

TA-01-D

Vedlegg D – Journalføring av endringer

Nytt Fagsystem

GARANTIKASSEN FOR FISKERE

D.1. Formål	2
D.2. Overordnet arkitektur	2
D.3. Hvilke data skal journalføres	2
D.4. Audit-informasjon	3
D.5. Forretningskontekst	3
D.6. Sikkerhet og integritet	4
D.7. Sikring av endringsjournal	4
D.8. Volum, ytelse og drift	4
D.9. Oppbevaring og behandling av endringsjournal	4
D.10. Bruk til revisjon og etterkontroll	6
D.11. Avgrensning av løsningens omfang	7

D.1. Formål

Dette kapittelet beskriver formålet med journalføring av endringer (audit) i løsningen. Journalføring er et sentralt virkemiddel for å sikre sporbarhet, kontroll og etterprøvnbarhet i systemet.

Manglende eller ufullstendig journalføring vil kunne føre til manglende tillit til data, redusert revisjonsevne og økt risiko for feilutbetalinger og misbruk.

D.1.1 Løsningen skal sikre full sporbarhet for alle endringer (INSERT, UPDATE og DELETE) på forretningskritiske data.

D.1.2 Løsningen skal dokumentere hvem som utførte en endring.

D.1.3 Løsningen skal dokumentere hva som ble endret.

D.1.4 Løsningen skal dokumentere når endringen ble utført.

D.1.5 Løsningen skal dokumentere relevant kontekst (sak, prosess, kilde og årsak) for endringen.

D.1.6 Løsningen skal beskytte auditdata mot manipulering.

D.1.7 Audit-loggen skal være append-only og ikke kunne oppdateres eller slettes av applikasjonen.

D.2. Overordnet arkitektur

Dette kapittelet beskriver hvordan auditløsningen er integrert i systemet. Journalføring skal være en innebygd del av datalaget og skje automatisk ved alle relevante endringer. Dersom audit ikke skjer konsistent og transaksjonelt, vil det kunne oppstå avvik mellom data og logg, noe som svekker etterprøvnbarheten.

D.2.1 Audit skal utføres automatisk ved endringer i forretningskritiske data.

D.2.2 Audit skal skje i samme transaksjon som den opprinnelige endringen.

D.2.3 Audit skal være uavhengig av hvilken applikasjon eller integrasjon som utfører endringen.

D.2.4 Auditdata skal lagres separat fra ordinære forretningsdata.

D.2.5 Auditdata skal ikke kunne endres eller slettes av applikasjonsroller.

D.3. Hvilke data skal journalføres

Dette kapittelet beskriver hvilke typer data som skal omfattes av journalføring. Fokus skal være på data som har betydning for vedtak, økonomi og rettigheter. Feil avgrensning vil enten gi manglende sporbarhet eller unødvendig datavolum.

D.3.1 Løsningen skal journalføre endringer i registerdata.

D.3.2 Løsningen skal journalføre endringer i vedtak og ordninger.

D.3.3 Løsningen skal journalføre økonomiske disposisjoner.

D.3.4 Løsningen skal journalføre endringer i tilgangsstyring og roller.

D.3.5 Løsningen skal kunne konfigurere hvilke tabeller som anses som forretningskritiske.

D.3.6 Tekniske hjelpetabeller og midlertidige data som ikke påvirker vedtak, økonomiske disposisjoner, tilgangsstyring eller revisjonsspor skal som hovedregel ikke journalføres.

D.3.7 Journalføringskravene skal også omfatte direkte endringer i forretningskritiske data som utføres utenom ordinære applikasjonsfunksjoner, herunder administrative eller tekniske databaseoperasjoner.

D.4. Audit-informasjon

Dette kapittelet beskriver hvilken informasjon som skal lagres for hver endring.

Mangelfull informasjon vil gjøre det vanskelig å forstå hva som faktisk har skjedd og hvorfor.

D.4.1 Løsningen skal lagre tidspunkt for endringen.

