Sertifiseringer og roadmap

Versjon 1.0 · 29. mai 2026 · Ærlig status på hva vi har og hva som kommer

> **Kort fortalt:** DigiReq har ingen formelle sertifiseringer i dag — vi er i pilot- og tidlig-produksjonsfase. Vi velger å være ærlige om dette i stedet for å late som. Roadmap nedenfor viser plan for hvilke rammeverk vi tar når kundebasen rettferdiggjør kostnaden.

1. Hva vi har i dag

1.1 GDPR-compliance

- Komplett personvernerklæring og databehandleravtale
- Sub-prosessor-liste på /underleverandorer
- Rettigheter og prosedyrer for de registrerte
- Audit-logg med 12 mnd retention
- Sletteprosedyrer dokumentert og implementert
- Datatilsynets veileder for risikovurdering fulgt i ROS-analysen

Påvakt AS har registrert behandlinger internt; ingen formell sertifisering kreves for at vi skal være GDPR-compliant.

1.2 Hetzners EU-hosting

Vår infrastruktur kjører på Hetzner Cloud i Helsinki-datasenteret (EU/EØS). Hetzner har:

- ISO 27001-sertifisert datasenter-drift
- ISO 9001-sertifisert kvalitetsledelse
- Tier-3+ datasenter med redundant strøm, kjøling og nettverk
- BSI C5-attestasjon (tysk Federal Office for Information Security)

Vi støtter oss på Hetzners sertifiseringer for fysisk og infrastruktur- sikkerhet, men har **ikke selv** ISO 27001-sertifisering for DigiReq-applikasjonen.

1.3 Andre sub-prosessor-sertifiseringer

- **Cloudflare:** ISO 27001, SOC 2 Type II, PCI DSS
- **Netlify:** SOC 2 Type II
- **Microsoft Entra ID:** ISO 27001, SOC 2, FedRAMP, ENS High
- **46elks:** GDPR-compliant SMS-leverandør i EU/EØS
- **Tickstar Galaxy:** Peppol-sertifisert Access Point

2. Roadmap for formelle sertifiseringer

2.1 ISO/IEC 27001 — Informasjonssikkerhet

- **Status:** Ikke startet
- **Plan:** Vurderes når vi har 50+ betalende kunder, eller når en stor kommunal kunde gjør det til et bindende krav
- **Estimert tidsramme:** 12-18 måneder fra start til Stage 2-sertifisering
- **Estimert kostnad:** 250 000-500 000 kr for første gangs sertifisering, deretter årlige overvåknings-revisjoner
- **Hvorfor utsatt:** Kostnad og innsats står ikke i forhold til nytte i pilot-fasen. Vi har implementert tekniske og organisatoriske tiltak på 27001-nivå allerede (se /sikkerhet), men har ikke ekstern revisjon.

2.2 ISO/IEC 27701 — Personvern-utvidelse til 27001

- **Status:** Ikke startet
- **Plan:** Tas samtidig som 27001 hvis vi går for det

2.3 SOC 2 Type II

- **Status:** Ikke startet
- **Plan:** Vurderes hvis vi får amerikanske kunder eller går inn i internasjonal SaaS-marked. Ikke nødvendig for norsk kommunalt marked.

2.4 NSM Grunnprinsipper for IKT-sikkerhet

- **Status:** Implementert som intern praksis, ikke ekstern verifisert
- **Plan:** Vi følger NSMs "Grunnprinsipper for IKT-sikkerhet" (versjon 2.1, 2020) i arkitektur og drift. Formelt revidert mot rammeverket vurderes ved første store kommunale anbudskrav.
- Referanse: nsm.no/grunnprinsipper

2.5 Schrems II / Internasjonal data-overføring

- **Status:** Alle persondata oppbevares i EU/EØS
- **Plan:** Beholder EU-only-arkitektur. Eventuelle US-leverandører som blir nødvendige (f.eks. Apple/Google for push) bruker Standard Contractual Clauses (SCCs) + Transfer Impact Assessment (TIA)

2.6 Eksplisitt penetrasjons-test

- **Status:** Ingen formell pen-test gjennomført ennå
- **Plan:** Q4 2026 — vi engasjerer en norsk pen-test-leverandør (Mnemonic, Defendable, eller tilsvarende) for first-pass test før vi går inn i bredere kommersialisering. Sammendrag deles med kunder under NDA.

2.7 WCAG 2.1 nivå AA-audit

- **Status:** Delvis samsvar, selvevaluert (se /tilgjengelighet)
- **Plan:** Ekstern audit av sertifisert WCAG-konsulent før første offentlig kommersiell utrullng (mål Q4 2026)

3. Hva som kreves for kommunal salg i dag

Norske kommuner kan kjøpe SaaS-tjenester under den nasjonale terskelverdien på 1,3 MNOK eks. mva. årlig uten kunngjøringsplikt på Doffin (se /pris §4 for detaljer). For pilot- og tidlig-kommersialisering kreves derfor ikke formelle sertifiseringer. Det som faktisk forventes:

- Personvernerklæring, DPA, sub-prosessor-liste — **vi har dette**
- Sikkerhets-dokumentasjon med tekniske detaljer — **vi har dette**
- SLA med målbar tilgjengelighet og responstider — **vi har dette**
- Risiko-analyse — **vi har dette**
- Beredskapsplan — **vi har dette**

- MFA-mulighet for admin-pålogging — **vi har dette via Entra ID**
- EU/EØS-hosting — **vi har dette (Hetzner Helsinki)**

4. Hvis du trenger sertifiseringer vi ikke har

Hvis ditt anskaffelses-krav inkluderer ISO 27001 eller annet vi ikke har:

- Ta kontakt — vi diskuterer gjerne om vår nåværende dokumentasjon kan dekke kravet på alternativ måte
- Vi kan tilby **akselerert sertifiserings-plan** med målrettet finansiering hvis en stor kunde er villig til å være pilot for sertifiserings-prosessen
- Vi kan delta i tredjeparts-revisjon på kundens regning der det er sikkerhets-/compliance-revisjon

5. Transparens-prinsipp

Vi velger å være ærlige om sertifiserings-statusen. Det er to ting vi forplikter oss til:

1. Aldri claim om sertifiseringer vi ikke har
2. Når vi får en sertifisering — publisere den her med utstedelses-dato og gyldighets-periode

6. Kontakt

- **Sikkerhets- og compliance-spørsmål:** sikkerhet@digireq.no
- **Anskaffelses- og dokumentasjon-spørsmål:** info@digireq.no

---

Dokument-versjon 1.0 · Sist oppdatert 29. mai 2026 · sikkerhet@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