NORDIVÉ AAVITSLAND
Org.nr 931 147 549 · Myrabakken 4, Norge
kontakt@nordiveai.no

DOK-NR: NOR-ARK-001
VERSJON: 2.0
DATO: 20.05.2026
OFFENTLIG

SIKKERHETSARKITEKTUR

Sikkerhetsarkitektur for tjenesten Nordivé

Teknisk beskrivelse av dataflyt, kryptering, autentisering, underbehandlere og residency-praksis for advokatfirma-vurdering.

Utsteder	Nordivé Aavitsland
Gjelder for	Tjenesten Nordivé (app.nordiveai.no) og marketing-nettstedet nordiveai.no
Målgruppe	Sikkerhets- og personvernansvarlige i advokatfirma som vurderer å ta i bruk Nordivé
Forankret i	GDPR art. 25 og 32, personopplysningsloven, advokatforskriften, NSM Grunnprinsipper for IKT-sikkerhet
Sist oppdatert	20. mai 2026

1. Sammendrag

Nordivé er en AI-assistert programvaretjeneste for norske advokater og juridiske avdelinger. Tjenesten leveres som SaaS og integreres med kundens eksisterende Microsoft 365-miljø.

Sikkerhetsarkitekturen er designet etter prinsippene *privacy by design*, *zero-trust* og *data minimization*. Kjerneprinsippet er at klientinnhold aldri lagres i en database eid eller drevet av Nordivé. Alt innhold lagres i kundens egen Microsoft OneDrive AppFolder, kryptert med nøkkel utledet fra kundens egen Microsoft-identitet.

Alle databehandlende komponenter er hostet innenfor EU/EØS. AI-inferens benytter AWS Bedrock i eu-west-1 (Irland) med konfigurert Zero Data Retention. Det skjer ingen overføring av klientinnhold til tredjeland i normal drift.

2. Systemkomponenter

2.1 Frontend

Tjenestens brukergrensesnitt leveres som en Progressive Web App (PWA) hostet hos Vercel Inc. Frontend kjøres lokalt i advokatens nettleser og henter data fra to kilder:

- Direkte fra Microsoft Graph API (e-poster, kalender, OneDrive) ved hjelp av advokatens egne OAuth-tokens
- Fra Nordivés backend (AI-prosessering, klassifisering, formatering) over TLS 1.3

2.2 Backend

Backend består av Azure Functions hostet i Microsoft Azure Norway East-regionen (Stavanger). Funksjonene er stateless, det vil si at de ikke holder noen brukerdata i hukommelse mellom forespørsler.

Backend benytter Azure Table Storage (samme storage-konto som Functions runtime) for å lagre operasjonelle data som månedlig bruks- og quota-opptelling og sync-metadata. Klientinnhold lagres ikke i Azure Table Storage.

2.3 AI-inferens

AI-prosessering skjer i AWS Bedrock i eu-west-1 (Irland). Nordivé bruker tre Claude-modeller fra Anthropic:

Modell	Bedrock-id	Brukstilfelle
Claude Sonnet 4.6	eu.anthropic.claude-sonnet-4-6	Standard AI-assistent og dokument-analyse
Claude Opus 4.6	eu.anthropic.claude-opus-4-6-v1	Dyp analyse for komplekse juridiske dokumenter
Claude Haiku 4.5	eu.anthropic.claude-haiku-4-5-20251001-v1:0	Lette klassifiserings- og taggingsoppgaver

Bedrock er konfigurert med Zero Data Retention. Det innebærer at AWS og Anthropic ikke lagrer prompter eller responser etter inferens, og at innholdet ikke benyttes til å trene modellene.

2.4 Persistens-lag

Klientinnhold (chathistorikk, vedlegg, AI-genererte analyser, dokumenter) lagres i kundens egen Microsoft OneDrive AppFolder. AppFolder er et isolert område innen brukerens OneDrive som kun kan leses og skrives av Nordivé-applikasjonen som har fått eksplisitt OAuth-samtykke fra brukeren.

