SPØRSMÅL FRA HORTEN KOMMUNE

INFORMASJONSSIKKERHET OG PERSONVERN

HORTEN
KOMMUNE

Innhold

Versjonslogg 1
Dokumentets formål 1
Generell beskrivelse av løsningen med formål 2
Behandling av personopplysninger 3
Behandling, lagring og sikkerhetskopiering 3
Tekniske og organsatoriske sikkerhetstiltak 4
Tilgangsstyring, autentisering og logging 7
Kunstig intelligens (KI) 8
Personvernkonsekvenser (DPIA) 9

VERSJONSLOGG

Versjon	Dato	Beskrivelse	Av
0.8	04.09.2024	Bearbeidet av IKT-seksjonen, drøftet med Innkjøpskontoret	Thomas Wullum,
0.9	17.09.2024	Drøftet med Innkjøpsavdelingen (SW/GT).	Thomas Wullum,
0.99	25.09.2024	Godkjent i Fagrådet for informasjonssikkerhet	Thomas Wullum,
1.0	01.10.2024	Godkjent i Kommunedirektørens ledermøte	Thomas Wullum,
1.1	20.05.2025	Oppdater layout, klart språk, nytt spørsmål vedr tilgangsstyring	Thomas Wullum

DOKUMENTETS FORMÅL

I de følgende underliggende punktene er det tabeller med spørsmål fra Horten kommune.

Formål er å kartlegge informasjonssikkerhet i løsninger som tilbys kommunen, og dokumentet kan bidra til å supplere behandlingsprotokoll, ROS og DPIA. Tabellen skal fylles ut, og besvarelsen vil inngå tilbyders besvarelse i konkurransen. Avhengig av løsningens formål og innhold, kan et tilbud bli avvist hvis samlet besvarelse ikke ansees å oppfylle nødvendig kvalitetsnivå til informasjonssikkerhet og personvern.

Informasjonssikkerhet og personvern evalueres under kvalitet i konkurransen, og det er besvarelsen i dette dokumentet som legges til grunn for evalueringen.

Kolonnen «Tilbyders beskrivelse» i tabellene under skal fylles ut av tilbyder. Spørsmål som ikke har relevans for tilbudt løsning, kan besvares med *«Ikke relevant».*

GENERELL BESKRIVELSE AV LØSNINGEN MED FORMÅL

Kommunens spørsmål	Tilbyders beskrivelse
Hva er navnet på tilbudt løsning?	
Beskrivelse av tilbudt løsning. *Beskriv formål og funksjon.*	
Er løsningen en skytjeneste? *Skytjenester er en samlebetegnelse på alt fra dataprosessering og datalagring, til programvare på servere som er tilgjengelig fra serverparker tilknyttet internett.*	
Er løsningen hybrid eller Co-location? *Hybride skytjenester er en betegnelse på tjenester som kombinerer elementer fra eksterne og interne skyer. Med Co-location menes skytjenester der kunden eier egne ressurser i eksterne skyer.*	
Hva slags skytjeneste er det? *Eksempler på skyløsninger er Saas (Software as a Service), PaaS (Plattform as a Service), IaaS (Infrastructure as a Service), LaaS (Logging as a Service), DBaaS (Database as a Service), FaaS (Function as a Service) eller SECaaS (Security as a Service).*	
Er løsningen samfunnskritisk? *Løsning som er nødvendig for å opprettholde viktige samfunnsfunksjoner og sikre befolkningens grunnleggende behov og sikkerhet. Dette kan inkludere løsninger for vannforsyning, energidistribusjon, transport, helse- og omsorgstjenester, og andre tjenester som er essensielle for at samfunnet skal fungere normalt.*	

BEHANDLING AV PERSONOPPLYSNINGER

Kommunens spørsmål	Tilbyders beskrivelse
Behandler tilbudt løsning personopplysninger? *Typiske personopplysninger er navn, adresse, telefonnummer, e-post og fødselsnummer (11 siffer).*	
Hva er omfanget av behandling av personopplysninger? *Ca. hvor mange fysiske personers personopplysninger vil bli behandlet på vegne av behandlingsansvarlig i løsningen.*	
Behandles sensitive personopplysninger i løsningen? *Sensitive personopplysninger er blant annet: Helseopplysninger, opplysninger om religion, opplysninger om rasemessig eller etnisk opprinnelse.*	

