# Vedlegg 4 til

# Bilag 1

## Kundens tekniske plattform

## og arkitekturprinsipper

## DGI

## Anskaffelse av velferdsteknologisk plattform

# Innhold

**1. Teknisk plattform - DGI ..... 3**

*1.1 Plattformmodell ..... 3*

*1.2 Sikkerhet og personvern ..... 4*

*1.3 Løsninger i plattformen ..... 4*

*1.4 Utviklingsretning ..... 4*

**1. Arkitekturprinsipper (DGI) ..... 5**

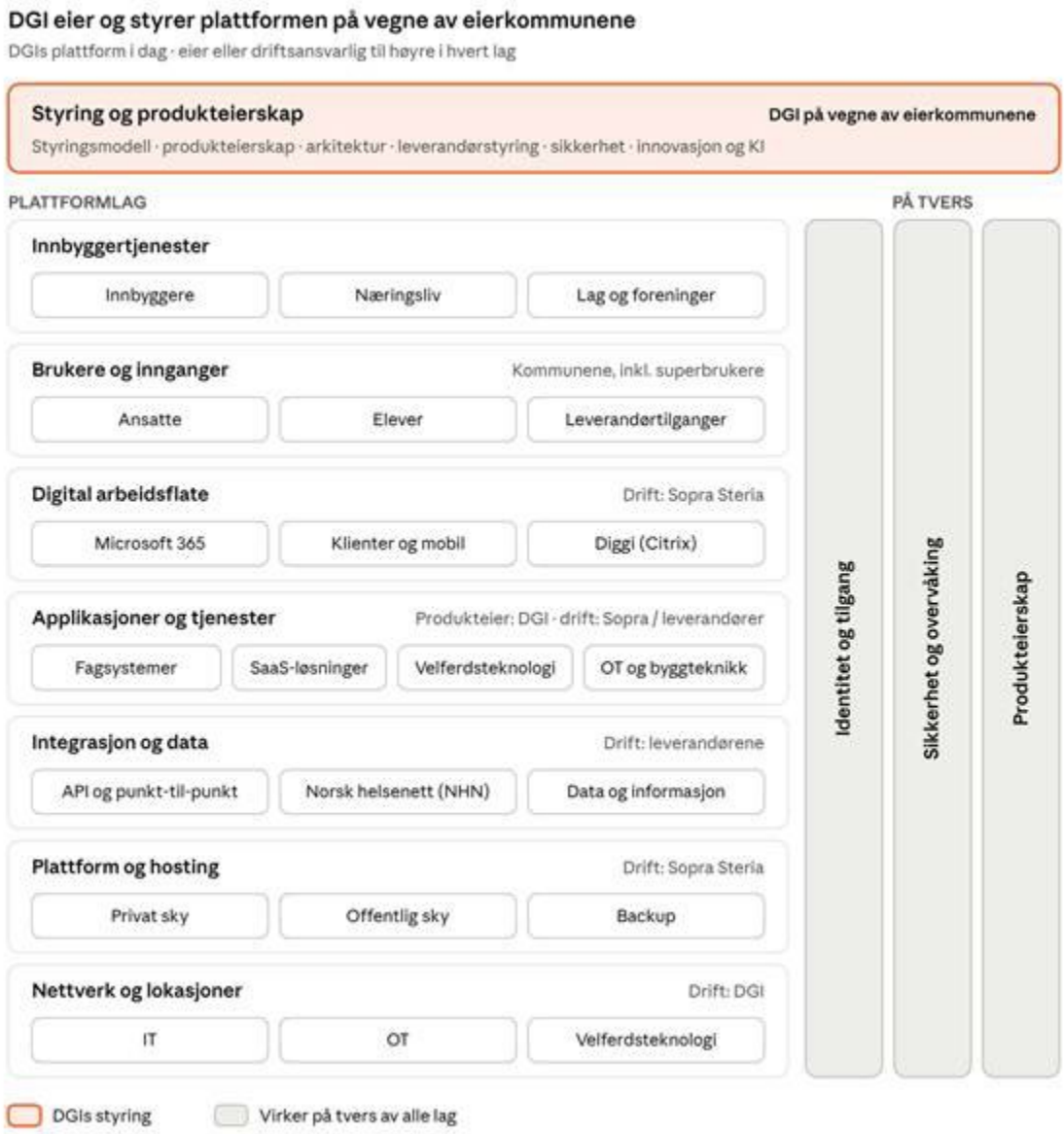
*1.1 Sentrale prinsipper for DGIs tjenesteplattform ..... 5*

# 1. Teknisk plattform - DGI

DGI (Digitale Gardermoregionen KO) leverer felles IKT-tjenester til eierkommunene gjennom en felles teknisk plattform.

