

Arkitekturprinsipper i Asker kommune

Innholdsfortegnelse

1	IKT I ASKER KOMMUNE.....	3
1.1	ORGANISERING OG DRIFTSMODELL.....	3
2	ARKITEKTUR OG DIGITALT ØKOSYSTEM.....	3
2.1	Å BYGGE FLEKSIBILITET OG ROBUSTHET I HELHETLIGE LØSNINGER.....	3
2.2	ARKITEKTURPRINSIPPER	3
2.3	SIKKERHETSARKITEKTUR	3
3	IDENTITETS- OG TILGANGSSTYRING	3
3.1	INTERN IDENTITETS- OG TILGANGSSTYRING	4
4	INFRASTRUKTUR.....	4
4.1	REALISERT INFRASTRUKTUR – SYSTEMTEKNISK BESKRIVELSE	4
5	SKYTJENESTER	6
5.1	DATALAGRING	6
5.2	SIKKERHETSKOPIERING/SPEILING.....	6
5.3	DATABEHANDLERAVTALE.....	6
5.4	BRUK AV UNDERLEVERANDØRER	6
6	IKT SERVICE OG VEDLIKEHOLD	6
7	NORM FOR INFORMASJONSSIKKERHET I HELSETJENESTEN (NORMEN).....	7
8	PERSONVERN OG GDPR	7
8.1	PRINSIPPENE OM ANSVAR, INTEGRITET OG KONFIDENSIALITET.....	7
8.2	PERSONVERN OG GDPR - KONSEKVENSER FOR KOMMUNENS LEVERANDØRER.....	7
9	FJERNTILGANG FOR LEVERANDØRER	8

1 IKT i Asker kommune

Asker kommune har etablert en driftsplattform for fagsystemer og andre støttesystemer. Et hovedmål for denne nye IKT-plattformen er å kunne understøtte både tradisjonelle installerte løsninger og skyløsninger på en god måte.

1.1 Organisering og driftsmodell

Asker kommune drifter sin IKT-plattform med egne ansatte som har bred kompetanse innen nødvendige fagområder og moderne IKT-drift. Kort avstand fra bruker til support er viktig for effektivitet og kvalitet i drift og utvikling. Kommunen har også egne utviklingsressurser med erfaring i krevende prosjekter.

2 Arkitektur og digitalt økosystem

2.1 Å bygge fleksibilitet og robusthet i helhetlige løsninger

Asker kommune ønsker å utvikle en moderne arkitektur for å levere effektive innbyggertjenester via digitale plattformer. Vi bruker mange fagsystemer, noen for innbyggerdialog og andre for interne funksjoner. Målet er å tilby et personalisert grensesnitt for innbyggere med tilgang til relevant informasjon og tjenester. Kommunen ønsker også å utnytte data fra disse systemene for å få innsikt i trender. Derfor legger vi vekt på å anskaffe løsninger med åpne og strukturerte grensesnitt for datahåndtering.

Asker kommune ønsker åpne API-er, levert som WebServices eller REST API-er over HTTP, med XML eller JSON som innholdsformat. Autentisering skal være basert på OpenID Connect eller OAuth 2.0, og all kommunikasjon skal være kryptert med HTTPS. Vi foretrekker løsninger med en tjenesteorientert arkitektur, som SOA eller MicroServices, for å sikre høy datakvalitet og uavhengige tjenester. Dette vil gi dem mulighet til å kombinere data fra mange API-er for å forbedre innbyggertjenestene.

2.2 Arkitekturprinsipper

Asker kommune vil bruke konsistente arkitekturprinsipper for alle løsninger for å støtte en helhetlig virksomhetsarkitektur. Disse prinsippene følger anbefalingene fra Digitaliseringsdirektoratet for nasjonal arkitektur.

2.3 Sikkerhetsarkitektur

Asker kommune bygger sin sikkerhetsarkitektur på moderne prinsipper, inkludert NSMs grunnprinsipper for IKT-Sikkerhet og internasjonale standarder som ISO27002:2017. Vi følger prinsippene "Defense-in-depth" og "Trust-no-one", sikrer at alle systemer er konfigurert etter beste praksis, og nettverket er segmentert i sikre soner med dedikerte brannmurer for sensitive data.

3 Identitets- og tilgangsstyring

Med over 8 500 ansatte og 13 000 elever er effektiv tilgangsstyring til kommunens systemer viktig. Kontroll på autentisering, autorisering, roller og rettigheter er

avgjørende for en sømløs arbeidshverdag. I tillegg er det viktig å kunne dokumentere tilgangene fra et revisjonsperspektiv.

