

SSA-L bilag 2C

A "Må-krav"		Krav kategorisert som A er definert som minstekrav. Disse kravene må som hovedregel oppfylles for at tilbudet ikke skal avvises. Tilbyder bes godta kravet ved å kvittere ut med «Lest og akseptert». Oppdragsgiver kan for enkelte A-krav be om beskrivelse/dokumentasjon for å kunne verifisere at kravet er oppfylt. De krav dette gjelder fremgår av kravtabellene. Har Leverandøren forbehold/ forutsetninger til A-krav, vil Kunden ut fra beskrivelse av forbehold/forutsetning vurdere om kravet er oppfylt eller ikke. Oppdragsgiver forbeholder seg retten til å avvise tilbud som inneholder avvik som nevnt i FOA § 24-8 (2). Det bemerkes imidlertid at ingen krav er absolutte. Oppdragsgiver kan derfor velge å akseptere tilbud som inneholder avvik, dersom disse ikke er vesentlige. Tilbud med vesentlige avvik fra kravspesifikasjonen vil bli avvist, jf. FOA § 24-8 (1).
--------------------	--	---

Krav nr.	Krav	Utfyllende kommentarer til oppdragsgiver og leverandør	Kravkode	Dokumentasjonskrav	Levernadørens beskrivelse
PV1	Leverandør må oppgi hvilke personopplysninger som skal behandles i systemet for å levere tjenesten. Bakgrunnen for kravet er at vilke personopplysninger som behandles i et system vil ha betydning for hvilke krav som stilles til sikkerheten i systemet. Leverandør må derfor si noe om hvilke personopplysninger som f.eks. samles inn, brukes, lagres, sammenstilles, deles i systemet.	Dersom systemet kun behandler alminnelige personopplysninger (f.eks. navn, telefonnummer, e-postadresse) vil ikke kravene til sikkerhet være like strenge som når det behandlles særlige kategori av personopplysninger (f.eks. helseopplysninger, personlige forhold andre taushetsbelagte opplysninger).	A	Utdyp og beskriv hvilke personopplysninger som behandles i systemet som anskaffes.	
PV2	Leverandøren må godkjenne Tromsø kommunes databehandleravtale med bilag. Bakgunnen for kravet er at dersom leverandør skal behandle personopplysninger på vegne av Oppdragsgiver vil leverandøren anses som en databehandler. Det skal da inngås en databehandleravtale. Denne skal være et vedlegg til selve avtalen for anskaffelsen. Tromsø kommune har en egen mal for databehandleravtale med bilag. Denne skal fylles ut av Leverandør og Oppdragsgiver i samarbeid.	Noen ganger er det vanskelig å avgjøre om det foreligger et databehandleroppdrag, og hvem som eventuelt er behandlingsansvarlig og databehandler i oppdraget. Det er en forutsetning at leverandøren faktisk skal behandle personopplysninger, og at formålet med avtalen helt eller delvis går ut på å behandle personopplysninger. Det skal inngås en databehandleravtale dersom det svares “ja” på et av disse spørsmålene: •Skal leverandøren drifte et av våre systemer? (for eksempel bruk av vaktelskap til å drifte og administrere kameraovervåkning) •Bruker vi en leverandørs skytjeneste for å lagre personopplysninger? •Har leverandør fjerntilgang til dine systemer der tjenesten består i å drive support for dine ansatte gjennom systemene. •Gjelder anskaffelsen kjøp av et fagsystem? •Plattform for deling av informasjon? •System for søknad og saksbehandling? •Gjelder anskaffelsen velferdsteknologi?	A	Bekreft Ja/Nei	
PV3	Løsningen skal være designet etter prinsippene om innebygget personvern og personvern som standardinnstilling. Formålet med kravet er å sikre at det er implementert tilstrekkelig tekniske og organisatoriske tiltak i løsningen slik at personvernregelverket overholdes. Hvilke tiltak som anses som tilstrekkelig vil avhenge av blant annet hvilke personopplysninger som behandles, omfanget av behandlingen, formålet med behandlingen mm.	Innebygd personvern betyr at løsningen skal ta hensyn til personvern i alle deler av utviklingen av programvaren/applikasjonen. En leverandør av en teknologisk tjeneste er ofte databehandler for sine kunder. Kunden er da behandlingsansvarlig og har ansvaret for å sørge for at løsningen oppfyller kravet til innebygd personvern. En av leverandørens oppgaver er å sette kunden i stand til å oppfylle sine forpliktelser. Ved anskaffelser skal vi kontrollere at leverandøren har ivare tatt dette ved å ha nødvendige standardinnstillinger i løsningen som f.eks: •Bare samler inn personopplysninger som er nødvendig for formålet •At personopplysninger automatisk slettes når de ikke lengre er nødvendig å oppbevare •Har hensiktsmessig tilgangsstyring- den enkelte bruker skal bare kunne se nødvendige opplysninger •Kryptering der dette er nødvendig •Logg som viser nødvendig aktivitet •Sikrer god og brukervennlig informasjon om personvern til våre innbyggere •Dersom samtykke er nødvendig for behandling skal dette fremgå tydelig	A	Utdyp og beskriv hvordan løsningen er utviklet for å overholde kravene til innebygget personvern og personvern som standardinnstilling. Dette innebærer en beskrivelse av blant annet kulepunktene til venstre.	
