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

DOK-NR: NOR-SIK-001
VERSJON: 2.4
DATO: 25.09.2026
OFFENTLIG

Sikkerhetserklæring og forpliktelser

Nordivés overordnede prinsipper, tekniske og organisatoriske tiltak for å beskytte personopplysninger og klientinformasjon.

Utsteder	Nordive AS
Gjelder for	Tjenesten Nordivé, nettstedet nordive.ai og alle interne systemer
Forankret i	GDPR art. 32, personopplysningsloven, ISO/IEC 27001:2022
Sist oppdatert	25. september 2026
Neste revisjon	Mai 2027

1. Formål og virkeområde

Denne sikkerhetserklæringen beskriver de tekniske, organisatoriske og fysiske tiltakene Nordive AS («Nordivé») iverksetter for å sikre konfidensialitet, integritet og tilgjengelighet av personopplysninger og klientinformasjon som behandles gjennom tjenesten Nordivé.

Erklæringen gjelder for alle ansatte, konsulenter, underleverandører og systemer i Nordivés tjenestekjede.

2. Sikkerhetsprinsipper

Nordivé bygger sin sikkerhetsarkitektur på følgende prinsipper:

- **Zero-trust:** Ingen tjeneste eller bruker stoles på som standard. Hver forespørsel autentiseres og autoriseres.

- **Defense-in-depth:** Flere uavhengige sikkerhetslag (nettverk, applikasjon, kryptering, logging) sikrer at svikt i ett lag ikke kompromitterer hele systemet.
- **Least privilege:** Brukere og tjenester får kun de rettighetene som er strengt nødvendige for sin funksjon.
- **Data minimization:** Nordivé samler kun de personopplysningene som er nødvendige for å levere tjenesten, og oppbevarer dem ikke lenger enn nødvendig.
- **Privacy by design:** Personvern er innebygget i designet av tjenesten, ikke et etterpåklokt tillegg.

3. Tekniske sikkerhetstiltak

3.1 Kryptering

Datakategori	I transitt	I ro
Klientinnhold (e-post, dokumenter)	TLS 1.2+	AES-256 i kundens egen Microsoft OneDrive AppFolder. De fleste filene krypteres i tillegg i applikasjonslaget med en nøkkel avledet fra brukerens OID; det laget er ikke ende-til-ende-kryptering (se Sikkerhetsarkitektur § 2.4)
Klient-data i nettleseren (klient-register, sak-meta, e-postutkast, dokument-versjoner, vault-cache, daglig digest, AI-analyser, chat-historikk)	n/a (lokalt)	AES-256-GCM i nettleserens localStorage med nøkkel avledet fra brukerens stabile Microsoft-OID via PBKDF2 (100 000 iterasjoner, SHA-256). Nøkkelen forblir i minnet, lagres aldri i klartekst.
Autentiseringstokens (refresh-token)	TLS 1.2+	AES-256-GCM i nettleserens localStorage. Access-token (1t levetid) lagres som plain JSON siden krypteringsnøkkelen uansett kan avledes fra tokenet.
Hemmelige nøkler (backend)	n/a	Kryptert i Azure Functions Configuration som applikasjonsinnstillinger
AI-prompter til Azure OpenAI (Terra, Sol)	TLS 1.2+	Ikke lagret av Nordivé. Behandles i EU-datasone. Brukes ikke til modelltrening. Microsofts misbruksovervåking kan velge ut forespørsler og oppbevare dem midlertidig i EU (Microsoft har oppgitt inntil 30 dager).
AI-prompter til AWS Bedrock (Claude)	TLS 1.2+	Ikke lagret. Bedrock lagrer ikke forespørsler og svar.
OCR-data (Azure Document Intelligence)	TLS 1.2+	Ikke lagret hos Document Intelligence etter behandling
Brukerkonto-metadata	TLS 1.2+	AES-256 hos Microsoft Azure (Norway East)

