DATABEHANDLERAVTALE (DPA)

Mellom

	Kunde / Behandlingsansvarlig:
Kunde registrert som følgende firmanavn i Brønnøysundregisterene/Foretaksregisteret:	
Org.nr.:	
Signeres av (Prokura / Signatur):	
Signeres av 2 (Prokura / Signatur):	

og

Blix AI AS
Lindeberg næringsvei 26, 1067 Oslo
Org.nr: 937 910 924
(heretter kalt "**Databehandler**")
hver for seg omtalt som en "Part" og i fellesskap som "Partene".

1. Formål og omfang

Formålet med denne Databehandleravtalen (heretter "Avtalen") er å sikre at behandling av personopplysninger skjer i samsvar med gjeldende personvernlovgivning, herunder EU/EØS generelle personvernforordning (GDPR) og gjeldende norsk personopplysningslov.
Denne Avtalen regulerer **Databehandlerens** behandling av personopplysninger på vegne av **Behandlingsansvarlig** i forbindelse med levering av API-tjenester for store språkmodeller fra databehandlerens dedikerte maskinvareinfrastruktur (heretter «Hovedavtalen (MSA)»).

2. Behandlingens art, formål og varighet

Art og formål: Databehandler skal drifte og tilgjengeliggjøre et API for inferens (prosessering av språkmodeller). Formålet er å la Behandlingsansvarlig prosessere data og tekstforespørsler (prompts) via AI-modeller tilbydt via APIet.
Varighet: Avtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig i henhold til Hovedavtalen.

3. Kategorier av personopplysninger og registrerte

Ettersom Behandlingsansvarlig selv definerer og sender inndata (prompts) til API-et, kontrollerer Behandlingsansvarlig omfanget av personopplysninger.
Kategorier av registrerte opplysninger: Kan omfatte Behandlingsansvarliges ansatte, kunder, klienter, innbyggere eller andre tilknyttede personer.
Typer personopplysninger: Fritekst, dokumenter, identifikatorer, forretningsdata, samt eventuelle andre kategorier av personopplysninger som Behandlingsansvarlig velger å sende gjennom API-grensesnittet.

4. Databehandlerens plikter (Instruks og formål)

Databehandleren skal bare behandle personopplysninger i samsvar med dokumenterte instrukser fra Behandlingsansvarlig, med mindre annet kreves i henhold til gjeldende EU-rett eller nasjonal rett som Databehandleren er underlagt. **Databehandleren** skal umiddelbart underrette **Behandlingsansvarlig** dersom en instruks etter **Databehandlerens** mening er i strid med GDPR eller andre personvernregler. **Databehandleren** skal sikre at alle personer som er autorisert til å behandle personopplysningene, har forpliktet seg til konfidensialitet via taushetserklæring (NDA) eller er underlagt en egnet lovfestet taushetsplikt.

5. Særlige vilkår for AI-prosessering: Zero Data Retention (ZDR)

Databehandleren garanterer herved en streng innstruks for dataminimering og flyktig behandling:

- **Ingen lagring på disk**: Innsendte forespørsler (prompts) og genererte svar (outputs) behandles utelukkende flyktig i serverens grafikkminne (VRAM) under selve utførelsen. Ingen data lagres permanent eller semi-permanent på harddisker eller andre lagringsmedier hos Databehandler.
- **Ingen modelltrening**: Databehandler garanterer skriftlig at data mottatt fra Behandlingsansvarlig aldri under noen omstendigheter vil bli benyttet til videre trening, finjustering (fine-tuning) eller optimering av AI-modeller, verken for eget formål eller for tredjeparter.
- **Logging**: Systemlogger lagrer kun tekniske metadata (tidsstempel, API-nøkkel-ID, antall tokens prosessert, feilkoder) for fakturerings- og feilsøkingsformål. Det faktiske innholdet i ledetekstene (the prompt payload) logges ikke.

