

## **TEKNISKE RAMMEBETINGELSER**

### **DATA OG INTEGRASJON I AVINOR**

#### **1 FORMÅL**

Dette dokumentet inneholder Avinors krav og retningslinjer for integrasjoner, data og utveksling av informasjon. Avinors Kontraktsparter forplikter seg til å etterleve kravene som følger av dette dokumentet. Det skal sikres at kravene også følges av eventuelle underleverandører og leverandørkjeden for øvrig, så langt det med rimelighet kan kreves.

Formålet med retningslinjene er å sikre at Avinor på en strukturert, sikker og effektiv måte kan motta, lagre, analysere og følge opp data fra leverandør i egne løsninger, herunder for løpende status-, trend- og kvalitetsoppfølging. Leverandøren skal ha en dokumentert og systematisk prosess for styring av informasjonssikkerhet, i tråd med god praksis på området, som også skal inneholde risikostyring for tjenesten og/eller systemer.

#### **2 OVERORDNET KRAV**

Leverandør plikter å etterleve Avinors gjeldende retningslinjer for dataoverføring, systemintegrasjon og informasjonssikkerhet i hele kontraktsperioden. Informasjon som Avinor genererer/prosesserer i tjenesten, skal eies av Avinor. Avinor skal ha tilgang til egne data vederlagsfritt. Avinors informasjon skal ikke kopieres eller brukes utenfor rammen av tjenesteleveransen som angitt i kontrakten.

Avinors retningslinjer kan endres over tid, og Leverandør har ansvar for å tilpasse leveransen i tråd med oppdaterte krav. Kun personell som er nødvendig for å oppfylle avtalen skal få tilgang basert på need-to-know og minste privilegium.

Ved behandling av personopplysninger fra Avinor, skal Leverandøren lagre og behandle data i EU/EØS. Leverandøren skal i tråd med GDPR/Personopplysningsloven varsle Avinor uten ugrunnet opphold etter å ha blitt kjent med et brudd på personopplysningssikkerheten eller ved sikkerhetshendelser som berører Avinor.

Leverandør skal sørge for løpende overvåking av relevante sikkerhetsoppdateringer, særskilt håndtering av kritiske oppdateringer, rollback-mulighet ved feil og tydelig ansvarsfordeling. Eventuelt skal kompensierende tiltak innføres, om relevante sikkerhetsoppdateringer ikke foreligger.

Om tjenesten leveres i leverandørforvaltet skyinfrastruktur, skal Leverandøren ha en dokumentert prosess for Cloud Security Posture Management (CSPM) som dekker

omfang, baselines, oppdagelse av feilkonfigurasjoner, prioritering, unntakshåndtering, utbedring og oppfølging.

Leverandør skal ha et drifts- og vedlikeholdsregime som sikrer at alle komponenter holdes oppdatert med sikkerhetsoppdatering, patcher og versjoner som er lisensierte. Det vil si at lisensene ikke skal være i perioder som benevnes av Leverandøren som EOS (End of service) eller EOL (End of life). Lisensene skal være reelle lisenser for virksomheter som Avinor, og ikke prøve-versjoner eller versjoner beregnet til privat forbruk.

### **3 KRAV TIL DATAOVERFØRING**

Leverandør skal sørge for at alle data som er omfattet av leveransen kan overføres elektronisk til Avinors systemer.

Dataoverføringen skal være helautomatisert, slik at:

- Avinor skal som hovedregel kunne motta data direkte fra Leverandørens systemer uten manuell behandling
- Data skal være maskinlesbart i et format som Avinor godkjenner og egnet for videre behandling i Avinors systemer

Leverandøren forventes å støtte dataoverføringsmetoder som:

- Messaging: Overføring av data ved bruk av asynkrone hendelsesbaserte protokoller (publish-subscribe), for eksempel Java Message Service, Apache Kafka eller WebHooks.
- Remote Procedure Invocation: Overføring av data ved bruk av synkrone spørringer (request-reply) til for eksempel et REST API eller ETL (Extract Transform Load) og ELT (Extract Load Transform).
- File Transfer: Overføring av data ved bruk av filoverføringsmetoder (for eksempel JSON, XML, CSV, XLSX, etc.)
- Delta Share: For sikker deling av store datasett i sanntid.