D.4.2 Løsningen skal lagre identitet på aktør (bruker eller system).

D.4.3 Løsningen skal lagre type operasjon (opprettelse, endring, sletting).

D.4.4 Løsningen skal lagre hvilket objekt som er endret.

D.4.5 Løsningen skal lagre verdier før og etter endringen.

D.4.6 Løsningen skal lagre hvilke felter som faktisk er endret.

D.4.7 Løsningen skal lagre tilgjengelig forretningskontekst.

D.4.8 For endringer utført av tekniske identiteter skal auditinformasjonen identifisere den tekniske aktøren og, der handlingen er initiert av en bruker, inneholde entydig og sporbar kobling til den initierende brukeren. Koblingen skal kunne dokumenteres uten omfattende manuell sammenstilling av informasjon fra flere kilder.

D.5. Forretningskontekst

Dette kapittelet beskriver hvordan kontekst knyttes til endringer. Kontekst er nødvendig for å forstå hvorfor en endring er gjort, ikke bare hva som er gjort.

Manglende kontekst vil redusere verdien av audit ved revisjon og etterkontroll.

D.5.1 Applikasjonen skal knytte kontekstopplysninger til endringer.

D.5.2 Kontekst skal inkludere identitet på aktør.

D.5.3 Kontekst skal inkludere kilde (applikasjon eller integrasjon).

D.5.4 Kontekst skal inkludere saks- eller prosessreferanse for hendelser knyttet til behandling, vedtak, utbetaling, tilgangsendringer eller andre forretningskritiske

operasjoner.

D.5.5 Kontekst skal inkludere begrunnelse der dette er tilgjengelig.

D.6. Sikkerhet og integritet

Dette kapittelet beskriver krav til beskyttelse av auditdata. Auditloggen må være troverdig og ikke kunne manipuleres.

Dersom auditdata kan endres, mister løsningen sin verdi ved revisjon.

D.6.1 Auditdata skal være beskyttet mot endring og sletting.

D.6.2 Auditdata skal kun kunne utvides (append-only).

D.6.3 Tilgang til auditdata skal være begrenset og kontrollert.

D.6.4 Løsningen skal støtte ekstern etterkontroll av auditdata.

D.7. Sikring av endringsjournal

Dette kapittelet beskriver hvordan selve journalen sikres.

Manglende sikring vil kunne føre til manipulering eller uautorisert innsyn.

D.7.1 Endringsjournalen skal være beskyttet mot uautorisert tilgang.

D.7.2 Endringsjournalen skal være beskyttet mot uautorisert endring og sletting.

D.7.3 Tilgang til endringsjournalen skal logges i løsningens sikkerhetslogging, men skal ikke journalføres i endringsjournalen.

D.7.4 Kun særskilt autorisert personell skal ha lesetilgang.

D.8. Volum, ytelse og drift

Dette kapittelet beskriver krav knyttet til datamengde og ytelse. Audit kan generere store datamengder og må håndteres uten å påvirke systemets funksjon.

Manglende håndtering av volum vil kunne føre til ytelsesproblemer og driftsutfordringer.

D.8.1 Journalføring skal ikke påvirke normal saksbehandling negativt.

D.8.2 Løsningen skal håndtere forventet datavolum over systemets levetid.

D.8.3 Løsningen skal kunne driftes og vedlikeholdes på en forutsigbar og kontrollerbar måte.

D.9. Oppbevaring og behandling av endringsjournal

Dette kapittelet beskriver hvordan auditdata skal lagres, behandles og beskyttes.

Auditdata er nødvendig for revisjon, etterprøvbarehet, internkontroll og rekonstruksjon av historiske tilstander.

Feil håndtering av auditdata kan føre til brudd på regelverk, uautorisert innsyn, tap av historikk eller redusert tillit til løsningens revisjonsspor.

