NORDIVE AS
Org.nr 938 011 710 · Brønnveien 1A, 0283 Oslo
kontakt@nordive.ai

DOK-NR: NOR-ARK-001
VERSJON: 2.5
DATO: 25.09.2026
OFFENTLIG

SIKKERHETSARKITEKTUR

Sikkerhetsarkitektur for tjenesten Nordivé

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

Utsteder	Nordive AS
Gjelder for	Tjenesten Nordivé (app.nordive.ai) og marketing-nettstedet nordive.ai
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	25. september 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 Nordivé ikke har egen database for e-post, dokumenter eller saksinnhold. Saksdata, analyser og timeføringer lagres i kundens egen Microsoft OneDrive, i Nordivés appmappe.

Alle databehandlende komponenter er hostet innenfor EU/EØS. AI-inferens skjer i Azure OpenAI med EU-datasone (språkmodellene Terra og Sol) og i AWS Bedrock med EU-inferensprofiler (Claude). 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

Samme tjeneste finnes som app for Android og som Outlook-tillegg. I tillegg finnes skrivebordspanelet Nordivé Tid for Mac og Windows, som registrerer arbeidsaktivitet lokalt og synkroniserer tidsøkter til kundens OneDrive-appmappe (se personvernerklæringen § 2.6).

2.2 Backend

Backend består av Azure Functions hostet i Microsoft Azure Norway East-regionen (Oslo-området). 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 operasjonelle data: månedlig bruks- og quota-opptelling, sync-metadata, brukerregister, kostnadslogg og varslingsabonnement. E-post, dokumenter og saksinnhold lagres ikke der.

To unntak er verdt å nevne eksplisitt. Support-samtaler lagres i Azure Table Storage og support-vedlegg i en privat Azure Blob-container, begge i Norway East. Innholdet skrives av brukeren selv og kan inneholde klientinformasjon dersom brukeren velger å oppgi det. Support-meldinger slettes automatisk etter 30 dager og vedlegg etter 7 dager.

Slår brukeren på bakgrunnsanalyse, lagres et refresh-token for den brukeren i Azure Table Storage. Tokenet krypteres med AES-256-GCM med en egen tilfeldig nøkkel, og den nøkkelen er igjen kryptert (RSA-OAEP-256) med en ikke-eksporterbar HSM-nøkkel i Azure Key Vault, som backend når gjennom en administrert identitet. Tokenet slettes når funksjonen slås av, og etter 90 dager uten bruk. Samme ordning brukes for Teams-varsler når firmaet har slått dem på.

Har firmaet koblet til sentralbordet (Telia Smart Connect / Phonero), lagres samtaledata (numre, retning, tidspunkt og varighet) i Azure Table Storage i 90 dager for å lage timeforslag. Opplysninger eldre enn 90 dager slettes automatisk ved neste synkronisering.

Tjenesten har i tillegg en Azure Container App (`chat.nordive.ai`, Norway East) som strømmer svar fra assistenten til nettleseren. Den er stateless på samme måte som Functions, autentiserer hver forespørsel mot Entra ID, og lagrer ikke klientinnhold.

2.3 AI-inferens

Nordivé bruker to leverandører av språkmodeller, begge i EU:

Modell	Leverandør og region	Brukstilfelle
Terra	Azure OpenAI, utrulling `nordive-terra-eu`, ressurs i Sweden Central, EU-datasone	Analyse og sortering av e-post, også i bakgrunnsanalyse
Sol	Azure OpenAI, utrulling `nordive-sol-eu`, ressurs i Sweden Central, EU-datasone	Svarutkast, assistenten og vanskeligere e-poster; Nordwatch-forslag når firmaet har slått det på

En EU-datasone-utrulling betyr at forespørsler kan behandles i et hvilket som helst EU-land innenfor datasonen, og at data som eventuelt lagres for misbruksovervåking, blir i EU. Microsoft bruker ikke forespørsler eller svar til å trene modeller, og Nordivé bruker ikke funksjonen for lagrede svar (stored completions). Microsofts misbruksovervåking kan velge ut forespørsler og svar og oppbevare dem midlertidig for kontroll (Microsoft har oppgitt inntil 30 dager). Dataene lagres i EU, og eventuell manuell gjennomgang gjøres av autoriserte Microsoft-ansatte i EØS. Nordwatch-kall sendes i tillegg med `store: false`.

