# GDPR system

## Prosjektnummer 1339

## SSA-L Bilag 1 – Kundens kravspesifikasjon

## Innhold

# 1 INNLEDNING

Kravene i kravspesifikasjonen er formulert som behov. I kolonnen for beskrivelse er det angitt hva som forventes av leverandørens besvarelse.

Kravene er kategorisert som følger:

| Kravkode | Beskrivelse |
|---|---|
| **A** | Krav som må være oppfylt ved tilbudsfrist (i dag). Leverandør må bekrefte og dokumentere i Bilag 2 at kravet er oppfylt i dag. |
| **V** | Vurderingskrav, krav som inngår i tildelingskriteriene. Dersom ikke kravet oppfylles i dag skal det brukes ulike svarkoder som beskrevet i Bilag 2. Leverandør må dokumentere/beskrive hvordan tjenesten og løsningen ivaretar kravet. |
| **AV** | Krav som er kategorisert som AV er både krav som må være oppfylt ved tilbudsfrist og vurderingskrav som inngår i tildelingskriteriene. Leverandør må dokumentere/beskrive hvordan tjenesten og løsningen ivaretar kravet. |

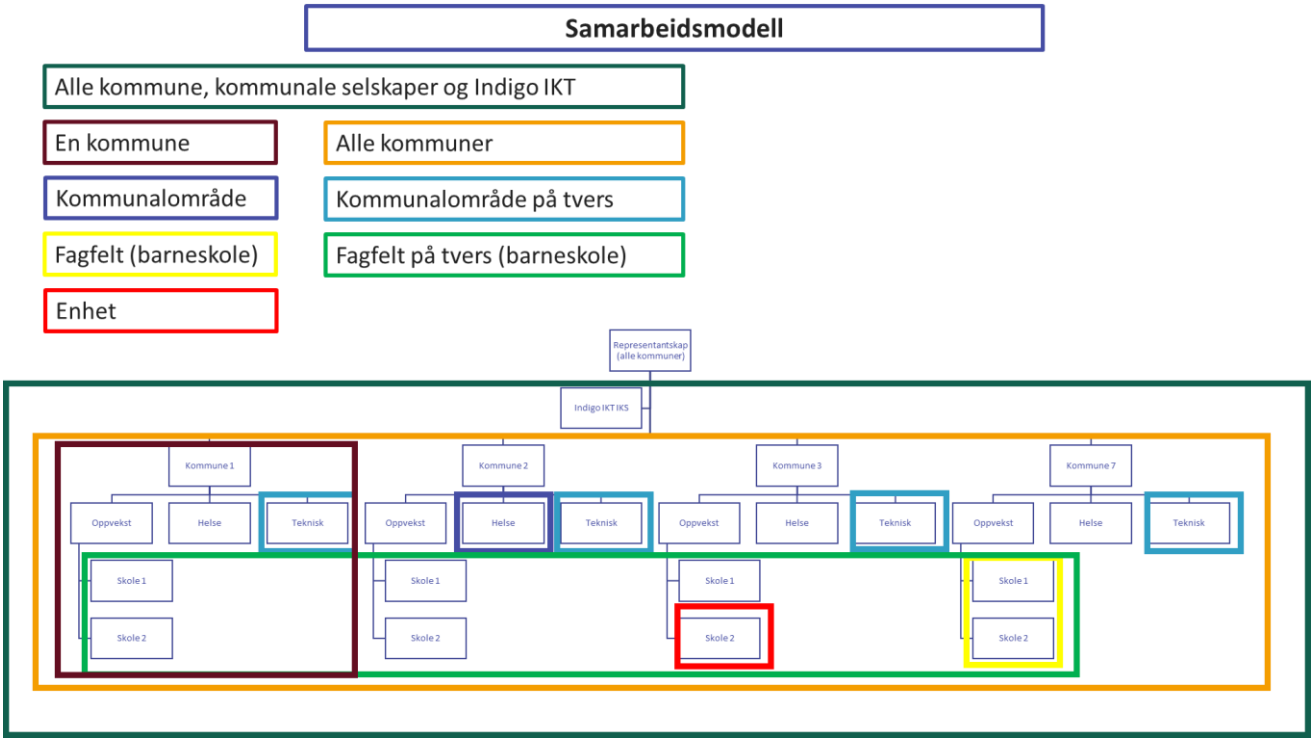
# 2 FORMÅL

Oppdragsgiver har behov for en digital løsning for samarbeid om ivaretakelse av lovpålagte plikter etter GDPR i Indigo-samarbeidet. Løsningen skal sørge for at de deltakende kommunene hver for seg og sammen effektiviserer sitt etterlevelsesarbeid og jobber etter en felles metodikk i et felles system. Målsettingen med å anskaffe et felles GDPR-system er å bidra til at interessenter i kommunene, samarbeidet og Indigo IKT får gode forutsetninger for å jobbe sammen med å utvikle, forvalte og dokumentere informasjonsprosesser rasjonelt i tråd med personvernforordningen og samarbeidets digitaliseringsstrategi.

Per dags dato foreligger det ikke noe system for felles metodikk, og de deltakende kommunene har arbeidet etter egne premisser og rammer.

På bakgrunn av dette er behovet og det funksjonelle omfanget som GDPR-systemet skal dekke gjennomgått og det er vurdert om andre eksisterende verktøy/løsninger sammen med et GDPR-system kan benyttes for samlet sett å dekke behovet. Oppdragsgiver innfører blant annet nå en forvaltningsløsning basert på Sharepoint der oversikt og forvaltning av IT-systemer og informasjon er dekket. Integrasjon mellom GDPR-system og forvaltningsløsning er vesentlig for at samhandlingsmodellen skal fungere effektivt.

**Samarbeidsmodellen i Indigo-samarbeidet**




Samarbeidsmodellen i Indigo-samarbeidet er bygget opp med et toppnivå som skal ha totaloversikt over og administrere behandlinger og tilhørende oppgaver for alle virksomheter (kommuner og IKS'er) i samarbeidet.

