester

## Bakgrunn

Etat for barn og familie i Bergen kommune, ønsker å tilby barn, unge og foreldre å gi direkte tilbakemeldinger på våre tjenester og videre å kunne utvikle våre tjenester ved hjelp av systematisk tilbakemelding og bruk av verktøy for dette formålet. Det er besluttet at FIT (Feedback Informed Treatment) skal benyttes som verktøy og at tilbakemeldingene registreres digitalt.

FIT er et kartleggingsverktøy for samarbeid og effekten av dette samarbeidet. Kartleggingsverktøyet kan benyttes på papir eller digitalt. Bruker besvarer på 5 enkle skalaer hvordan de opplever at den siste uken har vært og tilsvarende hvordan de har opplevd samtalen. FIT er ikke et verktøy som kan kartlegge symptomer e.l., det er først og fremst samarbeidet og dets effekt som undersøkes.

Etat for barn og familie ønsker å tilby tilbakemeldingssystemet blant annet for å imøtekomme ønsket om å kunne gi tilbakemelding som våre brukere har gitt uttrykk for, legge til rette for at hjelpen som gis kan bli mer målrettet og effektiv for bruker og for å arbeide systematisk mot måloppnåelse knyttet til planen «Bergen barn – byen fremtid» og visjon om økt åpenhet og deltakelse i våre tjenester.

FIT benyttes i deler av våre tjenester i dag, i papirform. I denne formen, vil tilbakemeldingene benyttes til å bedre individuell oppfølging. Ved bruk av FIT digitalt, vil en i tillegg kunne får tilgang på anonymiserte aggregerte data fra tilbakemeldingene, noe som gjør at tjenesten kan gjøre justering og tilpasninger på systemnivå i tråd med et gjennomsnitt av brukernes tilbakemeldinger.

Etat for barn og familie ønsker et digitalt system som er brukervennlig for alle parter, som gir den ønskede kliniske støtten og som samtidig ivaretar nødvendig sikkerhet.

FIT benyttes i tjenester som arbeider etter helse- og omsorgsloven og lov om barneverntjenester. FIT skal på lik linje med som annen kartlegging journalføres i brukers journal.