Single sign-on er en klar forventning til alle løsninger og fagapplikasjoner.

3.1 Intern identitets- og tilgangsstyring

Asker kommune benytter IDM- og IAM-løsninger for å opprette og synkronisere identiteter, grupper, roller og organisasjons-struktur mellom kataloger, databaser og applikasjoner.

HRM, økonomi og oppvekstadministrativt system (OAS) er viktige grunndatasystemer og blir «master-data» for identiteter, grupper, roller og organisasjons-strukturer. Kommunens kataloger (AD og Entra ID) vil bli bygget basert på data fra disse grunndatasystemene. Ved å bruke disse systemene vil kommunen sikre kontroll på tilganger og ikke minst vil administrasjon av tilganger bli automatisert. En annen viktig gevinst er at data oppdateres et sted og gjenbrukes.

Asker kommune skal samarbeide med «fagmiljøene/sektorene» og fagapplikasjonsleverandører og integrere deres systemer med IDM- og IAM-plattformen for tilordning av tilganger med brukere og roller.

3.1.1 ID-porten

Asker kommune foretrekker ID-porten for autentisering av eksterne brukere/tjenestemottakere, men kan vurdere andre løsninger som oppfyller samme sikkerhetskrav.

4 Infrastruktur

4.1 Realisert Infrastruktur – Systemteknisk beskrivelse

4.1.1 Kommunikasjon

Asker kommune bygger et sentralisert datanettverk som dekker alle tjenestestedene i kommunen, ca. 200 lokasjoner. Disse har oppkobling via både leide (xDSL/fiber) og eide linjer (fiber og radio). Båndbredden varierer mellom 2 Mbps - 20 Mbps (xDSL) og på fiberforbindelse fra 100 Mbps - 10 Gbps.

4.1.2 PC-park

Kommunens PC-park teller ca. 5000 PC-er på administrative nett, hvorav ca. 800 er tynnklienter (wyse thinOS), og ca. 14000 Chromebooks for elever og lærere.

Kommunen vil foretrekke løsninger som ikke krever lokal installasjon på PC, men som i stedet kjøres gjennom nettleser. Dette vil forenkle kommunens drift og vil gjøre det mulig å benytte alternative klientplattformer.

4.1.3 Windows plattform

Operativsystemer baseres på Microsoft Windows. Klienter kjører Windows 10 og Windows 11 (Windows 10 fases ut ila. 2025). Servere baseres på Windows server 2016/2019/2022.

4.1.4 Katalogtjeneste

Asker kommune skal benytte Microsoft Active Directory og Azure Active Directory/Entra ID som katalogtjenester. Katalogtjenestene inneholder alle brukere i Asker kommune og håndterer all pålogging mot nett og ressurser. Se også kapittel 3.1

4.1.5 Krav til sikkerhet

Asker kommune skal jobbe for at systemer får single-sign-on (SSO) ved hjelp av Microsoft Active Directory eller Entra ID/Azure Active Directory. Se også kapittel 2.1

4.1.6 Serverplattform og virtualisering

Datasenterløsning (serverplattform) i Asker kommune lages med utgangspunkt i en ny plattform hvor lokale løsninger og skytjenester skal spille på lag – en hybrid løsning.

Denne todelingen vil i hovedsak bestå av en Microsoft Windows plattform lokalt, bygget på DellEMC VXRail- infrastruktur, og en Microsoft Azure plattform i skyen.

Asker kommune skal benytte virtualiseringsteknologi på serverplattformen. Teknologiene som skal benyttes lokalt er VMware og Citrix.

4.1.7 Databaseteknologi

Asker kommune standardiserer på Microsoft SQL. Databaseservere skal kjøre under Windows 2019 server. Databasene standardiseres på MS SQL 2019 og nyere.

4.1.8 SharePoint / Samhandlingsplattform

Asker kommune skal benytte SharePoint online igjennom sitt Office365 miljø som samhandlingsplattform.

4.1.9 Sikker aksess

Asker kommune vil benytte multi-faktor-autentiseringsløsninger for pålogging fra "usikre nett". Løsninger vil basere seg på standard teknologier som finnes (SMS, App, biometri, smartkort, sertifikat, etc.). Løsningen vil bli benyttet av egne ansatte og eksterne aktører.