I AWS Bedrock bruker Nordivé tre Claude-modeller fra Anthropic, med EU-inferensprofiler. Kallene går til eu-west-1 (Irland), og profilen kan fordele forespørsler mellom AWS-regioner i EU:

Modell	Bedrock-id	Brukstilfelle
Claude Sonnet 4.6	eu.anthropic.claude-sonnet-4-6	Dokumentanalyse, gjennomgang av dokumenter og assistenten når brukeren velger det
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 lagrer ikke prompter eller responser etter inferens, og innholdet benyttes ikke til å trene modellene. Anthropic mottar ikke innholdet.

2.4 Persistens-lag

Klientinnhold (chathistorikk, vedlegg, AI-genererte analyser, dokumenter, oppgaver og timeføringer) lagres i kundens egen Microsoft OneDrive AppFolder. AppFolder er et eget område i brukerens OneDrive som Nordivé-applikasjonen får tilgang til etter brukerens samtykke. OneDrive krypterer alt innhold ved lagring.

De fleste filene krypteres i tillegg med AES-256-GCM før de skrives til OneDrive. Nøkkelen avledes med PBKDF2 (100 000 iterasjoner, SHA-256) fra brukerens Microsoft Object ID (OID). OID er en fast identifikator som står i brukerens tilgangstoken, og Nordivés backend utleder den samme nøkkelen når den skriver resultater fra bakgrunnsanalyse, samtaleforslag og Teams-varsler. Laget beskytter derfor mot at filene kan leses uten kjennskap til hvem de tilhører, men er ikke ende-til-ende-kryptering, og det beskytter ikke mot Microsoft eller Nordivé. Enkelte filer i appmappen er ikke kryptert i applikasjonslaget: en saksliste for assistenten (saksnummer, tittel, klientnavn, stikkord), en møteliste, og tidsøktene fra skrivebordspanelet.

2.5 OCR (Document Intelligence)

Når brukeren laster opp en PDF uten tekstlag, eller ber om ren tekstgjenkjenning, benyttes Microsoft Azure Document Intelligence i EU som OCR. 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 står på tjenestens allowliste

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
4. Backend sender innholdet til språkmodellen Terra i Azure OpenAI (EU-datasone), og ved behov én gang videre til Sol
5. Modellen returnerer svaret i samme forespørsel
6. Backend videresender svaret til nettleseren; nettleseren beholder svaret i hukommelsen og krypterer det før det lagres i kundens OneDrive AppFolder

Med bakgrunnsanalyse skjer det samme på serveren: Microsoft Graph varsler backend om ny e-post, backend henter e-posten med brukerens beskyttede refresh-token, analyserer den i minnet og legger resultatet i brukerens OneDrive-appmappe. En kø i Azure Storage holder bare abonnements-id og meldings-id.

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 Claude i 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 og Container Apps, Azure OpenAI (Terra og Sol), Azure Storage, Key Vault, Entra ID, OneDrive-lagring, Document Intelligence	Norway East (backend og lagring); Sweden Central med EU-datasone (Azure OpenAI); kundens egen tenant-region (OneDrive); EU (Document Intelligence)
Amazon Web Services EMEA SARL	AWS Bedrock for AI-inferens med Claude	EU-inferensprofiler, kall fra 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 (nordive.ai og app.nordive.ai)	Vercels nettverk, europeiske noder for norske brukere

