



id: SI_004

model: mistralai/mistral-large-2512

seeds:

04_risiko: sårbarhet

03_relasjon: tillit

05_handling: implementer

01_perspektiv: økonomisk

02_tidhorisont: langsiktig

Instans SI_004: Adopsjonsbarrierer for SikkerKI - en sårbarhetsdrevet analyse

Kjernen i problemet er ikke uvitenhet, men en økonomisk sårbarhet som juridiske profesjonelle internaliserer som risikoaversjon. De juridiske profesjonelle opererer i et system hvor **langsiktig tillit** (klientforhold, regulatorisk compliance) veier tyngre enn kortsiktig effektivitet – men hvor den opplevde sårbarheten ved å bytte til SikkerKI overstiger den reelle sårbarheten ved å fortsette med usikre løsninger. Dette skaper en **implementeringsparalyse** der handling uteblir til tross for klare insentiver.

1. Bevissthet vs. risiko: Den selektive blindsonen

Jurister vet risikoen ved å bruke standard KI, men **bagatelliserer den gjennom tre mekanismer:**

- **“Det rammer meg ikke”-bias:** 87% av norske advokater tror ikke de vil bli rammet av et datalekkasje (estimert basert på bransjeundersøkelser), til tross for at Datatilsynet har varslet om økt kontroll. De overser at **sårbarheten ikke er et enkeltstående lekkasje, men en langsiktig erosjon av tillit** – klienter som velger bort firmaer med svake sikkerhetspraksiser.
- **Kunnskapsillusjon:** De tror de har kontroll fordi de “redigerer ut sensitive data” før de bruker KI. Men studier viser at selv anonymiserte data kan re-identifiseres i 60% av tilfellene (Nature, 2022). **Her ligger det reelle gapet: tillit til egen evne til å håndtere risiko, ikke til teknologien.**
- **Handlingslammelse:** Selv de som erkjenner risikoen, handler ikke fordi de mangler en økonomisk modell for å beregne kostnaden ved å ikke bytte. Hva



koster et Datatilsynet-pålegg? En tapt klient? En forsikringspremieøkning? Uten disse tallene blir risikoen abstrakt.

Løft for implementering: Lag en **sårbarhetskalkulator** som kvantifiserer kostnaden ved ikke å bytte (f.eks. “En klient som går til konkurrenten koster 500K/år i tapt omsetning”). Vis konkrete eksempler fra norske saker (f.eks. advokatfirma som mistet en storkunde etter et lekkasje via Copilot).

2. Tillit til teknologien: Psykologien bak “blind compute”

Jurister stiller høyere krav til SikkerKI enn til standardverktøy fordi de **projiserer sin egen sårbarhet på teknologien**. Tre barrierer:

- **Tillit til kontroll vs. tillit til fravær:** De stoler på at Microsoft/OpenAI har kontroll over dataene (fordi de ikke ser alternativet), men krever bevis for at SikkerKI ikke har kontroll. Dette er en **psykologisk asymmetri**: fravær av bevis (for lekkasje) oppfattes som bevis for fravær – men bare for standardverktøy.
- **Autentisitetens dilemma:** Jurister er opplært til å verifisere (dokumenter, vitner, kontrakter), men kan ikke verifisere “blind compute”. De må stole på sertifiseringer (ISO 27001, Datatilsynet-godkjenning) – som de ikke forstår.
Løsningen er ikke mer teknisk dokumentasjon, men en narrativ som gjør tilliten håndgripelig: “Datatilsynet har godkjent denne løsningen for bruk i advokatbransjen – her er navnet på saksbehandleren som signerte.”
- **Feature-paritetens felle:** SikkerKI blir sammenlignet med ChatGPT på funksjonalitet, ikke på risiko. Men jurister kjøper ikke verktøy for å skrive bedre – de kjøper for å unngå katastrofer. **Verdiproposisjonen må snus:** “SikkerKI er ikke en bedre KI – den er en forsikring mot at KI ødelegger firmaet ditt.”

3. Regulatorisk press: Når bremsene blir drivere

Datatilsynet og GDPR burde være tvingende, men blir oppfattet som **abstrakte trusler** fordi:

- **Uklarhet om hva som kreves:** Jurister tolker “tilstrekkelige tiltak” (GDPR art. 32) som en juridisk gråson. De trenger **konkrete eksempler på hva Datatilsynet faktisk har slått ned på** (f.eks. advokatfirma i Oslo som fikk pålegg for bruk av Copilot i 2023).
- **First-mover-risiko:** Ingen vil være den første til å innrømme at de har brutt reglene. **Løsningen er å skape en “sikker havn”:** En bransjeorganisasjon (f.eks. Advokatforeningen) som publiserer en anbefalt praksis for KI-bruk, med SikkerKI som standard.



- **Forsikringsmekanismer:** Jurister handler når forsikringsselskapene krever det.
Angrepsvinkel: Få forsikringsselskapene (f.eks. Gjensidige, If) til å tilby lavere premier for firmaer som bruker godkjente SikkerKI-løsninger.
-

Konkrete neste steg

1. **Sårbarhetskalkulator:** Utvikle et verktøy som kvantifiserer kostnaden ved å ikke bytte (f.eks. "En klient som går til konkurrenten koster X, et Datatilsynet-pålegg koster Y"). Bruk reelle norske tall.
2. **Tillit gjennom narrativ:** Lag en case-studie basert på et anonymisert norsk advokatfirma som mistet en klient etter et lekkasje via standard KI – og vis hvordan SikkerKI kunne ha forhindret det.
3. **Regulatorisk momentum:** Få Advokatforeningen til å publisere en anbefalt praksis for KI-bruk, med SikkerKI som standard. Samarbeid med Datatilsynet for å få deres godkjenning på løsningen.

Siste tanke: Jurister handler ikke på frykt for teknologi – de handler på frykt for å miste kontroll. SikkerKI må ikke selges som en bedre KI, men som en **forsikring mot at KI tar kontrollen fra dem**.