BEHANDLING, LAGRING OG SIKKERHETSKOPIERING

Kommunens spørsmål	Tilbyders beskrivelse
Hvor behandles, lagres og gjøres sikkerhetskopiering av dataene i løsningen? *Oppgi minimum hvilke(t) land, hvilke(n) region(er) og hvilke(t) datasenter som brukes.*	
Hvordan overføres data? *Beskriv hvordan data sikres i transitt. Hvilke krypteringsmetoder benyttes og hvordan sikres sikker overføring av data mellom løsningen og andre enheter. Hvilke TLS-versjoner støttes? Hvordan håndteres TLS-versjoner med kjente cipher-svakheter?*	
Separeres kundedata i løsningens databaser? *Hvordan skilles dataene fra ulike kunder? Hvilke mekanismer brukes for å hindre utilsiktet tilgang eller blanding av data?*	
Sikkerhetskopi av egne data? *Beskriv mulighetene for at kunden selv kan lagre en synkronisert offline sikkerhetskopi.*	

Pseudonymiseres eller krypteres dataene i løsningen? *Hvilke algoritmer, standarder og nøkler brukes for pseudonymisering og/eller kryptering?*	
Brukes samme krypteringsnøkkel for data fra ulike kunder? *Hvis ja, hvordan sikrer dere at nøkkelen ikke kompromitteres eller deles med uvedkommende? Hvis nei, hvordan genereres og oppbevares nøklene for hver kunde?*	
Hvordan beskyttes dataen under lagring? *Hvilke metoder, standarder og nøkler brukes for å kryptere data som lagres i løsningen eller på sikkerhetskopier?*	
Hvordan er sikkerhetskopiering av data som behandles i løsningen iverksatt? *Brukes separate lagringsmedier og lokasjoner for sikkerhetskopi og originaldata? Beskriv tiltak for å sikre at sikkerhetskopier er immutable og ikke kan manipuleres?*	
Hvordan sikres arkivering? *Beskriv hvordan det sikres at data blir korrekt arkivert og beskyttet mot uautorisert tilgang under bruk av løsningen, og beskriv hvilke sak-/arkivløsninger løsningen tilbyr integrasjon mot.*	
Arkivering ved avslutning av løsningen. *Beskriv prosedyrer for sikker sletting og overføring av data ved avslutning av bruk av løsningen. Beskriv format data kan tilbakeleveres til kunde på.*	

TEKNISKE OG ORGANSATORISKE SIKKERHETSTILTAK

Kommunens spørsmål	Tilbyders beskrivelse
Fysiske sikkerhet. *Beskriv hvilke tiltak som er iverksatt for å hindre uautorisert tilgang, tyveri, brann, flom eller annen skade på de fysiske lokalene eller enhetene der dataen behandles?*	
Løsningsarkitektur. *Beskriv hvilke databaser som benyttes for lagring og håndtering av data i løsningen, og*	.

beskriv rammeverk som er i bruk for å støtte løsningens funksjonalitet	
Drift. *Beskriv hvem er ansvarlig for drift, vedlikehold, oppdatering og sikkerhetskopiering av løsningen?*	
Konfidensialitet, integritet, tilgjengelighet og robusthet i løsningen. *Beskriv sikkerhetstiltak og sikkerhets-mekanismer som er iverksatt for å beskytte løsningen mot uautorisert tilgang, endring, sletting, tap eller skade?*	
Gjenoppretting og beredskap. *Hvordan gjenopprettes tilgjengelighet og tilgang til løsning (eller data) etter en fysisk eller teknisk hendelse? Beskriv prosedyrer og hyppighet for øving og/eller trening.*	
Testes, vurderes og evalueres tekniske og organisatoriske sikkerhetstiltak? *Beskriv hvordan, inkludert hyppighet, dokumentasjon og rapportering.*	
Sårbarhetstesting (penetrasjonstesting). *Utføres sårbarhetstesting jevning? Beskriv rutiner og hyppighet, samt kundens tilgang til rapport fra sårbarhetstesting.*	
Grensesnitt til løsningen. *Beskriv hvilke grensesnitt som tilbys (f.eks. web, mobilapplikasjon el*	
Spørsmål om webgrensesnitt. *Beskriv minimum:* 1. *Hvordan håndteres autentisering i webgrensesnittet?* 2. *Brukes tofaktorautentisering (2FA)?* 3. *Er autentiseringen phisingresistent?* 4. *Hvordan autentiseres brukere mot applikasjonen? (Egen brukerbase, AD/Entra ID, ID-porten eller annet)* 5. *Hvordan sikres dataoverføring i webgrensesnittet?* 6. *Er dataoverføringen kryptert (f.eks. via HTTPS)?* 7. *Hvilke tiltak er på plass for å beskytte mot vanlige webangrep?* 8. *Hvordan håndterer dere trusler som SQL-injeksjon, XSS (Cross-Site Scripting), og CSRF (Cross-Site Request Forgery)?* **9.** *Er det caching av data i nettleseren? Hva slags data caches i nettleseren og hvordan sikres det at data ikke lagres i*	