Data skal kunne overføres enten periodisk (batch), på forespørsel eller nær sanntid, avhengig av Avinors løpende behov i samsvar med kontraktens formål og eventuelle krav.

Leverandøren skal som minimum levere data i en feltstruktur (navn, datatype, obligatorisk/valgfritt), og metadata må angi datasettets beskrivelse, tidsstempel og unik ID per melding/fil til Avinor.

Ved rapportering til Avinor i form av data knyttet til tjenestens utforming, forventer Avinor at Leverandør rapporterer på en standardisert måte, ref. beskrivelser i kapittel 2.

## **4 KRAV TIL INTEGRASJON**

Dataoverføring skal skje via standardiserte og dokumenterte integrasjoner.

Dataoverføringen skal benytte standardiserte metode for autentisering og kryptering mellom kommunikasjonspartnerne, som OpenID connect eller tilsvarende og overføring skal være kryptert med TLS 1.2 eller nyere.

Integrasjoner skal kun benyttes til overføring av data, og skal ikke etablere funksjonell avhengighet mellom partenes løsninger.

Utvikling av integrasjoner skal baseres på etablerte integrasjonsmønstre, fortrinnsvis:

- Publish-subscribe (messaging, events)
- Request-response (SOAP, REST, gRPC, eller tilsvarende)

Integrasjoner skal muliggjøre overvåking, feilhåndtering og sporbarhet, slik at Avinor kan følge opp:

- Datakvalitet
- Dataintegritet
- Datatilgjengelighet
- Leveransefrekvens
- Avvik og trender over tid

Integrasjonen skal sikre pålitelig og sikker datautveksling med Avinors systemer.

Alle eksternt eksponerte API-er skal håndheve autorisasjon på serversiden, slik at klienter kun får tilgang til ressurser de er autorisert til og mekanismer skal kunne regulere trafikk/trafikkmengde.

Eksternt eksponerte API-er skal ha tiltak mot misbruk, inkludert «rate limiting» og input-validering.

Tjenesten skal implementere en tilgangskontrollarkitektur basert på kontinuerlig verifisering, minste privilegium, segmentering og betinget tilgang for privilegerte eller høyrisiko-handlinger.

Tjenesten skal overvåkes, og aktiviteter og hendelser som påvirker sikkerheten skal loggføres. Logger skal beskyttes mot uautorisert endring og sletting, krypteres i hvile, og være underlagt streng tilgangsstyring.

## 5 KRAV TIL AUTENTISERING OG IDENTITETSFORVALTNING

I tilfeller der Leverandørs personell skal arbeide aktivt i samhandling med Avinors løsninger, utløses krav til autentisering og identitetsstyring. Samhandling med Avinors løsninger inkluderer:

- Bruk av Avinor-drevne løsninger
- Tilgang til Avinors digitale flater
- Gjennomføring av oppgaver som identitetskontroll

Leverandør skal gjennomgå og tilpasse egne IT-strukturer og arbeidsprosesser for å kunne etterleve Avinors gjeldende rammeverk for autentisering, autorisasjon og identitetsforvaltning.

All tilgang skal være personlig, sporbar og rollebasert, og følge Avinors til enhver tid gjeldende sikkerhetskrav. Basert på tjenstlig behov, minste privilegium, rollebasert tilgangsstyring, i tråd med god praksis på området, og håndheves på serversiden. Tilganger skal gjennomgå en gang per år, som et minimum. Dersom en bruker med tilgang fratrer eller endrer rolle, skal tilgangen revideres umiddelbart.

Tjenesten skal implementere en konsistent tilgangskontrollmekanisme (RBAC, ABAC eller tilsvarende) med deny-by-default og server-side håndhevelse på tvers av brukergrensesnitt, API-er og backend-tjenester.

Autorisasjon skal verifiseres på objekt- og funksjonsnivå slik at brukere kun får tilgang til ressurser og handlinger de eksplisitt er autorisert for.

