**VEDLEGG 04 - PERSONVERN OG INFORMASJONSSIKKERHET**

Oppdragsgiver mottar fakturaer som inneholder sensitive personopplysninger.

Kristiansand kommune mottar faktura med navn på personer som er bosatt i kommunen og fødselsdato. Dette gjelder ofte fakturaer som omhandler fritidsfond, barnevern og beboere på institusjoner. Slike fakturaer er, for Kristiansand kommune, ikke av interesse for bruken av systemet og skal slettes/utelates før data oversendes leverandør. Unntaksvis kan det skje feil, og faktura med sensitiv personinformasjon kan bli overført til leverandør. Denne informasjonen skal ikke behandles. Bestillere i kommunen oppgir sitt navn som referanse og enkelte fakturaer blir da merket med bestillers navn. Sistnevnte anses ikke som personsensitiv informasjon.

Utlendingsdirektoratet mottar fakturaer som inneholder informasjon om asylsøkere, herunder navn, bosted og fødselsdato.

1. Tilbyder bes beskrive hvordan de som leverandør ved drift og vedlikehold av systemet oppfyller gjeldende lovverk og krav slik at kunden er i stand til å sikre at prinsippene for behandling av personopplysninger er oppfylt, jf. personopplysningsloven og personvernforordningen (GDPR).

2. Tilbyder bes også beskrive hvordan de som leverandør ved drift og vedlikehold av systemet ivaretar krav til konfidensialitet, integritet, tilgjengelighet og robusthet.
    - Konfidensialitet (K): Personopplysninger og annen informasjon sikres mot uautorisert utlevering og tilgang.
    - Integritet (I): Personopplysninger og annen informasjon sikres mot utilsiktet og ulovlig ødeleggelse, tap og endringer.
    - Tilgjengelighet (T): Personopplysninger og annen informasjon er tilgjengelig for autoriserte med tjenstlig behov.
    - Robusthet (R): Programvaren som behandler personopplysninger og annen informasjon, er beskyttet mot for eksempel sårbarheter, angrep, og uhell.

3. Det er ønskelig at personopplysninger bare behandles innenfor EU/EØS, eventuelt i land som har adekvansbeslutning. Tilbyder bes redegjøre for hvor personopplysninger behandles.

   Tilbyder bes opplyse om eventuelle underdatabehandler(e) og i hvilke(t) land personopplysninger behandles.

   Dersom underdatabehandler benyttes bes Tilbyder redegjøre for hvordan Tilbyder fører kontroll/tilsyn med eventuelle underdatabehandler(e) for å sikre at prinsippene for behandling av personopplysninger som følger av personopplysningsloven (POL)/ personvernforordningen (GDPR) er oppfylt hos underdatabehandler(e).

   Dersom personopplysninger behandles i land utenfor EU/EØS som ikke har adekvansbeslutning må leverandør beskrive overføringsgrunnlaget. I tillegg må det vedlegges dokumentasjon som viser at overføringen i praksis får samme beskyttelsesnivå som i EU/EØS, se tilleggskrav beskrevet hos Datatilsynet: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/tilleggskrav-til-overforingsgrunnlag-schrems-ii/.

4. For Kristiansand kommune kan det unntaksvis komme over fakturainformasjon som inneholder sensitive personopplysninger. Disse opplysningene skal ikke behandles. Tilbyder bes redegjøre for hvordan disse fakturaene/opplysningene kan slettes. Tilbyder bes også opplyse om hvilke interne tiltak leverandøren iverksetter for at slike opplysninger ikke behandles (internkontroll).

5. Tilbyder bes redegjøre for hvilke muligheter systemet har for sladding av personinformasjon i systemet, eksempelvis sladding av navn på bestiller dersom dette er opplyst på faktura. Det er ikke ønskelig at denne personinformasjonen behandles i systemet.

Oppdragsgivers mal for databehandleravtale vil bli benyttet, se vedlegg 08, 09 og 10. Databehandleravtalen er påbegynt med foreløpig instrukser, men endelige instrukser vil bli fastsatt med valgt leverandør.

Kristiansand kommune og Utlendingsdirektoratet benytter ikke samme mal, og signerer hver sin databehandleravtale.