cash lengre enn nødvendig?	
Spørsmål om mobilapplikasjon. *Beskriv minimum:* 1. *Hvordan håndteres autentisering i mobilapplikasjonen?* 2. *Støttes biometrisk autentisering (f.eks. fingeravtrykk eller ansiktsgjenkjenning)?* 3. *Hvordan sikres dataoverføring i mobilapplikasjonen?* 4. *Er dataoverføringen kryptert (f.eks. via TLS)?* 5. *Hvilke tiltak er på plass for å beskytte mot sikkerhetstrusler i mobilapplikasjonen?* 6. *Hvordan håndterer dere trusler som man-in-the-middle-angrep og malware?* 7. *Hvordan sikrer dere at oppdateringer av iOS- eller Android-innstillinger, spesielt når det gjelder biometrisk pålogging, blir ivaretatt i mobilapplikasjonen?* 8. *Hvilke tilganger til enheten krever mobilapplikasjonen (eksempel: mikrofon, kamera **og** lokasjon)? Er alle tilgangene nødvendige for å utfylle formålet med applikasjonen?*	
IPV6. *Har løsningen støtte for eller planer for støtte for IPV6?*	
Underleverandører. *Beskriv risiko knyttet til potensielle oppkjøp av underleverandører av selskaper med uønskede tilknytninger, samt eventuelle tiltak for å forhindre slike oppkjøp eller konsekvensene av slike oppkjøp.*	
Hjemmearbeid/fjernarbeid for ansatte hos leverandør og underleverandør. *Beskriv retningslinjer og krav for å sikre kunder data på ansattes enheter?*	
Sertifiseringer. *Beskriv relevante sertifiseringer som dokumenterer kompetanse og praksis innen informasjonssikkerhet, personvern og/eller kunstig intelligens? Eksempler: ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 42001*	
Risikovurdering. *Beskriv hvordan tilbyder arbeider med risikovurderinger knyttet til identifisering og håndtering av sikkerhetstrusler.*	

Lenker til relevant sikkerhetsdokumentasjon. *Oppgi lenker til relevant sikkerhetsdokumentasjonen som tilbyder kan dele (f.eks. policyer, prosedyrer, manualer, sertifiseringer, rapporter eller annet som er relevant for informasjonssikkerheten i løsningen.)*	

TILGANGSSTYRING, AUTENTISERING OG LOGGING

Kommunens spørsmål	Tilbyders beskrivelse
Får ansatte hos kunden tilgang til data online? *Beskriv hvilke grader av autentisering/sikkerhet kan settes på tilgang? F.eks. muligheter for krav til VPN, IP-filtrering, bruk av Conditional Access-regler mv.*	
Autentisering. *Beskriv hvordan det sikres at autentiseringsløsningen til enhver tid er sikker i forhold til det globale trusselbildet?*	
Brukes brukernavn og passord for pålogging til løsningen? *Beskriv passordpolicy, inkludert krav til passordstyrke og hyppighet for endring*	
Støttes Azure AD/Entra ID tilgangsstyring? *Hvis Ja, kan rollestyring etableres dynamisk basert på kundedata fra kundens EntraID? Kan brukere importeres på enhets- eller gruppenivå? Hvis Nei, er det planer for å iverksette Entra ID-tilgangsstyring?*	
Roller og rettigheter i løsningen? *Beskriv hva slags roller som kan tildeles i løsningen, og tilgangen til hver rolle medfører. Beskriv hvordan tilgangsstyring kan granuleres.*	
Tilgangsstyring. *Beskriv hvordan tilgangsstyring administreres i løsningen. Hvem kan gi, endre og fjerne tilganger.*	
Logg. *Beskriv hvordan kundens og leverandørens påloginger, endringer og slettinger kundens brukerdatabase logges. Får kunden tilgang til slike logger? Beskriv ...*	