## Kravspesifikasjon

## Absolutte krav

**Generelle krav knyttet til løsning og system**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Krav** | **Kategori**A (Absolutt) |
| 1 | Programvaren |  |
| 1.1 | Programvaren må inneholde alle kjente versjoner av Outcome Rating Scale (ORS) og Session Rating Scale (SRS). Dette innebærer at skjema er tilpasset for alle aldersgrupper i tillegg til skjema som kan benyttes i grupper.  | A |
| 1.2 | Programvaren må kunne benyttes på PC og smarttelefon, samt nettbrett. Det er et absolutt krav om at programmet skal kunne benyttes via nettleser og skjermbildet må være tilpasset den enheten man benytter (responsiv design). | A |
| 1.3 | Programvaren må i tillegg til skalaene kunne vise en generert forventningskurve. Denne må presenteres på en måte som er brukervennlig for alle parter. | A |
| 1.4 | Programvaren må ha en funksjon som viser kombinerte forventningskurver (for eksempel som brukt i par- eller familiesamtaler). | A |
| 1.5 | Programvaren må kunne gjøre tilgjengelig aggregerte data på behandler-, avdelings- og organisasjonsnivå.  | A |
| 1.6 | Programvaren skal tilby en løsning for administrativ pålogging og styring og det må kunne legges til rette for ulike brukertilganger. | A |
| 1.7 | Programvaren må ha mulighet å legge inn tofaktorautentisering for systemadministratorer og andre roller i systemet. | A |
| 1.8 | Skalaene som presenteres i systemet, må være oversatt til norsk. | A |
| 1.9 | Demoversjon ellers test-lisens skal leveres sammen med tilbudet, inkludert veiledning, brukernavn og passord der det er nødvendig | A |
| 2 | **Support** |  |
| 2.1 | Teknisk- og brukersupport skal tilbys av leverandør og må kunne foregå på norsk, svensk eller engelsk. Svartid er minst innen fem arbeidsdager. | A |
| 3 | **Personvern** |  |
| 3.1 | Programvaren må tilfredsstille kravene i GDPR og kunne dokumentere at de lovpålagte kravene til tjenesten ivaretas og på hvilken måte. Tjenestene er regulert av lov om helse og omsorgstjenester i kommunen, lov om helsepersonell og lov om barneverntjenester. | A |
| 3.2 | **Innebygget personvern**Systemet skal utvikles/skal være utviklet med fokus på innebygget personvern og personvern som standardinnstilling. Leverandør må sørge for at dette er ivaretatt fra starten og gjennom hele utviklingsløpet for systemet. Datatilsynets veileder for programvareutvikling med innebygget personvern i utviklingsprosjekter beskriver prosessen med tilhørende sjekklister. Se også Datatilsynets syv prinspiller for innebygget personvern.  Systemet skal utvikles/tilpasses med fokus på personvern som standardinnstilling. Funksjonaliteten skal tilrettelegges for oppfyllelse av prinsippene for behandling av personopplysninger. | A |
| 3.3 | Leverandøren og løsningen som tilbys må følge og oppfylle den til enhver tid gjeldende versjonen av Datatilsynets veileder for programvareutvikling med innebygd personvern. | A |
| 3.4 | I tilbudet må det beskrives hvordan løsningen dekker innebygd personvern og de syv stegene i "privacy by design" og hvordan leverandøren garanterer (også i fremtiden) å oppfylle den til enhver tid gjeldende veiledningen fra Datatilsynet. Leverandøren bes i tillegg beskrive hvilke forutsetninger de eventuelt må legge til grunn for at behovet kan dekkes**.** | A |
| 3.5 | Dokumentasjonen skal også på forespørsel være tilgjengelig for det enkelte behandlingssansvarlige helseforetak, samt for Datatilsynet og Personvernnemnda. | A |
| 4. | **Styringssystem** |  |
| 4.1 | Leverandør av løsningen med eventuelle underleverandører skal ha et dokumentert og operasjonalisert styringssystem for informasjonssikkerhet (ISMS) tilsvarende god praksis og internasjonalt anerkjente standarder for informasjonssikkerhet, f.eks. ISO/IEC 27001:2017, som dekker teknologi, informasjon, organisasjon, personal og fysiske lokasjoner som kan påvirke leveransene. Jf. GDPR art. 28 nr. 3. Styringssystemet skal fremlegges for behandlingsansvarlig på forespørsel og skal som minimum svare for virkeområde, delegasjon og definisjoner, formål, sikkerhetsmål, roller og ansvar, kontroll og revisjon.Leverandøren beskriver hvordan kravet oppfyllesLeverandør skal beskrive informasjonssystemet og sikringstiltakeneLøsningen skal sørge for at personopplysninger sikres med hensyn til integritet, konfidensialitet, tilgjengelighet og robusthet.  