Innholdet krypteres med AES-256-GCM før det skrives til OneDrive. Krypteringsnøkkelen avledes fra brukerens Microsoft Object ID (OID) og holdes i applikasjons-minnet. Nøkkelen lagres aldri i klartekst på enheten eller på Nordivés servere.

2.5 OCR (Document Intelligence)

Når brukeren laster opp et skannet dokument som Claude ikke kan tolke direkte, benyttes Microsoft Azure Document Intelligence i EU-region som OCR-fallback. Document Intelligence beholder ikke kundeinnhold etter at OCR-prosessen er fullført.

3. Dataflyt

3.1 Pålogging

1. Brukeren klikker «Logg inn med Microsoft» i nettleseren
2. Microsoft Entra ID utfører OAuth 2.0 Authorization Code Flow med PKCE
3. Frontend mottar access-token og refresh-token; tokenene oppbevares kryptert lokalt i nettleseren og slettes ved utlogging
4. Backend verifiserer hver innkommende forespørsel ved å sjekke at tokenets eier matcher e-postadressen som er angitt i forespørselen, og at brukeren er på den allowlistede pilot-listen

3.2 E-post-lesning og triage

1. Nettleseren spør Microsoft Graph direkte etter brukerens innboks
2. E-postlisten kommer rett til nettleseren uten å passere Nordivés backend
3. Når brukeren åpner en e-post for AI-analyse, sendes innholdet til Nordivés backend over TLS 1.3
4. Backend videresender til AWS Bedrock (eu-west-1) for inferens
5. Bedrock returnerer respons i samme forespørsel-livssyklus uten å lagre noe
6. Backend videresender svaret til nettleseren; nettleseren beholder svaret i hukommelsen og krypterer det før det lagres i kundens OneDrive AppFolder

3.3 Dokument-analyse

1. Brukeren laster opp et dokument (PDF, DOCX) til nettleseren
2. For PDF: tekst ekstraheres i nettleseren via PDF.js. For DOCX: tekst ekstraheres via mammoth.js
3. Hvis dokumentet er skannet og tekstutvinning feiler, sendes det til Azure Document Intelligence i EU-region for OCR
4. Tekstinnholdet sendes til Nordivés backend, som videresender til AWS Bedrock for analyse
5. Respons leveres tilbake til nettleseren og lagres kryptert i OneDrive AppFolder

3.4 Sync på tvers av enheter

1. Nettleseren skriver og leser kryptert klientinnhold direkte til/fra Microsoft OneDrive AppFolder via Graph API
2. Sync-laget kjører i nettleseren, ikke på Nordivés backend
3. Når brukeren logger inn på en ny enhet, henter den nye enheten innholdet fra OneDrive og dekrypterer det med nøkkel utledet fra brukerens Microsoft OID

4. Underbehandlere

Tjenesten benytter fire aktive underbehandlere. Fullstendig oversikt med behandlingsformål, datakategorier og overføringsmekanisme finnes i separat dokument «Liste over underbehandlere» (NOR-UND-001).

Underbehandler	Rolle	Region
Microsoft Ireland Operations Limited	Azure Functions hosting, Entra ID, OneDrive-lagring, Document Intelligence OCR	Norway East (backend); kundens egen tenant-region (OneDrive); EU-region (Document Intelligence)
Amazon Web Services EMEA SARL	AWS Bedrock for AI-inferens	eu-west-1 (Irland)
Anthropic PBC	Leverandør av Claude-modellene som kjøres isolert i AWS Bedrock	EU (via AWS Bedrock)
Vercel Inc.	Hosting av frontend (nordiveai.no og app.nordiveai.no)	EU-edge (Frankfurt, Amsterdam)

Alle fire underbehandlerne er sertifisert under EU-U.S. Data Privacy Framework (DPF) som rettslig forsvarslag for tilfeller der morselskapet har hovedkontor i USA. Standard Contractual Clauses (SCC) er inntatt som subsidiær mekanisme i underbehandleravtalene. Nordivé har gjennomført Transfer Impact Assessment (TIA) for hver underbehandler i samsvar med Schrems II.