KUNSTIG INTELLIGENS (KI)

Kommunens spørsmål	Tilbyders beskrivelse
Brukes KI i løsningen? *Sett kryss/marker, og beskriv evt. Kort hvordan KI brukes til å behandle eller analysere data og/eller personopplysninger?*	○ JA ○ NEI
Hvilken risikokategori tilhører KI i løsningen? *EUs KI-forordning (Artificial Intelligence Act) klassifiserer KI-løsninger i fem risikokategorier, basert på potensialet deres for å forårsake skade (sett kryss/marker)*	○ KI med uakseptabel risiko ○ KI med høy risiko ○ KI der det nødvendig med særlig informasjon ○ KI med generelle formål ○ KI med lav risiko
Rettferdig, pålitelig og forklarlig. *Beskriv hvordan det sikres at algoritmene er rettferdige, pålitelige og forklarlige?*	
Etikk og ansvarlighet. *Beskriv hvordan det sikres at KI i løsningen brukes etisk forsvarlig? Beskriv hvem som er ansvarlig for feil eller skader forårsaket av KI i løsningen*	
Regelverk og samsvar. *Beskriv hvilke lover og forskrifter tilbyder forholder dere til når det utvikles KI til løsningen? Hvordan sikres samsvar med relevant regelverk?*	
Transparens og forklarbarhet. *Hvordan sikres KIs behandling av data i løsningen er transparente og forståelige?*	
Endringer. *Hvordan sikres at behandlingsansvarlig informeres om endringer i hvordan KI-løsningen lærer av eller bruker data for å skape resultater?*	
Maskinlæring. *Beskriv hvordan KI trenes på eller lærer av kundens data og/eller handlinger? Forklar hvordan slike prosessene fungerer, og hva slags mekanismer som er etablert for å beskytte kundens data samtidig som de gir verdi til kunden.*	
Datadeling mellom kunder. *Beskriv hva slags tiltak som er etablert for å sikre at KI i løsningen ikke deler eller eksponerer data fra én kunde til andre kunder? Beskriv mekanismer og tiltak som er iverksatt for å sikre at kundens data forblir isolert og beskyttet innenfor kundens egen kontekst*	

PERSONVERNKONSEKVENSER (DPIA)

Kommunens spørsmål	Tilbyders beskrivelse
Informasjonsplikten. *Beskriv hvordan informasjonsplikten overfor de registrerte oppfylles, slik at de er klar over hvilke personopplysninger som samles inn, hvordan de behandles, hvem som har tilgang til dem, og hvilke rettigheter de har.*	
Utøvelse av den registrertes rettigheter. *Beskriv hvordan de registrerte kan utøve sine rettigheter, for eksempel begrensning av behandling, innsyn, retting og sletting.*	
Risiko ved behandling av personopplysninger. *Beskriv hvordan mulige skadevirkninger av behandling av personopplysninger identifiseres og håndteres. For eksempel tiltak som reduserer eller eliminerer risiko for tap, uautorisert tilgang eller manipulering av personopplysninger.*	
Rapportering og håndtering av brudd på personopplysnings-sikkerhet. *Beskriv rutiner og prosedyrer for å oppdage, rapportere og håndtere eventuelle hendelser som medfører brudd på personopplysnings-sikkerhet, slik som tap, tyveri, lekkasje, hacking eller annen uønsket eller ulovlig behandling.*	
Kontinuerlig forbedring. *Beskriv hvilke prosedyrer eller rutiner som er iverksatt for å evaluere og forbedre etterlevelsen av alle tiltak som er iverksatt for å beskytte personopplysninger i løsningen. Beskrivelsen bør inkludere en kontinuerlig prosess for å overvåke, revidere og oppdatere alle innførte tiltak som er innført for å sikre at behandlingen av personopplysningene er i samsvar med personvernregelverket og de registrertes forventninger.*	