Under dette nivået er det sektorfora som skal ha oversikt over og administrere sine respektive behandlinger og oppgaver på tvers av samme virksomhetsområde i de ulike virksomhetene (f.eks. sektorforum oppvekst, sektorforum helse etc.).

Under dette ligger de enkelte virksomhetene (kommuner og IKS'er) som skal ha totaloversikt over og administrere sine behandlinger og tilhørende oppgaver lokalt.

Under dette ligger områdeledere som skal ha oversikt og administrere behandlinger og aktiviteter for sitt virksomhetsområde lokalt (f.eks. kommunalsjef helse, kommunalsjef oppvekst etc.)

Nederst ligger den enkelte enhet (skole, barnehage, helsestasjon etc.) som har behov for å ha oversikt over og administrere sine behandlinger og tilhørende oppgaver lokalt.

Det kan være behov for flere nivåer (for eksempel avdelingsnivå som ungdomsskoler, barneskoler, barnevern etc.)

Enkeltpersoner kan ha flere roller innenfor samarbeidsmodellen, eksempelvis deltaker i et sektorforum samt lokalt ansvarlig på ulike nivåer i en enkelt virksomhet.

**Ønsket effekt av løsningen - samarbeidsmodellen**
IT-løsningen skal legge til rette for bedre samhandling slik at organisasjonen kan jobbe mer effektivt og målrettet med oppgaver relatert til informasjonssikkerhet og personvern, både lokalt i den enkelte virksomhet, men også på tvers av virksomhetene, samt at ledelsen kan få bedre styring og kontroll med informasjonsbehandlingen i egen virksomhetene.

**Behov som skal dekkes av løsningen**
Systemet skal benyttes av sikkerhetsressurser, felles personvernombud, ledere og nøkkelpersoner på tvers av Indigo -samarbeidet, og de skal få rask og god oversikt, både lokalt og for flere virksomheter i fellesskap, fordele oppgaver, gjennomføre aktiviteter og dokumentere aktiviteter.
Virksomhetsledelsen har behov for en samlet oversikt og kontroll over sine behandlinger og mulige risikoer tilknyttet disse slik at de kan risikostyre sikkerhetsarbeidet og dokumentere at de følger loven, målstyre tjenestene og bruke ressursene hensiktsmessig.

- Sikkerhetskoordinatorer har behov for totaloversikt i egen kommune, fordele oppgaver og sette frister, samt å samarbeide om, felles aktiviteter i Indigosamarbeidet og dokumentere disse.
- Behandlingsansvarlige ledere har behov for oversikt over hva som er gjort og hva som må gjøres innenfor sitt område, for å ivareta sine behandlinger.
- Virksomhetenes ansatte har behov for Tilgang etter behov ved tildelte oppgaver for gjennomføring, ROS/dpia etc.
- Alle aktører innenfor utvikling, bruk og forvaltning av IT-løsninger har behov for oversikt over sammenhengen mellom informasjonsbehandlingene, sikkerhetsaktivitetene og systemene som benyttes under behandlingen for å sikre hensiktsmessig og sikker forvaltning og utvikling av IT-porteføljen.
- Personvernombudene har behov for totaloversikt både i den enkelte virksomhet og for alle deltakerne i Indigosamarbeidet, både overordnet, sektorvis og lokalt i hver virksomhet.
- Kommunenes innbyggere har behov for å få realisert sine rettigheter knyttet til behandlingene kontinuerlig.

## 3 LEVERANDØRS OPPFYLLELSE AV FORMÅL

Leverandørs oppfyllelse av formålet med anskaffelsen, skal inntas i Bilag 2. Leverandøren skal gi en overordnet beskrivelse av tilbudt løsning, samt beskrive sin forståelse av anskaffelsens formål, herunder hvordan Leverandøren skal bidra for å oppnå dette.

## 4 LEVERANDØRS FORUTSETNINGER FOR LEVERANSEN

Leverandørs forutsetninger for leveransen skal inntas i Bilag 2. Leverandøren skal beskrive de forutsetninger Leverandør finner nødvendig å ta for å vedstå seg sine forpliktelser under avtalen. Alle forutsetninger av generell, merkantil, funksjonell eller teknisk karakter som er relevante for at Kunden skal kunne benytte den tilbudte løsningen skal beskrives.

## 5 MYNDIGHETSKRAV OG EKSTERNE RETTSLIGE KRAV

Løsningen skal innfri aktuelle og relevante myndighetskrav. Dette omfatter krav pålagt gjennom lov og forskrifter, standarder og kodeverk, samt sikkerhetsmessige krav. Kravene omfatter både løsning og Leverandør, og skal besvares i Bilag 2.

Leverandøren skal holde seg orientert om regelverksendringer og ha en strategi for å holde løsningen oppdatert til enhver tid.

Følgende styrende dokumenter, lover og forskrifter, veiledere og standarder skal legges til grunn (listen er ikke uttømmende):

- LOV-1967-02-10 – Lov om behandlingsmåten i forvaltningssaker (Forvaltningsloven)
- LOV-2006-05-19-16 – Lov om rett til innsyn i dokument i offentleg verksemd (Offentleglova)
- LOV-2018-06-15-38 - Lov om behandling av personopplysninger (Personopplysningsloven)
- LOV-1992-12-04-126 – Lov om arkiv (Arkivloven)
- Regjeringens Digitaliseringsstrategi for offentlig sektor (2019 – 2025)
- Digitaliseringsdirektoratets veileder «Internkontroll i praksis – informasjonssikkerhet»
- NSMs grunnprinsipper for informasjonssikkerhet

## 6 SPESIFIKASJON AV PROGRAMVARE

Leverandøren skal i Bilag 2 gi en komplett oversikt over tilbudt programvare. Oversikten skal være en spesifisering av alle relevante komponenter og moduler, inkludert versjonsnummer. I tillegg skal det gis en roadmap over kommende versjoner med datoangivelse de neste 2-4 år. All annen programvare som er en forutsetning for at tilbudt programvare skal fungere optimalt, skal spesifiseres på tilsvarende måte.