Integritet (I): Personopplysninger skal sikres mot utilsiktet og ulovlig ødeleggelse, tap og endringer. Konfidensialitet (K): Personopplysninger skal sikres mot uautorisert utlevering og tilgang. Tilgjengelighet (T): Personopplysninger skal være tilgjengelig for autoriserte med tjenstlig behov. Robusthet (R): Programvaren som behandler personopplysninger, skal være robuste mot for eksempel sårbarheter, angrep, og uhell.Leverandøren skal ha et styringssystem for informasjonssikkerhet som er i henhold til alminnelig anerkjente standarder på områdetDersom leverandøren har et sertifisert styringssystem for informasjonssikkerhet, er fremleggelse av sertifikatet tilstrekkelig som beskrivelse. | A |
| 4.2 | **Tilgjengeliggjør av dokumentasjon**Dokumentasjonen skal også på forespørsel være tilgjengelig for det enkelte behandlingssansvarlige helseforetak, samt for Datatilsynet og Personvernnemnda.  | A |
| 4.3 | **Loggføring**Løsningen skal som et minimum logge systemhendelser og sikkerhetshendelser, inkludert feilsituasjoner, endringer og uautoriserte forsøk på tilgang. Jf. Pasientjournalloven §§ 7 og 22. Løsningen skal som et minimum logge systemhendelser, inkludert feilsituasjoner, endringer og uautoriserte forsøk på tilgang. Jf. pasientjournaloven §§ 7 og 22. | A |
| 4.4 | **Risikovurdering** Leverandør skal ha gjennomført en risikovurdering av sin løsning og fremlegge/presentere denne for behandlingsansvarlig. Leverandøren skal levere en løsningsskisse og beskrive dataflyt i sitt system som en del av risikovurderingen. Leverandør skal minst årlig gjennomføre risiko- og sårbarhetsanalyse knyttet til alt som omfatter leveransen av tjenesten. Dette gjelder også for bruk av eventuelle underleverandører. Risikovurderingen skal som et minimum identifisere kristika aktiva, trusler og sårbarhet og resultere i en formelt dokumentert risikoanalyse som kan tilgjengeliggjøres for behandlingsansvarlig.Leverandøren skal dokumentere informasjonssystemet og sikkerhetstiltakene.Leverandøren skal ha gjennomført en risikovurdering av sin løsning og fremlegge/presentere denne for behandlingsansvarlig. | A |
| 4.5 | **Databehandleravtale** Som databehandler for kommunen skal leverandøren behandle opplysninger slik det fremgår av databehandleravtalen. Leverandøren kan ikke behandle personopplysningene på annen måte, jf. GDPR art. 28. Dette innebærer bl.a. at databehandler ikke kan behandle eller benytte personopplysninger til egne formål.Universell utforming Løsningen må oppfylle krav til enhver tid gjeldende versjon av Forskrift om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger (<https://lovdata.no/dokument/SF/forskrift/2013-06-21-732>)Det forutsettes av Bergen kommune eier data som registreres i systemet, og databehandleravtalen til Bergen kommune skal benyttes og etterfølges.Beskriv de geografiske lokasjonene (land) hvor personopplysninger blir behandlet. Avhengig av kravene til sikring av personopplysningene som skal behandles vektes det positivt at personopplysningene behandles i prioritert rekkefølge Norge (1), EU/EØS (2) og andre land (3). Hvis andre land enn Norge, skriv hvilket land.Vedlegg 1: Databehandler avtalen til Bergen kommuneDet stilles krav til universell utforming, jfr. https://lovdata.no/dokument/SF/forskrift/2013-06-21-732. | A |
| 5 | **Tilgang- og rollestyring**Løsningen skal tilby fleksible muligheter for å knytte roller til en eller flere ansatte. Tilganger tildeles en rolle begrenset til informasjon, dokumentert gjennom rollens tjenstlige behov, for å utføre en oppgave. Løsningen skal ha fleksibilitet og konfigurasjonsmuligheter knyttet til hvordan ansatte tildeles roller i systemet ut fra hvilke arbeidsoppgaver og/eller organisasjonstilhørighet den ansatte har. | A |
| 6 | Leverandøren skal levere en løsningsskisse og beskrive dataflyt i sitt system som en del av risikovurderingen. | A |
| 7 | Systemet skal minimum kunne brukes på følgende nettlesere: Safari, Chrome, Microsoft Edge, Firefox. | A |
| 8 | Leverandør skal kunne sende en oversikt på hvem som har tilgang til løsningen og hvilken tilgang de har. | A |