Personell hos Leverandøren med privilegert tilgang til tjenesten skal bruke separate privilegerte kontoer og være underlagt minst like strenge eller strengere kontroller enn ordinære kundebrukere, inkludert godkjenning, multifaktorausentisering, logging, overvåking og periodisk gjennomgang. Privilegert tilgang skal bare gis for definerte oppgaver og fjernes eller reduseres når behovet opphører.

Multifaktoraутентisering (MFA) skal benyttes ved all innlogging til tjenesten, inkludert for privilegerte og administrative kontoer. MFA skal også kreves ved endring av sikkerhetssoner, kryssing av tillitsgrenser eller ved heving av privilegier i tjenesten. Leverandøren skal benytte robuste MFA-metoder (f.eks. app-basert autentisering, maskinvaretoken eller FIDO2) og ha dokumentert policy for håndtering av unntak og fallback-løsninger. Passord skal være sterke og skal lagres med anerkjent, sterk hashing med salt. Standardpassord skal ikke forekomme

## **6 HÅNDTERING AV FEILSITUASJONER**

Tjenesten skal være innrettet slik at Leveransen raskt kan komme tilbake til normal driftssituasjon, uten nevneverdig tap av data, om en feilsituasjon eller hendelse oppstår.

Leverandøren skal ha en prosess for håndtering av hendelser med en kundedialog som ivaretar Avinors behov for informasjon om operativ status og underlag for videreformidling til overordnede myndigheter.

Avinor, v. avtalens representant/kontaktperson, skal varsles uten ugrunnet opphold med tilstrekkelig informasjon for å kunne tilrettelegge for nødvendige endring(er) i sitt miljø.

## **7 KRAV TIL UNDERLEVERANDØRER**

Underleverandører skal ikke benyttes uten godkjenning fra Avinor. Ved bruk av underleverandører skal det foreligge en eksplisitt godkjenningsprosedyre for godkjenning av slike underleverandører.

Leverandør skal ikke benytte underleverandører som behandler Avinors data eller inngår i leveransen uten forhåndsgodkjenning fra Avinor.

Leverandør skal sikre at underleverandører er underlagt minst tilsvarende krav til sikkerhet, personvern, logging, varsling, tilgangsstyring og revisjon.

Leverandør skal kunne dokumentere hvor i leverandørkjeden Avinors data behandles.

## **8 LEVERANDØRAVTALER SKAL SIKRE SIKKERHETSREVISJON OG OPPFØLGING**

Leverandøren skal inngå skriftlige avtaler med sine underleverandører og samarbeidspartnere som sikrer Avinors rett til revisjon og kontroll av etterlevelse av avtalte krav, herunder ved bruk av egenerklæring og/eller tredjepartsrevisjon.

Avtalene skal videre pålegge underleverandører og samarbeidspartnere å fremlegge relevant dokumentasjon uten ugrunnet opphold ved forespørsel fra Leverandøren eller Avinor.

Underleverandører og samarbeidspartnere skal også være forpliktet til å dokumentere gjennomførte risikovurderinger, registrerte hendelser, identifiserte sårbarheter samt iverksatte og planlagte tiltak. Slik dokumentasjon skal på forespørsel gjøres tilgjengelig for Avinor.

Leverandøren er ansvarlig for at de nevnte forpliktelsene etterleves av underleverandører og samarbeidspartnere som om de var Leverandørens egne forpliktelser.

## **9 BRUDD PÅ TEKNISKE KRAV**

Leverandøren skal uten ugrunnet opphold melde fra om ethvert avdekket brudd på kravene i dette dokumentet, både i egen virksomhet og hos eventuelle underleverandører.

Leverandør skal umiddelbart iverksette nødvendige aksjoner for å rette de aktuelle brudd. Avinor kan kreve at det legges fram en tiltaksplan for når og hvordan bruddene skal rettes.

Brudd på Avinors tekniske krav vil kunne anses som vesentlig mislighold av kontraktens forpliktelser, og vil kunne medføre at Avinor:

- Iverksetter midlertidig stans i leveransen. Avinor vil under midlertidig stans ha anledning til å foreta erstatningskjøp hos annen leverandør.
- Krever at Leverandør bytter underleverandør. Dette skal skje uten kostnad for Avinor.
- Hever kontrakten med Leverandøren jf. også kontraktens bestemmelser.