DPIA-mal for kunden

Hjelpe-mal kommuner og kommunale foretak kan bruke som utgangspunkt for sin egen DPIA (Data Protection Impact Assessment / vurdering av personvernkonsekvenser) ved innføring av DigiReq.

> **Status:** Mal — ikke en ferdig DPIA. Som behandlingsansvarlig er det **kunden selv** som skal gjennomføre DPIA-en (GDPR art. 35). Denne malen sparer tid ved å samle fakta om DigiReq på ett sted.
> **Når DPIA er påkrevd:** Datatilsynet krever DPIA ved systematisk og omfattende vurdering av personlige forhold, særlig sensitive data, eller systematisk overvåkning. **Standard DigiReq-bruk faller normalt under DPIA-terskelen** (ikke-sensitive rekvisisjons-metadata, ingen profilering, ingen automatisert beslutningstaking med rettsvirkninger), men noen organisasjoner ønsker likevel å gjennomføre lett DPIA som god praksis.

1. Beskrivelse av behandlingen

1.1 Hva

DigiReq er en mobil-app og web-tjeneste som erstatter papir-rekvisisjoner for kommunalt felt-arbeid. Ansatte oppretter rekvisisjoner i felt, ledere godkjenner med push-notifikasjon, butikker mottar rekvisisjonsnummer, og faktura matches automatisk mot rekvisisjonen via EHF/Peppol.

1.2 Formål med behandlingen

- Digital opprettelse, godkjenning og sporing av kommunale rekvisisjoner
- Automatisk fakturamatching for kjøp under bestilling
- Sporbarhet og internkontroll i innkjøps-prosessen
- Audit-logg for sikkerhets- og revisjons-formål

1.3 Rettslig grunnlag (GDPR art. 6)

- **Avtale** (art. 6 nr. 1 bokstav b): for ansatte i kommunens tjeneste — rekvisisjons-håndtering er del av arbeidsforholdet
- **Berettiget interesse** (art. 6 nr. 1 bokstav f): for audit-logging og sikkerhetsovervåkning
- **Rettslig forpliktelse** (art. 6 nr. 1 bokstav c): bokføringsloven §13 — oppbevaring av regnskaps-bilag

2. Personopplysninger som behandles

KATEGORI	EKSEMPLER	KILDE	RETTSLIG GRUNNLAG
Identifikasjon	Navn, telefonnummer, e-postadresse	Admin oppretter ved invitasjon; bruker bekrefter	Avtale
Rolle og organisasjons-tilknytning	Rolle (ansatt/godkjenner/admin), avdeling	Admin tildeler	Avtale
Aktivitets-data	Rekvisisjoner opprettet, godkjent, avvist; tidsstempler	Brukerens egen handling	Avtale
Teknisk metadata	IP-adresse, enhet-ID, app-versjon, login-tidspunkt	Automatisk ved bruk	Berettiget interesse (sikkerhet)
Audit-data	Hvem gjorde hva, når, fra hvor	Automatisk ved privilegerte handlinger	Berettiget interesse (sikkerhet)
Microsoft Entra-data (hvis SSO)	Entra `oid`, e-post, tenant-ID	Microsoft Entra ID via OIDC	Avtale

2.1 Hva som IKKE behandles

- Helseopplysninger eller særlige kategorier (GDPR art. 9)
- Strafferettslige opplysninger
- Biometriske data (Face ID/fingeravtrykk valideres lokalt på enheten — biometri sendes aldri til oss)

- Lokasjons-data (GPS)
- Innhold i kalender, e-post, filer, Teams
- Profilering eller automatisert beslutningstaking med rettsvirkninger

3. Hvem behandles opplysningene for

- **De registrerte:** ansatte hos kunden som har fått tilgang til DigiReq
- **Antall registrerte:** bestemmes av kunden (typisk 10-500 per kommune-enhet)
- **Vurdering av sårbarhet:** ingen sårbare grupper er i scope (barn, syke, etc.)