## Avtalens punkt 3.4 Dokumentasjon og opplæring

Det er ikke behov for opplæring fra leverandør.

## Avtalens punkt 3.5 Oppgradering/vedlikehold av tjenesten etter Leveringsdag

Programvaren skal være leverandørens nyeste versjon til enhver tid.

## Avtalens punkt 3.6 Ytterligere utvikling etter Leveringsdag

[Eventuell tekst]

## Avtalens punkt 6.1 Informasjonssikkerhet

## Avtalens punkt 6.2 Personopplysninger

Databehandleravtalen skal være vedlegg 1 til SSA kontrakten.

## Avtalens punkt 7.1 Partenes rettigheter

Bergen kommune vil leie lisens til leverandørens verktøy.

Viser for øvrig til krav i databehandleravtalen.

## Avtalens punkt 8 Rekonstruksjon av data

# Bilag 2: Leverandørens beskrivelse av tjenesten

Leverandøren svarer her

**Generelle krav knyttet til løsning og system**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **Krav** | **Kategori**A (Absolutt) | JA /NEI |
| 1 | Programvaren |  |  |
| 1.1 | Programvaren må inneholde alle kjente versjoner av Outcome Rating Scale (ORS) og Session Rating Scale (SRS). Dette innebærer at skjema er tilpasset for alle aldersgrupper i tillegg til skjema som kan benyttes i grupper.  | A |  |
| 1.2 | Programvaren må kunne benyttes på PC og smarttelefon, samt nettbrett. Det er et absolutt krav om at programmet skal kunne benyttes via nettleser og skjermbildet må være tilpasset den enheten man benytter (responsiv design). | A |  |
| 1.3 | Programvaren må i tillegg til skalaene kunne vise en generert forventningskurve. Denne må presenteres på en måte som er brukervennlig for alle parter. | A |  |
| 1.4 | Programvaren må ha en funksjon som viser kombinerte forventningskurver (for eksempel som brukt i par- eller familiesamtaler). | A |  |
| 1.5 | Programvaren må kunne gjøre tilgjengelig aggregerte data på behandler-, avdelings- og organisasjonsnivå.  | A |  |
| 1.6 | Programvaren skal tilby en løsning for administrativ pålogging og styring og det må kunne legges til rette for ulike brukertilganger. | A |  |
| 1.7 | Programvaren må ha mulighet å legge inn tofaktorautentisering for systemadministratorer og andre roller i systemet. | A |  |
| 1.8 | Skalaene som presenteres i systemet, må være oversatt til norsk. | A |  |
| 1.9 | Demoversjon ellers test-lisens skal leveres sammen med tilbudet, inkludert veiledning, brukernavn og passord der det er nødvendig | A |  |
| 2 | **Support** |  |  |
| 2.1 | Teknisk- og brukersupport skal tilbys av leverandør og må kunne foregå på norsk, svensk eller engelsk. Svartid er minst innen fem arbeidsdager. | A |  |
| 3 | **Personvern** |  |  |
| 3.1 | Programvaren må tilfredsstille kravene i GDPR og kunne dokumentere at de lovpålagte kravene til tjenesten ivaretas og på hvilken måte. Tjenestene er regulert av lov om helse og omsorgstjenester i kommunen, lov om helsepersonell og lov om barneverntjenester. | A |  |
| 3.2 | **Innebygget personvern**Systemet skal utvikles/skal være utviklet med fokus på innebygget personvern og personvern som standardinnstilling. Leverandør må sørge for at dette er ivaretatt fra starten og gjennom hele utviklingsløpet for systemet. Datatilsynets veileder for programvareutvikling med innebygget personvern i utviklingsprosjekter beskriver prosessen med tilhørende sjekklister. Se også Datatilsynets syv prinspiller for innebygget personvern.  Systemet skal utvikles/tilpasses med fokus på personvern som standardinnstilling. Funksjonaliteten skal tilrettelegges for oppfyllelse av prinsippene for behandling av personopplysninger. | A |  |
| 3.3 | Leverandøren og løsningen som tilbys må følge og oppfylle den til enhver tid gjeldende versjonen av Datatilsynets veileder for programvareutvikling med innebygd personvern. | A |  |
| 3.4 | I tilbudet må det beskrives hvordan løsningen dekker innebygd personvern og de syv stegene i "privacy by design" og hvordan leverandøren garanterer (også i fremtiden) å oppfylle den til enhver tid gjeldende veiledningen fra Datatilsynet. Leverandøren bes i tillegg beskrive hvilke forutsetninger de eventuelt må legge til grunn for at behovet kan dekkes**.** | A |  |
| 3.5 | Dokumentasjonen skal også på forespørsel være tilgjengelig for det enkelte behandlingssansvarlige helseforetak, samt for Datatilsynet og Personvernnemnda. | A |  |
| 4. | **Styringssystem** |  |  |
