

TA-01-A

Vedlegg A – Arkitekturprinsipper

Nytt fagsystem

GARANTIKASSEN FOR FISKERE

A.1 Formål, omfang og sammenheng.....	2
A.2 Grunnleggende arkitekturprinsipper.....	2
A.3 Konfigurasjon, regelverk og endringshåndtering	3
A.4 Dataprinsipper, historikk og sporbarhet	3
A.5 Integrasjons- og datakildeprinsipper	4
A.6 Sikkerhetsprinsipper	4
A.7 Personvern, etterlevelse og kontroll.....	5
A.8 Robusthet, drift og skalerbarhet.....	5

A.1 Formål, omfang og sammenheng

Dette vedlegget beskriver overordnede arkitektur- og kvalitetsprinsipper som skal legges til grunn for utvikling, videreutvikling og forvaltning av nytt fagsystem hos Garantikassen for Fiskere (GFF).

Formålet er å sikre at løsningen utformes som en robust, fleksibel og langsiktig plattform som:

- kan videreutvikles og forvaltes på en kontrollert måte
- kan understøtte både mannskapsbaserte og fartøybaserte ordninger
- muliggjør etablering av nye ordninger med minst mulig behov for endringer i programkode

Vedlegget omfatter prinsipper knyttet til:

- arkitektur og modularisering
- konfigurasjon og regelstyring
- datahåndtering, historikk og sporbarhet
- integrasjoner og datakilder
- sikkerhet, personvern og etterlevelse
- robusthet, drift og skalerbarhet

Prinsippene i dette vedlegget er normerende og skal være styrende for arkitekturvalg, teknisk design, implementasjon og videreutvikling av løsningen. Avvik fra prinsippene skal identifiseres, begrunnes og dokumenteres i leverandørens tilbud.

Detaljerte og utfyllende krav knyttet til sikkerhet, identitet og tilgang, logging, sporbarhet og revisjon fremgår av tilhørende vedlegg:

- TA-01-B – Sikkerhetsarkitektur
- TA-01-C – Identitet- og tilgangsstyring
- TA-01-D – Sporbarhet og revisjon

Dette vedlegget skal leses i sammenheng med disse, men inneholder de overordnede arkitektur- og kvalitetsmessige føringene for løsningen.

A.2 Grunnleggende arkitekturprinsipper

Dette kapittelet beskriver de grunnleggende prinsippene for hvordan løsningen skal struktureres. Prinsippene skal sikre at systemet er forståelig, endringsbart og motstandsdyktig mot feil.

Dersom disse prinsippene ikke følges, vil løsningen raskt bli vanskelig å vedlikeholde, krevende å videreutvikle og sårbar for feil ved endringer.

A.2.1 Løsningen skal bygges som en modulær og løst koblet arkitektur der hovedkomponenter og domener kan utvikles, endres eller erstattes uten omfattende endringer i øvrige deler av systemet.

A.2.2 Løsningen skal struktureres rundt tydelige forretningsdomener, herunder blant annet Fartøy, Mannskap, Ordninger og økonomiske prosesser, med klare ansvarsgrenser mellom domenene.

A.2.3 Arkitekturen skal være teknologinøytral og ikke låst til spesifikke produkter eller leverandører, og skal støtte utskiftning av komponenter uten vesentlig ombygging.

A.3 Konfigurasjon, regelverk og endringshåndtering

Dette kapittelet beskriver hvordan regelverk og konfigurasjon skal håndteres i løsningen. Regelendringer er en naturlig del av GFFs virksomhet, og løsningen må kunne håndtere dette uten omfattende utviklingsarbeid.

Dersom regelverk implementeres som hardkodet logikk, vil selv små endringer kunne medføre kostbare og risikofylte systemendringer.

A.3.1 Regelverk, parametere og satser skal i størst mulig grad styres gjennom konfigurasjonsdata og ikke implementeres som hardkodet logikk.

A.3.2 Endringer i regler, parametere og budsjetter skal versjoneres slik at historiske konfigurasjoner bevares.

A.3.3 Løsningen skal støtte etablering av nye ordninger og regeltyper uten at eksisterende historiske vedtak eller data påvirkes.

A.4 Dataprinsipper, historikk og sporbarhet

Dette kapittelet beskriver hvordan data skal håndteres for å sikre konsistens, historikk og etterprøvbarehet. Dette er kritisk for økonomiske prosesser, revisjon og tillit til systemet.

Manglende sporbarhet eller historikk vil gjøre det vanskelig å forklare vedtak, håndtere klager og gjennomføre revisjon.

A.4.1 Systemet skal sikre konsistens mellom søknad, vedtak, budsjett og utbetaling.

