Databehandleravtale

Sist oppdatert 5. mai 2026. Versjon 1.0.

Hva er dette? Når en kommune eller et kommunalt foretak tar i bruk DigiReq, blir kommunen "behandlingsansvarlig" og DigiReq (Påvakt AS) blir "databehandler" iht. GDPR art. 28. Denne avtalen regulerer forholdet og signeres før produksjonsbruk.
Teksten følger malen til Datatilsynet og kan justeres etter kundens egne krav. Send forespørsel til info@digireq.no for signert eksemplar (PDF) tilpasset deres organisasjon.

1. Partene

- **Behandlingsansvarlig:** Kunden (kommunen / kommunalt foretak), heretter "Kunden".
- **Databehandler:** Påvakt AS, org.nr. 937 620 187 (DigiReq drives som virksomhet under Påvakt AS — Digireq, org.nr. 937 700 539), heretter "Leverandøren".

2. Behandlingens art og formål

Leverandøren behandler personopplysninger på vegne av Kunden for å levere tjenesten DigiReq — en mobilapplikasjon for digital rekvisisjon, godkjenningsflyt, og match mot innkommende fakturaer.

3. Type personopplysninger og kategorier av registrerte

Kategorier av registrerte: Kundens ansatte (ansatte, godkjennere, administratorer).

Personopplysninger som behandles:

- Telefonnummer
- Fullt navn
- Rolle (ansatt / godkjenner / admin)
- Avdelingstilhørighet

- Rekvisisjons-data: butikk, beskrivelse, beløp, tid
- Godkjennings-data: hvem, beslutning, tid, eventuell kommentar
- Tekniske data: enhets-ID, push-token, app-versjon, IP ved OTP-forespørsel

Sensitive personopplysninger (særlige kategorier iht. GDPR art. 9) behandles **ikke** i tjenesten.

4. Varighet

Avtalen gjelder så lenge Kunden bruker tjenesten. Ved opphør slettes eller pseudonymiseres personopplysninger iht. punkt 9.

5. Leverandørens forpliktelser

Leverandøren skal:

- Bare behandle personopplysninger etter dokumenterte instrukser fra Kunden, jf. GDPR art. 28 nr. 3 a.
- Sørge for at personer med tilgang har taushetsplikt.
- Iverksette egnede tekniske og organisatoriske tiltak for å sikre tilfredsstillende sikkerhet, jf. GDPR art. 32. Konkrete tiltak er oppsummert i punkt 7.
- Bistå Kunden ved henvendelser om innsyn, retting, sletting og dataportabilitet fra de registrerte.
- Bistå Kunden ved sikkerhetsbrudd, konsekvensanalyser (DPIA) og forhåndsdrøftelser med Datatilsynet.
- Slette eller tilbakelevere alle personopplysninger ved opphør, etter Kundens valg.
- Stille til rådighet all informasjon Kunden trenger for å påvise overholdelse av denne avtalen.

6. Bruk av underleverandører

Leverandøren har generell forhåndsgodkjennelse til å bruke underleverandører (databehandlere) som listet på underleverandører. Listen oppdateres minimum ved endringer.

Ved bytte eller tillegg av underleverandør varsles Kunden skriftlig minst 30 dager i forveien. Kunden kan ved saklig grunn motsette seg endringen og si opp avtalen uten kostnad om partene ikke finner annen løsning.

Leverandøren er ansvarlig for at underleverandørene oppfyller samme forpliktelser som Leverandøren etter denne avtalen.

7. Tekniske og organisatoriske tiltak

- All kommunikasjon over TLS 1.2+ (HTTPS) med moderne chiffer-suiter.
- Database er kun tilgjengelig fra applikasjonsserveren via lokalt nettverk; ikke eksponert mot internett.
- Innloggingskoder hash-es med bcrypt før lagring; lagres aldri i klartekst.
- JWT-tokens med kort levetid + refresh-token-rotasjon.
- Rollebasert tilgangskontroll: ansatt ser kun sine egne, godkjenner ser sin avdeling, admin ser sitt firma.
- Kryptert backup av database, oppbevart i samme EU-region.
- Tilgang til produksjonsmiljø er begrenset til navngitte personer hos Leverandøren med to-faktor-autentisering.
- Sikkerhetsoppdateringer av OS, biblioteker og avhengigheter overvåkes kontinuerlig.
- Logging av tilgang og endringer for revisjons-spor.

8. Lokasjon for behandling

Hovedbehandling skjer i datasenter i Helsinki, Finland (EU/EØS). Enkelte underleverandører overfører data til USA — slike overføringer baserer seg på EU-kommisjonens standardklausuler (SCC) og DPF-rammeverket. Se underleverandører for detaljer.

9. Tilbakelevering eller sletting ved opphør

Ved opphør av avtalen, og innen 30 dager etter opphørsdato, skal Leverandøren etter Kundens valg:

- Levere tilbake alle personopplysninger i et strukturert, maskinlesbart format (JSON-eksport).
- Slette eller pseudonymisere alle personopplysninger.

Personopplysninger knyttet til revisjons-spor (rekvisisjoner, godkjenninger) som er underlagt bokføringslovens 5-årskrav beholdes i pseudonymisert form til retentionsperioden er over.

10. Sikkerhetsbrudd

Leverandøren varsler Kunden uten ugrunnet opphold, og senest innen 24 timer, ved kjennskap til brudd på personopplysningssikkerheten. Varselet skal inneholde informasjonen Kunden trenger for å oppfylle sin meldeplikt til Datatilsynet (innen 72 timer etter at Kunden ble kjent med bruddet, jf. GDPR art. 33).

11. Revisjon

Kunden, eller en revisor utpekt av Kunden, har rett til å gjennomføre revisjon av Leverandørens etterlevelse av avtalen med rimelig varsel og minst én gang per år. Leverandøren stiller til rådighet nødvendig dokumentasjon og bistand.

12. Erstatning og ansvar

Partenes ansvar for brudd på denne avtalen følger av GDPR art. 82 og Bruksvilkår punkt 8. Begrensninger i Bruksvilkår punkt 8 gjelder ikke for ansvar etter GDPR art. 82.

13. Lovvalg og tvister

Avtalen reguleres av norsk rett. Eventuelle tvister søkes løst ved dialog først; hvis det ikke fører frem, er Midtre Hålogaland tingrett verneting.

Dokument-versjon 1.0 · Sist oppdatert 5. 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