4.1.10 Distribuering av programvare

Asker kommune skal benytte teknologi for pakking og distribuering av programvare til PCer. Her benyttes Intune.

4.1.11 Overvåking

Asker kommune benytter Whatsup og PRTG til overvåking av applikasjoner og infrastruktur.

4.1.12 Datalagring og sikkerhetskopiering

Asker kommune benytter hyperkonvergent infrastruktur i sitt datasenter. Sikkerhetskopi blir tatt og lagret iht. gjeldende interne regler og rutiner.

4.1.13 Kontorstøtteapplikasjoner

Asker kommune benytter Office365 på PCer med Windows 10/Windows 11. Epost er tilgjengelig via Office365.

4.1.14 Utskriftstjenester

Asker kommune benytter sikker print/follow-me fra Canon (Canon Uniflow) for utskrift.

5 Skytjenester

5.1 Datalagring

Vi ønsker at en leverandør av skytjenester fortrinnsvis lagrer data i Norge, alternativt EU/EØS.

5.2 Sikkerhetskopiering/speiling

Leverandører som vil overføre personopplysninger til utlandet må følge bestemmelsene i personopplysningsloven.

5.3 Databehandleravtale

Det er den behandlingsansvarlige som velger å ta i bruk skytjenesten. Hvis tjenesten gjennomfører en behandling på vegne av den behandlingsansvarlige, er leverandøren å anse som en databehandler. Datatilsynet anser derfor en leverandør av skytjenester som en databehandler, uavhengig av hvilken tjeneste som leveres.

Det skal dermed skrives en databehandleravtale når det tas i bruk skytjenester, uavhengig av tjenestens innhold.

Databehandleravtale skal veie tyngre enn leverandørens eventuelle personvernerklæring

5.4 Bruk av underleverandører

Underleverandører skal være kjent og godkjent av virksomheten. Dette relaterer til problemstillingen over om hvor data lagres og om det overføres data til tredjeland.

6 IKT Service og vedlikehold

Asker kommune har IKT-prosesser for tjenesteleveranse og styring. Fagapplikasjons- og driftsleverandører bistår ved feilsøking og planlegging. Leverandører skal levere konfigurasjonsdata til kommunens CMDB. Kommunen ønsker å være oppdatert om endringer i alle systemer for å informere brukere om feilrettinger og funksjonalitetsendringer.

7 Norm for informasjonssikkerhet i helsetjenesten (Normen)

Alle fagsystemer som benyttes til behandling av helse- og personopplysninger i helse- og omsorgstjenesten, f.eks. elektronisk pasientjournal, pasientadministrasjon, laboratoriesystem, rekvisisjon og svar og elektromedisinsk utstyr som inneholder helse- og personopplysninger er underlagt kravene i «Norm for informasjonssikkerhet».

8 Personvern og GDPR

System som behandler personopplysninger i Asker kommune skal følge de til enhver tids gjeldende krav i personopplysningsloven, inklusive GDPR.

Det er derfor viktig at de fagsystemer kommunen anskaffer har godt innebygget personvern og således behandler sensitive personopplysninger i henhold til forordningen.

Hvordan hvert enkelt system, både fagsystemer og støttesystemer behandler personopplysninger og hvilke, må dokumenteres.

8.1 Prinsippene om ansvar, integritet og konfidensialitet

Et av de viktige prinsippene for det nye personvernregelverket er at det er virksomheten som bruker personopplysningene som har ansvar for at personvernprinsippene overholdes. Dette innebærer at virksomheten skal kunne vise at de behandler personopplysninger i tråd med personvernprinsippene.

Behandlingsansvarlig skal blant annet å sørge for tilstrekkelig og forholdsmessig sikkerhet, at personopplysningene er sikret mot uautorisert eller ulovlig behandling eller utilsiktet tap, ødeleggelse eller skade.

Dette er nedfelt i artikkel 5 i det nye regelverket.

Forskjellen fra dagens regelverk er at det blir mindre forhåndskontroll ved at melde- og konsesjonspliktene forsvinner. Men det er også en viktig endring at ansvaret blir plassert hos virksomheten. Det kommer flere og til dels tydeligere rettigheter og plikter, og det blir krav om å iverksette risikobaserte tiltak. Mer etterkontroll kan medføre strengere sanksjoner om man ikke har «orden i eget hus».

