



id: SI\_006

model: anthropic/claude-opus-4.6

seeds:

04\_risiko: mulighet

03\_relasjon: tillit

05\_handling: implementer

01\_perspektiv: strategisk

02\_tidhorisont: kortsiktig

## Instans SI\_006

**Seeds:** strategisk | kortsiktig | tillit | mulighet | implementer

### Diagnose: Tillitsparadokset er kjerneproblemet

Norske advokater har **null tillit til at noe er 100% sikkert** — det er selve yrkesdeformasjonen. De dissekerer risiko profesjonelt. Paradokset: denne samme skepsisen rettes hardere mot SikkerKI enn mot ChatGPT. Hvorfor? Fordi ChatGPT brukes som et **uformelt verktøy** (mentalt kategorisert som “Google-søk”), mens SikkerKI presenterer seg som en **formell sikkerhetsløsning** — og dermed inviterer til formell granskning. Jo høyere løfter, desto strengere kravene.

**Det reelle gapet er ikke bevissthet om risiko. Det er fravær av konsekvens.** Ingen norsk advokat har mistet bevillingen pga. ChatGPT-bruk. Ingen klient har reist krav. Datatilsynet har ikke sanksjonert. Så lenge konsekvensen er null, er risikoen teoretisk — og jurister er trent til å skille teoretisk fra aktuell risiko.

### Kortsiktig mulighetsvindu

Akkurat nå finnes et **strategisk vindu**: Advokatforeningens veileder om KI (2024), Datatilsynets skjerpede oppmerksomhet, og EU AI Act-implementering. Men vinduet lukkes raskt — fordi bransjen konsoliderer seg rundt “good enough”-løsninger (Microsoft Copilot med Entra-innpakning). Copilot blir den ufarlige defaulten, ikke fordi den er sikker nok, men fordi **ingen får sparken for å velge Microsoft**.



---

## Implementerbare angrepsvinkler

**1. Ikke selg sikkerhet — selg forsikring mot det første tilfellet.** Den dagen Datatilsynet tar en sak, eller en klient krever dokumentasjon på databehandling, vil alle ønske de hadde byttet. SikkerKI må posisjoneres som **forhåndsdokumentert compliance** — en databehandleravtale som faktisk tåler granskning, ikke en teknologiplattform.

**2. Utnytt klientpress som brekkstang.** Større bedriftsklienter (finans, energi, helse) begynner å stille krav i engasjementsbrev om hvordan advokaten behandler data. Én konkret handling: hjelp tre store klienter med å formulere slike krav. Da snur presset — fra push til pull.

**3. Fjern byttebarrieren totalt for de første 90 dagene.** Den reelle friksjonen er ikke pris, men vaneendring. Implementer en løsning der SikkerKI kjører **parallelt** med eksisterende verktøy — samme interface, samme prompter, men med logging som viser hva som ville blitt sendt til tredjepart. Gjør risikoen synlig uten å kreve umiddelbart bytte.

---

## Skarpt dilemma

Tillitskravet er asymmetrisk og kanskje uløselig på kort sikt: advokater krever **beviselig sikkerhet** fra SikkerKI, men aksepterer **antatt usikkerhet** fra ChatGPT. Å forsøke å bevise sikkerhet 100% inviterer til flere spørsmål. Alternativet: slutt å argumentere for perfeksjon, og argumenter for **dokumenterbar forbedring**.

---

## Tre konkrete neste steg

- 1. Denne måneden:** Få Advokatforeningens teknologiutvalg til å publisere en konkret sjekkliste for KI-databehandling — der SikkerKI-modellen oppfyller punktene og standard ChatGPT ikke gjør. Normering, ikke markedsføring.
- 2. Innen Q3:** Inngå avtale med 2-3 store bedriftsklienter (typisk Equinor, DNB, Statkraft-segmentet) om å inkludere KI-databehandlingskrav i sine advokatinstrukser. Klientkrav trumfer alt.
- 3. Innen 30 dager:** Lanser en gratis “risiko-audit” — et 10-minutters verktøy der advokatfirmaer kan se nøyaktig hvilke data deres nåværende KI-bruk eksponerer. Gjør den usynlige risikoen synlig og konkret, uten å kreve kjøpsbeslutning.