## 7 FUNKSJONELLE KRAV

Kundens funksjonelle behov og krav til løsning spesifiseres i kapitlene under. Leverandøren skal besvare kravene i Bilag 2. Der leverandøren i sin besvarelse refererer til sin egen dokumentasjon skal nøyaktig plassering (kapittel, avsnitt, punkt etc. oppgis).

### 7.1 Generelt om løsningen

| Nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| F1 | Utvalg og presentasjon av informasjon og funksjoner (verktøy), må kunne tilpasses den enkeltes behov og arbeidssituasjon. Brukergrensesnittet må være oversiktlig og arbeid med flere programmer samtidig må fremstå sømløst for bruker. | V | Beskriv hvordan dette er ivaretatt i løsningen og hvordan den enkelte ansatte kan konfigurere brukergrensesnittet slik at kun deres aktiviteter og meldinger vises på skjermen |
| F2 | Leverandøren og løsningen skal oppfylle de til enhver tid gjeldende obligatoriske krav i «Referansekatalog for IT-standarder i offentlig sektor». | A | Beskriv hvordan dette er ivaretatt i løsningen. |
| F3 | Løsningen skal være tilpasset digitale flater, være responsiv og støtte ulike nettlesere. | AV | Beskriv hvordan dette er ivaretatt i løsningen og hvilke nettlesere som støttes. Angi også støtte til W3C. |
| F4 | Det er ønskelig med stor grad av filtrering i søkefunksjonen. | V | Beskriv hvordan dette er ivaretatt i løsningen. |
| F5 | Hvis brukere gjør feil ved bruk av systemet skal han/hun bli presentert med informative meldinger som gir nok forklaring til at brukeren selv kan korrigere eventuelle feil og mangler og komme videre i prosessen. | V | Bekreft og beskriv standard funksjonalitet for dette i tilbudt løsning |

| Nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| F6 | Løsningen skal være tilgjengelig på norsk. Dette gjelder både brukergrensesnitt og standard tekster. | A | Vennligst bekreft overensstemmelse med kravet. |
| F7 | Kunden ønsker at fagsystemer tilfredsstiller relevante krav til universell utforming med gjeldende standarder for WAD og WCAG. Se https://www.uutilsynet.no/regelverk/offentlig-sektor/1584 | V | Beskriv hvordan leverandør arbeider med denne problemstillingen og hvordan dette er synbart i løsningen. |
| F8 | For brukere skal systemet fremstå som raskt og effektivt i den aktuelle brukersituasjon. | AV | Beskriv hvordan løsningen møter slike forventninger. |
| F9 | Brukerdialogen skal være entydig slik at risiko for å registrere feil data reduseres. | AV | Bekreft og beskriv hvordan kravet er oppfylt. |
| F10 | Brukeren har behov for å motta varslinger ved tildeling av oppgave, når frister nås og ved godkjenning. | AV | Beskriv hva som er omfattet i løsningen og hvordan kravet er ivaretatt. |

## 7.2 **Konsernmodell (samarbeidsmodell)**

| Nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| F11 | Kunden har behov for å samarbeide i henhold til samarbeidsmodellen (konsernmodell). | AV | Beskriv hvordan løsningen ivaretar dette behovet og understøtter et sømløst samarbeid. |
| F12 | Kunden har behov for at roller i samarbeidet kan være interkommunale. | AV | Beskriv hvordan løsningen understøtter virksomhetsovergripende rollers (f.eks. interkommunale rådgivere og personvernombud) behov for å enkelt kunne velge ulike virksomheter eller sektor på tvers av virksomheter med en og samme brukerkonto (samme pålogging). |

## 7.3 **Brukeradministrasjon**

| Nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| F13 | Systemet skal ha funksjon for enkelt å håndtere og forvalte brukere i systemet. Administrasjon skal være rollebasert – dvs. at rettigheter skal kunne settes for ulike typer moduler, oppgaver og nivåer og gjenspeile samarbeidsmodellen. | AV | Bekreft og beskriv hvordan kravet er oppfylt. |
| F14 | Brukerprofiler skal kunne deaktiveres. Deaktiverte brukerprofiler skal lagres for å | A | Vennligst bekreft. |

| Nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| | sikre konsistens i data og logger, men brukeren skal ikke lenger ha aktiv tilgang til systemet. | | |

## 7.4 **Behandlingsprotokoll**

| Nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| F15 | Kunden har behov for å kunne registrere behandlingsaktiviteter i egendefinerte maler. | AV | Beskriv:<br>• hvordan prosessen for å legge inn en behandlingsaktivitet er lagt opp i løsningen<br>• hvilke felt kan hentes fra forhåndsdefinerte registre<br>• hvordan maler kan tilpasses. |
| F16 | Kunden har behov for å hente data fra annen funksjonalitet i løsningen til behandlingsprotokollen. | V | Beskriv hvilke felt som kan hentes fra annen funksjonalitet i løsningen, for eksempel DPIA. |
| F17 | Kunden har behov for å samhandle om å registrere en aktivitet. | AV | Beskriv hvordan en aktivitet kan registreres på tvers av kommuner og tilpasses lokale ulikheter, for eksempel ulike systemer, ansvarlige osv. |
| F18 | Kunden har behov for å tilgjengeliggjøre behandlingsprotokoll til Datatilsynet. | AV | Beskriv og vis ved eksempel hvordan en behandlingsprotokoll art. 30 med minimumskravene kan tilgjengeliggjøres for Datatilsynet i et lesbart format. |
| F19 | Kunden har behov for å kunne definere egen visning av behandlingsprotokoller. | AV | Beskriv mulighet for å tilpasse visning av behandlingsprotokoller ut ifra samarbeidsmodellen og andre egendefinerte parametere for eksempel rolle, sektor, nivå, behandlingsaktiviteter, behandlingsansvarlig. |
| F20 | Kunden har behov for å publisere personvernerklæring på kommunens hjemmesider. | V | Beskriv hvordan tilpasset innhold fra behandlingsprotokoll automatisk kan presenteres i personvernerklæring på kommunens hjemmeside. |
| F21 | Kunden har behov for å tildele oppgaver i tilknytning til behandlingsprotokollen, sette frister og godkjenne oppgavene. | AV | Beskriv hvordan løsningen støtter dette. |
| F22 | Kunden har behov for statusvisning på fremdrift av ulike oppgaver og aktiviteter. | AV | Beskriv hvordan løsningen kan vise status på fremdrift |

