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

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

SIKKERHETSERKLÆRING

Sikkerhetserklæring og forpliktelser

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

Utsteder	Nordivé Aavitsland
Gjelder for	Tjenesten Nordivé, nettstedet nordiveai.no og alle interne systemer
Forankret i	GDPR art. 32, personopplysningsloven, ISO/IEC 27001:2022
Sist oppdatert	20. mai 2026
Neste revisjon	Mai 2027

1. Formål og virkeområde

Denne sikkerhetserklæringen beskriver de tekniske, organisatoriske og fysiske tiltakene Nordivé Aavitsland («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 1.3	AES-256 i kundens egen Microsoft OneDrive AppFolder, med ekstra applikasjons-lag kryptering før lagring
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 1.3	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 AWS Bedrock	TLS 1.3	Ikke lagret. Zero Data Retention bekreftet ved Bedrock-konfigurasjon.
OCR-data (Azure Document Intelligence)	TLS 1.3	Ikke lagret hos Document Intelligence etter behandling
Brukerkonto-metadata	TLS 1.3	AES-256 hos Microsoft Azure (Norway East)
Sikkerhetslogger	TLS 1.3	AES-256 hos Microsoft Azure (Norway East)
Quota-/bruksdata	TLS 1.3	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
- Rollebasert tilgangskontroll (RBAC) i Azure med separasjon mellom utviklings-, test- og produksjonsmiljø
- Privileged Access Management (PAM): tilgang til produksjon krever just-in-time-godkjenning
- Logging av alle administrator-handlinger med uforanderlige logger

3.3 Nettverkssikkerhet

- Azure Functions med innebygd DDoS-beskyttelse i Azure-plattformen
- Vercel sin innebygde DDoS-beskyttelse og edge-WAF for nordiveai.no og app.nordiveai.no
- Backend-til-AWS-Bedrock-kommunikasjon over TLS 1.3 mot Bedrock-endpoint (eu-west-1)
- Hemmelige nøkler (API-nøkler, AWS-credentials) lagres i Azure Functions Configuration som krypterte applikasjonsinnstillinger
- HTTPS overalt, automatisert sertifikathåndtering via Vercel og Azure

3.4 Applikasjonssikkerhet

- Sikkerhetsgransking av all kode før produksjonsutrulling (code review-prosess)
- Avhengighetsovervåking via GitHub Dependabot
- OWASP Top 10 mitigasjoner som baseline (inkludert prompt injection-forsvar for AI-grensesnitt)
- Innebygde forsvar mot prompt injection via input-klassifisering og output-sanitering
- Penetrasjonstesting planlagt før første betalende advokatfirma-kunde, deretter årlig av uavhengig tredjepart
- Bug-bounty-program planlagt etter første pen-test (Q3 2026)

4. Organisatoriske tiltak

4.1 Ansatte og opplæring

- Alle ansatte signerer taushetserklæring ved oppstart
- Obligatorisk sikkerhetsopplæring ved oppstart
- Sikkerhetsbevissthet inngår som del av løpende intern utvikling
- Tilgang til produksjonsmiljø begrenset til nøkkelpersoner

4.2 Sikkerhetsledelse

- Sikkerhetsansvar er utpekt i daglig ledelse
- Risikoregister oppdateres ved vesentlige endringer i tjenesten
- Tilpasning til ISO/IEC 27001:2022-rammeverket er igangsatt, med sertifisering planlagt etterhvert som kundebasen vokser

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 formell prosess for å oppdage, vurdere og respondere på sikkerhetshendelser:

Fase	Maks-tid	Beskrivelse
Deteksjon	Kontinuerlig	Logging og alarmering i Azure Monitor / Application Insights
Triage	< 4 timer fra deteksjon	Innehaver eller utpekt sikkerhetsansvarlig vurderer alvorlighetsgrad
Varsel til kunde (behandlingsansvarlig)	< 24 timer fra bekreftet brudd	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

- Tjenestenivåavtale (SLA): 99,5 % oppetid målt månedlig (gjelder for betalende kunder med signert tjenesteavtale)

- Backup av konfigurasjon og infrastruktur-tilstand (klientinnhold er lagret i kundens egen OneDrive og inngår ikke i Nordivés backup-omfang)
- Hosting i Azure Norway East med innebygd zonal redundans
- Recovery Time Objective (RTO): 4 timer for kritiske komponenter
- Recovery Point Objective (RPO): 24 timer for konfigurasjonsdata
- Periodisk test av beredskapsplan

7. Sertifiseringer og rammeverk

Standard	Status	Forventet milepæl
GDPR / personopplysningsloven	Compliant	Løpende
ISO/IEC 27001:2022	Tilpasning igangsatt	Avhengig av kundebase-vekst
NSM Grunnprinsipper for IKT-sikkerhet	Implementert (selvevaluert)	Løpende
Schrems II Transfer Impact Assessment	Gjennomført og dokumentert	Revurderes årlig
SOC 2 Type II	Planlagt	Etter første betalende advokatfirma-kunder

8. Rapportering av sårbarheter

Sikkerhetsforskere og kunder oppfordres til å rapportere oppdagede sårbarheter til **kontakt@nordiveai.no** 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 i tråd med vår vulnerability disclosure-policy

9. Kontakt

Spørsmål om denne sikkerhetserklæringen eller forespørsler om sikkerhetsdokumentasjon (revisjonsrapporter, SOC-rapporter når tilgjengelige) kan 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	Korrigert kryptering-tabell (§ 3.1) til å reflektere AES-GCM på klient-data i nettleseren, fjernet uverifiserte påstander, samlet sikkerhetskontakt under kontakt@nordiveai.no	Innehaver

---

Nordivé Aavitsland
Org.nr 931 147 549 · Myrabakken 4, Norge · kontakt@nordiveai.no
Dokument-id: NOR-SIK-001 · Versjon 2.0 · Klassifisering: Offentlig