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

DOK-NR: NOR-TIA-001
VERSJON: 1.0
DATO: 20.05.2026
OFFENTLIG

TRANSFER IMPACT ASSESSMENT

Schrems II Transfer Impact Assessment

Vurdering av overføringer til amerikanskeide underbehandlere i samsvar med EU-domstolens dom i sak C-311/18 (Schrems II) og EDPB Recommendations 01/2020 om supplerende tiltak.

Behandlingsansvarlig (eksportør)	Det enkelte advokatfirma som bruker Nordivé
Databehandler (sub-eksportør)	Nordivé Aavitsland (org.nr 931 147 549)
Hjemmel	GDPR kap. V (art. 44–49), EDPB Recommendations 01/2020
Sist oppdatert	20. mai 2026
Neste revisjon	Årlig eller ved vesentlig endring

1. Formål og avgrensning

Dette dokumentet utgjør Nordivés Transfer Impact Assessment (TIA) for de fire amerikanskeide underbehandlerne som leverer tjenester til Nordivé: Microsoft Corporation, Amazon Web Services Inc., Anthropic PBC og Vercel Inc. Vurderingen følger metodikken i EDPB Recommendations 01/2020 om tiltak som supplerer overføringsverktøy for å sikre samsvar med EUs beskyttelsesnivå for personopplysninger.

TIA-en gjelder for de databehandlinger Nordivé utfører på vegne av advokatfirmaer som benytter tjenesten. Advokatfirmaet (behandlingsansvarlig) bør sammenholde dette dokumentet med egen risikovurdering og databehandleravtale før tjenesten tas i bruk.

2. Metodikk

For hver underbehandler er det gjort en strukturert vurdering i seks trinn, i samsvar med EDPB Recommendations 01/2020:

1. **Kjenn din overføring:** hvilke data overføres, til hvem, for hvilket formål, og fra hvilken jurisdiksjon
2. **Identifiser overføringsverktøyet:** hjemmel for overføringen (DPF, SCC, etc.)
3. **Vurder lovgivningen i mottakerlandet:** særlig overvåkningslovgivning som kan begrense personvernet
4. **Identifiser og iverksett supplerende tiltak:** tekniske, kontraktsmessige og organisatoriske
5. **Iverksett prosessuelle skritt:** dokumentasjon, varsling, oppdateringer
6. **Periodisk re-evaluering:** ved endringer i lovgivning, tjeneste eller risiko

3. Felles risikobilde for USA

Alle fire underbehandlere har morselskaper med hovedkontor i USA. Følgende amerikansk overvåkningslovgivning er relevant:

- **FISA 702 (50 USC § 1881a):** Tillater U.S. National Security Agency å innhente «foreign intelligence information» fra elektronisk kommunikasjon hos «electronic communication service providers». EU-domstolen vurderte i Schrems II at denne loven gir myndighetene tilgang utover hva som er nødvendig og forholdsmessig etter EU-retten.
- **Executive Order 12333:** Tillater signaletterretning utenfor USA. Mindre direkte trussel mot data lagret i EU, men relevant ved internasjonal kabel- og satellittovervåkning.
- **CLOUD Act (18 USC § 2713):** Pålegger amerikanske selskaper å utlevere data, uavhengig av lagringssted, dersom de mottar lovlig forespørsel fra amerikanske myndigheter.

Disse lovene representerer en strukturell svakhet ved alle U.S.-baserte tjenester, uavhengig av hvor data fysisk lagres. EDPB krever derfor at man iverksetter supplerende tiltak som «in their substance and effect, ensure essentially equivalent» beskyttelse til EU-retten.

Forsvarslag som er felles for alle fire underbehandlere:

- **EU-U.S. Data Privacy Framework (DPF):** Vedtatt av EU-kommisjonen 10. juli 2023 som adekvat overføringsmekanisme for amerikanske selskaper som er DPF-sertifisert. Erstatter Privacy Shield. Alle fire underbehandlere er aktivt sertifisert (status verifisert mai 2026 på dataprivacyframework.gov).
- **Standard Contractual Clauses (SCC):** Modul 3 (databehandler-til-databehandler) er inntatt i databehandleravtalen som subsidiær mekanisme dersom DPF skulle falle bort. Bruker EU-kommisjonens 2021-versjon (Beslutning 2021/914).
- **Kryptering i transitt:** TLS 1.3 for alle forbindelser.
- **Geografisk minimering:** All databehandling skjer i EU/EØS-regioner.

