



id: SI_001

model: mistralai/mistral-large-2512

seeds:

04_risiko: mulighet

03_relasjon: tillit

05_handling: implementer

01_perspektiv: juridisk

02_tidhorisont: langsiktig

Instans SI_001

Analyse: Adopsjonsbarrierer for SikkerKI blant norske juridiske profesjonelle

1. Juridisk blindsoner - risikoen er abstrakt til den blir konkret Advokater opererer i et landskap der juridisk risiko er velkjent, men teknologisk risiko fremstår som teoretisk. De forstår taushetsplikt, men mangler en juridisk hendelse som gjør KI-risikoen håndgripelig. Eksempel: Ingen har (ennå) fått et Datatilsynet-pålegg for å bruke ChatGPT med klientdata. **Løsningen ligger i å gjøre risikoen langsiktig og juridisk håndfast** – f.eks. ved å utarbeide en bransjestandard for KI-bruk, signert av Advokatforeningen, eller ved å få Datatilsynet til å publisere en konkret veileder med eksempler på brudd.

2. Tillit som teknologisk og psykologisk barriere Målgruppen stoler ikke på at on-premise-løsninger faktisk er sikre – de mistenker “backdoors” eller at data likevel lekker. Dette er en tillitssvikt som ikke løses med tekniske garantier alene.

Implementeringsnøkkelen er å la dem se sikkerheten: Tilby uavhengige revisjoner (f.eks. av NSM), vis kildekode for kritiske komponenter, eller la dem kjøre pilottester der de selv overvåker datatrafikk. Tillit bygges gjennom gjentatt verifisering, ikke salgsargumenter.

3. Regulatorisk limbo - uklare krav skaper handlingslammelse Datatilsynet har ikke uttalt seg eksplisitt om KI-bruk, og advokatloven er vag på teknologiske detaljer. Resultatet? En juridisk gråsoner der profesjonelle velger å vente. **Muligheten** ligger i å skape klarhet: SikkerKI kan samarbeide med Advokatforeningen om å utforme en “KI-sertifisering” for verktøy som oppfyller norske krav. Dette gir advokater et juridisk skjold – “vi fulgte bransjestandarden” – og fjerner unnskyldningen “vi visste ikke hva som var lov”.

4. Sosial norm som brems - ingen vil være først I et miljø der status quo er “alle bruker ChatGPT”, føles det risikabelt å være den som bytter. **Langsiktig løsning:**



Identifiser normentreprenører – store firmaer eller offentlige aktører (f.eks. Domstoladministrasjonen) – som kan ta ledelsen. Når en “safe player” adopterer SikkerKI, blir det lettere for andre å følge etter. **Implementeringsnøkkel:** Tilby disse aktørene en tillitsbyggende pakke (f.eks. gratis pilot med revisjon).

5. Verdiproposisjonen er feilformulert Advokater tenker ikke “compliance”, de tenker “risiko for meg og min klient”. **Muligheten** er å omformulere SikkerKI fra “et sikkerhetsverktøy” til “en forsikringspolise”. Eksempel: Samarbeid med forsikringsselskaper om rabatter for firmaer som bruker godkjente KI-løsninger. Eller vis konkrete klientkrav – f.eks. at store bedrifter allerede krever at deres advokater bruker sikre KI-verktøy.

Konkrete neste steg:

1. **Lag en “juridisk risikorapport”** i samarbeid med Advokatforeningen og Datatilsynet, med konkrete eksempler på hva som kan gå galt (f.eks. “Hvis du bruker ChatGPT med klientdata, kan klienten saksøke deg for brudd på taushetsplikt”).
2. **Tilby en “tillitspakke”** for pilotkunder: Uavhengig revisjon av SikkerKI, mulighet for å overvåke egen datatrafikk, og en juridisk garanti fra et advokatfirma om at løsningen oppfyller norsk lov.
3. **Start en normendring** ved å få med et stort firma (f.eks. BAHN eller Thommessen) som vil være “first-mover” – gi dem en høyprofilert rolle i markedsføringen.