* 1. Krav til Personvern, sikkerhet og tilgangskontroll
     1. Kravtabell - Personvern

| 1. Nr. | | 2. Krav | 3. Prioritet (A/V) | 4. Svar  (J/D/N) |
| --- | --- | --- | --- | --- |
| 1 | | Leverandøren skal følge det til enhver tid gjeldende personvernregelverk. Det skal etableres databehandleravtale mellom KUNDEN og leverandøren som er i tråd med gjeldende personvernregelverk, basert på KUNDENs malverk. | A |  |
| 1 | | **Leverandørens utfyllende kommentar:** | | |
| 2 | | Leverandøren skal beskrive hvordan arbeid med personvern er organisert i virksomheten, med betydning for ivaretakelse av personvern i gjennomføringen av kontrakten, herunder om det er tydelige definert roller og ansvar som er godt implementert i virksomheten. | V |  |
| 2 | | **Leverandørens utfyllende kommentar:** | | |
| 3 | | Leverandøren skal tilby tjenester som oppfyller personvernforordningens krav til innebygd personvern og personvern som standardinnstilling (personvernforordningen artikkel 25) og som videre legger til rette for at KUNDEN på en effektiv måte kan oppfylle individers rettigheter etter personvernforordningen, inkludert rett til transparens, innsyn, retting og sletting.  Leverandøren skal beskrive hvordan tilbudt tjeneste ivaretar disse kravene gjennom hele livsløpet til tjenesten. Beskrivelsen skal inkludere en beskrivelse av hvordan Leverandøren ivaretar personvern i sine prosesser, rutiner og rammeverk som en del av utvikling, test og produksjonssetting, og som en del av forvaltningen, eksempelvis i forbindelse med endringer, utvidelser eller innføring av nye produkter i tjenesten.  . | V |  |
| 3 | | **Leverandørens utfyllende kommentar:** | | |
| **4** | Alle innstillinger i tjenesten skal som standard være satt opp med den mest personvernvennlige innstillingen. Leverandøren skal beskrive i hvilken grad KUNDEN selv har anledning til å gjøre aktive valg i konfigurasjonen av oppsett for å tilgjengeliggjøre personopplysninger som behandles i tjenesten. | | V |  |
| **4** | **Leverandørens utfyllende kommentar:** | | | |
| **5** | Leverandøren skal beskrive hvordan tjenesten legger til rette for at KUNDEN på en effektiv måte kan oppfylle individers rettigheter etter gjeldene personvernregelverk, inkludert rett til transparens, innsyn, retting og sletting. | | V |  |
| **5** | **Leverandørens utfyllende kommentar:** | | | |
| **6** | Leverandøren skal beskrive sine løsninger for enkel og funksjonell sletting av personopplysninger som behandles i, og gjennom bruk av tjenesten, herunder i hvilken grad løsningen har manuell og automatisk slettemulighet. Videre hvordan sletting av personopplysninger håndteres i eldre backup-og sikkerhetskopier. | | V |  |
| **6** | **Leverandørens utfyllende kommentar:** | | | |
| **7** | Dersom det benyttes underdatabehandler(e) i leveransen av tjenesten som tilbys, skal Leverandøren beskrive hvilke prosesser og rammeverk (herunder risikovurdering) som lå til grunn for godkjenning av denne/disse underdatabehandler(ne) med fokus på personvern og sikkerhet.    Det skal også beskrives hvordan det sikres at underdatabehandlere til enhver tid overholder sine forpliktelser knyttet til personvern og sikkerhet samt hvordan dette vil dokumenteres overfor KUNDEN. | | V |  |
|  | **Leverandørens utfyllende kommentar:** | | | |
| 7 | | Leverandøren skal beskrive hvordan KUNDEN enkelt kan få oversikt over hvor personopplysninger befinner seg, og hvordan personopplysninger behandles til enhver tid. Dataflyt kan gjerne illustreres ved et flytskjema. | V |  |
| 7 | | **Leverandørens utfyllende kommentar:** | | |