## 7.5 **DPIA**

| Nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| F23 | Kunden har behov for å gjennomføre en forhåndsvurdering av behandlingsaktivitet(er) (initialvurdering DPIA). Datatilsynets liste over behandlingsaktiviteter som alltid krever at det gjennomføres en DPIA må være forhåndsdefinert. | AV | Beskriv hvordan<br>• dette gjøres i løsningen<br>• en vurdering kan knyttes til flere behandlingsaktiviteter<br>• dette knyttes til behandlingsprotokollen<br>• en vurdering kan registreres på tvers av kommuner. |
| F24 | Kunden har behov for å gjennomføre en DPIA iht. GDPR artikkel 35 og mulighet for egne definerte tilpasninger. | AV | Beskriv hvordan<br>• dette gjøres i løsningen<br>• en vurdering kan knyttes til flere behandlingsaktiviteter<br>• dette knyttes til behandlingsprotokollen<br>• en DPIA kan registreres på tvers av kommuner og tilpasses lokale ulikheter f.eks. lokal risikoaksept. |
| F25 | Kunden har behov for å tildele oppgaver (tiltak), godkjenne disse og validere DPIA, eventuelt godkjenne restrisiko. | AV | Beskriv hvordan dette gjøres i løsningen. |
| F26 | Kunden har behov for aggregerte visninger over status på gjennomføring av DPIA, identifiserte risikoer, tiltak og status på disse. | AV | Beskriv hvordan dette gjøres i løsningen. |

## 7.6 **Risiko og sårbarhetsvurdering**

| Nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| F27 | Kunden har behov for å gjennomføre en risikovurdering, herunder å definere og identifisere mulige hendelser. | AV | Beskriv hvordan<br>• dette gjøres i løsningen<br>• en vurdering ved behov kan knyttes til flere behandlingsaktiviteter<br>• dette knyttes til behandlingsprotokollen og evt DPIA<br>• løsningen kan benytte egendefinert maler med redefinerte hendelser. |
| F28 | Kunden har behov for å prioritere risikoene basert på deres alvorlighetsgrad og potensiale for skade. | V | Beskriv hvordan løsningen presenterer prioritering. |
| F29 | Basert på sannsynlighet og konsekvenser, har Kunden behov for å kunne beregne risikonivået for hver identifisert risiko. Resultat | V | Beskriv hvordan en ROS kan registreres på tvers av kommuner og tilpasses lokale ulikheter f.eks. lokal risikoaksept, risikomatrise. |

| Nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| | av vurderingen skal vises i en matrise av konsekvens og sannsynlighet. | | |
| F30 | Kunden har behov for å tildele oppgaver (tiltak), godkjenne disse og eventuelt godkjenne restrisiko. | AV | Beskriv hvordan dette gjøres i løsningen. |
| F31 | Kunden har behov for aggregerte visninger over status på gjennomføring av ROS, identifiserte risikoer, tiltak og status på disse. | V | Beskriv hvordan dette gjøres i løsningen. |

### 7.7 **Rapporter og dashbord**

| Nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| F32 | Løsningen skal inneholde standard rapporter. | AV | Beskriv hvilke standardrapporter som er definert i løsningen. |
| F33 | Kunden har behov for selv å kunne definere rapporter. | AV | Beskriv hvilke muligheter som finnes i løsningen for å utarbeide egne rapporter. |
| F34 | Kunden har behov for fleksibilitet i visning og format på rapporter. | V | Beskriv hvilke muligheter løsningen har for filtrering, sortering og formater i rapporter og vis ved eksempler. |
| F35 | Kunden har behov for et dashboard med egendefinert tilpasning per bruker. | V | Beskriv mulighet for egendefinert utvalg og visninger i dashboard. |
| F36 | Kunden har behov for statusvisning av aggregerte data med mulighet for drill down (flere nivåer). | V | Beskriv hvordan aggregerte data i sanntid vises i et dashbord og hvordan dette kan tilpasses til samarbeidsmodellen. |

## 8 PERSONVERN OG INFORMASJONSSIKKERHET

Kunden har etterspurt en løsning som ikke installeres i Kundens eget driftsmiljø, og data lagres utenfor Kundens eksisterende driftsmiljø/infrastruktur. Det er et viktig prinsipp for denne type leveranse at Kunden eier dataene.

Leverandøren skal forplikte seg på å bidra til gjennomføring av en ROS-analyse av løsningen i samarbeid med kunden ved behov.

Behandling av personopplysninger skal skje i henhold til Personopplysningsloven og EU's personvernforordning gjeldende fra mai 2018. Det skal inngås en databehandleravtale mellom Kunde og Leverandør basert på oppdragsgivers standard databehandleravtale (DFØ).