| 4.1 | Leverandør av løsningen med eventuelle underleverandører skal ha et dokumentert og operasjonalisert styringssystem for informasjonssikkerhet (ISMS) tilsvarende god praksis og internasjonalt anerkjente standarder for informasjonssikkerhet, f.eks. ISO/IEC 27001:2017, som dekker teknologi, informasjon, organisasjon, personal og fysiske lokasjoner som kan påvirke leveransene. Jf. GDPR art. 28 nr. 3. Styringssystemet skal fremlegges for behandlingsansvarlig på forespørsel og skal som minimum svare for virkeområde, delegasjon og definisjoner, formål, sikkerhetsmål, roller og ansvar, kontroll og revisjon.Leverandøren beskriver hvordan kravet oppfyllesLeverandør skal beskrive informasjonssystemet og sikringstiltakeneLøsningen skal sørge for at personopplysninger sikres med hensyn til integritet, konfidensialitet, tilgjengelighet og robusthet.  Integritet (I): Personopplysninger skal sikres mot utilsiktet og ulovlig ødeleggelse, tap og endringer. Konfidensialitet (K): Personopplysninger skal sikres mot uautorisert utlevering og tilgang. Tilgjengelighet (T): Personopplysninger skal være tilgjengelig for autoriserte med tjenstlig behov. Robusthet (R): Programvaren som behandler personopplysninger, skal være robuste mot for eksempel sårbarheter, angrep, og uhell.Leverandøren skal ha et styringssystem for informasjonssikkerhet som er i henhold til alminnelig anerkjente standarder på områdetDersom leverandøren har et sertifisert styringssystem for informasjonssikkerhet, er fremleggelse av sertifikatet tilstrekkelig som beskrivelse. | A |  |
| 4.2 | **Tilgjengeliggjør av dokumentasjon**Dokumentasjonen skal også på forespørsel være tilgjengelig for det enkelte behandlingssansvarlige helseforetak, samt for Datatilsynet og Personvernnemnda.  | A |  |
| 4.3 | **Loggføring**Løsningen skal som et minimum logge systemhendelser og sikkerhetshendelser, inkludert feilsituasjoner, endringer og uautoriserte forsøk på tilgang. Jf. Pasientjournalloven §§ 7 og 22. Løsningen skal som et minimum logge systemhendelser, inkludert feilsituasjoner, endringer og uautoriserte forsøk på tilgang. Jf. pasientjournaloven §§ 7 og 22. | A |  |
| 4.4 | **Risikovurdering** Leverandør skal ha gjennomført en risikovurdering av sin løsning og fremlegge/presentere denne for behandlingsansvarlig. Leverandøren skal levere en løsningsskisse og beskrive dataflyt i sitt system som en del av risikovurderingen. Leverandør skal minst årlig gjennomføre risiko- og sårbarhetsanalyse knyttet til alt som omfatter leveransen av tjenesten. Dette gjelder også for bruk av eventuelle underleverandører. Risikovurderingen skal som et minimum identifisere kristika aktiva, trusler og sårbarhet og resultere i en formelt dokumentert risikoanalyse som kan tilgjengeliggjøres for behandlingsansvarlig.Leverandøren skal dokumentere informasjonssystemet og sikkerhetstiltakene.Leverandøren skal ha gjennomført en risikovurdering av sin løsning og fremlegge/presentere denne for behandlingsansvarlig. | A |  |
| 4.5 | **Databehandleravtale** Som databehandler for kommunen skal leverandøren behandle opplysninger slik det fremgår av databehandleravtalen. Leverandøren kan ikke behandle personopplysningene på annen måte, jf. GDPR art. 28. Dette innebærer bl.a. at databehandler ikke kan behandle eller benytte personopplysninger til egne formål.Universell utforming Løsningen må oppfylle krav til enhver tid gjeldende versjon av Forskrift om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger (<https://lovdata.no/dokument/SF/forskrift/2013-06-21-732>)Det forutsettes av Bergen kommune eier data som registreres i systemet, og databehandleravtalen til Bergen kommune skal benyttes og etterfølges.Beskriv de geografiske lokasjonene (land) hvor personopplysninger blir behandlet. Avhengig av kravene til sikring av personopplysningene som skal behandles vektes det positivt at personopplysningene behandles i prioritert rekkefølge Norge (1), EU/EØS (2) og andre land (3). Hvis andre land enn Norge, skriv hvilket land.Vedlegg 1: Databehandler avtalen til Bergen kommuneDet stilles krav til universell utforming, jfr. https://lovdata.no/dokument/SF/forskrift/2013-06-21-732. | A |  |
| 5 | **Tilgang- og rollestyring**Løsningen skal tilby fleksible muligheter for å knytte roller til en eller flere ansatte. Tilganger tildeles en rolle begrenset til informasjon, dokumentert gjennom rollens tjenstlige behov, for å utføre en oppgave. Løsningen skal ha fleksibilitet og konfigurasjonsmuligheter knyttet til hvordan ansatte tildeles roller i systemet ut fra hvilke arbeidsoppgaver og/eller organisasjonstilhørighet den ansatte har. | A |  |
| 6 | Leverandøren skal levere en løsningsskisse og beskrive dataflyt i sitt system som en del av risikovurderingen. | A |  |
| 7 | Systemet skal minimum kunne brukes på følgende nettlesere: Safari, Chrome, Microsoft Edge, Firefox. | A |  |
| 8 | Leverandør skal kunne sende en oversikt på hvem som har tilgang til løsningen og hvilken tilgang de har. | A |  |

