



id: SI_002

model: openai/gpt-5.4-mini

seeds:

04_risiko: usikkerhet

03_relasjon: tillit

05_handling: vent

01_perspektiv: operasjonell

02_tidhorisont: kortsiktig

Instans SI_002

Seeds: operasjonell | kortsiktig | tillit | usikkerhet | vent

Den reelle barrieren er sjelden **manglende forståelse av risiko**. De fleste juridiske profesjonelle skjønner intuitivt at klientdata ikke bør flyte fritt til åpne LLM-er. Problemet er mer operasjonelt og kortsiktig: **risikoen er diffus, gevinsten er umiddelbar, og konsekvensen oppleves som ventende** — altså noe som kanskje skjer senere, med lav sannsynlighet og uklart ansvar.

1) Bevissthet vs. handling

Gapet ligger i at folk vet nok til å være urolige, men ikke nok til å endre vane. Det blir en **stiltiende aksept**: “Jeg bruker bare anonymiserte tekstbiter”, “alle andre gjør det”, “vi har ikke hatt en sak ennå”. Dette er ikke uvitenhet, men **normalisering av usikkerhet**.

2) Tillit til teknologien

SikkerKI møter høyere tillitskrav enn ChatGPT fordi den må bevise et negativt: at data **ikke** lekker, logges eller brukes videre. Standardverktøy får gratis tillit via kjent merke, mens sikker løsning må levere **verifiserbar kontroll**. For jurister er “blind compute” bare troverdig hvis det er konkret: norsk/EØS-drift, loggkontroll, revisjonsspor, databehandleravtale, tydelig modellarkitektur.



3) Regulatorisk press

GDPR, taushetsplikt og advokatetikk er sterke på papiret, men svake som drivere fordi håndhevingen oppleves som **ventende**. Mange antar at Datatilsynet ikke kommer først på dem, og at risikoen først blir reell ved avvik. Det skaper passivitet. I Norge er det dessuten mye **ansvarsdeling**: partner, firma, IT, compliance — alle venter på at noen andre skal definere normen.

4) Sosial dynamikk

Adopsjon styres mer av **bransjestandard enn av regeltekst**. Hvis konkurrenten bruker åpne verktøy uten synlige konsekvenser, blir sikker KI lett et kostnadsprosjekt, ikke et krav. Det som kan vippe normene er ikke propaganda, men **signalhendelser**: klientkrav, forsikringsvilkår, eller at et toneangivende firma publiserer egen policy.

5-6) Pris og byttebarrierer

Den synlige kostnaden ved SikkerKI er onboarding, integrasjon, tregere arbeidsflyt og usikker feature-paritet. Den usynlige kostnaden ved å ikke bytte er større: tap av klienttillit, due diligence-problemer, fremtidige krav fra store oppdragsgivere. Men den kostnaden er for “ventende” til å vinne i dag.

Leverage-punkter

1. Gjør risiko operasjonell: konkrete scenarioer, ikke abstrakt compliance.
2. Gjør tillit verifiserbar: tekniske garantier + ekstern attestasjon.
3. Gjør bytte sosialt normalt: referansefirmaer, klientkrav, forsikring.

Neste steg:

- Kartlegg 10 norske firmaers faktiske AI-praksis og deres uuttalte risikologikk.
- Test hvilke bevis på sikkerhet som faktisk endrer tillit: revisjon, sertifisering, norsk drift, kontrakt.
- Identifiser én “trigger” per målgruppe: klientkrav, forsikringspremie eller intern policy.