6. Informasjonssikkerhet (ISO 27001)

Databehandleren skal iverksette egnede tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er egnet med hensyn til risikoen, i samsvar med GDPR artikkel 32.
Databehandleren garanterer at all fysisk infrastruktur og tilhørende maskinvare driftes i et datasenter lokalisert i Norge, som er sertifisert etter standarden ISO/IEC 27001 for informasjonssikkerhet. Fysisk og logisk adgangskontroll til maskinvaren er strengt begrenset til autorisert personell og oppfyller kravene i ISO 27001-rammeverket.

7. Bruk av underdatabehandlere

Databehandleren skal ikke overlate personopplysninger til en underdatabehandler uten forutgående skriftlig særskilt eller generelt samtykke fra Behandlingsansvarlig.
Databehandler benytter per dags dato følgende underdatabehandlere for fysisk fasilitetsdrift (datasenter):
Underdatabehandler: Blix Solutions AS, org.nr. 993128708.
Tjeneste: ISO 27001-sertifisert samlokalisering (colocation), strøm, kjøling og fysisk sikkerhet.
Lokasjon: Dataenterene kjent som Blix NR5 Oslo og Blix BDC Oslo.
Dersom Databehandler planlegger å skifte ut eller legge til underdatabehandlere, skal **Behandlingsansvarlig** varsles skriftlig minimum 30 dager i forkant, og har rett til å fremme innsigelser mot slike endringer.

8. Overføring til tredjeland

Databehandleren skal ikke overføre eller tilgjengeliggjøre personopplysninger til land utenfor EU/EØS-området (tredjeland) uten forutgående skriftlig godkjenning fra Behandlingsansvarlig. All prosessering skal skje i sin helhet i Norge.

9. Bistand til Behandlingsansvarlig

Databehandleren skal, i den grad det er mulig og under hensyntagen til behandlingens art (herunder ZDR-policyen), bistå **Behandlingsansvarlig** med egnede tekniske og organisatoriske tiltak for å oppfylle **Behandlingsansvarlig** plikt til å svare på forespørsler fra registrerte som vil utøve sine rettigheter (innsyn, retting, sletting osv.).
Merk: Siden data ikke lagres etter endt sesjon, bekrefter Partene at historiske personopplysninger ikke vil eksistere i **Databehandlerens** systemer etter at API-kallet er fullført.

10. Sikkerhetsbrudd (Avvikshåndtering)

Ved brudd på personopplysningssikkerheten (sikkerhetsbrudd) skal **Databehandleren** varsle **Behandlingsansvarlig** skriftlig uten ugrunnet opphold, og senest 24 timer etter å ha fått kjennskap til bruddet. Varselet skal beskrive bruddets art, berørte datakategorier, og tiltak som er iverksatt for å avbøte situasjonen.

Behandlingsansvarlig har det formelle ansvaret for å vurdere og eventuelt melde bruddet videre til Datatilsynet i samsvar med gjeldende lovgivning (p.t. innen 72 timer). **Databehandleren** skal bistå **Behandlingsansvarlig** med nødvendig informasjon for å oppfylle denne meldeplikten.

11. Revisjon og inspeksjon

Databehandleren skal gjøre tilgjengelig for **Behandlingsansvarlig** all informasjon som er nødvendig for å påvise at forpliktelsene i denne Avtalen er oppfylt, samt muliggjøre og bidra til revisjoner, herunder inspeksjoner, gjennomført av **Behandlingsansvarlig** eller en annen revisor på vegne av denne. Dokumentasjon på gyldig ISO 27001-sertifisering for datasenteret skal gjøres tilgjengelig på forespørsel.

12. Opphør og sletting

Ved opphør av Hovedavtalen skal **Databehandleren** stanse all prosessering av data på vegne av Behandlingsansvarlig. Siden BlixAI opererer med Zero Data Retention, vil det ikke eksistere aktive databaser eller sikkerhetskopier av **Behandlingsansvarliges** prompts/outputs som krever sletting ved avtalens slutt, med unntak av ordinære fakturerings- og loggdata av brukte tokens (metadata) som oppbevares i henhold til bokføringsloven.

Signatur

Dette dokumentet er signert elektronisk/i to eksemplarer.

	Behandlingsansvarlig		**Databehandler**
Sted/Dato:		Sted/Dato:	
Navn:		Navn:	
Signatur:		Signatur:	
Tittel:		Tittel:	
Selskap:		Selskap:	