| 8 | | Leverandøren skal beskrive hvordan innsyn for de registrerte gjennomføres i tjenestene (f.eks. mulighet for å gjøre uttrekk, søke opp informasjon per Kunde ol.) | V |  |
| 8 | | **Leverandørens utfyllende kommentar:** | | |
| 9 | | Leverandøren skal beskrive hvordan tjenestene sikrer at kun personopplysninger som er nødvendig blir registrert og videre behandlet (dataminimering). | V |  |
| 9 | | **Leverandørens utfyllende kommentar:** | | |
| 10 | | Behandling av personopplysninger, med unntak av  nødvendig påloggingsinformasjon og bruksmetrikk/analysedata/tekniske diagnosedata knyttet til KUNDENs ansatte og eksterne konsulenter, skal skje i EØS eller Europakommisjonens forhåndsgodkjente tredjeland. | A |  |
| 10 | | **Leverandørens utfyllende kommentar:** | | |
| **11** | Behandling av nødvendig påloggingsinformasjon og bruksmetrikk/analysedata/tekniske diagnosedata knyttet til KUNDENs ansatte og eksterne konsulenter skal som hovedregel skje i /fra EØS eller i Europakommisjonens forhåndsgodkjente tredjeland.  Leverandøren skal beskrive hvordan dette er ivaretatt i tjenesten som tilbys.  Dersom det som en del av tjenesten vil behandles personopplysninger i/fra geografiske lokasjoner utenfor EØS / forhåndsgodkjent tredjeland, skal dette skje i tråd med personvernforordningens kapittel V. Leverandøren skal i så tilfelle beskrive hvilket overføringsgrunnlag som legges til grunn samt hvilke ytterligere tiltak som er iverksatt for å sikre behandlingen tilsvarende beskyttelse som innenfor EØS.  I vurderingen av om KUNDEN vurderer tiltakene tilstrekkelige, vil KUNDEN se hen til de til enhver tid gjeldende veiledninger fra det europeiske personvernrådet (EDPB) og Datatilsynet. | | V |  |
| 11 | | **Leverandørens utfyllende kommentar:** | | |
| 12 | | Leverandøren skal beskrive om Leverandøren selv, Leverandørens morselskap eller eventuelle underdatabehandlere er underlagt overvåkningslovgivning som undergraver forpliktelsene som følger av overføringsgrunnlagene. | V |  |
| 12 | | **Leverandørens utfyllende kommentar:** | | |
| 13 | | Dersom det benyttes underdatabehandler(e) i leveransen av skytjenesten som tilbys, skal Leverandøren beskrive hvilke prosesser og rammeverk (herunder risikovurdering) som lå til grunn for godkjenning av denne/disse underdatabehandler(ne) med fokus på personvern og sikkerhet.  Det skal også beskrives hvordan det sikres at underdatabehandlere til enhver tid overholder sine forpliktelser knyttet til personvern og sikkerhet samt hvordan dette vil dokumenteres overfor KUNDEN. | V |  |
| 13 | | **Leverandørens utfyllende kommentar:** | | |
| 14 | | Leverandøren skal beskrive hvordan et eventuelt bytte/endring av underdatabehandler vil håndteres overfor KUNDEN – både juridisk og praktisk. Beskrivelsen skal inkludere informasjon om varslingstid ved slikt bytte/endring, samt informasjon om KUNDENs rett til å motsette seg slikt bytte/endring og hvordan dette vil håndteres. | V |  |
| 14 | | **Leverandørens utfyllende kommentar:** | | |

* + - 1. Kravtabell – informasjonssikkerhet

| 1. Nr. | | 2. Krav | 3. Prioritet (A/V) | 4. Svar  (J/D/N) |
| --- | --- | --- | --- | --- |
| 1 | | Leverandøren må forsikre KUNDEN om at KUNDENs data er tilstrekkelig beskyttet når de er i transitt, både ved transitt til og fra skytjenesten (også via tilgjengelige APIer) og internt i skytjenesten. Beskriv hvordan dette løses, inkl. kryptering og nøkkelhåndtering, og hvilke alternativer KUNDEN har, utover standard tilbudt løsning, for å sikre sine data ytterligere. | V |  |
| 1 | **Leverandørens utfyllende kommentar:** | | | |