PV4	Løsningen skal være designet for å ivareta personvernrettigheter. Bakgrunnen for kravet er at de personene som personopplysningene gjelder skal ha mulighet til å håndheve sine rettigheter i form av f.eks. medbestemmelse og kontroll over hvordan personopplysningene behandles.	For å sikre at de som eier personopplysnngene har medbesemmelse og kontroll på hvordan kommunen behandler deres personopplysninger, har den enkelte (på visse vilkår) disse rettighetene: •Rettt til informasjon om behandlingen (f.eks. formålet med behandlingen av personopplysninger og eventuelle andre mottakere av personopplysningene) •Rettt til innsyn •Rettt til retting/korrigerering •Rettt til sletting •Rettt til begrensning av behandling •Rettt til dataportabilitet •Rettt til å protestere	A	Utdyp og beskriv hvordan løsningen ivaretar de grunnleggende personvernrettigheter.	
PV5	Leverandøren skal redegjøre for og dokumentere overføringsgrunnlaget som benyttes dersom personopplysninger overføres til land utenfor EØS-området, for eksempel dersom leverandør anvender underleverandører eller datasentre i slike land. Bakgrunnen for kravet er at det er ulovlig å overføre personopplysninger til et tredjeland (land utenfor EØS) eller til en internasjonal organisasjon, med mindre det finnes et gyldig overføringsgrunnlag.	Oppdragsgiver vil vurdere dokumentasjonen og forbeholder seg retten til å avvise leverandører som ikke kan dokumentere: •At overføringen skjer i tråd med reglene i kapittel 5 i personvernforordningen (GDPR) •At personopplysninger har tilsvarende beskyttelsesnivå som i EØS. Noen land utenfor EØS er forhåndsgodkjent av EU-kommisjonen. Dette er da er uproblematisk, men dersom overføringen baserer seg på et annet grunnlag, må det gjøres en vurdering av om dette er lovlig. Det vanligste rettslige grunnlaget er EUs standardkontrakt (ScC). Vi gjør oppmerksom på at overføring ikke bare gjelder hvor server er plassert i land utenfor EØS, men også sporadisk/midlertidig tilgang f.eks. i forbindelse med support fra tredjeland, morselskap i tredjeland. Derne st ber vi om at det eventuelt vises til overføringsgrunnlag dersom det er aktuelt.	A	Leverandøren skal levere dokumentasjon som bekrefter at overføring av personopplysninger til områder uten adekvansbeslutning skjer i tråd med kapitel 5 i GDPR og har tilsvarende beskyttelsesnivå som i EØS Dersom overføringsgrunnlaget er ScC eller annet, skal vedlegg "Vurdering av sikkerhetsnivå ved overføring av personopplysninger til tredjeland" fylles ut slik at vi kan sikre at kravet til tilstrekkelig beskyttelsesnivå er oppfylt.	

Krav nr.	Krav	Kravkode	Dokumentasjonskrav	Levernadørens besvarelse
IS1	Robuste løsninger Leverandør må arbeide kontinuerlig for å få oversikt over trusselbildet, samt arbeide aktivt for å begrense sårbarheter.	A	Beskriv hvordan dere arbeider proaktivt for å begrense sårbarheter. Beskriv hvilke rutiner og tiltak som gjøres for å identifisere, vurdere og prioritere sårbarheter.	
IS2	Endring og avlytting av data under overføring: Leverandør må ha sikringstiltak som beskytter data under overføring, herunder beskyttelse av nettverk og bruk av kryptering. Data som overføres via nettverk kan tappes/avlyttes og endres dersom de ikke sikres. Dette gjelder både data som overføres til og fra tjenesten, internt i tjenesten og data som utveksles med andre tjenester f.eks. ved bruk av API.	A	Beskriv hvordan data under overføring beskyttes, herunder beskyttelse av nettverk og bruk av kryptering. Beskriv hvordan data beskyttes ved mellomlagring.	