4. Vurdering per underbehandler

4.1 Microsoft Corporation

Selskap	Microsoft Corporation, Redmond WA, USA
Tjenester	Azure Functions, Azure Table Storage, Azure Document Intelligence, Microsoft Graph (OneDrive AppFolder), Microsoft 365 OAuth, Entra ID
Behandlingssted	Azure Norway East (Stavanger) for backend. Document Intelligence i EU-region. OneDrive følger kundens egen tenant-region.
Data eksponert	Brukerkonto-metadata (navn, e-post, OID), autentiseringstokens (kryptert), klientinnhold (lagret kryptert i kundens egen OneDrive AppFolder), kortvarig prosessering av dokumenter ved OCR-fallback
Overføringsmekanisme	EU-U.S. DPF (sertifisert); SCC Modul 3 i Microsoft Online Services DPA; intra-konsern SCC-er for Microsoft Ireland Operations Ltd. → Microsoft Corp.

Risikovurdering:

- *FISA 702-risiko:* Microsoft er «electronic communication service provider» og kvalifiserer som mottaker av FISA 702-bestillinger. Microsoft publiserer transparency-rapporter (Law Enforcement Requests Report) som viser at omtrent 0–249 FISA-orders mottas per halvår; bekreftet kun i aggregerte intervaller, ikke per kunde.
- *Supplerende tiltak iverksatt:*
  - Applikasjonslag-kryptering av klientinnhold i OneDrive AppFolder (AES-256-GCM, OID-derivert nøkkel som ikke deles med Microsoft) — innholdet er ulesbart for Microsoft.
  - Databehandling utelukkende i EU-regioner.
  - Microsoft EU Data Boundary (lansert 2024) holder ytterligere prosesseringsdata innenfor EU.
  - Customer Lockbox-funksjonalitet kan aktiveres for å kreve eksplisitt samtykke ved Microsoft-tilgang til kundedata.
- *Restrisiko:* Lav. Selv om Microsoft skulle motta en FISA 702-bestilling, vil klientinnholdet være kryptert med en nøkkel Microsoft ikke har tilgang til. Metadata om brukerkontoen (e-postadresse, OID) kan i teorien utleveres, men inneholder ikke klient-data.
- *Konklusjon:* Overføringen anses forsvarlig med supplerende tiltak.

4.2 Amazon Web Services, Inc.

Selskap	Amazon Web Services, Inc., Seattle WA, USA
Tjenester	AWS Bedrock (AI-inferens med Anthropic-modeller)
Behandlingssted	eu-west-1 (Irland)

Data eksponert	AI-prompter med e-post-/dokumentinnhold under inferens (transient). Zero Data Retention er konfigurert — ingen logging eller lagring etter inferens.
Overføringsmekanisme	EU-U.S. DPF (sertifisert); SCC Modul 2/3 i AWS Service Terms / Data Processing Addendum; AWS GDPR DPA godkjent av CNIL/EDPB.

Risikovurdering:

- *FISA 702-risiko:* AWS kvalifiserer som «electronic communication service provider». AWS publiserer kvartalsvise transparency-rapporter. Risikoen er konsentrert om perioden hvor prompter passerer gjennom AWS' infrastruktur for inferens.
- *Supplerende tiltak iverksatt:*
  - Zero Data Retention (ZDR) på Bedrock — ingen prompter, ingen modell-output, ingen feillogger lagres etter inferens. Verifisert i Bedrock service-konfigurasjon.
  - EU-only region (eu-west-1, Irland) — ingen automatisk failover til amerikanske regioner.
  - TLS 1.3 mellom Azure (Norway East) og AWS Bedrock-endpoint.
  - Modell-tilbyderen Anthropic mottar ikke prompter direkte; alt går via AWS Bedrock under deres egen kontroll og ZDR-policy.
  - Ingen langtidslagring av AI-output hos AWS — output returneres til Nordivé-backenden og persisteres aldri på AWS-siden.
- *Restrisiko:* Lav. AWS har ikke vedvarende tilgang til klient-data; eksponeringen er begrenset til de millisekunder en prompt blir prosessert under inferens. En FISA 702-bestilling vil i praksis kun kunne fange data i sann tid og krever målrettet, ikke generell, tilgang.
- *Konklusjon:* Overføringen anses forsvarlig med supplerende tiltak. ZDR er den mest effektive tekniske mekanismen og er bekreftet aktiv.

4.3 Anthropic PBC

Selskap	Anthropic PBC, San Francisco CA, USA
Tjenester	Claude-modellene Sonnet 4.6, Opus 4.6 og Haiku 4.5 (leveres via AWS Bedrock)
Behandlingssted	Anthropic mottar ikke prompter direkte. All inferens skjer hos AWS Bedrock i eu-west-1 (Irland) under AWS sin kontroll.
Data eksponert	Ingen direkte eksponering. Anthropic mottar kun aggregert bruksstatistikk fra Bedrock (antall token, ikke innhold).
Overføringsmekanisme	EU-U.S. DPF (sertifisert september 2023); Anthropic kontraktsmessig forpliktet av AWS Bedrock-service-terms.

Risikovurdering:

- *FISA 702-risiko:* Anthropic kvalifiserer formelt som «electronic communication service provider», men har ikke faktisk tilgang til Nordivé-kunders prompter siden disse aldri når Anthropic-

infrastrukturen i Bedrock-modellen.