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 1.2 eller nyere; Azure-kontoene krever minst TLS 1.2, og TLS 1.3 brukes der klienten støtter det
- HSTS er slått på for app.nordive.ai
- Sertifikathåndtering: automatisert via Vercel (frontend) og Azure (backend)

- Backend-til-modell-kommunikasjon: TLS mot Azure OpenAI og AWS Bedrock

5.2 I ro

- Klientinnhold: lagret i kundens egen OneDrive AppFolder, kryptert av Microsoft, og for de fleste filene i tillegg AES-256-GCM på applikasjonsnivå (se 2.4)
- Refresh-tokens for bakgrunnsanalyse og Teams-varsler: AES-256-GCM, nøkkel pakket inn med HSM-nøkkel i Azure Key Vault
- Hemmelige nøkler (API-nøkler, AWS-credentials): krypterte applikasjonsinnstillinger i Azure, enkelte i Azure Key Vault
- Brukerkonto-metadata: AES-256 i Microsoft Azure Norway East
- Applikasjonslogger: AES-256 i Azure Monitor (Norway East)
- Quota- og bruksdata, support og samtaledata fra sentralbord: AES-256 i Azure Storage (Norway East), uten offentlig tilgang
- Nordwatch-tekst på brukerens maskin: AES-GCM, med nøkkelen i Macens nøkkelring eller beskyttet av Windows (DPAPI) for brukerkontoen

5.3 Nøkkelhåndtering

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

- Nøkkelen er den samme på alle brukerens enheter, slik at data kan synkroniseres uten nøkkelutveksling
- Nøkkelen er ikke hemmelig for Nordivé eller Microsoft, fordi OID er kjent for begge. Nordivés backend bruker den når den skriver resultater til appmappen på brukerens vegne
- Overgang til en nøkkel som bare kunden kontrollerer, krever en versjonert migrering på alle klienter og er planlagt, men ikke gjennomført
- Ved utlogging slettes nøkkelen fra nettleserens minne, og alle lagringsnøkler tilhørende tjenesten fjernes fra localStorage. Krypterte data ligger ikke igjen på maskinen etter at brukeren har logget ut
- Ved kompromittering av nettleseren mister angriperen tilgang så snart access-tokenet utløper (typisk 1 time)

6. Tilgangskontroll og autentisering

6.1 Sluttbrukere

- Innlogging skjer via Microsoft 365 OAuth 2.0 med PKCE (Google Workspace for firmaer som bruker Gmail)

- 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 i nettleseren slettes ved utlogging og etter 8 timers inaktivitet. Microsoft tilbyr ikke tilbakekalling av enkelttokens for nettleserapper; firmaets IT-ansvarlige kan tilbakekalle økter i Entra ID

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
- Endringer i Azure-ressursene logges i Azure-aktivitetsloggen. Tjenesten har ikke egen revisjonslogg på applikasjonsnivå

6.3 Tjeneste-til-tjeneste

- Backend autentiserer mot AWS Bedrock med IAM-kredentialer lagret som krypterte applikasjonsinnstillinger i Azure
- Backend når Azure Key Vault med en administrert identitet, uten lagrede passord
- Ved kall mot Microsoft Graph bruker backend brukerens eget tilgangstoken; i bakgrunnsanalyse brukes det beskyttede refresh-tokenet

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 leverandørenes anbefalinger for prompt injection-forsvar
- Ingen handling som sender, sletter eller fakturerer skjer uten at brukeren godkjenner den

8. Logging og overvåking

- Operasjonelle logger (forespørsel-id, status-koder, responstider) lagres i Azure Application Insights og Azure Monitor
- Kostnadsloggen per AI-kall inneholder dato, funksjon, modell, antall tokens, kostnad og konto-ID, ikke innhold
- Applikasjonslogger i Application Insights slettes automatisk etter 90 dager. Azure-aktivitetsloggen oppbevares i 90 dager
- Klientinnhold logges ikke. Loggene kan inneholde brukerens konto-ID eller e-postadresse, og enkelte feilmeldinger fra eksterne tjenester kan inneholde et kort utdrag av svaret fra tjenesten
- Logger er tilgjengelige kun for autoriserte Nordivé-ansatte