Auditdata kan inneholde personopplysninger og andre sensitive opplysninger dersom dette er nødvendig for revisjon, etterprøvbarhet og dokumentasjon av historiske endringer. Tilgang til slike opplysninger skal være særskilt regulert og begrenset til autoriserte roller.

Løsningen skal støtte skjerming eller pseudonymisering av sensitive identifikatorer i visninger, søk og rapporter der full identitet ikke er nødvendig for arbeidsoppgaven.

Eksempler:

- Fødselsnummer: *****4321
Kontonummer: *****7890

Dersom løsningen benytter strukturerte logger eller hendelsesmodeller, skal sensitive felt kunne klassifiseres eller merkes slik at visning, eksport og rapportering kan styres basert på sensitivitet og tilgangsnivå.

Eksempel på strukturert loggmodell:

```
{
  "eventType": "PaymentValidation",
  "personId": {
    "value": "12345678901",
    "classification": "sensitive",
    "masking": "last4"
  },
  "accountNumber": {
    "value": "12345678901",
    "classification": "sensitive",
    "masking": "last4"
  },
  "caseId": {
    "value": "SAK-2026-00123",
    "classification": "internal",
    "masking": "none"
  }
}
```

Eksempelet er illustrerende og beskriver ønsket prinsipp for klassifisering og håndtering av sensitive felt. Leverandør står fritt til å velge teknisk implementasjon.

D.9.1 Oppbevaringstid skal fastsettes per datakategori.

D.9.2 Oppbevaring skal følge gjeldende regelverk og arkivkrav.

D.9.3 Auditdata skal behandles som sensitiv informasjon.

D.9.4 Tilgang til auditdata skal begrenses etter prinsippet om minste privilegium og være underlagt særskilt tilgangskontroll.

D.9.5 Løsningen skal støtte rollebasert tilgang til auditdata og revisjonsinformasjon.

D.9.6 Administrative visninger og rapporter skal støtte skjerming eller pseudonymisering av sensitive identifikatorer der dette er relevant.

D.9.7 Personidentifikatorer og andre sensitive identifikatorer skal som hovedregel ikke eksponeres i klartekst i administrative rapporter, søkevisninger eller generelle arbeidsflater. Full visning skal kreve særskilt autorisasjon og være begrunnet i definert arbeidsoppgave.

D.9.8 Tilgang til fullstendige identifikatorer skal være særskilt autorisert og revisjonssporbar.

D.9.9 Eksport og rapportering av auditdata skal følge samme krav til tilgangskontroll og skjerming som visning i løsningen.

D.9.10 Løsningen skal støtte klassifisering av loggede felt eller attributter slik at visning, eksport og rapportering kan styres etter sensitivitet og tilgangsnivå.

D.9.11 Løsningen skal støtte maskering eller pseudonymisering av sensitive felt i loggvisninger og rapporter basert på feltklassifisering, rolle og kontekst.

D.10. Bruk til revisjon og etterkontroll

Dette kapittelet beskriver hvordan audit skal brukes i praksis.

Uten gode muligheter for analyse og innsyn mister audit sin verdi.

D.10.1 Løsningen skal vise historikk for enkeltobjekter.

D.10.2 Løsningen skal vise endringer utført av en aktør.

D.10.3 Løsningen skal muliggjøre rekonstruksjon av tidligere tilstand.

D.10.4 Løsningen skal knytte endringer til sak eller prosess der dette er relevant.

D.10.5 Tilgang til auditdata skal være lesebasert og særskilt regulert.

D.11. Avgrensning av løsningens omfang

Dette kapittelet beskriver hva auditløsningen ikke skal dekke. Dette er viktig for å unngå feil forventninger til løsningen.

D.11.1 Journalføring skal kun omfatte strukturerte endringer i forretningsdata.

D.11.2 Løsningen skal ikke erstatte arkivsystem.

D.11.3 Løsningen skal ikke erstatte dokumenthåndtering.

D.11.4 Løsningen skal ikke erstatte generell applikasjons- eller driftslogging.