



id: SI\_008

model: google/gemma-4-26b-a4b-it

seeds:

04\_risiko: sårbarhet

03\_relasjon: tillit

05\_handling: vent

01\_perspektiv: operasjonell

02\_tidhorisont: kortsiktig

## Instans SI\_008

**Seeds:** operasjonell | kortsiktig | tillit | sårbarhet | vent

### Diagnose: Den asymmetriske risiko-illusjonen

Motstanden er ikke teknologisk, men en kombinasjon av **operasjonell bekvemmelighet** og en dyp, ubevisst **sårbarhet** for det som ikke kan måles i sanntid.

**1. Gapet mellom bevissthet og handling (Kortsiktig opportunisme)** Jurister opererer i et regime av kortsiktig effektivitet. Å mate en klientkonfidensiell kontrakt inn i ChatGPT er en operasjonell snarvei som gir umiddelbar gevinst (tidsbesparelse). Risikoen (GDPR-brudd eller tap av privilegium) er en abstrakt, fremtidig hendelse. De vet om risikoen, men de bagatelliserer den fordi den ikke stopper dagens fakturering. De venter på at en "skandale" skal definere normen, ikke på at regelverket skal forklare den.

**2. Tillitsparadokset (Teknisk vs. Psykologisk)** Det er et gap mellom teknisk proof of concept (at data ikke lagres) og juridisk assurance. En advokat stoler ikke på koden; de stoler på ansvars plassering. SikkerKI må ikke selge "sikker compute", de må selge "ansvarsfraskrivelse". Den psykologiske barrieren er: "Hvis jeg bruker SikkerKI og det feiler, hvem saksøker jeg? Hvis jeg bruker ChatGPT og det feiler, kan jeg skylde på teknologisk uforutsigbarhet."

**3. Sosiale drivere og leverage-punkter** Adopsjon skjer ikke via pedagogikk, men via **forsikring og klientkrav**.

- **Leverage:** Det som faktisk flytter dem er ikke Datatilsynet (for langsomt), men at forsikringsselskaper (f.eks. Gjensidige/Tryg) endrer vilkårene for ansvarsforsikring ved bruk av usikre KI-verktøy, eller at store klienter (Equinor, Statkraft) krever en spesifikk "AI-sikkerhets-audit" av sine rådgivere.



#### 4. Skarpe dilemmaer (Trade-offs)

- **Feature-paritet vs. Sikkerhet:** Brukeren vil ha Claude 3.5 Sonnets intelligens, men vil ha den i en “sandkasse”. Hvis SikkerKI er 10 % tregere eller mangler én integrasjon, vinner ChatGPT hver gang i det operasjonelle øyeblikket.
- **Kontroll vs. Friksjon:** Jo mer sikkerhet (on-prem/lukkede miljøer), desto mer friksjon i arbeidsflyten.

#### Konkrete neste steg

1. **Skift narrativ:** Slutt å snakke om “datasikkerhet”. Begynn å snakke om “beskyttelse av advokatprivilegiet og forsikringsbetingelser”.
2. **Operasjonell integrasjon:** Eliminer friksjon ved å tilby “Zero-Config” løsninger som fungerer som en browser-extension eller et lag over eksisterende verktøy, slik at den kortsiktige gevinsten er identisk med åpne modeller.
3. **Trigger-punkt:** Utvikle en “Compliance Check”-rapport som jurister kan sende direkte til sine klienter for å bevise at de bruker SikkerKI – gjør sikkerhet til et salgsargument for advokaten.