



id: SI_003

model: google/gemini-2.5-flash

seeds:

04_risiko: sårbarhet

03_relasjon: makt

05_handling: vent

01_perspektiv: juridisk

02_tidhorisont: syklisk

Instans SI_003

Seeds: juridisk | syklisk | makt | sårbarhet | vent

Deres forslag om KI-basert risikoanalyse er ikke bare en ny tjeneste, men en forskyvning av **makt** – fra intuitiv ingeniørvurdering til datadrevet prediksjon. Dette er et tveegget sverd, spesielt når vi snakker om kommersialisering av historiske data.

Historiske prosjektdata er ikke bare tall; de er konkrete historier om suksess og feil, ofte preget av alvorlige hendelser og **sårbarhet** i operasjonelle systemer. Å forvalte dette krever en dyp forståelse for den **juridiske** bindingen som ligger i hver eneste kontraktslinje. Hver kundeavtale fra de siste 15 årene må granskes. Er det en standard konfidensialitetsklausul? Eller er det spesifikke formuleringer rundt “datautnyttelse” eller “sekundærbruk”? Min prediksjon er at mange av disse eldre avtalene ikke adresserer KI-modelltrening eksplisitt, noe som skaper et juridisk gråområde. Dette er en **sårbarhet** for dere.

Problemet er **syklisk**: selskapene som ga dere dataen forventet ikke at den skulle brukes til å bygge en kommersiell tjeneste. Dersom dere nå tilbyr en ny innsikt basert på deres data til konkurrentene deres, er det en direkte utfordring av den tilliten som ble etablert. Dette kan skade relasjoner mer enn nyinntektene forsvarer.

Vent. Før dere gjør noe, **vent**. Det haster ikke å kommersialisere rådataene.

Det er en felle å tro at “anonymisering” er tilstrekkelig. Med tilstrekkelig granularitet og ekstern informasjon kan anonymiserte datasett ofte de-anonymiseres. Risikoen for å avsløre kundespesifikk operasjonell **sårbarhet** er for høy.

Konkrete neste steg:

- Juridisk gransking og samtykkeinnhenting:** Engasjer et spesialisert advokatfirma (f.eks. Wiersholm eller Schjødt) til å analysere alle relevante kundekontrakter fra de siste 15 årene. Identifiser presist hvilke avtaler som ikke



tillater sekundærbruk for KI-modellering. For disse kundene må dere aktivt søke eksplisitt, skriftlig samtykke til spesifikke, aggregerte og anonymiserte dataformater. Tilby dem en andel av den fremtidige KI-tjenestens fortjeneste (f.eks. 5%) som insentiv.

2. **Modellutvikling med syntetisk data/"kunstig anonymisering":** Fokuser på å utvikle KI-modeller på data som er sterkt transformert eller syntetisk generert basert på de historiske dataene, snarere enn rådataene. Målet er å identifisere mønstre og korrelasjoner (det **sykliske** aspektet ved risiko), ikke spesifikke prosjekthendelser. Dette reduserer **sårbarheten** for kundene og dermed også den **juridiske** risikoen for dere. Vurder å bruke Secure Multi-Party Computation (SMPC) eller Federated Learning-prinsipper der modellene tren