

Databehandleravtale

Språki · mal v2.1 · GDPR art. 28 · org.nr. 998639255 MVA

Databehandleravtale

DATABEHANDLERAVTALE

Denne avtalen er inngått mellom:

Behandlingsansvarlig:

[Organisasjonsnavn], org.nr. [xxxxxxx xxx]

Kontaktperson: [Navn]

E-post: [e-post]

Heretter kalt «Behandlingsansvarlig»

Databehandler:

Tilvo Tek Thøgersen («Tilvo»), leverandør av Språki

Org.nr.: 998639255 MVA

Kontaktperson: Gaute Thøgersen

E-post: kontakt@spraki.no

Heretter kalt «Databehandler»

1. Avtalens bakgrunn og formål

Denne databehandleravtalen regulerer Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig i forbindelse med levering av læringsplattformen Språki.

Avtalen er inngått for å sikre at personopplysninger behandles i samsvar med personopplysningsloven og EUs personvernforordning (GDPR), særlig artikkel 28.

Denne avtalen er et tillegg til tjenesteavtalen mellom partene og gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig.

2. Beskrivelse av behandlingen

2.1 Behandlingens art og formål

Databehandler leverer en nettbasert læringsplattform for språklæring som bruker kunstig intelligens (KI). Behandlingen omfatter:

- Lagring og forvaltning av brukerkontoer og læringsdata
- KI-basert prosessering av tekst for tilbakemelding, oversettelse og samtaletrening
- KI-basert analyse av elevens taleopptak for uttaletrening (opptaket analyseres og forkastes; lydfilen lagres ikke hos Databehandler — transkripsjon og vurdering lagres)

- Sanntids KI-samtale med lyd (og eventuelt video dersom brukeren aktiverer kamera); strømmen behandles i sanntid og lagres ikke
- Behandling og lagring av bilder brukeren selv laster opp (f.eks. foto av egen håndskrevet tekst for tekstgjenkjenning/skrivetrening)
- Generering av systemlyd (tekst-til-tale) og transkribering av brukerens taleopptak (tale-til-tekst, midlertidig)
- Generering og lagring av bilder, dokumenter og presentasjoner
- Utsendelse av e-post knyttet til kontoadministrasjon (kontoverifisering, tilbakestilling av passord)
- Administrasjon av brukergrupper og læringsframgang

2.2 Behandlingens varighet

Behandlingen varer så lenge tjenesteavtalen mellom partene er gjeldende. Ved opphør gjelder bestemmelsene i punkt 4.7 og 7.3.

2.3 Kategorier av registrerte

- Elever/deltakere ved Behandlingsansvarliges virksomhet
- Lærere/instruktører
- Administratorer

2.4 Typer personopplysninger som behandles

Kategori	Personopplysninger
Kontoinformasjon	Navn, e-postadresse, passord (kryptert), rolle, morsmål, tilknytning til organisasjon
Læringsdata	Læringsframgang, nivå, øvelsesresultater, ordlister
Brukergenerert innhold	Tekst skrevet av brukere, lagrede tekster, genererte bilder og dokumenter
Taleopptak	Elevens stemme ved uttaletrening og taleøvelser (sendes til KI-tjeneste for analyse; lagres ikke som lydfil hos Databehandler — transkripsjon og vurdering lagres)
Sanntidsstrøm	Lyd (og eventuelt video) i KI-samtale; behandles i sanntid, lagres ikke
Opplastede bilder	Foto brukeren laster opp, f.eks. av egen tekst (lagres i skylagring med EU-jurisdiksjon)
Innhold laget av lærere	Presentasjoner, undervisningsmateriell, eventuelt elevtekst lærer legger inn for vurderingsstøtte
Tekniske data	IP-adresse, innloggingstidspunkt, nettleserinformasjon, brukslogger

Det behandles ingen særlige kategorier av personopplysninger (sensitive data) som del av tjenestens tiltenkte bruk. Brukere kan i fritekst og taleopptak selv velge å dele personlige opplysninger; se Vedlegg D om dataminimering.

3. Behandlingsansvarliges rettigheter og plikter

3.1 Behandlingsansvarlig har det overordnede ansvaret for at behandlingen av personopplysninger skjer i samsvar med GDPR, jf. artikkel 24.