## Avtalens punkt 1.1 Avtalens omfang

[Eventuell tekst]

Dersom det etter Leverandørens mening er åpenbare feil eller uklarheter i Kundens kravspesifikasjon skal Leverandøren påpeke dette her.

## Avtalens punkt 2.1. Tjenesten

[Eventuell tekst]

Leverandøren skal, basert på bilag 1 (Kundens kravspesifikasjon),beskrive tjenesten her.

Leverandøren skal også beskrive de krav som eventuelt stilles til Kundens tekniske plattform for at Kunden skal kunne utnytte tjenesten. Leverandøren er nærmest til å vite hva slags teknisk plattform Kunden må ha for at Leverandørens tjeneste skal fungere i henhold til de kravene Kunden har gitt. Leverandøren skal derfor gi informasjon til Kunden dersom Kundes tekniske plattform/driftsmiljø må oppgraderes for at Leverandørens tjeneste skal kunne fungere.

 Avtalens punkt 6.2 Personopplysninger

[Eventuell tekst]

## Avtalens punkt 7.1 Partenes rettigheter

Dersom Kunden i bilag 1 har åpnet for at de opphavs-, disposisjons- eller eiendomsrettighetene partene hadde før avtalen skal kunne endres, skal Leverandøren beskrive hvordan disse rettighetene endres her.