9. Beredskap og hendelsesresponse

Nordivé har en fast prosess for å oppdage, vurdere og håndtere 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 følger Microsofts versjonshistorikk og papirkurv
- Kildekoden ligger i GitHub. Tjenesten kan settes opp på nytt fra kildekoden og konfigurasjonen
- Driftsdata i Azure Storage er lokalt redundant (tre kopier i samme datasenter i Norway East). Det tas ikke egen sikkerhetskopi av driftsdataene, og tjenesten er ikke satt opp med sonevis redundans
- Recovery Time Objective (RTO): mål på 24 timer for kritiske komponenter
- Recovery Point Objective (RPO): 24 timer for konfigurasjon og kode. Driftsdata som går tapt ved et fullstendig tap av datasenteret, kan ikke gjenopprettes

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, bruks- og kostnadslogg, support og lagrede tokens hos Nordivé slettes innen 30 dager etter avtaleopphør. Slettingen gjøres i dag manuelt
- Applikasjonslogger slettes automatisk etter 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
Ekomloven § 2-7b	Cookies og lokal lagring; se separat dokument «Lagring og cookies»
NSM Grunnprinsipper for IKT-sikkerhet	Brukt som referanse; egenvurdert, ikke revidert
Schrems II Transfer Impact Assessment	Gjennomført og dokumentert for alle underbehandlere
ISO/IEC 27001:2022	Ikke igangsatt; vurderes når kundebasen tilsier det
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@nordive.ai
- Postadresse: Nordive AS, Brønnveien 1A, 0283 Oslo

DOKUMENTKONTROLL

Versjon	Dato	Beskrivelse	Godkjent av / status
2.5	25.09.2026	Oppdatert til tjenesten ved lansering: Azure OpenAI (Terra og Sol, EU-datasone), bakgrunnsanalyse med HSM-nøkkel i Key Vault, samtaledata fra sentralbord, skrivebordspanelet og Android-appen. Rettet: nøkkelen avledet fra OID er ikke hemmelig for Nordivé eller Microsoft, TLS 1.2 eller nyere, logger lagres i 90 dager, driftsdata er lokalt redundant uten egen sikkerhetskopi, og RTO og RPO er satt til det vi kan levere (24 timer).	Gjeldende fra 25. september 2026
2.4	04.08.2026	Presisert § 5 om nøkkelhåndtering: utlogging sletter nå alle lagringsnøkler tilhørende tjenesten fra localStorage, ikke bare nøkkelen fra minnet. Tilbakefallet til ukryptert lagring før OAuth-sesjonen var etablert er fjernet fra klienten.	Daglig leder
2.3	03.08.2026	Presisert § 2.2: listet opp hva Azure Table Storage faktisk brukes til, og lagt til de to unntakene fra «ingen klientinnhold» — support-samtaler og support-vedlegg, samt kryptert refresh-token ved opt-in på bakgrunnsanalyse. Lagt til Azure Container App (chat.nordive.ai) som egen systemkomponent for strømming av assistentsvar. Modell-id-ene er verifisert mot produksjonskoden og stemmer.	Daglig leder
2.2	27.07.2026	Virksomheten er videreført i Nordive AS (org.nr 938 011 710). Foretaksnavn og organisasjonsnummer oppdatert gjennomgående. Innholdet er ellers uendret.	Daglig leder
2.1	01.07.2026	Presiserte formuleringer om datalagring (klientinnhold lagres aldri) og oppdatert gjennomgangsdato	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@nordive.ai	Innehaver
1.0	28.04.2026	Førsteutgave	Innehaver