5. Kryptering

5.1 I transitt

- All HTTPS-trafikk benytter TLS 1.3
- Sertifikathåndtering: automatisert via Vercel (frontend) og Azure (backend)
- Backend-til-Bedrock-kommunikasjon: TLS 1.3 mot AWS Bedrock endpoint i eu-west-1

5.2 I ro

- Klientinnhold: AES-256-GCM på applikasjonsnivå, lagret i kundens egen OneDrive AppFolder (som i tillegg er kryptert av Microsoft)
- Hemmelige nøkler (API-nøkler, AWS-credentials): kryptert i Azure Functions Configuration
- Brukerkonto-metadata: AES-256 i Microsoft Azure Norway East
- Sikkerhetslogger: AES-256 i Microsoft Azure Norway East
- Quota- og bruksdata: AES-256 i Azure Table Storage (Norway East)

5.3 Nøkkelhåndtering

Applikasjonsnivå-krypteringsnøkkelen for klientinnhold avledes deterministisk fra brukerens Microsoft Object ID (OID). Det innebærer at:

- Nordivé har ikke selv tilgang til nøkkelen
- Nøkkelen kan ikke gjenopprettes uten gjenautentisering hos Microsoft
- Ved utlogging slettes nøkkelen fra nettleserens minne
- Ved kompromittering av nettleseren mister angriperen tilgang så snart access-tokenet utløper (typisk 1 time)

6. Tilgangskontroll og autentisering

6.1 Sluttbrukere

- Innlogging skjer utelukkende via Microsoft 365 OAuth 2.0 med PKCE
- Multifaktor-autentisering håndheves av kundens egen Microsoft 365-tenant; Nordivé arver kundens MFA-policy
- Access-tokens utløper etter 1 time og fornyes stille i bakgrunnen
- Refresh-tokens revokeres ved utlogging og slettes etter 8 timers inaktivitet

6.2 Administratortilgang (Nordivé-ansatte)

- Tilgang til produksjonsmiljø er begrenset til navngitte ansatte
- Multifaktor-autentisering er obligatorisk for all admin-tilgang
- Tilgang gis etter prinsipp om minste privilegium
- Alle administrative handlinger logges

6.3 Tjeneste-til-tjeneste

- Backend autentiserer mot AWS Bedrock med IAM-kredentialer lagret kryptert i Azure Functions Configuration
- Backend videresender brukerens egne tokens ved kall mot Microsoft Graph (on-behalf-of-flow)

7. Forsvar mot prompt injection

Tjenesten implementerer flere lag forsvar mot prompt injection, en kjent angrepsvektor mot generative AI-systemer:

- Input-klassifisering: eksternt innhold (e-post fra motpart, vedlegg, dokumenter) wrappes i markerte tagger som AI-modellen instrueres å behandle som data og ikke som instruksjoner
- Per-request UUID-salt rundt trusted instruksjoner gjør det umulig for angriper å lukke instruksjons-blokken
- Output-sanitering fjerner instruksjoner som modellen forsøker å gi til brukeren eller systemet (tool calls, URL-injeksjon)
- Følger Anthropics anbefalinger for prompt injection-forsvar i Claude 4-serien

8. Logging og overvåking

- Operasjonelle logger (forespørsel-id, status-koder, responstider) lagres i Azure Application Insights og Azure Monitor i Norway East
- Sikkerhetslogger oppbevares i 12 måneder
- Klientinnhold logges aldri
- Logger er tilgjengelige kun for autoriserte Nordivé-ansatte

9. Beredskap og hendelsesresponse

Nordivé har en formell prosess for å oppdage, vurdere og respondere på sikkerhetshendelser. Detaljer finnes i separat dokument «Sikkerhetserklæring» (NOR-SIK-001), seksjon 5.