Dette er regulert i artikkel 25 om innebygd personvern, artikkel 35 om vurdering av personvernkonsekvenser og artikkel 36 om forhåndsdrøftelse.

8.2 Personvern og GDPR - Konsekvenser for kommunens leverandører

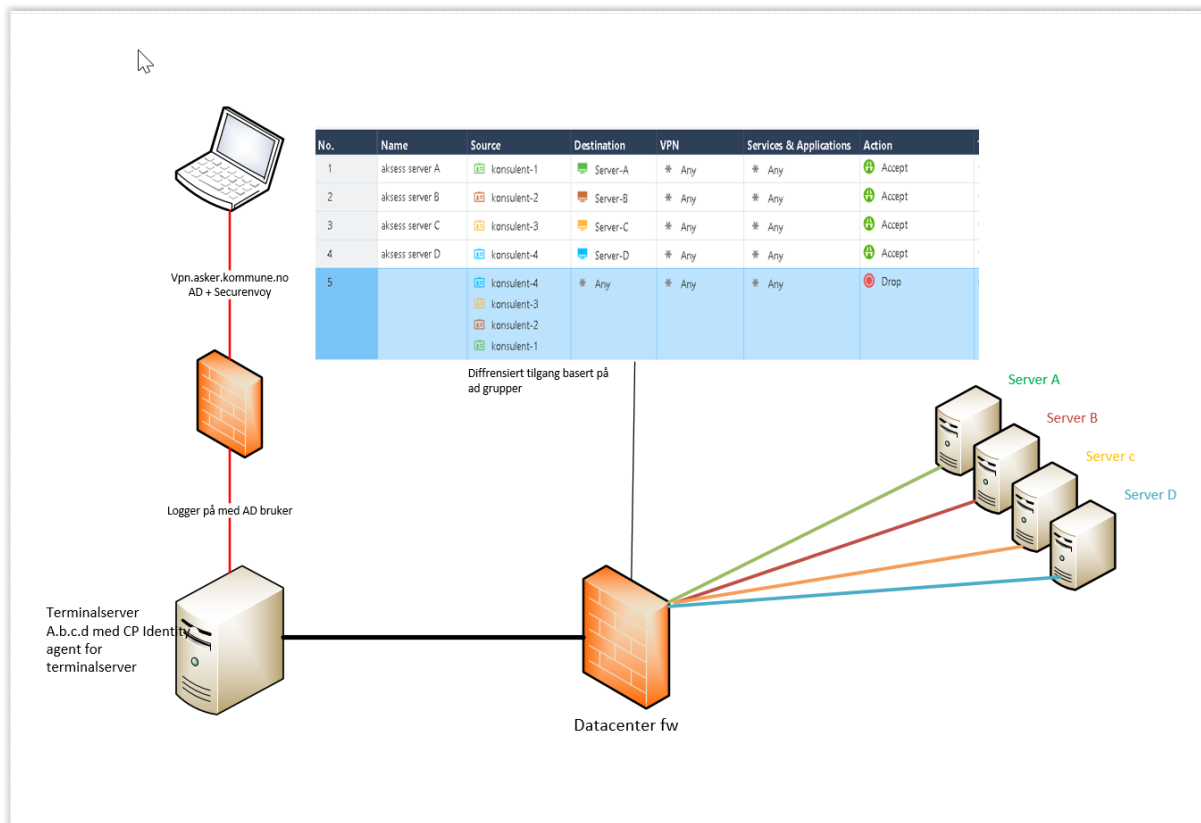
Asker kommunes leverandører må kunne dokumentere hvordan personopplysninger brukes og lagres i hvert spesifikt fagsystem. Dette gjelder også hvordan personopplysninger blir kommunisert inn og ut av systemet.

Kravene til avviksbehandling, varsling av berørte skjerpes i det nye regelverket, og som en konsekvens må kommunens leverandører eksplisitt beskrive hvordan avvikshåndtering utføres.

En godt definert databehandleravtale vil bli påkrevd i et hvert leverandørforhold for systemer som behandler personopplysninger.

9 Fjerntilgang for leverandører

For fjerntilgang inn til systemer med div sensorikk/styring som f.eks SD-anlegg, adgangskontrollanlegg, sykesignalanlegg osv, er det krav om VPN-oppkobling med to-faktorsautentisering



For fjerntilgang til andre generelle IT-systemer brukes enten samme metode som over, eller remote tilgang via Citrix påloggingsportal.

Oppkobling til begge disse løsningene avtales med IKT.