Datakategori	I transitt	I ro
Applikasjonslogger	TLS 1.2+	AES-256 i Azure Monitor (Norway East). Slettes automatisk etter 90 dager.
Support-samtaler	TLS 1.2+	AES-256 i Azure Table Storage (Norway East). Én tråd per bruker, nøklet på e-postadresse. Innholdet skrives av brukeren selv og kan inneholde klientinformasjon dersom brukeren velger å oppgi det. Slettes automatisk etter 30 dager.
Support-vedlegg (skjermbilder, PDF)	TLS 1.2+	AES-256 i privat Azure Blob-container (Norway East), uten anonym tilgang. Hentes kun via administrator-endepunkt med egen nøkkel. Skjermbilder kan inneholde klientinformasjon. Slettes automatisk etter 7 dager.
Refresh-token for bakgrunnsanalyse (kun ved uttrykkelig opt-in)	TLS 1.2+	AES-256-GCM i Azure Table Storage (Norway East), med nøkkelen pakket inn av en ikke-eksporterbar HSM-nøkkel i Azure Key Vault. Lagres kun for brukere som selv slår på bakgrunnsanalyse, og slettes når funksjonen slås av eller etter 90 dager uten bruk.
Samtaledata fra sentralbord (Phonero), kun når firmaet har koblet til	TLS 1.2+	AES-256 i Azure Table Storage (Norway East). Numre, retning, tidspunkt og varighet. Slettes etter 90 dager.
Nordwatch-tekst (skrivebordspanelet, kun når brukeren har slått det på)	n/a (lokalt)	AES-GCM på brukerens maskin, nøkkel i Macens nøkkelring eller beskyttet av Windows (DPAPI). Slettes etter sju dager.
Varslingsabonnement (Web Push)	TLS 1.2+	AES-256 i Azure Table Storage (Norway East). Endepunkt-URL og nøkler for push, ingen innhold.
Quota-/bruksdata	TLS 1.2+	AES-256 i Azure Table Storage (Norway East)

3.2 Tilgangskontroll

- Multifaktor-autentisering (MFA) er obligatorisk for alle Nordivé-ansatte med tilgang til produksjonsmiljø
- Brukere autentiseres med eksisterende Microsoft 365-konto, slik at advokatfirmaets MFA-policy gjelder
- Tilgang til produksjonsmiljøet er begrenset til to navngitte personer, og styres med rollebasert tilgangskontroll (RBAC) i Azure
- Endringer i Azure-ressursene logges i Azure-aktivitetsloggen

3.3 Nettverkssikkerhet

- Azure Functions med innebygd DDoS-beskyttelse i Azure-plattformen

- Vercel sin innebygde DDoS-beskyttelse og edge-WAF for nordive.ai og app.nordive.ai
- Backend-til-modell-kommunikasjon over TLS mot Azure OpenAI (EU-datasone) og AWS Bedrock (EU-inferensprofiler)
- Tjenesten har to backend-komponenter: Azure Functions (Norway East) for analyse og integrasjoner, og en Azure Container App (`chat.nordive.ai`) som strømmer svar fra assistenten. Begge autentiserer hver forespørsel mot Microsoft Entra ID og lagrer ikke klientinnhold
- Hemmelige nøkler (API-nøkler, AWS-credentials) lagres som krypterte applikasjonsinnstillinger i Azure; nøkkelen som beskytter refresh-tokens ligger i Azure Key Vault (HSM)
- Lagringskontoen har offentlig blob-tilgang slått av og krever HTTPS og minst TLS 1.2
- HTTPS overalt, automatisert sertifikathåndtering via Vercel og Azure

3.4 Applikasjonssikkerhet

- Typesjekk, tester og bygg kjøres før hver utrulling, og utrulling skjer fra en bestemt commit
- Avhengighetsovervåking via GitHub Dependabot, og skanning etter hemmeligheter (Gitleaks) i kildekode og bygg
- Content Security Policy, HSTS og andre sikkerhetshoder på app.nordive.ai
- OWASP Top 10 mitigasjoner som baseline (inkludert prompt injection-forsvar for AI-grensesnitt)
- Innebygde forsvar mot prompt injection via input-klassifisering og output-sanitering

4. Organisatoriske tiltak

4.1 Ansatte og opplæring

- Nordivé har i dag to personer med tilgang til produksjonsmiljøet
- Det finnes ennå ikke et eget opplæringsprogram, bakgrunnssjekk eller faste phishing-øvelser. Rutiner for taushetserklæring og opplæring ved oppstart innføres før nye personer får tilgang
- Maskinen som brukes til utvikling og drift, har kryptert disk (FileVault)

4.2 Sikkerhetsledelse

- Sikkerhetsansvar er utpekt i daglig ledelse
- Sikkerhetsrisiko vurderes ved vesentlige endringer i tjenesten
- Sertifisering etter ISO/IEC 27001:2022 er ikke igangsatt; den vurderes når kundebasen tilsier det

4.3 Underleverandørstyring

- Alle underleverandører gjennomgår sikkerhetsvurdering før kontraktsinngåelse
- Databehandleravtaler (DPA) inngås med alle underleverandører som behandler personopplysninger

- Årlig revurdering av underleverandørenes sikkerhetsstatus
- Se separat dokument «Liste over underbehandlere» for fullstendig oversikt