IS3	Datasenterets fysiske sikkerhet Leverandør må ha fysiske sikringstiltak i sine datasentre slik at uvedkommende ikke får tilgang til data, systemer og utstyr. Uvedkommende kan få tilgang til data, gjøre endringer på systemer og urettmessig fjerne utstyr dersom datasentre ikke er fysisk sikret.	A	Beskriv hvilke fysiske sikringstiltak som benyttes i de datasenter som brukes for å levere tjenesten (ytelsen jfr. SSA-SKY avsnitt 1.1.1.Leverandørens ytelse) slik at uvedkommende ikke får tilgang til data, systemer og utstyr.	
IS4	Separasjon mellom kunder Leverandør må skille oppdragsgivers tjenester/data fra andre kunder. En kunde kan påvirke en annen kundes tjeneste/data dersom det ikke er tilfredsstillende skille mellom disse.	A	Beskriv hvordan oppdragsgivers data/tjenester skilles fra andre kunders data/tjenester, både logisk og fysisk.	
IS5	Sletting av data Leverandøren må slette data på forsvarlig måte når utstyr byttes og data flyttes over til nytt utstyr. Leverandøren må også sikre at kundens data ikke blir tilgjengelig på det gamle utstyret. Data som slettes kan komme på aveie eller gjenskapes dersom leverandør ikke sletter kundens data på en forsvarlig måte. Dette gjelder også dersom leverandøren bytter ut sitt utstyr og flytter kundens data over til nytt utstyr.	A	Beskriv hvordan data slettes og sikrer at slettede data ikke kan bli tilgjengelig for andre eller kan gjenskapes. Beskriv også hvordan slettede data ikke blir tilgjengelig for andre ved utskifting og fornyelse av infrastruktur.	
IS6	Robusthet Leverandøren må ha tiltak/prosedyrer som kan sikre en robust tjeneste. Tjenesten kan bli utilgjengelig dersom den ikke er tilstrekkelig robust for å kunne stå imot ondsinnede angrep, tekniske feil, etc.	A	Beskriv hvilke tiltak/prosedyrer som er etablert for å sikre en robust tjeneste.	
IS7	Sporbarhet Leverandør må ha logger for å forebygge og avdekke sikkerhetsbrudd i informasjonssystemene. Løsningen skal som minimum ha logger for å: ■ kunne avdekke både autorisert og uautorisert tilgang ■ avdekke forsøk på uautorisert tilgang Løsningen må ivareta integriteten til loggene. De må sikres mot endring/sletting. Løsningen må gi mulighet for at kunden får tilgang til logger.	A	Beskriv hvordan løsningen avdekker både uautorisert og autorisert tilgang, samt forsøk på uautorisert tilgang. Beskriv hvordan logger sikres mot endring/sletting. Beskriv hvordan kunden får tilgang til logger.	
IS8	Identifisering av brukere - Autentisering Løsningen må ha sikker autentisering av brukere. Felles brukerkontoer er ikke tillatt. Identifisering av brukere (autentisering) må gjenspeile hvilket sikkerhetsbehov en har til informasjonen som skal beskyttes.	A	Beskriv hvordan kundens brukere autentiseres, og i tillegg hvordan andre brukere som for eksempel administratorer blir autentisert. Beskriv hvordan løsningen gir støtte for brukerautentisering mot kommunens autentiseringstjeneste.	
IS9	Styring av tilganger - Autorisasjon Løsningen må sikre at brukere ikke får for vide rettigheter til systemet. Brukere må ha tilgang til rett informasjon ut fra tjenstlig behov.	A	Beskriv hvordan løsningen gir støtte for rollebasert tilgangsstyring.	
IS10	Sikkerhetsbrudd / Varsling Løsningen må ha system for overvåking av tjenesten og rutiner for varsling.	A	Beskriv prosesser, overvåkningsrutiner, etc. som er til hjelp for å avdekke sikkerbrudd i løsningen. Leverandøren må som minimum legge ved egen rutine for avviksbehandling.	
IS11	Leverandør og underleverandørs tilgang til data. Leverandør må ha sikkerhetsrutiner for hvordan de får tilgang til kundens data, når det er behov for det. Dette gjelder også for eventuelle underleverandørs tilgang.	A	Beskriv hvordan informasjonssikkerheten blir ivaretatt når det behov for tilgang til kundens data.	
IS12	Backup (sikkerhetskopiering) Leverandøren må ha rutiner for backup av data. Backupløsningen må være separert fra levandørens driftsplattform.	A	Beskriv rutiner for backup (full og/eller inkrementell backup), og hvordan den er sikret.	
IS13	Systemarkitektur Leverandør må fremlegge overordnet systemarkitektur. Løsningsdesign og systemdokumentasjon er nødvendig for å få tilstrekkelig innsikt i hvordan løsningen fungerer.	A	Leverandøren skal fremlegge et overordnet løsningsdesign og systemdokumentasjon som på en tydelig og oversiktlig måte viser de relevante hovedkomponenter, overordnet dataflyt og kommunikasjonsgrensesnitt internt og eksternt for løsningen.	