## Avtalens punkt 8 Rekonstruksjon av data

#

Dersom Kunden i bilag 1 har spesifisert at Leverandøren tar ansvar for kostnader utover det som følger av avtalens punkt 8, skal Leverandøren angi sine forpliktelser knyttet til dette her.

# Bilag 3: Plan for etableringsfasen

## Avtalens punkt 3.2 Leveransefrist og leveransemelding

Tjenesten skal være tilgjengelig så snart som mulig og senest to uker etter kontraktinngåelse.

## Avtalens punkt 3.3 Godkjenningsprøve og leveringsdag

Se bilag 1 absolutte krav punkt 9.

# Bilag 4: Tjenestenivå med standardiserte kompensasjoner

## Avtalens punkt 2.1

Teknisk- og brukersupport skal tilbys av leverandør og må kunne foregå på norsk, svensk, dansk eller engelsk. Åpningstid for teknisk- og brukersupport skal være minimum mandag til fredag 10:00-14:00, unntatt helligdager og offentlige fridager.

Oppdatering og vedlikehold av systemet skal foregå i tidsrommet 21:00 – 06:00, eller i helgene.

Krav til oppetid settes til 50% i arbeidsdagen.

# Bilag 5: Administrative bestemmelser

Det er ikke behov for oppfølgningsmøte.

## Avtalens punkt 1.5 Partenes representanter

Maria Elisabeth L Norheim MariaElisabethL.Norheim@bergen.kommune.no

Norheim, Bjarte A. Bjarte.Norheim@bergen.kommune.no

## Avtalens punkt 5.1 Varighet

Anbudet gjelder 120 lisenser samtidige brukere

Det er behov for lisenser for FIT programvare, i størrelsesorden for 120 samtidige brukere i 12 måneder. Med lisensiert programvare menes her tilgang til nettbasert kartleggingsverktøy. I tillegg gjelder en opsjon på inntil 100 enkeltlisenser, hvor antall enkeltlisenser bestilles etter behov. Videre er det en opsjon på 1-6 måneder, som kan inngås underveis.

Etat for barn og familie sitt fremtidig behov er totalt 700 lisenser, men det vil bli lyst ut som en senere konkurranse.

Se bilag 6 prisskjema for krav til varighet for dette anbudet.

## Avtalens punkt 5.2 Avbestilling

## Avtalens punkt 6.2 Personopplysninger

Det er ikke godkjent at personopplysninger kan behandles av Leverandørens underleverandør(er) utenfor EØS-området.

Det er ikke godkjent at leverandør kan behandle personopplysninger utenfor EØS-området.

## Avtalens punkt 11.2. Lønns- og arbeidsvilkår

Dersom det foreligger allmenngjort tariffavtale eller landsomfattende tariffavtale for den aktuelle bransje kontrakten gjelder skal dokumentasjon av Leverandørens oppfyllelse av forpliktelser som nevnt i avtalens punkt 11.2 (Lønns- og arbeidsvilkår) fremkomme her.

Dokumentasjonen kan bestå av en egenerklæring eller en tredjepartserklæring om at det er samsvar mellom aktuell tariffavtale og faktiske lønns- og arbeidsvilkår for oppfyllelse av Leverandørens og eventuelle underleverandørers forpliktelser.

# Bilag 6: Samlet pris og prisbestemmelser

Alle priser og nærmere betingelser for det vederlaget Kunden skal betale for Leverandørens ytelser skal fylles på **pris- og produktskjema på Mercell**. Prisen skal inkludere samtlige kostnader. Eksempler på dette kan være inkluderer lisens, programvare, support, vedlikehold, oppdateringer, etc.

Det skal oppgis pris pr lisens pr år ekskl. mva.

## Avtalens punkt 3.4. Dokumentasjon og opplæring

Ikke bedt om opplæring.