5. Hendelsesresponse

Nordivé har en fast prosess for å oppdage, vurdere og håndtere sikkerhetshendelser. Fristene under er det vi kan overholde med dagens bemanning:

Fase	Maks-tid	Beskrivelse
Deteksjon	Kontinuerlig	Logging og alarmering i Azure Monitor / Application Insights
Triage	Samme dag, senest innen 1 virkedag	Daglig leder eller utpekt sikkerhetsansvarlig vurderer alvorlighetsgrad
Varsel til kunde (behandlingsansvarlig)	Uten ugrunnet opphold, om mulig innen 24 timer	Som databehandler varsler vi behandlingsansvarlig uten ugrunnet opphold, jf. GDPR art. 33 nr. 2
Varsel til Datatilsynet	< 72 timer	Behandlingsansvarlig sender meldingen; Nordivé bistår med nødvendig informasjon, jf. GDPR art. 33 nr. 1 og art. 28 nr. 3 bokstav f
Detaljert rapport	< 30 dager	Inkluderer årsak, omfang, kategorier av berørte registrerte, sannsynlige konsekvenser og avhjelpende tiltak, jf. GDPR art. 33 nr. 3

Nordivé fører oversikt over alle sikkerhetshendelser i et internt register, uavhengig av om de utløser meldeplikt.

6. Tilgjengelighet og kontinuitet

- Oppetid: mål om 99,5 % målt månedlig (best effort). Målet er ikke en garanti; kontraktsfestet tjenestenivå krever egen skriftlig avtale
- Kildekoden ligger i GitHub, og tjenesten kan settes opp på nytt fra kode og konfigurasjon. Klientinnhold ligger i kundens egen OneDrive og inngår ikke i Nordivés gjenoppretting
- Driftsdata i Azure Storage (Norway East) er lokalt redundant, uten egen sikkerhetskopi og uten sonevis redundans
- Recovery Time Objective (RTO): mål på 24 timer for kritiske komponenter
- Recovery Point Objective (RPO): 24 timer for konfigurasjon og kode

7. Sertifiseringer og rammeverk

Standard	Status	Forventet milepæl
GDPR / personopplysningsloven	Etterleves, egenvurdert	Løpende
ISO/IEC 27001:2022	Ikke igangsatt	Avhengig av kundebase-vekst
NSM Grunnprinsipper for IKT-sikkerhet	Brukt som referanse, egenvurdert og ikke revidert	Løpende
Schrems II Transfer Impact Assessment	Gjennomført og dokumentert	Revurderes årlig
SOC 2 Type I og Type II	Ikke startet	Forberedelsene starter ved 50 betalende kunder

8. Rapportering av sårbarheter

Sikkerhetsforskere og kunder oppfordres til å rapportere oppdagede sårbarheter til **kontakt@nordive.ai** med emne «Sikkerhetsrapport». Vi forplikter oss til å:

- Bekrefte mottak av rapporten innen 48 timer
- Holde rapportøren oppdatert om fremdriften
- Ikke iverksette rettslige skritt mot rapportører som handler i god tro og holder funnet konfidensielt til det er utbedret

9. Kontakt

Spørsmål om denne sikkerhetserklæringen eller forespørsler om sikkerhetsdokumentasjon (revisjonsrapporter, SOC-rapporter når tilgjengelige) kan rettes til:

- Generelt og sikkerhet: kontakt@nordive.ai
- Postadresse: Nordive AS, Brønnveien 1A, 0283 Oslo

DOKUMENTKONTROLL

Versjon	Dato	Beskrivelse	Godkjent av / status
2.4	25.09.2026	Krypteringstabellen omfatter Azure OpenAI (Terra og Sol), samtaledata og Nordwatch, med TLS 1.2 eller nyere. Tilgang, logging, opplæring og beredskap er beskrevet slik de faktisk er. Oppetid er et mål uten garanti, RTO og RPO er 24 timer, logger lagres i 90 dager, og mottak av sårbarhetsrapporter bekreftes innen 48 timer.	Gjeldende fra 25. september 2026
2.3	03.08.2026	Utvidet § 3.1 med fire datakategorier som lagres på Nordivés egen Azure-infrastruktur og ikke var oppført: support-samtaler, support-vedlegg, refresh-token for bakgrunnsanalyse ved opt-in, og varslingsabonnement. Presisert i § 3.3 at tjenesten har to backend-komponenter, inkludert Azure Container App for strømming av assistentsvar.	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	Korrigert kryptering-tabell (§ 3.1) til å reflektere AES-GCM på klient-data i nettleseren, fjernet uverifiserte påstander, samlet sikkerhetskontakt under kontakt@nordive.ai	Innehaver
1.0	28.04.2026	Førsteutgave	Innehaver