



Debrief — qwen/qwen3.6-plus

- Instanser: 9
 - Tokens inn: 9,011
 - Tokens ut: 24,707
 - Kostnad: \$0.0511
 - Kjørt: 2026-04-12 13:16:58.308604+00:00
-

Sverm-debrief

Konsensus

1. **Aldri selg rådata eller eksporter datasett.** Alle instanser er enige om at verdien ligger i avledede mønstre, sannsynlighetsfordelinger og beslutningsstøtte, ikke i selve dataarkivet.
 2. **Tekniske sikkerhetslag er ikke-valgfrie.** Differensiell personvern ($\epsilon \leq 0,5-1,2$), syntetisk datagenerering og isolerte miljøer (air-gapped sandbox/VPC) er felles minimumskrav for å bryte koblingen til identifiserbar prosjektdata.
 3. **Start internt og i «shadow mode».** Valider modelltreffsikkerhet mot faktisk prosjekthistorikk (NCR-er, forsinkelser) før ekstern lansering. Bruk eksisterende kunder kun til kontrollerte piloter.
 4. **Kontraktene må redesignes.** Tradisjonelle NDA-er dekker ikke avledet KI-innsikt. Nye avtaleverk (Data Trust, Consent Dividend, Aggregated Insight License) må eksplisitt skille rådataeierskap fra modellrettigheter.
 5. **Makten flyttes fra dataeierskap til standardsetting.** Målet er å bli den uavhengige referansen for subsea-risiko, ikke en datamegler.
-

Dissens

- **Fart vs. juridisk robusthet:** SI_001, SI_003, SI_005 og SI_009 anbefaler å vente 6–12 måneder på regulatorisk avklaring (EU AI Act, DNV) og grundig kontraktskartlegging. SI_007 og SI_008 argumenterer for rask lansering (30–90 dager) med påstanden at «juridikk følger markedet» og at tjenstedesign kan omgå NDA-triggere.



- **Arkitektur:** Federert læring/TEE (SI_002, SI_004) står opp mot sentralisert syntetisk trening med streng differensiell personvern i lukket sandbox (SI_001, SI_006, SI_008).
- **Prising:** Resultatbasert/abonnement (SI_003, SI_004) vs. pay-per-insight/audit (SI_006, SI_007, SI_008).
- **Ansvar:** SI_009 krever eget juridisk selskap, 15 % ansvarslokk og tvungen «human-in-the-loop». Andre ser dette som en kommersiell brems.

Blindsoner avdekket

- **Konkurransesklausuler > GDPR:** Offshore-kontrakter definerer ofte «konfidensiell informasjon» bredt nok til å omfatte avledede algoritmer, ikke bare rådata. En enkelt AI ville sannsynligvis kun fokusert på personvern/anonymisering.
- **Tjenestedesign som juridisk bypass:** Ved kun å akseptere ikke-konfidensielle inngangsparametere (dybde, rørklasse, værvindu) og kun levere aggregerte risikoscore, kan NDA-triggere omgå arkitektonisk uten å forhandle kontrakter på nytt.
- **Regulatorisk vollgrav:** Å vente på DNV/Ptil-pre-sertifisering skaper en defensiv grøft konkurrenter ikke enkelt kan kopiere, i stedet for å jakte på kortsiktig hype.

Anbefalinger

1. Etabler et tverrfaglig Data Stewardship Committee (jurist, sikkerhet, ledende ingeniør) for å revidere 50 nøkkelkontrakter og utarbeide en «Aggregated Insight License» som eksplisitt unntar syntetiske/avledede innsikter fra taushetsplikten.
2. Bygg en lukket sandbox med differensiell personvern ($\epsilon \leq 0,5$) og syntetisk pipeline. Kjør 90 dagers «shadow mode» mot 3 historiske prosjekter for å validere prediktiv nøyaktighet mot faktiske NCR-er og forsinkelser.
3. Lanser en kontrollert «Risk Blackbox»-pilot med 3 ikke-konkurrerende kunder. Fakturer per analyse, lever kun «Decision Cards» (sannsynlighetsintervaller), og ekskluder eksplisitt rådata og modellvekter fra leveransen.
4. Søknad om metodisk pre-sertifisering hos DNV og innfør 15 % ansvarslokk med obligatorisk «human-in-the-loop»-signatur før alle feltkritiske anbefalinger.