4. Hvor lenge oppbevares opplysningene

- **Brukerprofil:** så lenge brukerforholdet eksisterer + arbeidsforholdets rettslige oppfølgings-tid
- **Rekvisisjoner:** 5 år iht. bokføringsloven §13
- **Audit-logg:** 12 måneder (deretter automatisk slettet via cron)
- **OTP-koder:** umiddelbart etter consumed/expired (TTL 5 minutter)
- **Session-tokens:** access 60 min, refresh 60 dager
- **Backup:** 7 dagers rullerende

5. Hvem har tilgang

5.1 Hos behandlingsansvarlig (kunden)

- **Ansatt (employee):** egne rekvisisjoner
- **Godkjenner (approver):** avdelingens rekvisisjoner
- **Admin:** alt for sin organisasjon, inkludert audit-logg

5.2 Hos databehandler (DigiReq/Påvakt AS)

- **Super_admin (Markus):** kun organisasjons-metadata (firma-opprettelse, admin-tildeling). Ingen automatisk tilgang til rekvisisjons-data på tvers av firmaer. Eventuell tilgang krever midlertidig opphøyelse til admin der, som loggføres synlig for kunden.

5.3 Underleverandører

Se /underleverandorer for komplett liste. Kort:

- **Hetzner** (DE/FI) — drift og lagring
- **Cloudflare** (US/EU edge) — DNS, DDoS, edge-cache
- **Netlify** (US/EU edge) — landingsside-hosting
- **46elks** (SE) — SMS-utsending for OTP
- **Apple, Google** — push-notifikasjon (token + minimal metadata)
- **Microsoft (Entra ID)** — pålogging hvis kunden velger SSO
- **Tickstar Galaxy** (SE) — Peppol Access Point (hvis valgt)

Alle er i EU/EØS eller på lov-godkjent overføringsmekanisme.

6. Tekniske og organisatoriske tiltak

Detaljert i /sikkerhet. Sammendrag:

- **Tilgangskontroll:** rollebasert, audit-logget
- **Autentisering:** SMS-OTP eller Entra ID (anbefalt MFA via Conditional Access)
- **Kryptering:** TLS 1.2+ i transit, kryptert database i hvile
- **Backup:** daglig, kryptert, 7 dagers retention
- **Sub-prosessor-kontroll:** DPA med hver, GDPR-compliance verifisert
- **Audit-logg:** append-only, 12 mnd retention
- **Hendelseshåndtering:** 24-timers varsel ved sikkerhetsbrudd (DPA §10)

7. Risiko-vurdering

DigiReqs egen ROS-analyse identifiserer 16 trusler. Se /ros-analyse. Etter implementerte tiltak er alle på akseptabelt nivå for pilot- og tidlig-produksjonsfase.

For DPIA-en bør kunden gjøre sin egen vurdering av:

- Sannsynligheten for kompromittering av kunde-admin-konto (mitigeres via Entra+CA-MFA — sterkt anbefalt)
- Konsekvensen av lekkasje av rekvisisjons-metadata (typisk: lav — ikke-sensitive innkjøps-data)
- Andre risiko-faktorer spesifikt for kommunens IT-landskap

8. Rettigheter og prosedyrer for de registrerte

Brukerne har alle GDPR-rettigheter (innsyn, retting, sletting, dataportabilitet, innsigelse). Se /data-rettigheter for praktiske steg.

Som behandlingsansvarlig er kunden hoved-kontaktpunkt for de registrerte. DigiReq bistår innen 5 virkedager når kunden videresender en forespørsel.

9. Behov for forhåndskonsultasjon med Datatilsynet

GDPR art. 36 krever forhåndskonsultasjon med Datatilsynet hvis DPIA-en viser høy restrisiko. **For standard DigiReq-bruk forventes ikke høy restrisiko** dersom de tekniske og organisatoriske tiltakene i §6 følges.

10. Konklusjons-mal

Kunden kan bruke følgende konklusjon som utgangspunkt (tilpass til egen vurdering):

Bruken av DigiReq medfører behandling av personopplysninger om kommunens ansatte med formål rekvisisjons-håndtering og internkontroll. Behandlingen er begrenset til navn, kontakt-info, rolle og aktivitets-data. Tekniske og organisatoriske tiltak (Entra ID med MFA, audit-logg, tenant-isolasjon, kryptering) er vurdert som tilstrekkelige. Restrisiko er vurdert som lav. Forhåndskonsultasjon med Datatilsynet anses ikke nødvendig.

DPIA-en revideres ved vesentlige endringer i behandlingen eller minst hvert annet år.

11. Vedlegg som kan refereres

- Personvernerklæring
- Databehandleravtale (DPA)
- Underleverandører
- Sikkerhet
- Risiko- og sårbarhetsanalyse
- SLA
- Beredskap og kontinuitet

12. Hjelp og kontakt

Ved spørsmål til DigiReq som dukker opp under DPIA-arbeidet: personvern@digireq.no. Vi svarer innen 5 virkedager i pilot-fasen.

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