- *Supplerende tiltak iverksatt:*
  - Arkitektonisk skille: Anthropic-modellene kjøres som inferens-endpoints inne i AWS Bedrock — Anthropic selv har ikke tilgang til prompter eller output.
  - Zero Data Retention på Bedrock-laget hindrer at noe innhold når Anthropic-systemer.
  - Anthropics egne policies bekrefter at API-data ikke brukes til modelltrening uten eksplisitt samtykke.
- *Restrisiko:* Veldig lav. Anthropic er en formell underbehandler i kjeden, men har i praksis ingen tilgang til kundeinnhold.
- *Konklusjon:* Overføringen anses forsvarlig.

4.4 Vercel Inc.

Selskap	Vercel Inc., San Francisco CA, USA
Tjenester	Hosting av frontend (nordiveai.no, app.nordiveai.no)
Behandlingssted	EU edge-noder (primært Frankfurt, Amsterdam)
Data eksponert	Statiske ressurser (HTML/CSS/JS-bundles, ikoner). Vercel ser IP-adresser og User-Agent i edge-logger (anonymisert/aggregert). Vercel ser **ikke** klientinnhold — all dataflyt skjer direkte fra nettleseren til Azure-backend uten å passere Vercel.
Overføringsmekanisme	EU-U.S. DPF (sertifisert); SCC Modul 3 i Vercel Data Processing Addendum.

Risikovurdering:

- *FISA 702-risiko:* Vercel kvalifiserer som CDN-leverandør. Det viktigste risikoflate er edge-logger med IP-adresser.
- *Supplerende tiltak iverksatt:*
  - Vercel ser ingen klient-data. Frontend-koden kommuniserer direkte med Azure-backend i Norway East — Vercel fungerer kun som CDN for statiske filer.
  - EU-edge-noder benyttes for serving av filer til norske brukere.
  - Vercel-logger er minimaliserte og inneholder ikke personopplysninger utover IP-adresser (som anses som personopplysning i seg selv).
- *Restrisiko:* Lav. Eksponeringen er begrenset til metadata om sidehenting (IP, tidspunkt, sti) — ingen klient-data.
- *Konklusjon:* Overføringen anses forsvarlig.

5. Samlet konklusjon

For alle fire underbehandlere foreligger det:

- Aktiv DPF-sertifisering (verifisert mai 2026)
- SCC som subsidiær mekanisme i underbehandleravtalene
- Konkrete tekniske supplerende tiltak (kryptering, ZDR, geografisk minimering, arkitektonisk skille)
- Organisatoriske tiltak (transparency-rapporter, dokumentert hendelsesrespons)

Nordivé vurderer at risikobildet, sammenholdt med de tekniske og kontraktsmessige supplerende tiltakene, gir et beskyttelsesnivå som i hovedsak er ekvivalent med EUs beskyttelsesnivå (jf. EDPB Recommendations 01/2020 pkt. 45). Overføringene er derfor forsvarlige etter GDPR kap. V.

6. Periodisk re-evaluering

Denne TIA-en skal revurderes:

- Minst én gang per år (neste planlagt mai 2027)
- Ved enhver vesentlig endring i amerikansk overvåkningslovgivning (f.eks. dom som invaliderer DPF)
- Ved enhver vesentlig endring i underbehandlerens tjenester, regioner eller policies
- Ved enhver alvorlig hendelse hos underbehandler som kan påvirke risikovurderingen

Endringer som krever ny vurdering varsles til advokatfirmaene som benytter tjenesten, jf. databehandleravtalens regler om endring av underbehandlere.

7. Referanser

- EU-domstolens dom 16. juli 2020 i sak C-311/18 (Schrems II)
- EDPB Recommendations 01/2020 om tiltak som supplerer overføringsverktøy, vedtatt 18. juni 2021
- EU-kommisjonens gjennomføringsbeslutning (EU) 2023/1795 av 10. juli 2023 om adekvat beskyttelse i USA under EU-U.S. Data Privacy Framework
- EU-kommisjonens gjennomføringsbeslutning (EU) 2021/914 av 4. juni 2021 om standard kontraktsklausuler
- GDPR (EU) 2016/679 kapittel V (artikkel 44–49)
- U.S. Foreign Intelligence Surveillance Act § 702 (50 USC § 1881a)
- U.S. Executive Order 12333 av 4. desember 1981
- U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act, Pub. L. 115-141)

8. Kontakt

Spørsmål om denne vurderingen, forespørsler om utfyllende underlag (per-vendor risk register, kontraktssklausuler, transparency-rapporter), eller varsel om endringer i risikobildet rettes til:

- E-post: kontakt@nordiveai.no
- Postadresse: Nordivé Aavitsland, Myrabakken 4, Norge

DOKUMENTKONTROLL

Versjon	Dato	Beskrivelse	Godkjent av
1.0	20.05.2026	Førsteutgave	Innehaver