### 8.1 **Styring og kontroll med informasjonssikkerheten**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P1 | Leverandør må ha et etablert ledelsessystem for informasjonssikkerhet i henhold til en anerkjent standard, for eksempel ISO/IEC 27001:2023. | AV | Leverandøren bes beskrive sitt styringssystem for informasjonssikkerhet |
| P2 | Leverandøren skal ha tydelig definerte sikkerhetsmål og strategier. Videre skal leverandøren ha sikkerhetsdokumentasjon for bruk i egen virksomhet, herunder instrukser, sjekklister og beredskapsplaner for å understøtte arbeidet med sikkerhet i virksomheten og mot kunder. | AV | Leverandøren bes om en overordnet beskrivelse av sine sikkerhetsmål og strategier. |
| P3 | Leverandøren skal regelmessig gjennomføre en metodisk risikovurdering for å evaluere risiko, samt beslutte sikringskrav og -tiltak. Risikovurderingen skal som minimum utføres årlig, og resultatet av denne, samt tilhørende tiltak for risikohåndtering skal på forespørsel gjøres tilgjengelig for tilsynsmyndighet og kunden. | AV | Leverandøren bes beskrive hvorledes de gjennomfører risikovurderinger og implementerer risikoreduserende tiltak for løsningene de leverer |
| P4 | Det er ønskelig at leverandøren innehar gyldige sertifiseringer og/eller kan vise til tredjepartsattestasjoner som er relevante for utvikling, drift og forvaltning av løsningen, med hensyn til informasjonssikkerhet. Eksempler kan være ISO 9001, 27001-sertifisering, sertifisering av datasentre, ISAE 3402-rapporter, CSA STAR-sertifisering, osv. | V | Leverandøren bes beskrive relevante sertifiseringer og/eller tilgjengelige attestasjonsprodukter for seg selv og eventuelle underleverandører. |
| P5 | Dersom leverandøren innehar gyldige sertifiseringer, skal de fremlegge ekstern revisjonsrapport vedrørende oppfyllelse av krav til de aktuelle sertifikatene. Dokumentasjon av gjennomførte revisjoner skal ikke være eldre enn to år. | V | Leverandøren bes fremlegge relevant dokumentasjon for seg selv og eventuelle underleverandører. |
| P6 | Leverandøren skal jevnlig gjennomføre interne revisjoner, herunder testing av tekniske, organisatoriske og fysiske sikkerhetstiltak. | AV | Leverandøren bes beskrive hvordan de planlegger, gjennomfører og dokumenterer revisjoner og testing. |
| P7 | Leverandøren skal sørge for at eventuelle underleverandører følger sikkerhetsrelaterte retningslinjer og krav. | AV | Leverandøren bes beskrive hvordan de følger opp sikkerhetsarbeidet hos sine underleverandører. |

## 8.2 **Tilgangsstyring**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P8 | Løsningen skal legge til rette for autentisering og autorisasjon basert på tjenstlig behov. Flere personer skal ikke benytte samme autentiseringskriteria. | AV | Leverandøren bes beskrive hvordan løsningen tilrettelegger for tildeling av brukerautentiseringsmekanisme og autorisasjon på en betryggende måte |

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P9 | Løsningen skal skille mellom rettigheter til å lese, registrere, rette, slette vurderingene. All tildeling av autorisasjon skal registreres i et autorisasjonsregister. Registeret skal som minimum inneholde:<br>• informasjon om hvem som er tildelt autorisasjon<br>• til hvilken rolle autorisasjonen er tildelt (om rolle benyttes i virksomheten)<br>• formålet med autorisasjonen<br>• tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt<br>• tidsbegrensninger på autorisasjoner, f.eks. forskningsprosjekt, ansettelses- eller avtaleforhold<br>• informasjon om hvilken virksomhet den autoriserte er knyttet til<br>• roller og rettigheter som har blitt tildelt brukerne<br>• alle innlegginger, endringer og sletting av tilganger basert på autorisasjoner. | AV | Leverandøren bes beskrive hvordan løsningen legger til rette for et autorisasjonsregister. |
| P10 | Autorisasjonsregisteret skal være beskyttet mot uautoriserte endringer, og skal kunne benyttes til å hente ut informasjon om autorisasjoner minimum 5 år etter en autorisasjon er trukket tilbake. | AV | Leverandøren bes beskrive hvordan de sikrer autorisasjonsregisteret |
| P11 | Leverandøren skal hindre uautorisert bruk og ivareta integritet og konfidensialitet ifb. fjernaksess. | AV | Leverandøren bes beskrive sine rutiner for fjernaksess. |
| P12 | Leverandøren skal implementere fysiske sikringstiltak hvor Kundens data er tilgjengelig. | AV | Leverandøren bes på en overordnet måte beskrive sine fysiske sikringstiltak. |
| P13 | Leverandøren skal separere data som tilhører forskjellige kunder. Leverandørens egne data skal separeres fra kundenes data. | AV | Leverandøren bes beskrive sin sikkerhetsarkitektur med hensyn til separasjon av data som tilhører forskjellige kunder. |

## 8.3 **Hendelsesregistrering**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P14 | For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres logg over følgende:<br>• Autorisert bruk av informasjonssystemene skal registreres.<br>• Sikkerhetsbarrierene skal registrere sikkerhetsrelevante hendelser, bl.a. forsøk på uautorisert bruk av informasjonssystemet.<br>• Nettverksoperativsystemer skal registrere alle forsøk på uautorisert bruk. | AV | Leverandøren bes beskrive hvordan de vil etablere hendelsesregistrering i løsningen. |

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| | • Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk. | | |
| P15 | Logger (data og informasjon) i hendelsesregistrene skal kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd. Videre skal loggene fra hendelsesregistre kunne eksporteres eller gjøres tilgjengelig for eksterne analyseverktøy. | V | Leverandøren bes beskrive hvordan data fra hendelsesregistre kan tilgjengeliggjøres for analyse. |
| P16 | Loggene i hendelsesregistrene skal sikres mot uautorisert endring og sletting. | AV | Leverandøren bes beskrive hvordan de sikrer hendelsesregistrene. |

## 8.4 **Kryptering**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P17 | Leverandøren skal ha mekanismer for sikring av data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet. | AV | Leverandøren bes beskrive hvordan de sikrer data under transport, prosessering og lagring. |
| P18 | Kryptering forutsetter en forsvarlig behandling av partenes krypteringsnøkkel(er). | AV | Leverandøren bes beskrive hvordan de håndterer nøkler (f.eks. passord, sertifikater). |

