



id: SI_008

model: anthropic/claude-opus-4.6

seeds:

04_risiko: usikkerhet

03_relasjon: makt

05_handling: vent

01_perspektiv: juridisk

02_tidhorisont: kortsiktig

Instans SI_008

Seeds: juridisk | kortsiktig | makt | usikkerhet | vent

Dissens: Dere bør ikke innføre agentisk KI nå.

Mitt perspektiv er ubehagelig men nødvendig: **vent**.

Maktkonsentrasjon uten juridisk fundament

En autonom agent som endrer data, trigger hendelser og kaller tredjeparts-API-er utøver makt — forvaltningsrettslig, operasjonelt og informasjonsmessig. I en offentlig virksomhet er maktutøvelse bundet av legalitetsprinsippet. Per i dag finnes det **ingen norsk lovhjemmel** som eksplisitt regulerer autonome agents rett til å fatte eller iverksette beslutninger med rettsvirkning. EU AI Act artikkel 6/26 klassifiserer offentlig sektorbruk som høyrisiko, med krav (conformity assessment, human oversight, logging) dere ikke kan oppfylle innen 6–9 måneder gitt nåværende modenhet.

Usikkerheten er strukturell, ikke taktisk

Dere mangler ikke én ting — dere mangler **fem fundamentale lag samtidig**: sentralisert policy-motor, Zero Trust, konsolidert audit, safe execution environments, og finmasket IAM. Å bygge disse parallelt med en agentisk pilot er ikke ambisiøst — det er hasard. Usikkerheten forsterkes av legacy-monolitter uten deterministiske API-kontrakter: agenten opererer i et landskap der dere selv ikke fullt ut kjenner sideeffektene av API-kall.



Kortsiktig gevinst, langsiktig juridisk gjeld

Pilotvinduet på 6–9 måneder tvinger frem snarveier. Typisk resultat: brede service accounts, manglende rollback, logging som «fikses etterpå». Hver snarvei blir **juridisk gjeld** — revisjonsfunn, Datatilsynet-pålegg, eller verre: en agent som endrer vedtaksdata i et fagsystem uten sporbar begrunnelse. Forvaltningsloven §§ 24–25 krever etterprøvbar begrunnelse. Hvordan begrunner en agent som har traversert 14 API-kall?

Emergent behavior i et svakt regime

Worst-case er ikke at agenten gjør noe galt. Worst-case er at agenten gjør noe **som ser riktig ut** — men via en uforutsett koblingskjede (latent coupling) endrer data i et integritets-kritisk system, uten at noen oppdager det før virkningen materialiserer seg uker senere. Uten event-sourcing har dere ingen forensic-kapasitet.

Konkrete neste steg

1. **Sett piloten på pause i 3 måneder.** Bruk tiden på å etablere minimums-fundament: deploy OPA som sentralisert policy-motor, implementér konsolidert audit-pipeline (ELK/OpenTelemetry), og gjennomfør juridisk vurdering opp mot forvaltningsloven og EU AI Act.
2. **Start med en «agent-simulator» — ikke en ekte agent.** La den foreslå handlinger i et skygge-modus (human-in-the-loop for alle steg) i 8 uker. Logg alt. Analyser emergent behavior-mønstre før dere gir den autonomi.
3. **Bestill en makt- og legalitetsanalyse** fra juridisk avdeling eller eksternt (f.eks. NIDS/IKT-Norge-miljøet): Hvilke handlinger agenten vil utføre utgjør myndighetsutøvelse? Svaret avgjør alt.

Kjernebudskap: Usikkerhet er ikke et problem å løse med mer teknologi — det er et signal om å vente til fundamentet tåler vekten.