| 2 | | Leverandøren må forsikre KUNDEN om at KUNDENs data er tilstrekkelig beskyttet når de er lagret. Beskriv hvordan dette løses, inkl. kryptering og nøkkelhåndtering, og hvilke alternativer KUNDEN har, utover standard tilbudt løsning, for å sikre sine data ytterligere. | V |  |
| 2 | **Leverandørens utfyllende kommentar:** | | | |
| 3 | | KUNDEN beholder eierskapet til sine data lagret i tjenestene også etter at kontrakten er avsluttet og inntil data er flyttet og slettet fra tjenesten. | A |  |
| 3 | **Leverandørens utfyllende kommentar:** | | | |
| 4 | | Sikkerhet og drift/vedlikehold ivaretas i henhold til anerkjente standarder i markedet. Beskriv hvilke standarder og sertifiseringer Leverandøren overholder og er sertifisert til. Eksempeler er (ikke begrenset til) ISO 27001, ISO 27002, ISO 27017, ISO 27018, ISO 22313, eller tilsvarende | V |  |
| 4 | **Leverandørens utfyllende kommentar:** | | | |
| 5 | | Tjenestene tilbyr reaktive og proaktive overvåkingstjenester, inkludert helsestatus. Beskriv hvilke reaktive og proaktive overvåkingstjenester som er tilgjengelig for KUNDEN (inkludert i tjenesten) og hvilke opsjoner som finnes. Beskriv også om det finnes API’er tilgjengelig for KUNDEN hvor data fra overvåkningstjenesten han hentes ut for visning i KUNDENs egen overvåkningsløsning. | V |  |
| 5 | **Leverandørens utfyllende kommentar:** | | | |
| 6 | | Leveandøren har sikkerhetsovervåking av tilbudte tjenester. Beskriv teknologi, rutiner og prosesser Leverandøren har knyttet til sikkerhetsovervåkningen. Beskrive også hvordan sikkerhetslogger, alarmer og varsler kan gjøres tilgjengelig for KUNDEN via API’er for visning i KUNDENs egen sikkerhetsovervåkingsløsning | V |  |
| 6 | **Leverandørens utfyllende kommentar:** | | | |
| 7 | | Ved en sikkerhetshendelse knyttet til brudd på informasjonssikkerheten i de tjenester KUNDEN benytter har leverandøren prosedyrer og rutiner på plass for å kartlegge omfanget av sikkerhetshendelsen og sikre spor/bevis. Beskriv hvilke prosedyrer som følges for å sikre data i etterforskningen. Beskriv også hvor mye bistand Leverandøren vil gi KUNDEN hvis KUNDEN på egenhånd oppdager, og ønsker undersøke, en sikkerhetshendelse i de tjenestene hvor KUNDENs data behandles. | V |  |
| 7 | **Leverandørens utfyllende kommentar:** | | | |
| 8 | | Tjenestene som tilbys skal være sikret mot hacking og forsøk fra tredjepart på å hente kundedata ut av løsningen. Beskriv hvordan ekstern penetrasjonstesting, eller andre mekanismer, brukes for kontroll av tjeneste-, applikasjons- og infrastruktursikkerhet. | V |  |
| 8 | **Leverandørens utfyllende kommentar:** | | | |
| 9 | | Programmer og programmeringsgrensesnitt (API-er) utformes, utvikles, distribueres og testes i samsvar med ledende bransjestandarder (f.eks. OWASP ASVS og "tolvfaktorappen») for å oppnå et høyt nivå av integritet og kvalitet. Beskriv hvilke standarder er og prosedyrene som Leverandører følger knyttet til dette. | V |  |
| 9 | **Leverandørens utfyllende kommentar:** | | | |
| 10 | | Tjenestene som tilbys har funksjonalitet for sikkerhetskopiering av KUNDENs lagrede data. Leverandøren bes beskrive tilgjengelige alternativer for sikkerhetskopiering i form av typer og hyppighet av kopier, oppbevaringsperioder, hvor sikkerhetskopier lagres, hvordan sikkerhetskopier sikres osv.  Beskriv også rutiner for restore og gjenoppretting av sikkerhetsskopier og hvilke muligheter KUNDEN har for selv å konfigurere sikkerhetskopieringen. | V |  |
| 10 | **Leverandørens utfyllende kommentar:** | | | |
| 11 | | I situasjonen hvor KUNDENs data går tapt eller ødelegges, enten ved feilaktig handling fra leverandøren eller på grunn av en permanent katastrofal feil eller naturlig/menneskeskapt katastrofe, bes leverandøren beskrive mekanismene som brukes av leverandøren for å gjenopprette eller rekonstruere KUNDENs data fra beredskapskopier (disaster recovery/business continuity). | V |  |
