



id: SI_005

model: anthropic/claude-opus-4.6

seeds:

04_risiko: sårbarhet

03_relasjon: makt

05_handling: forhandle

01_perspektiv: strategisk

02_tidhorisont: kortsiktig

Instans SI_005

Seeds: strategisk | kortsiktig | makt | sårbarhet | forhandle

Diagnose: Et maktspill der sårbarheten er skjult bak kortsiktig komfort

Den reelle barrieren er ikke uvitenhet — det er en **strategisk kalkulasjon der kortsiktig gevinst trumfer langsiktig sårbarhet**, fordi makten til å definere konsekvensene ligger hos aktører som ennå ikke har slått til.

Kjerneproblemet er forhandlingsposisjonen. Norske advokater opererer i et stilltiende forhandlingsrom med fire parter: klienter, Datatilsynet, forsikringsselskaper og konkurrenter. Ingen av disse har ennå stilt ultimatum. Dermed er status quo den rasjonelle kortsiktige strategien. Å bytte til SikkerKI er en ensidig innrømmelse i en forhandling ingen har startet.

Sårbarhetens paradoks

Advokater forstår risiko profesjonelt, men **deres egen sårbarhet er abstrakt**. Ingen norsk advokat har (offentlig) mistet bevilling eller fått erstatningskrav fordi klientdata lekket via ChatGPT. Uten presedens finnes ingen felt sårbarhet. Det er som ulovlig parkering uten lapper — alle vet det er galt, ingen endrer atferd.

Maktdynamikken som blokkerer

Partnerne i de store firmaene (Wiersholm, Thommessen, Schjødt) sitter på **definisjonsmakten** for bransjepraksis. Disse firmaene har allerede enterprise-avtaler med Microsoft/OpenAI. Å innrømme at disse avtalene er utilstrekkelige betyr å



innrømme strategisk feilvalg — et makttap internt. Mellomstore firmaer venter på hva de store gjør. Soloadvokater mangler forhandlingsmakt overfor enhver leverandør.

Det kortsiktige kalkulus

Konkret: En advokat bruker 45 minutter mindre per dag med ChatGPT. SikkerKI-onboarding koster kanskje 2-3 dager produktivitetstap. I et firma med 1.800 kr/time-rater er det **direkte målbart tap mot diffus risiko**. Kortsiktig vinner alltid uten ekstern tvang.

Leverage-punkter — gjennom forhandlingslogikk

1. **Klientmakt er den eneste reelle driveren.** Hvis Equinor, Statkraft eller DNB krever dokumentert KI-sikkerhet i sine retainer-avtaler, endres kalkylen over natten. Én stor klient er mer verdt enn ti Datatilsynet-veiledere.
2. **Forsikringssårbarheten er uutnyttet.** Profesjonsansvarsforsikring (via Berkley/Zurich) har ennå ikke priset inn KI-risiko. Den dagen et polise-vilkår ekskluderer dekning ved uautorisert datadeling med tredjeparts-KI, kollapser hele “det rammer meg ikke”-narrativet.
3. **Datatilsynet mangler makt — men kan låne den.** Et tilsynsvedtak mot ett mellomstor firma (ikke de største, som har ressurser til å kjempe) ville skape presedens uten å kreve full regulatorisk kapasitet.

Det skarpe dilemmaet

SikkerKI trenger andres maktbruk for å lykkes. Produktet løser et problem markedet ennå ikke anerkjenner som akutt. Å bygge adopsjonen organisk er strategisk naivt. Å vente på regulatorisk tvang er risikabelt fordi markedet kan konsolideres rundt Microsofts “good enough”-løsninger først.

Tre konkrete neste steg

1. **Forhandle med 3-5 store innkjøpere** (Equinor juridisk, DNB compliance) om å inkludere KI-sikkerhetskrav i sine advokatavtaler — dette skaper tvang nedover i næringskjeden uten å vente på regulering.
2. **Engasjer forsikringsbransjen direkte.** Presenter risikoanalyse til If/Gjensidige om profesjonsansvar og KI-lekkasje — et forsikringsunntak er et maktgrep som treffer alle simultant.
3. **Provosér én offentlig sårbarhet.** Bestill en teknisk audit som demonstrerer konkret hva som skjer med norsk klientdata i standard ChatGPT — publiser



gjennom Rett24 eller Advokatbladet. Gjør det abstrakte til noe partnerne ikke kan ignorere i neste partnermøte.