A.4.2 Historiske vedtak, beregninger og betalingsfiler skal ikke kunne endres, og full historikk skal bevares.

A.4.3 Alle vedtak og betalingsfiler skal kunne reproduseres basert på historiske data og konfigurasjoner.

A.4.4 Alle sentrale objekter skal ha entydige og stabile identifikatorer.

A.5 Integrasjons- og datakildeprinsipper

Dette kapitlet beskriver hvordan løsningen skal integrere med eksterne systemer og håndtere datakilder. Løsningen vil være avhengig av informasjon fra flere eksterne kilder, og det er avgjørende at disse integrasjonene er stabile, sporbare og konsistente.

Uklare ansvarsforhold for data eller svake integrasjoner vil føre til feil beslutningsgrunnlag, inkonsistente data og økt risiko for feilutbetalinger.

A.5.1 Integrasjoner skal baseres på åpne, dokumenterte og standardiserte grensesnitt.

A.5.2 Løsningen skal støtte API-baserte og filbaserte integrasjoner avhengig av den enkelte integrasjonens behov og tilgjengelige grensesnitt. Det er ikke krav om at samme integrasjon skal implementeres med begge integrasjonsformer.

A.5.3 Integrasjoner skal være robuste og håndtere feil, forsinkelser og avvik uten å kompromittere datakvalitet.

A.5.4 Løsningen skal sikre sporbarhet for data mottatt fra eksterne systemer.

A.5.5 Løsningen skal sikre at data fra eksterne kilder kan valideres og kontrolleres.

A.5.6 Tekniske identifikatorer og integrasjonsgrensesnitt skal utformes uten bruk av nasjonale spesialtegn (æ, ø, å) for å sikre robusthet, interoperabilitet og forutsigbar håndtering av tegnssett på tvers av systemer og integrasjoner.

Dette gjelder blant annet identifikatorer, feltnavn, API-parametere og andre tekniske navn som benyttes i datamodeller og integrasjoner.

A.6 Sikkerhetsprinsipper

Dette kapitlet beskriver grunnleggende prinsipper for informasjonssikkerhet.

Løsningen skal beskytte sensitive data og sikre korrekt bruk av systemet.

Manglende sikkerhet vil kunne føre til datalekkasjer, misbruk av systemet og tap av tillit.

A.6.1 Tilgang til funksjoner og data skal begrenses til det som er nødvendig for brukerens rolle (minste privilegium).

A.6.2 Kritiske oppgaver skal fordeles mellom roller for å redusere risiko for feil og misbruk.

A.6.3 Alle kritiske operasjoner skal være sporbare til identifisert bruker eller systemkomponent.

A.6.4 Løsningen skal forhindre at samme vedtak eller utbetaling kan gjennomføres flere ganger.

A.7 Personvern, etterlevelse og kontroll

Dette kapittelet beskriver krav til personvern og etterlevelse av regelverk. Løsningen skal håndtere personopplysninger på en kontrollert og forsvarlig måte.

Feil håndtering av personopplysninger kan føre til brudd på lovverk, økonomiske sanksjoner og tap av tillit.

A.7.1 Løsningen skal utformes etter prinsippet om innebygd personvern.

A.7.2 Systemet skal kun behandle personopplysninger som er nødvendige for definerte formål.

A.7.3 Tilgang til personopplysninger skal være rollebasert og kontrollerbar.

A.7.4 Bruk av personopplysninger skal logges på en måte som muliggjør revisjon.

A.7.5 Løsningen skal støtte dokumentasjon, arkivering og innsyn i henhold til gjeldende krav.

A.7.6 Løsningen skal støtte internkontroll og etterprøvbarhet av økonomiske disposisjoner.

A.7.7 Løsningen skal legge til rette for risikobasert informasjonssikkerhet.

A.8 Robusthet, drift og skalerbarhet

Dette kapittelet beskriver krav til stabil drift og evne til å håndtere endringer i belastning og feil. Systemet må kunne håndtere både normal drift og avvikssituasjoner uten å kompromittere datakvalitet.

Manglende robusthet vil føre til driftsavbrudd, datatap og redusert tillit til systemet.

A.8.1 Kritiske operasjoner skal være atomiske og enten fullføres helt eller ikke gjennomføres.

A.8.2 Løsningen skal håndtere driftsavbrudd uten å etterlate inkonsistente data.

A.8.3 Løsningen skal støtte gjenopptak av behandling etter avbrudd.

A.8.4 Løsningen skal støtte ny utsendelse av tidligere genererte betalingsfiler uten ny beregning.

A.8.5 Løsningen skal legge til rette for full revisjonssporbarhet.

A.8.6 Løsningen skal kunne håndtere økt volum av data og transaksjoner uten vesentlig ombygging.