3.2 Behandlingsansvarlig fastsetter formålene med og midlene for behandlingen, jf. artikkel 4 nr. 7.

3.3 Behandlingsansvarlig skal gi Databehandler dokumenterte instruks for behandlingen av personopplysninger. Instruks utover det som er avtalt i denne avtalen, skal gis skriftlig.

3.4 Behandlingsansvarlig er ansvarlig for å ha rettslig grunnlag for behandlingen, herunder å informere de registrerte om behandlingen.

3.5 Behandlingsansvarlig har rett til å gjennomføre eller la gjennomføre revisjoner, jf. punkt 4.8.

4. Databehandlers plikter

4.1 Behandling kun etter instruks (art. 28(3)(a))

Databehandler skal kun behandle personopplysninger etter dokumenterte instruks fra Behandlingsansvarlig, herunder med hensyn til overføring av personopplysninger til et tredjeland. Dersom Databehandler er pålagt behandling etter EU-rett eller norsk rett, skal Databehandler underrette Behandlingsansvarlig om dette rettslige kravet før behandlingen, med mindre slik underretning er forbudt.

Databehandler skal umiddelbart varsle Behandlingsansvarlig dersom en instruks etter Databehandlers mening er i strid med GDPR eller annet personvernregelverk.

4.2 Taushetsplikt (art. 28(3)(b))

Databehandler skal sikre at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til taushetsplikt eller er underlagt lovbestemt taushetsplikt. Taushetsplikten gjelder også etter avtalens opphør.

Tilgang til personopplysninger skal begrenses til personell som har et tjenstlig behov.

4.3 Sikkerhetstiltak (art. 28(3)(c))

Databehandler skal gjennomføre alle tiltak som kreves etter GDPR artikkel 32, herunder egnede tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er egnet med hensyn til risikoen.

Sikkerhetstiltakene er nærmere beskrevet i Vedlegg B.

4.4 Bruk av underdatabehandlere (art. 28(3)(d))

Databehandler skal ikke benytte andre databehandlere (underdatabehandlere) uten forhåndsgodkjenning fra Behandlingsansvarlig.

Behandlingsansvarlig gir herved **generell skriftlig godkjenning** til bruk av underdatabehandlere som er oppført i Vedlegg C. Databehandler skal informere Behandlingsansvarlig skriftlig minst **30 dager** før planlagte endringer i listen over underdatabehandlere (tillegg eller erstatning). Behandlingsansvarlig kan protestere mot slike endringer innen 14 dager etter varsling.

Alternativ (kryss av dersom valgt): ☐ Spesifikk godkjenning

Dersom Behandlingsansvarlig krever det, gjelder i stedet spesifikk godkjenning: enhver endring i listen over underdatabehandlere i Vedlegg C krever skriftlig forhåndsgodkjenning fra Behandlingsansvarlig før endringen iverksettes.

Databehandler skal inngå skriftlig avtale med alle underdatabehandlere som pålegger dem de samme forpliktelsene som følger av denne avtalen. Databehandler er fullt ansvarlig overfor Behandlingsansvarlig dersom en underdatabehandler ikke oppfyller sine forpliktelser.

4.5 Bistand med registrertes rettigheter (art. 28(3)(e))

Databehandler skal, under hensyntaken til behandlingens art, bistå Behandlingsansvarlig med egnede tekniske og organisatoriske tiltak, slik at Behandlingsansvarlig kan oppfylle sin plikt til å svare på forespørsler om utøvelse av de registrertes rettigheter etter GDPR kapittel III (innsyn, retting, sletting, begrensning, dataportabilitet, protest).

Databehandler skal varsle Behandlingsansvarlig uten ugrunnet opphold dersom Databehandler mottar en henvendelse fra en registrert.

4.6 Bistand med sikkerhet, avvik og konsekvensvurderinger (art. 28(3)(f))

Databehandler skal bistå Behandlingsansvarlig med å oppfylle forpliktelsene etter GDPR artiklene 32–36, herunder:

- **Sikkerhet** (art. 32): Bidra til å sikre et egnet sikkerhetsnivå.
- **Avvikshåndtering** (art. 33–34): Varsle Behandlingsansvarlig **uten ugrunnet opphold, og senest innen 48 timer**, etter å ha blitt kjent med et brudd på personopplysningssikkerheten. Varselet skal inneholde tilgjengelig informasjon om bruddet, berørte kategorier og antall registrerte, sannsynlige konsekvenser, og tiltak som er iverksatt eller foreslått.
- **Personvernkonsekvensvurdering (DPIA)** (art. 35): Bistå med nødvendig informasjon for gjennomføring av vurderinger av personvernkonsekvenser. Databehandler har utarbeidet et eget DPIA-støttedokument som stilles til rådighet.
- **Forhåndsdrøfting** (art. 36): Bistå ved eventuell forhåndsdrøfting med Datatilsynet.