| 11 | **Leverandørens utfyllende kommentar:** | | | |
| 12 | | Det skal ikke være mulig for Leverandøren å gjenskape data som er bevisst slettet av KUNDEN. I tillegg skal KUNDENs data slettes permanent etter at kontrakten er avsluttet (og etter at KUNDEN har kopiert sine data ut av tjenestene). Leverandøren bes beskrive rutiner, prosess og tidsløpet for sletting av lagret informasjon inkludert kopier i redundans, backupløsninger og beredskapskopier | V |  |
| 12 | **Leverandørens utfyllende kommentar:** | | | |
| 13 | | Leverandøren bes beskrive hvem som eier og driver datasentre og infrastruktur som brukes til produksjon av skytjenesten, hvilke fysiske og organisatoriske sikkerhetstiltak som er på plass for datasenteret og hvilke sikkerhetsstandarder leverandøren for datasenter er sertifisert i henhold til. | V |  |
| 13 | **Leverandørens utfyllende kommentar:** | | | |
| 14 | | Leverandøren bes om å beskrive hvordan de bruker sårbarhet og risikovurderinger som en del av deres styringssystem. | V |  |
| 14 | **Leverandørens utfyllende kommentar:** | | | |

* + - 1. Kravtabell - Tilgangskontroll

| 1. Nr. | 2. Krav | 3. Prioritet (A/V) | 4. Svar  (J/D/N) |
| --- | --- | --- | --- |
| 1 | En bruker (person, prosess eller program) må identifiseres og godkjennes på en entydig måte før tilgang gis til kundedata og relevante deler av informasjonssystemet i løsningen. | A |  |
| 1 | **Leverandørens utfyllende kommentar:** | | |
| 2 | KUNDEN har standardisert på autentisering og singel-sign-on (SSO) fra Microsoft Azure AD for KUNDENs ansatte. Leverandøren bes beskrive hvordan tjenestene støtter SSO mot Microsoft Azure AD og om det støttes ulike standarder for integrasjon. | V |  |
| 2 | **Leverandørens utfyllende kommentar:** | | |
| 3 | KUNDEN har behov for en rik og fleksibel brukertilgangskontroll i sine løsninger. Leverandøren blir bedt om å beskrive hvordan tilgangskontroll er bygget opp og hvilke mekanismer KUNDEN kan bruke i tjenestene for å kontrollere og administrere enkeltbrukers og gruppers tilgang til data (tilgangsnivåer, roller og gruppetilhørighet). Dette gjelder også for de API’er som tilbys i tjenestene. | V |  |
| 3 | **Leverandørens utfyllende kommentar:** | | |
| 4 | For at KUNDEN skal kunne administrere (og eventuelt bruke) skytjenesten når ekstern autentiseringskilde er utilgjengelig, og for å kunne lage lokale test-/utviklingsbrukere, bes Leverandøren beskrive hvordan løsningens innebygde autentiseringsløsning kan brukes parallelt med eksterne. | V |  |
| 4 | **Leverandørens utfyllende kommentar:** | | |
| 5 | Dersom tilbudt tjenester er bygget opp rundt et sett systemer skal ikke en bruker behøve logge seg på hvert enkelt system - SSO skal støttes mellom systemene. Leverandøren bes beskrive hvordan dette er løst i tilbudt skytjeneste | V |  |
| 5 | **Leverandørens utfyllende kommentar:** | | |
| 6 | KUNDEN benytter et sentralt Identity Management (IdM) system for forsyning av tilgangsnivåer, grupper og roller i våre løsninger og tjenester. KUNDEN søker at det standardiseres på bruk av System for Cross-domain Identity Management (SCIM 2.0) - IETF RFCs 7643 eller tilsvarende.  Beskriv hvordan tilbudt skytjeneste støtter bruk av et sentralt IdM system for forsyning av tilganger, gruppe- og rolletilhørighet. | V |  |
| 6 | **Leverandørens utfyllende kommentar:** | | |
