



id: SI\_006

model: mistralai/mistral-large-2512

seeds:

04\_risiko: sårbarhet

03\_relasjon: konkurranse

05\_handling: vent

01\_perspektiv: operasjonell

02\_tidhorisont: kortsiktig

## Instans SI\_006

---

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

---

### Diagnose: Hvorfor SikkerKI ikke adopteres

Den reelle barrieren er **kortsiktig operasjonell bekvemmelighet** som overstyrer **langsiktig sårbarhet**. Juridiske profesjonelle er ikke naive – de vet risikoen, men aksepterer den fordi:

1. **Konkurransepresset er øyeblikkelig:** Klienter forventer raske svar, konkurrenter leverer med ChatGPT, og tidsmarginene er knappe. SikkerKI oppleves som en operasjonell friksjon – tregere, dyrere, mindre intuitivt.
  2. **“Vent-og-se”-mentaliteten:** Bransjen venter på at noen andre skal bli rammet først (Datatilsynet-aksjon, lekkasje, klagesak). Sårbarheten føles teoretisk – til den blir konkret.
  3. **Tillit til teknologi er relativ:** De stoler mer på Microsoft/OpenAI (fordi de er “store”) enn på SikkerKI (som oppleves som en ukjent, mindre robust aktør). Psykologisk er det tryggere å feile sammen med alle andre enn å feile alene med en “sikker” løsning.
  4. **Regulatorisk tvetydighet:** Datatilsynet har ikke slått ned på KI-bruk ennå – og advokater tolker manglende handling som stilltiende aksept. “Hvis det var ulovlig, hadde de stoppet oss allerede.”
-



## Leverage-punkter: Hva ville tvinge bytte?

### 1. Klientkrav som trigger handling

- Konkret eksempel: En stor bedriftsklient (f.eks. Equinor, DNB) krever i kontrakten at advokatfirmaet ikke bruker tredjeparts-KI for deres saker. Dette ville umiddelbart endre kostnadsberegningen – tap av klient vs. kostnad ved SikkerKI.
- Angrepsvinkel: SikkerKI bør samarbeide med forsikringsselskaper (f.eks. Gjensidige) for å tilby rabatterte cyberansvarsforsikringer til firmaer som bruker godkjente løsninger.

### 2. Datatilsynet som “trigger-hendelse”

- Nå: Taushet. Snart: En konkret pålegg mot et advokatfirma for KI-bruk (f.eks. for brudd på GDPR art. 32 om “passende tekniske tiltak”).
- Angrepsvinkel: SikkerKI kan lage en simulert Datatilsyns-rapport som viser hva som ville skjedd hvis en klients data ble lekket via ChatGPT – med konkrete bøter og medieoppslag.

### 3. Sosial norm som skifter retning

- Nå: “Alle bruker ChatGPT, så det må være greit.” Snart: “De som ikke bruker SikkerKI, blir sett på som uansvarlige.”
- Angrepsvinkel: SikkerKI må få en stor aktør (f.eks. BAH, Thommessen) til å gå foran – ikke som “pilot”, men som offisiell policy. Presset vil komme nedenfra: yngre advokater som nekter å risikere karrieren sin.

### 4. Operasjonell friksjon redusert til null

- Problem: SikkerKI oppleves som en “ekstra” løsning, ikke en erstatning. Brukerne må logge inn et nytt system, lære nye prompts, akseptere tregere respons.
- Løsning: **API-integrasjon** som gjør SikkerKI usynlig. Eksempel: En plugin i Outlook som automatisk ruter sensitive e-poster til SikkerKI for oppsummering – uten at brukeren trenger å tenke på det.

---

## Dilemmaer (ingen enkle løsninger)

- **Feature-paritet vs. sikkerhet:** SikkerKI kan aldri matche ChatGPT i bredde – men må den det? Kanskje løsningen er å begrense bruksområder (f.eks. kun for klientdata, ikke generell research).
- **Pris vs. risiko:** Advokater vil ikke betale for sikkerhet de ikke føler de trenger. Men hva om SikkerKI tilbyr gratis prøveperiode – med en simulert lekkasje som avslutning? (“Her er hva som ville skjedd med dine data i ChatGPT.”)



- **First-mover-risiko:** Den første advokaten som krever SikkerKI kan miste kunder til konkurrenter. Løsningen? Kollektiv handling – f.eks. en bransjeavtale initiert av Advokatforeningen.
- 

## Neste steg (konkrete handlinger)

### 1. Trigger en “sårbarhetsdemonstrasjon”

- Lag en fiktiv (men realistisk) nyhetssak: “Advokatfirma X bøtelagt med 4% av omsetning etter at klientdata lekket via ChatGPT”. Send den til 50 norske advokatfirmaer med spørsmålet: “Kunne dette vært dere?” Mål responsen.

### 2. Få en “anker klient” til å kreve SikkerKI

- Identifiser en bedriftsklient som allerede har strenge krav til eksterne rådgivere (f.eks. en bank eller energiselskap). Tilby dem å sponse en pilot hos deres faste advokatfirma – med krav om at SikkerKI brukes for deres saker.

### 3. Gjør SikkerKI til “standardvalget” i eksisterende verktøy

- Partner med en juridisk programvareleverandør (f.eks. Visma, Wolters Kluwer) for å integrere SikkerKI som default i deres løsninger. Brukerne vil ikke engang merke at de bytter – bare at “noe er litt tregere, men tryggere”.
- 

**SI\_006 avslutter:** Kortsiktig bekvemmelighet vinner alltid – inntil sårbarheten blir operasjonell. Nøkkelen er å gjøre risikoen umiddelbar og byttet usynlig.