Innovasjon og AI

Versjon 1.0 · 29. mai 2026 · Hva vi gjør i dag, hva vi ikke gjør, og hva vi ser for fremtiden

> **Kort fortalt:** Vi bruker AI som utvikler-verktøy, ikke som produkt-komponent. Ingen kundedata, personopplysninger eller produksjons-secrets sendes til AI-tjenester. Roadmap-ideer i seksjon 3 er retning, ikke leveringsplan.

1. AI i utvikling — det vi faktisk gjør i dag

Vi bruker AI-verktøy aktivt for å heve kode-kvalitet og sikkerhets- praksis. Det er en utvikler-side-prosess, ikke en del av tjenesten kunden bruker.

1.1 Anthropic Claude som kode-assistent

DigiReq sin daglige utvikling skjer pair-programming-aktig sammen med Anthropic Claude. Vi bruker AI til:

- Generere første-utkast til kode med kontekst fra repo-en
- Forklare og kvalitetssikre eksisterende kode
- Foreslå tester og dekke kant-tilfeller
- Generere dokumentasjon og kommentarer som matcher faktisk kode

1.2 Multi-agent kode-review

For sikkerhets-sensitiv kode (autentisering, EHF-generering, ekstern- integrasjon) kjører vi parallelle review-pass med spesialiserte agenter — security-fokusert review, type-safety review, og generelt code-quality review samtidig. Det fanger mønstre som en enkelt human-review lett overser.

1.3 Kontinuerlig sårbarhets-overvåking

GitHub Dependabot scanner avhengighetene våre kontinuerlig. CVE-er genererer automatiske pull-requests gruppert per økosystem. **Sårbare versjoner oppdateres innen 7**

dager (kritiske: 24 timer). Den 29. mai 2026 lukket vi for eksempel 41 sårbarheter på én dag, inkludert én kritisk i autentiserings-biblioteket.

1.4 Faktum-baserte versjoner og forsterket disiplin

AI-assistanse gjør det praktisk å holde dokumentasjon, kode og tester i synk. Når vi endrer en formulering på sikkerhets-siden, oppdaterer vi samtidig ROS-analysen, SLA-en og endringsloggen i samme runde. Det reduserer drift mellom det vi sier og det vi gjør.

2. AI i produktet — det vi IKKE gjør

Det er like viktig å være tydelig på hva vi **ikke** gjør. Defensiv posisjonering for IT-revisor:

- **Ingen ML-modeller trent på kundedata.** Kundens rekvisisjons-data brukes ikke til å trene noen modell hos oss eller hos en tredjepart.
- **Ingen automatiserte godkjenninger via AI.** Godkjenninger gjøres alltid av et menneske (eller mot eksplisitte, kunde-konfigurerte terskler — ikke AI-modeller).
- **Ingen AI har tilgang til persondata.** Verken navn, telefon, e-post, rolle, eller rekvisisjons-innhold sendes til AI-tjenester i produksjon eller utvikling.
- **Ingen profilering av brukere.** Vi analyserer ikke individuelle ansattes innkjøps-mønstre for AI-formål.
- **Ingen tredjeparts-AI mottar Peppol-trafikk.** EHF-genereringen er deterministisk XML-bygging, ikke AI.

3. AI i produkt — hvor det kan gi verdi senere

Disse er **retnings-ideer for roadmap, ikke leveringsplan**. Hvis vi bygger noe av dette, kommer det med eksplisitt samtykke, oppdatert DPA, og synlig dokumentasjon her — ikke som en stille endring.

3.1 Anomali-deteksjon i innkjøps-mønstre

Mønster-gjenkjenning som flagger uvanlige innkjøp for økonomi- saksbehandler. Eksempel: samme leverandør får mange rekvisisjoner på beløp like under en terskel-grense — kan tyde på splittet innkjøp som bør sees på. Forutsetter at kunden aktivt opt-in og at all analyse skjer på kundens egen data, ikke aggregert på tvers.

3.2 Automatisk KOSTRA-art-forslag

Når en vaktmester taster "skrutrekker" foreslår systemet konteringsstreng automatisk — art 120 (arbeidstøy/verneutstyr) eller annet relevant. Bruker KOSTRA-kontoplanen som regel-basert kunnskaps- kilde, ikke åpen-AI. Lavere risiko enn ren ML.

3.3 Naturlig-språk rekvisisjon

"Jeg trenger fire ruller maskeringstape, str. 50 mm, og to liter whitespirit" → ferdig-strukturert rekvisisjon med vare-linjer, anslag og butikk-forslag. Reduserer felt-friksjon ytterligere. Hvis vi bygger dette er det mot lokal/EU-hostet modell, ikke send-til-USA.

3.4 Pris-sammenligning på tvers av leverandører

For kommunale innkjøp under terskelverdien — peker ansatten på den leverandøren som er billigst i nærmeste prisklasse for det aktuelle produktet, basert på historiske faktura-data fra kundens egen Visma. Krever toveis-integrasjon, ikke planlagt i 2026.

3.5 Klargjøring for norsk AI-infrastruktur

Stargate Norway (OpenAI-datasenter i Narvik, planlagt Q4 2026) gjør norsk-host AI-infrastruktur til en konkret mulighet. Hvis det blir kommersielt tilgjengelig med GDPR-konforme vilkår, vil DigiReq vurdere å migrere AI-bruken vår dit for å holde all data på norsk territorium.

4. Hva som styrer beslutningene

- **Default på ingen AI** — eksisterende deterministiske flyt-er er trygge og forutsigbare. AI kommer kun inn der det gir målbar verdi som veier opp for kompleksiteten.
- **Eksplisitt samtykke ved produkt-AI** — hvis vi bygger AI-features, må kunden eksplisitt opt-in. Default off.
- **Audit-spor** — alle AI-bidrag i produksjons-flyt (hvis vi noen gang bygger det) logges som handlinger med "ai:<model-name>" som actor, slik at IT-revisor kan se hva AI gjorde og hvor.
- **Personvern over funksjonalitet** — hvis en AI-feature ikke kan bygges uten å eksponere persondata, bygges den ikke.
- **EU-only data-flyt** — eventuell AI-bruk skal kunne dokumenteres innenfor EU/EØS eller på godkjent overføringsmekanisme.

5. Hvorfor være transparente om dette?

AI er nyttig, men det er også et tillit-spørsmål. Kommune-IT som evaluerer oss i 2026 og 2027 vil ha to bekymringer: (1) at vi overpromisser AI-features vi ikke har, og (2) at vi skjuler AI-bruk som påvirker persondata. Vi velger å være eksplisitte begge veier. Det vi har, dokumenterer vi. Det vi ikke har, sier vi at vi ikke har. Det vi planlegger, kommer med tydelig "hvis vi bygger"- forbehold.

6. Kontakt

- **Spørsmål om vår AI-bruk:** sikkerhet@digireq.no
- **Forslag til AI-features:** info@digireq.no

Dokument-versjon 1.0 · Sist oppdatert 29. mai 2026 · info@digireq.no

OM LEVERANDØREN

Tjenesten DigiReq leveres av **Påvakt AS** (org.nr. **937 620 187**), heretter omtalt som «Leverandør». DigiReq er registrert som virksomhet under Påvakt AS (**Digireq**, org.nr. **937 700 539**). Avtaler signeres med Påvakt AS som juridisk enhet; EHF-fakturaer fra DigiReq utstedes på Digireqs virksomhets-org-nr.

Kontakt: info@digireq.no · Sikkerhet: sikkerhet@digireq.no · Personvern: personvern@digireq.no