



id: SI_006

model: openai/gpt-5.4-mini

seeds:

04_risiko: mulighet

03_relasjon: makt

05_handling: implementer

01_perspektiv: juridisk

02_tidhorisont: historisk

Instans SI_006

Seeds: juridisk | historisk | makt | mulighet | implementer

Den egentlige barrieren er **ikke primært uvitenhet**, men **styringsvakuum**. Mange norske jurister vet nok til å ane risiko, men ikke nok til å føle personlig konsekvens. Da blir standard-LLM-bruk en akseptert gråson: “alle gjør det”, “vi har ikke fått et forbud”, “det går sikkert bra”. Historisk ser vi dette i profesjoner med taushetsplikt: praksis endres først når norm, revisjon eller sanksjon gjør risikoen konkret.

1) Bevissthet vs. risiko

Gapet ligger mellom generell bekymring og operasjonell handling. De vet at klientdata ikke bør inn i åpne modeller, men de undervurderer ofte at også metadata, promptinnhold og dokumentfragmenter kan utløse pliktbrudd. Handling skjer når risiko blir knyttet til **personlig ansvar**, ikke abstrakt compliance.

2) Tillit til teknologien

Skepsisen mot SikkerKI handler mindre om kryptering og mer om **makt over usikkerhet**: “Kan jeg bevise at dette ikke lekker?” Standardverktøy tolereres fordi ansvaret er diffust og friksjonen lav. SikkerKI møter høyere beviskrav fordi den ber dem bytte vane og stole på en ny kontrollflate. On-prem/EU-sikker compute må derfor dokumenteres som **reviderbar praksis**, ikke bare som løfte.

3) Regulatorisk press

GDPR og taushetsplikt virker svakt fordi de oppleves som **sjeldent håndhevet**. Datatilsynet har høy symbolmakt, men lav daglig sanksjon. Uten konkrete tilsynssaker eller forsikringskrav blir det “mulig, men ikke påkrevd”. First-mover-frykt er reell: ingen vil være den første som bruker tid og penger uten å få konkurransefordel.

4) Sosial dynamikk

Bransjen styres av normativ etterligning. Hvis ledende byråer bruker åpne verktøy, blir det de facto standard. For at sikker KI skal bli normalt, må den kobles til **prestisje og**



profesjonalitet: “seriøse aktører beskytter klientdata.” Ikke moraliser; gjør det til tegn på modenhet.

5) Pris og friksjon

Kostnaden ved å ikke bytte er latent men stor: klientmistillit, revisjonskritikk, forsikringspremier, og i verste fall brudd på taushetsplikt. Men byttebarrieren er umiddelbar: integrasjon, opplæring, hastighet, feature-gap, og frykt for at verktøyet blir en ny IT-flaskehals.

6) Konkrete byttebarrierer

Det som stopper dem er ofte ikke vilje, men **arbeidsflyt**: Word/Outlook-integrasjon, dokumenthåndtering, sakssystem, tilgangsstyring, loggføring. Hvis SikkerKI ikke løser deres faktiske brukstilfeller, blir sikkerhet en teoretisk fordel.

Mulighetsrom: gjør sikker KI til standard i de mest sensitive oppgavene først: due diligence, kontraktsutkast, intern research, klientfiler.

Neste steg:

1. Lag 3–5 norsk-juridiske “risiko-scenarier” med ansvarskonsekvens, ikke bare policytekst.
2. Pakk SikkerKI inn i arbeidsflyt-integrasjoner som reduserer friksjon til nær null.
3. Bruk revisjon, forsikring og klientkrav som presspunkt — ikke bare teknisk argumentasjon.