Som databehandler varsler Nordivé behandlingsansvarlig (kunden) uten ugrunnet opphold ved bekreftet brudd på personopplysningssikkerhet, jf. GDPR art. 33 nr. 2. Behandlingsansvarlig sender deretter melding til Datatilsynet innen 72 timer, jf. art. 33 nr. 1.

10. Backup og forretningskontinuitet

- Klientinnhold lagres i kundens egen Microsoft OneDrive og inngår i Microsofts egne backup-mekanismer
- Nordivé tar backup av konfigurasjon, infrastruktur-tilstand og kildekode
- Recovery Time Objective (RTO): 4 timer for kritiske komponenter
- Recovery Point Objective (RPO): 24 timer for konfigurasjonsdata
- Hosting i Azure Norway East med innebygd zonal redundans

11. Sletting og dataportabilitet

11.1 Sletting av brukerkonto

Ved oppsigelse av kundekonto:

- Tilgang til tjenesten suspenderes umiddelbart
- Kunden har 30 dager til å eksportere klientinnhold fra sin egen OneDrive AppFolder
- Brukerkonto-metadata hos Nordivé slettes innen 30 dager etter avtaleopphør
- Quota- og bruksdata anonymiseres innen 90 dager

11.2 Sletting på brukerens forespørsel

Brukeren kan til enhver tid slette egne chats og dokumenter fra applikasjonen. Slettingen propageres til OneDrive AppFolder innen 5 minutter via sync-mekanismen.

11.3 Dataportabilitet

Kunden eier sitt eget innhold som ligger i Microsoft OneDrive AppFolder. Innholdet kan til enhver tid eksporteres via Microsoft Graph API uten Nordivés mellomledd.

12. Compliance-rammeverk

Rammeverk	Anvendelse
GDPR (forordning 2016/679)	Behandling av personopplysninger i hele tjenestens livssyklus
Personopplysningsloven (LOV-2018-06-15-38)	Norsk implementering av GDPR; gjelder fullt ut
Advokatforskriften	Taushetsplikt og lojalitetsplikt; tjenesten er designet for ikke å bryte disse

Rammeverk	Anvendelse
Ekomloven § 2-7b	Cookies og lokal lagring; se separat dokument «Lagring og cookies»
NSM Grunnprinsipper for IKT-sikkerhet	Selvevaluert implementert; relevante kontroller dokumentert
Schrems II Transfer Impact Assessment	Gjennomført og dokumentert for alle underbehandlere
ISO/IEC 27001:2022	Tilpasning til rammeverket er igangsatt; sertifisering planlagt
OWASP Top 10	Baseline-mitigasjoner implementert

13. Tilknyttede dokumenter

- Personvernerklæring (NOR-PER-001)
- Sikkerhetserklæring (NOR-SIK-001)
- Liste over underbehandlere (NOR-UND-001)
- Bruksvilkår (NOR-BRV-001)
- Lagring og cookies (NOR-COK-001)
- Databehandleravtale (DPA): inngås individuelt med hvert advokatfirma og er ikke offentlig distribuert

14. Kontakt

Spørsmål om sikkerhetsarkitekturen eller forespørsler om utfyllende dokumentasjon (TIA, DPIA, revisjonsrapporter under NDA) rettes til:

- Generelt og sikkerhet: kontakt@nordiveai.no
- Postadresse: Nordivé Aavitsland, Myrabakken 4, Norge

DOKUMENTKONTROLL

Versjon	Dato	Beskrivelse	Godkjent av
1.0	28.04.2026	Førsteutgave	Innehaver
2.0	20.05.2026	Komplett omskrivning til ren saksstil: fjernet konkurrentreferanser, korrigert AWS-region (eu-west-1), oppdatert kryptering-omtale, samlet sikkerhetskontakt under kontakt@nordiveai.no	Innehaver