| 7 | KUNDEN har ulike kategorier av data hver med et dedikert sett med krav knyttet til isolasjonsstyrke og robusthet i tilgangskontroll.  Leverandøren blir bedt om å beskrive hvordan KUNDENs forretningslogikk/tjenester, kundespesifikk konfigurasjon, plattform, infrastruktur og datalagring er atskilt fra andre kunder, hvordan denne separasjonen kan kontrolleres/administreres av kunden og hva styrken på separasjonen er.  Leverandøren bes også gjøre referanser til kapitler, i standarder de er kompatible/sertifisert til, der isolasjonsstyrke og robusthet i tilgangskontroll er beskrevet og etterlevd. | V |  |
| 7 | **Leverandørens utfyllende kommentar:** | | |
| 8 | Leverandørens tilganger, og spesielt for administratorer, til infrastruktur og tjenester der KUNDENs data overføres, lagres eller behandles må kontrolleres på en sikker måte. Leverandøren bes beskrive, også for sine underbehandlere, hvordan administratorene godkjennes, hvordan rettigheter gis, og om tilganger gis personell på permanent basis.  Leverandøren bes videre om å beskrive hvordan KUNDEN kan gjøre revisjon av leverandørens tilganger, både tildelt og brukt, til infrastruktur og tjenester der kundedataene lagres, overføres eller behandles. | V |  |
| 8 | **Leverandørens utfyllende kommentar:** | | |

* + 1. Kravtabell - Integrasjon

| 1. Nr. | 2. Krav | 3. Prioritet (A/V) | 4. Svar  (J/D/N) |
| --- | --- | --- | --- |
| 1 | Systemløsningen bør ha funksjonalitet for å aksessere og hente data fra andre datakilder.  Beskriv hvilke datakilder og metoder som støttes. | V |  |
| 1 | **Leverandørens utfyllende kommentar:** | | |
| 2 | Systemløsningen bør ha funksjonalitet for å bearbeide og transformere datasett som importeres fra andre systemer, slik at disse passer inn i modellene i løsningen.  Beskriv funksjonaliteten og hvordan denne støttes. | V |  |
| 2 | **Leverandørens utfyllende kommentar:** | | |
| 3 | Systemløsningen bør ha funksjonalitet for å eksportere data, datasett, datastrukturer og kommentarer til eksterne databaser og datalager.  Beskriv hvilke datatyper, databaser og metoder som støttes. | V |  |
| 3 | **Leverandørens utfyllende kommentar:** | | |
| 4 | Systemløsningen bør ha funksjonalitet for å eksportere alle vedlegg som har blitt lastet inn i løsningen, sammen med nødvendige referanser slik at det er mulig å finne tilbake data i modellene som vedleggene gjelder. Dette gjelder også når dataene er eksportert ut. Beskriv hvordan dette støttes. | V |  |
| 4 | **Leverandørens utfyllende kommentar:** | | |
| 5 | Systemløsningen bør ha funksjonalitet for schedulering av import og eksport av data. | V |  |
| 5 | **Leverandørens utfyllende kommentar:** | | |
| 6 | Systemløsningen bør støtte ulike metoder for hendelsesbasert import.  Beskriv hvilke teknologier/metoder/formater som støttes | V |  |
| 6 | **Leverandørens utfyllende kommentar:** | | |
| 7 | Systemløsningen bør ha funksjonalitet for hendelsesbasert eksport.  Beskriv hvilke teknologier/metoder/formater som støttes | V |  |
| 7 | **Leverandørens utfyllende kommentar:** | | |
| 8 | Systemløsningen bør på vegne av en bruker kunne hente ut informasjon fra andre systemer hos KUNDEN. Leverandøren bes beskrive hvordan integrasjon og autentisering mot andre systemer/tjenester gjøres og om «trust chaining» støttes. | V |  |
| 8 | **Leverandørens utfyllende kommentar:** | | |
| 9 | KUNDEN ønsker å bruke egendefinerte brukere (systembruker i målsystemet) for å hente ut informasjon fra systemer og registere hos KUNDEN (dvs ikke på vegne av en personbruker). Leverandøren bes om å beskrive hvordan egendefinerte brukere og passord kan lagres, administreres og brukes av KUNDEN i integrasjonskall fra tilbudte systemløsningen og mot systemer/ registere hos KUNDEN. | V |  |
| 9 | **Leverandørens utfyllende kommentar:** | | |