## 8.5 **Konfigurasjonskontroll**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P19 | Det er en forutsetning at leverandøren har oversikt over og kontroll på alt eget utstyr og programvare som benyttes i behandlingen av personopplysninger slik at konfidensialitet, integritet og tilgjengelighet blir ivaretatt. | AV | Leverandøren bes beskrive hvordan de ivaretar oversikt over og kontroll på utstyr og programvare som benyttes i løsningen. |
| P20 | Konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, skal ikke settes i drift før risikoreduserende tiltak er gjennomført.<br>Eksempler kan være:<br>• Prosess for godkjenning og gjennomføring av endringer<br>• Risikovurdering som viser at nivå for akseptabel risiko er oppnådd<br>• Test som sikrer at forventede funksjoner er ivaretatt<br>• Implementering som sikrer mot uforutsette hendelser<br>• Ny konfigurasjon er dokumentert<br>• Konfigurasjonsendringer er godkjent av kunden. | AV | Leverandøren bes beskrive hvordan de planlegger og gjennomfører konfigurasjonsendringer i utstyr og/eller programvare. |

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P21 | Leverandøren skal dokumentere alle konfigurasjoner i et konfigurasjonskart over informasjonssystemene og teknisk beskrivelse av konfigurasjonen. Dokumentasjonen skal vise leverandørens og eventuelle underleverandørers datasentre og lokasjoner. | AV | Leverandøren bes beskrive hvorledes de dokumenterer konfigurasjoner av utstyr og programvare |

## 8.6 **Lagring og rekonstruksjon av data**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P22 | Det skal jevnlig tas sikkerhetskopi av data og informasjon som er nødvendig for gjenoppretting av normal bruk. | AV | Leverandøren bes beskrive sine rutiner for sikkerhetskopiering. |
| P23 | Sikkerhetskopier skal oppbevares avlåst og brannsikret, og adskilt fra driftsutstyret. | AV | Leverandøren bes beskrive hvordan sikkerhetskopier sikres og oppbevares. |
| P24 | Det skal jevnlig foretas test av at sikkerhetskopiene er korrekte og kan tilbakeføres. | AV | Leverandøren bes beskrive hvordan de tester og dokumenterer gjenoppretting sikkerhetskopier. |

## 8.7 **Tiltak mot digitale angrep**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P25 | Løsningen skal sikres mot sikkerhetstruende hendelser. | AV | Leverandøren bes beskrive på en overordnet måte hvorledes løsningen sikres mot digitale angrep. |

## 8.8 **Krise- og beredskapsplaner**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P26 | Det skal vedlikeholdes dokumentasjon og oversikt over informasjonssystemer som er kritiske for drift av løsningen. | AV | Leverandøren bes beskrive hvorledes de dokumenterer løsningen og tilhørende informasjonssystemer med henblikk på kritikalitet. |
| P27 | Med utgangspunkt i klassifiseringen av informasjonssystemene skal det etableres nødprosedyrer for alternativ drift av løsningen uten informasjonssystemene, og alternativ drift med delvis støtte fra informasjonssystemene, samt testing av nevnte prosedyrer. | AV | Leverandøren bes beskrive sine nødprosedyrer og hvorledes disse testes. |

## 8.9 **Personvern**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| P28 | Leverandøren skal sette kunden i stand til å etterleve personvernregelverket i avtaleperioden og også etter at avtaleforholdet avsluttes, herunder ved å legge til rette for dette i utformingen av løsningen. | AV | Leverandøren bes beskrive overordnet hvordan dette kravet vil oppfylles. |
| P29 | Løsningen skal tilrettelegges for å ivareta personvernprinsippene, herunder særlig prinsippene om åpenhet, dataminimering, lagringsbegrensning og riktighet. | AV | Leverandøren bes beskrive hvordan personvernprinsippene tenkes ivaretatt i løsningen.<br>Beskrivelsen bør peke på tiltak, prosesser og rutiner som sikrer ivaretakelse av hvert av personvernprinsippene. |
| P30 | Løsningen skal ha innebygd personvern og personvern som standardinnstilling. | AV | Leverandøren bes beskrive hvilke tiltak, prosesser og rutiner som vil bidra til å ivareta innebygd personvern og personvern som standardinnstilling. |
| P31 | Løsningen skal ivareta den registrertes rettigheter, herunder både søkere og saksbehandlere. | AV | Leverandøren bes beskrive hvordan den registrertes rettigheter ivaretas, herunder blant annet rett til innsyn til egne opplysninger, informasjon om egen søknadshistorikk og logger, rett til retting og sletting, rett til begrensning av behandling og rett til dataportabilitet. |

# 9 INTEGRASJONER

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| I1 | Integrasjoner skal utvikles og tilpasses etter et metodeverk. | AV | Beskriv metodeverk for utvikling og tilpassing av integrasjoner med tredjeparts løsninger. Det skal fremkomme både teknisk tilnærming, prosjektmetodikk og kvalitetssikring. |
| I2 | Løsningen bør ha et åpent API for både lesing og skriving. | V | Beskriv teknisk tilnærming/arkitektur. |
| I3 | Det skal være mulig å importere og eksportere data til/fra eksterne kilder som MS Excel, tekstfiler og/eller XML filer. | AV | Bekreft og beskriv hvordan kravet er oppfylt. |
| I4 | Løsningen skal støtte federert pålogging i form av SAML2.0 eller OpenID Connect mot kundens IdP (ADFS eller AzureAD). | V | Beskriv hvilken løsning som støttes |
| I5 | Løsningen må støtte direktelenking (URL), f.eks lenke direkte til en ROS. | AV | Bekreft og beskriv hvordan kravet er oppfylt. |

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| I6 | Tilgangsstyring skal kunne håndteres og administreres via API f.eks. SCIM 2.0 eller på annen måte kunne benytte informasjon fra kundens brukerkatalog. | V | Beskriv hvordan kravet er ivaretatt |

## 10 PLAN FOR ETABLERING

### 10.1 **Prosjektgjennomføring**

Det er behov for en effektiv og vellykket implementering og innføring av løsningen og tjenesten.

