



id: SI_007

model: openai/gpt-5.4-mini

seeds:

04_risiko: mulighet

03_relasjon: tillit

05_handling: utforsk

01_perspektiv: strategisk

02_tidhorisont: historisk

Instans SI_007

Seeds: strategisk | historisk | tillit | mulighet | utforsk

Magnus bør ikke velge mellom “kjør” og “vent”, men mellom **ukontrollert pilot** og **styrt læringsløp**. I kommunal praksis er den forsvarlige tredjeveien ofte: **trinnsvis avgrenset pilot med eksplisitt beslutningsspor**.

1) Risikostyring i grånyanser

Kategoriser usikkerhet i fire bokser:

- **R1: Avklart** – dokumentert akseptabelt.
- **R2: Tolkbar** – juridisk/sikkerhetsmessig uenighet, men håndterbar med tiltak.
- **R3: Vesentlig usikker** – krever politisk eksplisitt aksept.
- **R4: Uakseptabel** – stopp.

Lag en enkel **risikomatrise med tiltak, rest-risiko og beslutningstaker**. “Akseptert risiko” blir forsvarlighet når den er: **bevisst, begrenset, tidsavgrenset, dokumentert, og forankret i riktig nivå** (ledergruppe/politisk nivå, ikke bare CDO).

2) Ansvar og dokumentasjon

Krev en **trefoldig beslutningsprosess**:

1. Juridisk notat: hva er uavklart + hvilke forutsetninger gjelder.
2. Sikkerhetsvurdering: hvilke kontroller som må på plass.
3. Felles beslutningsnotat: hva som aksepteres, av hvem, til hvilken dato.



Bruk et møte med **juridisk + sikkerhet + fag + ledelse** og avslutt med signert beslutningslogg. Unngå “råd uten eier”.

3) Kontraktskrav mot leverandør

Krev ikke garanti for “compliance”; krev:

- **DPA/databehandleravtale** med underleverandørkontroll
- **Revisjonsrett** og dokumentasjonsinnsyn
- **Varslingsplikt** ved avvik/endrede modellvilkår
- **Sletting/retur** ved avslutning
- **Ansvarsfordeling for sikkerhetsbrudd**
- **Klausul om modell-/tjenesteendringer** utenfor formål krever ny godkjenning
- **Egne testmiljøer / ingen trening på kommunale data uten særskilt avtale**

4) Absolutt minimum for pilot

- Begrenset datamengde, lavrisiko-brukstilfelle
- Ingen automatiserte vedtak; kun beslutningsstøtte
- Manuell kontroll før utadrettet bruk
- Logging, tilgangsstyring, sletting, hendelsesplan
- Tidsavgrensning: 8–12 uker
- Predefinerte stoppkriterier

5) Politisk språk

Si: **“Dette er ikke et ja/nei-spørsmål, men et valg mellom risiko, fart og læring.”** Be politisk ledelse ta stilling til **hva som kan aksepteres**, ikke skyve det ned til deg.

6) Midtveisstrategi

Gjør en **pilot med “sandkasse + menneskelig kontroll + evalueringsport”**. Det gir noe å vise nå, samtidig som juridisk avklaring kan modnes.

Kjente kommunale mønstre: Bergen/Oslo/Flere kommuner har brukt begrensede AI-piloter i support, saksforberedelse og intern informasjonsgjenfinning før full produksjon—typisk med streng avgrensning og styringsgruppe.



Neste steg

1. Sett opp et 60-min beslutningsmøte med juridisk, sikkerhet og linjeledelse.
2. Lag én side risikomatrise + stoppkriterier for piloten.
3. Be politisk nivå velge mellom tre alternativer: vente, begrenset pilot, eller bred utrulling.