



id: SI\_001

model: openai/gpt-5.4-mini

seeds:

04\_risiko: sårbarhet

03\_relasjon: makt

05\_handling: forhandle

01\_perspektiv: strategisk

02\_tidhorisont: langsiktig

## Instans SI\_001

---

**Seeds:** strategisk | langsiktig | makt | sårbarhet | forhandle

Den reelle adopsjonsbarrieren er trolig ikke først og fremst **kunnskap**, men **maktbalanse og friksjon**. Juridiske profesjonelle vet ofte at standard-KI er risikabelt, men de **forhandler med risikoen i praksis**: “Ingen klager”, “alle gjør det”, “vi må være raske”, “det blir nok ikke et tilsyn”. Det er en strategisk rasjonalisering, ikke bare uvitenhet.

**1) Bevissthet vs. risiko** Gapet ligger i at risikoen oppleves som **asymmetrisk og diffus**: Gevinsten ved KI er umiddelbar, mens skade ved brudd på taushetsplikt er lav sannsynlighet, høy konsekvens, og ofte utsatt i tid. Det gjør handling vanskelig. For å endre adferd må risikoen bli **operasjonell**: konkrete scenarier, klientkrav, interne rutiner, og tydelig ansvarslinje fra ledelsen.

**2) Tillit til teknologien** Mange stoler mer på “store” leverandører enn på sikkerhetsgarantier i on-prem/EU-løsninger, fordi de vurderer **merkenavn som en maktsignatur**. SikkerKI må derfor ikke bare være sikker; den må være **etterprøvbar**. Norsk juridisk målgruppe vil ofte kreve: datalagringskart, loggkontroll, modellgrenser, revisjonsspor, og klar kontraktsfesting. Uten dette blir “blind compute” oppfattet som en påstand, ikke en garanti.

**3) Regulering som brems** Datatilsynet og GDPR skaper mer **forsiktighetsretorikk** enn faktisk endring, fordi konsekvensen oppleves fjern og håndhevingen ujevn. Advokatvirksomhet har dessuten et klassisk **first-mover-problem**: Ingen vil være den første som bruker penger på sikkerhet hvis markedet ikke belønner det.

**4) Sosial norm** Adopsjon følger bransjesignaler. Hvis konkurrenter bruker åpne modeller, blir sikkerhet en kostnad uten statusgevinst. For at SikkerKI skal bli “normalt”, må det kobles til **standardverk**: klientpolicyer, forsikringskrav, og felles praksis i advokat-/revisjonsmiljøer.



**5) Pris og friksjon** Den største skjulte kostnaden er ikke lisenspris, men **byttefriksjon**: integrasjoner, vane, manglende feature-paritet, og utydelig ansvar. Mange vil betale mer for sikkerhet, men ikke for å jobbe tregere.

**6) Konkrete byttebarrierer** Det som stopper de mest motiverte er ofte: e-post/Word-integrasjon, søk i dokumenter, kvalitet på norsk juridisk språk, og usikkerhet om hvem som “eier” risikoen internt.

### Leverage-punkter

- Klientkrav: standard klausuler om KI-håndtering i oppdragsbrev
- Forsikring: vilkår/rabatt knyttet til sikker KI-bruk
- Revisjon: dokumenterbar policy og loggkontroll
- Bransjenorm: felles minimumsstandard for taushetsplikt og KI

### Neste steg

1. Kartlegg 10–15 norske firmaer: hvor ligger faktisk motstand i workflow, styring eller tillit?
2. Lag en “ansvars- og risiko-pakke” som oversetter GDPR/taushetsplikt til beslutningsspråk for partnere.
3. Reduser friksjon i 2–3 kritiske arbeidsflyter først, ikke hele produktet.