Leverandør skal i Bilag 3 beskrive en plan for gjennomføring fra signering av kontrakt til leveringsdag, inkludert etablering av vedlikeholdstjenesten. Planen skal inneholde alle nødvendige aktiviteter med ansvar og estimert tidsbruk. Kundens aktiviteter og ansvar skal også inngå i planen.

Leveransen skal gjennomføres ved anvendelse av Leverandørens etablerte prosjektmetoder samt Leverandørens beste praksis for tilsvarende leveranser.

### 10.2 **Test og godkjenning**

Kunden skal undersøke leveransen ved å gjennomføre en akseptansetest, jfr. de alminnelige kontraktsbestemmelsene punkt 3.3.

Leverandør skal i Bilag 3 beskrive plan for test og godkjenning, og legge ved en generisk testplan.

Kunden skal ikke være begrenset av de alminnelige kontraktsbestemmelsenes regulering av en testperiode på 10 dager. Testperioden avsluttes når alle planlagte tester er gjennomført og godkjenningskriteriene er oppnådd.

### 10.3 **Opplæring**

Kunden har følgende målgruppe for opplæring:

- Administrator
- Interkommunalt personvernombud
- Virksomhetsledere (godkjenningsfullmakt)
- Ansvarlig for registering av behandlinger/personvernkoordinator
- Sikkerhetskoordinator

Leverandør skal tilby tilpasset opplæring av de ulike målgruppene.

Leverandøren skal i Bilag 2 beskrive hvordan leverandøren gjennomfører opplæring av målgruppene og i hvilken form.

Beskrivelsen skal inneholde følgende informasjon: Målgruppe, målsetting, innhold, varighet, sted/form på opplæring, krav til forkunnskap, resultat etter opplæring, dokumentasjon og anbefalt antall deltakere.

Kunden forbeholder seg retten til enten selv å gjennomføre kurs i bruk av tilbudt applikasjon, eller å hente inn annen ekstern undervisningskompetanse.

### 10.4 **Dokumentasjon**

Kunden skal kunne bygge egen kompetanse på løsningen.

Det skal leveres brukerdokumentasjon på norsk som presenterer systemets virkemåte og funksjonalitet for brukerne, og dekker alle de ulike roller brukere av systemet kan ha.

Det skal leveres systemdokumentasjon som skal gi innsikt i og forståelse av applikasjonen.

All dokumentasjon skal foreligge elektronisk for kunde med mulighet til å redigere/editere på dokumentasjonen og kopiere denne til internt bruk.

All dokumentasjon skal være oppdatert, og klart merket med hvilken versjon, revisjon, rettelse etc. den relaterer seg til.

Leverandøren skal i Bilag 2 beskrive tilbudt dokumentasjon.

## 11 ADMINISTRATIVE BESTEMMELSER

Leverandøren skal i Bilag 5 beskrive sin planlagte organisering og bemanning av etableringsprosjektet. Dette skal dokumenteres med CV med relevant erfaring og referanser, for følgende roller.

- Prosjektleder
- Integrasjonsansvarlig
- Opplæringsansvarlig

Leverandøren skal i Bilag 5 beskrive organisasjonen som kreves for gjennomføring av ytelsen etter etablering, herunder roller og tilbudt kompetanse. Det skal også redegjøres for hvilke krav som stilles til medvirkning fra Kundens side.

## 12 DRIFT OG VEDLIKEHOLD

Kundens behov og krav til tjenestens drift og vedlikehold spesifiseres i kapitlene under. Leverandøren skal besvare kravene i kravtabellen i Bilag 2 og tekstlig i Bilag 4.

Under er det gitt en definisjon av begreper som benyttes i dette kapittelet.

| Begrep | Definisjon |
|---|---|
| Tjenestens oppetid | Den tidsperioden hvor tjenesten normalt skal være tilgjengelig, og hvor måling og rapportering av tjenestekvalitet foregår. |
| Tilgjengelighet | Tjenesten regnes som tilgjengelig dersom det ikke er registrert en A- eller B-feil for tjenesten. |
| Svartid | Med svartid menes tiden fra Kunden ringer til brukerstøtte til operatør svarer (tid i kø). |
| Responstid | Med responstid menes tiden fra en henvendelse er meldt inn fra Kunden til arbeidet med henvendelsen er påbegynt av Leverandøren. |

| Begrep | Definisjon |
|---|---|
| Løsningstid | Den tid, i Tjenestens oppetid, det tar fra en sak er registrert til Leverandøren har rapportert den som utført. Tid fra status «utført» til status «lukket» inngår ikke. |
| Tjenesteperiode | 1 (én) kalendermåned |

## 12.1 **Drift av løsning**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| D1 | Det skal være mulig å spore og dokumentere egenskaper ved tjenesteleveransens driftsdel. | A | Oppgi hvilke datasentre og hvilke fasiliteter som benyttes eller kan benyttes for å levere tjenesten. |
| D2 | Eventuelle endringer i oppgitte datasentre og/eller i bruk av datasentre skal varsles til Kunden, se også Databehandleravtalens bestemmelser knyttet til bruk av underdatabehandlere. | A | Vennligst bekreft. |
| D3 | Datasenteroperatøren skal ha energibesparende tiltak for kjølingen av datasenteret som f.eks. styring og design av lufttilførsel, temperaturoptimering, vedlikehold av kjølesystem mm. | AV | Beskriv hvordan kravet er ivaretatt og i hvilken grad det er i tråd med «EU Code of conduct for datacenter efficiency». |
| D4 | Datasenteret skal benytte kjølemidler som gir lavest mulig drivhuspotensiale (GWP) | AV | Angi GWP i overensstemmelse med utregningsmetoden som er beskrevet i bilag IV til forordning (EU) nr. 517/2014. |
| D5 | Det er ønskelig at spillvarmen fra datasenteret gjenbrukes, som f.eks. til fjernvarme. | V | Angi fasilitetens energigjenbruksfaktor (ERF) som en verdi mellom 0 og 1. |
| D6 | Det er ønskelig at datasenteret benytter vedvarende energikilder. | V | Angi hvor stor del av datasenterets forbrukte energi som kommer fra vedvarende energikilder med anvendelse av standarden REF med en verdi mellom 0 og 1. |

## 12.2 **Brukerstøtte**

Brukerstøtte skal være inkludert i den faste avgiften. Med brukerstøtte menes bistand fra Leverandøren som ikke har tilknytning til feil i programvaren. Dette kan eksempelvis være forhold som:

- Kunden trenger forklaring på prosesser i systemet.
- Kunden ber om råd for å optimalisere bruken av systemet.
- Kunden har et rapportbehov og trenger hjelp til å finne ut hvilke rapporter de kan bruke i den sammenheng.

