SIKKERHETSERKLÆRING

Slik beskytter vi dine data

Sist oppdatert	Versjon	Selskap	Kontakt
25. april 2026	1.0	Nordivé AS · org.nr. 931 147 501	sindre@nordive.no

Nordivé bygges for advokater. Klientkonfidensialitet og taushetsplikt er kjernen i deres arbeid — derfor er det også kjernen i hvordan vi designer Tjenesten. Denne erklæringen oppsummerer hvordan vi beskytter dataene deres.

For full teknisk dokumentasjon, se SECURITY.md eller be om en kopi.

Det viktigste først

Vi lagrer ikke e-postene deres. Innhold i e-poster, vedlegg og AI-svar prosesseres i minne hos oss og slettes umiddelbart når svaret er levert. Det er ingen database, ingen JSON-fil, ingen logg på vår side som inneholder klientnavn, e-postemner, mottakere eller saksopplysninger.

AI-prosessering forlater aldri EU. Vi bruker AWS Bedrock med en `eu.`-cross-region inference profile. AWS' API-lag avviser kallet før det kan rute utenfor EU-regionene Irland, Frankfurt, Stockholm eller Paris. Det er en hardkodet teknisk garanti, ikke en muntlig forsikring.

Vi trener ingen AI-modell på dataene deres. AWS Bedrocks tjenestevilkår forbyr eksplisitt at kundeprompter og -svar brukes til modelltrening. Vi forsterker dette med en kontraktsklausul i databehandleravtalen.

Datalagring og -plassering

Datatype	Hvor lagres det?	Hvor lenge?
E-postinnhold	Aldri lagret hos Nordivé	Slettes umiddelbart etter behandling

Datatype	Hvor lagres det?	Hvor lenge?
Vedlagte dokumenter	Aldri lagret hos Nordivé	Slettes umiddelbart etter behandling
AI-genererte svar	Aldri lagret hos Nordivé	Slettes etter levering til brukeren
AI-analyse-cache	Brukerens egen enhet (kryptert localStorage)	30 dager, deretter slettes automatisk
Tidsregistreringsforslag	Brukerens egen enhet (kryptert localStorage)	Inntil bruker godkjenner/avviser
Kontoinfo (navn, e-post)	Microsoft Azure Norway East	Så lenge kontoen er aktiv + 30 dager
Driftslogger	Application Insights, Norway East	30 dager

Kryptering

- **I transit:** TLS 1.3 (med fallback til 1.2) på alle nettverksforbindelser
- **På brukerens enhet:** AES-GCM 256-bit, nøkkel derivert fra brukerens unike Azure AD Object ID via PBKDF2 (100 000 iterasjoner). Forskjellige brukere på samme PC kan ikke dekryptere hverandres data.
- **Hos underbehandlere:** AES-256 i hvile (Microsoft Azure og AWS' standard)

Tilgangskontroll

- MFA påkrevd for alle Nordivé-ansatte med produksjonstilgang
- Prinsipp om minste privilegium
- Umiddelbar tilbaketrekking ved arbeidsforhold opphør
- Rotering av API-nøkler hver 90. dag
- Tilgangslogger gjennomgås kvartalsvis

Underbehandlere

Tre selskaper står for infrastrukturen:

Selskap	Rolle	Lokasjon
Microsoft Azure	Backend, OCR, telemetri	Norway East
AWS	AI-prosessering	EU-regioner kun
Vercel	Statisk frontend (ingen kundedata)	EU edge

Alle tre har SOC 2 Type II og ISO 27001. Komplette revisjonsrapporter kan deles på forespørsel via deres respektive trust portals.

Hvorfor advokat-IT bør være komfortable

Bekymring	Hvordan vi løser det
Klient-konfidensialitet	Ingen lagring av e-postinnhold på vår side. Period.
Datalokasjon (CLOUD Act)	Ingen data i USA. Microsoft Norge + AWS EU + Vercel EU.
AI-trening på sensitiv data	Forbudt av AWS-vilkår + DPA-klausul
Brudd-håndtering	24-timers varslingsplikt i DPA
Sletting ved opphør	30 dager til full sletting + skriftlig bekreftelse
Compliance-revisjoner	Underbehandleres SOC 2 / ISO 27001 tilgjengelig

Sertifiseringer og roadmap

Per i dag har Nordivé selv:

- Microsoft Publisher Verification (i prosess)
- Verifisert Microsoft AppSource-listing (i prosess)

Underbehandlerne våre har:

- Microsoft: SOC 2 Type II, ISO 27001, ISO 27018, ISO 27017, FedRAMP High
- AWS: SOC 2 Type II, ISO 27001, ISO 27018, ISO 27017, PCI DSS Level 1
- Vercel: SOC 2 Type II

Roadmap (fra og med 50 betalende kunder):

- SOC 2 Type I rapport
- Årlig ekstern penetrasjonstest av norsk leverandør (Mnemonic / Watchcom)
- SOC 2 Type II (12 måneder etter Type I)
- Microsoft 365 Certified

Hva vi gjør hvis det skjer noe

Sikkerhetshendelse hos oss:

1. Internt varsel innen 1 time
2. Stansing/innesperring av påvirket systemkomponent
3. Kunde-varsel innen 24 timer (skriftlig, til avtalt sikkerhetskontakt)
4. Hjelp til kunden med Datatilsynet-melding (GDPR art. 33)
5. Etterforskning og rapport innen 14 dager

Sikkerhetshendelse hos underbehandler:

- Vi videresender deres varsel til dere uten forsinkelse
- Vi bistår med tolkning og innvirkning på deres systemer

Slutten

Vi tar dette på alvor fordi advokater må ta det på alvor. Hvis noe i denne erklæringen ikke matcher det dere trenger for å være komfortable, ring oss. Vi heller mot å si "ja" på rimelige sikkerhetsforespørsler enn "nei".

Kontakt:

- E-post: sindre@nordive.no
- Telefon: +47 900 46 239

- Adresse: Nordivé AS, Myrabakken 4, Norge