## Avtalens punkt 4.2 Faktureringstidspunkt og betalingsbetingelser

Leverandøren skal levere elektronisk faktura til Bergen kommune på Elektronisk handels-format (EHF). Nærmere beskrivelse finnes her:
<https://www.bergen.kommune.no/tjenestetilbud/naring/handel-og-service/offentlig-innkjop/elektronisk-faktura-til-bergen-kommune>

[Information om elektronisk faktura](https://www.anskaffelser.no/leverandorer/slik-moter-du-det-offentliges-krav-til-digitalisering/faktura-og-kreditnota), [komme i gang med e-faktura](https://www.anskaffelser.no/leverandorer/slik-moter-du-det-offentliges-krav-til-digitalisering/faktura-og-kreditnota), [Takler økonomisystemet ditt standarden?](https://www.anskaffelser.no/leverandorer/slik-moter-du-det-offentliges-krav-til-digitalisering/faktura-og-kreditnota)
[Oversikt over fakturasystemer og enkle webportaler som kan levere EHF](https://www.anskaffelser.no/verktoy/fakturasystemer-som-kan-levere-elektronisk-handelsformat-ehf)
[Forskrift om IT-standarder i offentlig forvaltning](http://lovdata.no/dokument/SF/forskrift/2013-04-05-959).

**Fakturaformat og innhold**

* Organisasjonsnummer til Bergen kommune må være angitt. Bergen kommune er registrert med følgende organisasjonsnummer i ELMA: 964 338 531.
* Elektronisk faktura skal merkes med bestillers navn og fakturabehandlers ressursnummer. Ressursnummeret består av 5 eller 6 siffer, og skal legges i feltet «Party.Contact.identifier». Det er kun ressursnummeret med numeriske tall som skal være i dette feltet. Bestillers navn skal legges i feltet «party.contact.name»
* Kontraktsnummer skal inkluderes i faktura i tråd med <https://test-vefa.difi.no/ehf/guide/invoice-and-creditnote/2.0/no/#_kontraktsnummer>.
* For innkjøpsordrer som mottas elektronisk fra Bergen kommunes E-handelsløsning skal Bergen kommunes ordrenummer angis i feltet «»Order Reference.identifier». For innkjøpsordrer som ikke er merket med oppdragsgivers ordrenummer skal dette feltet vært tomt.
* Kreditnota skal ha oppdragsgivers ressursnummer eller ordrenummer i feltet Party.Contact.Identifier og feltet OrderReference skal være tomt.
* Det skal være minst 10 års intervall hvis leverandør gjenbruker fakturanummer.
* I de tilfeller følgende organisasjonsenheter er inkludert i leveranseavtalen skal korrekt organisasjonsnummer benyttes:

**Feil i fakturaformat**

Faktura som har feil eller mangler i forhold til beskrivelsen ovenfor vil ikke bli betalt, men tilbakemeldt som feil. Leverandør må i slike tilfeller sende ny og korrekt faktura med ny fakturadato og tilsvarende ny forfallsdato. Kreditnota skal i slike tilfeller ikke utstedes/sendes til oppdragsgiver.

## Avtalens punkt 4.5 Prisendringer

## Avtalens punkt 5.2 Avbestilling

## Avtalens punkt 5.3 Partenes plikter i avslutningsperioden

## Det skal legges til rette for å eksportere data til Excel.

## Avtalens punkt 8 Rekonstruksjon av data

# Bilag 7: Endringer i den generelle avtaleteksten

## Avtalens punkt 1.3 Tolkning – rangordning

# Bilag 8: Endringer av tjenesten etter avtaleinngåelsen

## Avtalens punkt 1.4 Endringer av tjenesten etter avtaleinngåelsen

[Eventuell tekst]

# Bilag 9: Vilkår for Kundens tilgang og bruk av tredjepartsleveranser

## Avtalens punkt 2.2 Leverandørens ansvar for tredjepartsleveranser

[Eventuell tekst]