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| D7 | Kunden har i normal arbeidstid behov for et kompetent brukerstøtteapparat som kan løsningen som supporteres | AV | Beskriv supportapparatet deriblant:<br>• Tilgjengelighet |

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| | | | • Antall faste supportmedarbeidere<br>• Medarbeidernes kompetanse og erfaring<br>• Gjennomsnittlig svartid<br>• Gjennomsnittlig responstid<br>• Gjennomsnittlig løsningstid<br>• Support kanaler, eksempelvis epost, telefon mm. |
| D8 | Kunden har behov for support på norsk. | A | Bekreft at kravet er oppfylt. |

### 12.3 **Feilretting**

Når kunden oppdager feil eller mangler ved leveransen, skal disse rapporteres til Leverandøren med kategori. Ved feilmelding foretar Kunden selv kategorisering av feil innenfor de kategorier som er gitt i de alminnelige kontraktsvilkårene.

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| D9 | Det er Kunden som kategoriserer hva som er feil og hva som er endringsønsker.<br>Kunden rapporterer opplevde feil. Leverandøren kan ikke endre kategoriseringen uten Kundens samtykke. | AV | Beskriv rutiner for mottak, behandling og retting av feil |
| D10 | Dersom Kunden er i tvil om feilen skyldes programvare, utstyr eller nettverk kan Kunden kreve at Leverandøren iverksetter nødvendige tiltak for diagnostisering. | A | Leverandøren bes akseptere dette |
| D11 | Leverandøren plikter å informere Kunden om kjente feil, og å informere om hvordan og når feilen er tenkt løst samt informasjon om eventuelle midlertidige løsninger. | AV | Beskriv hvordan dette er ivaretatt |
| D12 | I spesielle situasjoner vil det være hensiktsmessig med en midlertidig løsning for å omgå innmeldte feil. Dette skal ikke påvirke opprinnelig kategorisering og heller ikke bli en permanent løsning for innmeldte feil. | A | Leverandøren bes akseptere dette |

### 12.4 **Tjenestenivå**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| D13 | Kunden har behov for en robust tjeneste med høy tilgjengelighet og rask responstid.<br><br>Leverandøren skal garantere stabiliteten på tjenesten. Manglende tilgjengelighet som skyldes forhold utenfor tjenesten levert av Leverandøren, eller planlagte ekstraordinære | AV | Beskriv hvordan dette er ivaretatt i Bilag 4 eller i egen, vedlagte SLA.<br><br>Beskrivelsen skal minimum inneholde:<br>• Garantert oppetid<br>• Responstider på feilhåndtering etter kategori<br>• Responstid på brukerstøtte |

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| | driftsstanser, omfattes ikke av tilgjengelighetsgarantien | | |
| D14 | Ved brudd på tilgjengelighetsgarantien har Kunden rett på kompensasjon. Dersom bortfallet bare gjelder deler av tjenesten, reduseres betalingsplikten forholdsmessig etter omfang, skyld og avbruddstid. | AV | Forholdsmessig prisavslag ved brudd på tilgjengelighetsgarantien skal være angitt i Bilag 4 eller vedlagt SLA. Metode for utregning skal også beskrives. |
| D15 | Tjenestenivået i en gitt tjenesteperiode skal dokumenteres av leverandøren i en rapport som oversendes Kunden, og eventuell kompensasjon skal basere seg på rapporten. | AV | Beskriv prosess for rapportering samt dokumenter hvordan en rapport vil se ut ved å legge ved et eksempel. |
| D16 | Kunden har behov for varsling før planlagt nedetid. | A | Beskriv hvordan dette er ivaretatt i Bilag 4 eller i egen, vedlagte SLA. |

### 12.5 **Nye versjoner**

| Krav nr | Kundens behov, beskrivelse av krav | Krav type | Krav til besvarelse |
|---|---|---|---|
| D17 | Nye versjoner av programmer er inkludert i avtalen. Når nye versjoner av programmer er utgitt, skal Leverandøren så snart som mulig tilgjengeliggjøre disse for Kunden. | A | Leverandøren bes bekrefte dette |
| D18 | Nye eller endrede funksjoner skal være ferdig utviklet og testet internt hos Leverandør før tilgjengeliggjøring til Kunden. | AV | Leverandøren bes beskrive rutiner og metoder som benyttes ved endringer og videreutvikling av løsningen. |
| D19 | Løsningen skal til enhver tid være kompatibel med eksisterende versjoner av annen eller tredjeparts programvare den er integrert med. | A | Leverandøren bes bekrefte dette |
| D20 | Dersom nye versjoner krever endringer i teknisk infrastruktur eller 3. partsverktøy, må dette varsles Kunden i god tid, og endringene skal beskrives. | AV | Leverandøren bes beskrive rutiner og metoder som benyttes ved endringer og videreutvikling av løsningen. |
| D21 | Kunden ønsker mulighet til å påvirke utviklingen av løsningen. | V | Leverandøren bes beskrive hvordan kundens behov for å påvirke endringer og videreutvikling av funksjonalitet blir ivaretatt. |

## 13 SAMLET PRIS OG PRISBESTEMMELSER

Leverandøren skal, som Bilag 6, fylle ut priser basert på oppdragsgivers vedlagte mal. Regulering av pris skjer etter de alminnelige avtalebestemmelsene og presiseringene i Bilag 6.