



id: SI_005

model: mistralai/mistral-large-2512

seeds:

04_risiko: sårbarhet

03_relasjon: tillit

05_handling: implementer

01_perspektiv: operasjonell

02_tidhorisont: langsiktig

Instans SI_005

Analyse: Adopsjonsbarrierer for SikkerKI i norsk juridisk sektor

Sårbarhet som operasjonell blindflekk Juridiske profesjonelle kjenner risikoen ved åpne KI-verktøy, men bagatelliserer den som en teoretisk sårbarhet – ikke en operasjonell trussel. De ser ikke lekkasjer som et umiddelbart problem fordi konsekvensene (Datatilsynet-bøter, klienttap) føles fjerne. **Ekte barriere:** De mangler en håndgripelig forståelse av hvordan dataeksponering rammer deres daglige drift (f.eks. tap av advokatprivilegium i en konkret sak). Løsningen må gjøre sårbarheten konkret – f.eks. gjennom simuleringer av hvordan en klients forretningshemmeligheter kan havne i en konkurrentfirma sin KI-trening.

Tillitsparadokset: “Sikker” føles usikrere Standard KI-verktøy (ChatGPT, Copilot) har implisitt tillit fordi de er “godt nok” for de fleste brukere. SikkerKI krever derimot eksplisitt tillit – advokater må tro på at teknologien faktisk fungerer som lovet. **Ekte barriere:** De stiller høyere krav til SikkerKI fordi de ikke kan se at dataen er beskyttet (manglende transparens i “blind compute”). **Løsning:** Implementer uavhengige revisjoner (f.eks. av PwC eller Datatilsynet) som verifiserer sikkerheten, og kommuniser dette som en langsiktig tillitsbyggende prosess – ikke en engangshendelse.

Regulatorisk limbo: Handlingslammelse i uklarhet Datatilsynet og advokatloven gir rammer, men ikke handlingsregler. Jurister er vant til presise lovtekster – når regulatoriske krav er vage (“tilstrekkelige tiltak”), blir de handlingslammede. **Ekte barriere:** De venter på at noen andre (Datatilsynet, bransjeorganisasjoner) skal definere “standarden”. **Løsning:** SikkerKI må operasjonalisere regulatoriske krav – f.eks. ved å tilby maler for klientavtaler som eksplisitt nevner on-premise KI som “tilstrekkelig tiltak”.

Sosial norm: “Alle gjør det” vs. “Ingen gjør det” I dag er det en implisitt norm om at “alle bruker åpne KI-verktøy”, noe som gjør SikkerKI til en outsider-løsning. **Ekte**



barriere: Advokater frykter å bli sett på som teknologisk bakstreverske hvis de insisterer på sikkerhet. **Løsning:** Skap en ny norm gjennom kollektiv implementering – f.eks. ved å samarbeide med en stor advokatkjede (som Thommessen eller BAHR) for å gjøre SikkerKI til “bransjestandard”.

Implementeringsfriksjon: Den usynlige kostnaden Selv om SikkerKI er billigere på lang sikt (unngår bøter, klienttap), er kortsiktig friksjon en stor barriere: onboarding, integrasjon med eksisterende systemer, læringskurve. **Ekte barriere:** Jurister prioriterer operasjonell stabilitet – de vil ikke risikere at en ny løsning skaper kaos i en pågående sak. **Løsning:** Tilby en faset implementering med garantert “fallback” til gamle verktøy, og dokumenter hvordan overgangen reduserer operasjonell risiko (f.eks. gjennom case-studier fra pilotbrukere).

Konkrete neste steg

1. **Gjør sårbarheten håndgripelig:** Lag en interaktiv demo som viser hvordan en konkret klients data kan lekke via åpne KI-verktøy (f.eks. ved å bruke ekte, anonymiserte eksempler fra norske saker).
2. **Bygg tillit gjennom transparens:** Publiser en uavhengig revisjonsrapport (f.eks. fra Datatilsynet eller en stor revisjonsbyrå) som verifiserer SikkerKIs sikkerhetsgarantier.
3. **Operasjonaliser regulatoriske krav:** Utvikle maler for klientavtaler og interne retningslinjer som eksplisitt nevner SikkerKI som et “tilstrekkelig tiltak” for å oppfylle taushetsplikt og GDPR.