DGI eier plattformen og har produkteierskapet og styringsmodellen på vegne av eierkommunene. Sentral drift er satt ut til Sopra Steria. DGI drifter selv nettverk og lokasjoner, og styrer arkitektur, sikkerhet og leverandører.

## 1.1 Plattformmodell




Modellen viser plattformen i sju lag, under et felles lag for styring. DGI styrer plattformen gjennom produkteierskap, styringsmodell, arkitektur og leverandørstyring, og har kontroll på sikkerhet, innovasjon og KI.

Ansvaret for drift er fordelt slik:

- Sopra Steria drifter digital arbeidsflate, fagsystemer og den sentrale plattformen.
- Leverandørene drifter egne løsninger innen blant annet velferdsteknologi og OT. DGI forvalter disse løsningene.
- Integrasjoner mellom løsningene leveres og driftes av leverandørene. I dag er de dels API-baserte og dels punkt-til-punkt-integrasjoner.
- DGI drifter nettverk og lokasjoner.

Identitet og tilgang, sikkerhet og overvåking og produkteierskap gjelder for alle lag og alle løsninger i plattformen.

## 1.2 Sikkerhet og personvern

DGI bruker flere felles mekanismer for å sikre løsninger og informasjon, også løsninger som behandler helse- og personopplysninger:

- **Entra ID** for autentisering av ansatte.
- **HelseID** for autentisering av helsepersonell.
- **ID-porten** for autentisering av innbyggere og pårørende.
- **Norsk helsenett (NHN)** for sikker kommunikasjon og datautveksling i helsesektoren.

I tillegg kommer segmentert nettverk, sikkerhetsovervåking og leverandørtilganger.

## 1.3 Løsninger i plattformen

Løsninger som skal inngå i plattformen, skal:

- bruke DGIs mekanismer for identitet, autentisering og sikker kommunikasjon
- samhandle med andre løsninger og fagsystemer gjennom åpne, standardiserte API-er og åpne standarder for datautveksling, og støtte hendelsesbasert informasjonsdeling der det er hensiktsmessig. Nasjonale samhandlingskomponenter, som KS Fiks og Norsk helsenett, foretrekkes der de dekker behovet
- følge DGIs føringer ved tilkobling til DGIs nettverk
- inngå i DGIs drift, tjenestestyring og sikkerhetsovervåking, og følge DGIs rutiner for tilgang for leverandører
- følge nasjonale standarder og tjenestemodeller for fagområdet, for eksempel KS' helhetlige tjenestemodell for velferdsteknologi

## 1.4 Utviklingsretning

Plattformen utvikles etter DGIs målarkitektur. Løsninger som anskaffes, skal kunne følge denne retningen i avtaleperioden:

- **SaaS og standard skytjenester først**, med krav til dataportabilitet og exit.
- **Identity First og Zero Trust:** tilgang styres av identitet, rolle og kontekst, ikke av nettverk. Maskin- og tjenesteidentiteter forvaltes på samme måte.
- **Standardiserte API-er og datakontrakter** erstatter punkt-til-punkt-integrasjoner.
- **Data og innsikt:** kommunene eier dataene, som skal kunne brukes i felles dataplattform, analyse og KI.

# 1. Arkitekturprinsipper (DGI)

### Felles prinsipper for DGI-samarbeidet

Arkitekturprinsippene bygger på nasjonale prinsipper fra Digdir og skal legges til grunn for alle beslutninger, anskaffelser og endringer i DGI-samarbeidet.

**1. Sett oppgaven i sentrum**

**2. Ta beslutninger på riktig nivå**

**3. Vær tydelig bestiller**

**4. Del og gjenbruk data og løsninger**

**5. Bygg for samhandling med åpne API-er**

**6. Sikre tillit og kontroll**

**7. Ha orden i eget hus**

**8. Reduser avhengighet**

**9. Tenk helhetlig**

**10. Styrt arkitektur og kravstilling**

## 1.1 Sentrale prinsipper for DGIs tjenesteplattform

- **Identity First** — identitet er den primære sikkerhetsmekanismen
- **Least priviledge** – Identitetene skal ikke har mer tilganger en nødvendig for å utføre sitt tjenstlige behov
- **Joiner–Mover–Leaver (JML)** — tilganger håndteres gjennom hele livssyklusen
- **SaaS First** — standard skytjenester er hovedregelen
- **Informasjonssikkerhet og personvern**
  - Datalokasjon i EU/EØS,
  - Samsvar med Normen, GDPR og NSM grunnprinsipper
  - Sårbarhetshåndtering og fjernoppdatering av enheter