4.7 Sletting eller tilbakelevering av data (art. 28(3)(g))

Ved opphør av tjenesteavtalen skal Databehandler, etter Behandlingsansvarliges valg:

- **Returnere** alle personopplysninger til Behandlingsansvarlig i et strukturert, vanlig brukt og maskinlesbart format, **og deretter slette** alle kopier, eller
- **Slette** alle personopplysninger og bekrefte skriftlig at sletting er gjennomført.

Sletting omfatter både databaseinnhold og mediefiler (bilder, lyd, dokumenter) lagret i skylagring. Sletting skal gjennomføres innen **90 dager** etter avtalens opphør, med mindre lovgivning krever lagring.

Databehandler skal dokumentere at sletting er gjennomført.

Behandlingsansvarlig har rett til å be om dataeksport i avtalens løpetid.

4.8 Etterlevelse og revisjon (art. 28(3)(h))

Databehandler skal gjøre tilgjengelig all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i artikkel 28 er oppfylt.

Databehandler skal tillate og bidra til revisjoner, herunder inspeksjoner, som gjennomføres av Behandlingsansvarlig eller en annen revisor som Behandlingsansvarlig har gitt fullmakt. Revisjon kan gjennomføres med **14 dagers** skriftlig varsel, og normalt ikke oftere enn én gang per år. Partene bærer egne kostnader ved revisjon.

5. Overføring til tredjeland

5.1 Serverinfrastruktur, database og fillagring er lokalisert i **EU** (server og database i Tyskland; fillagring i Cloudflare R2 konfigurert med EU-jurisdiksjon). Personopplysninger sendes til amerikanske KI-tjenester for prosessering under API-kall, men lagres ikke permanent utenfor EU.

5.2 Databehandler overfører personopplysninger til USA gjennom bruk av underdatabehandlere som angitt i Vedlegg C. Overføringen skjer med følgende overføringsgrunnlag:

- **EU-US Data Privacy Framework (DPF)** for leverandører som er sertifisert under rammeverket, jf. EU-kommisjonens adekvansbeslutning av 10. juli 2023.
- **EUs standardkontraktsklausuler (SCCs)** som er inntatt i databehandleravtalene med samtlige amerikanske underdatabehandlere, og som utgjør selvstendig overføringsgrunnlag dersom DPF-beslutningen skulle bli opphevet.

5.3 DPF-beslutningen er per juli 2026 gyldig, men er gjenstand for rettslig prøving (anke til EU-domstolen, sak C-703/25 P). Databehandler har utarbeidet en egen vurdering av tredjelandsoverføringene (Transfer Impact Assessment) som stilles til rådighet for Behandlingsansvarlig, og som beskriver tilleggstiltak og beredskap dersom overføringsgrunnlaget endres.

5.4 Databehandler skal varsle Behandlingsansvarlig dersom overføringsgrunnlaget endres vesentlig (f.eks. dersom DPF-rammeverket ugyldiggjøres).

6. Formålsbegrensning og tiltenkt bruk (KI)

6.1 Språki er et frivillig trenings- og øvingsverktøy for språklæring. Tjenesten, herunder dens KI-genererte tilbakemeldinger, vurderinger og nivåindikasjoner, er **ikke** utformet for eller ment å brukes til:

- formell vurdering eller karaktersetting av elever/deltakere,
- eksamen eller prøver med rettsvirkning,
- opptak til eller tildeling av utdanning/opplæringstilbud, eller
- nivåplassering eller andre beslutninger med rettsvirkning eller tilsvarende betydelig innvirkning for den registrerte.

6.2 Behandlingsansvarlig forplikter seg til ikke å bruke tjenestens resultater som grunnlag for slike beslutninger, og ikke som eneste grunnlag for noen beslutning av betydning for den enkelte deltaker. Lærers egen faglige vurdering skal alltid ligge til grunn.

6.3 Denne formålsbegrensningen innebærer at tjenesten etter partenes felles forståelse ikke utgjør et høyrisiko KI-system etter EU-forordningen om kunstig intelligens (AI Act) vedlegg III nr. 3. Dersom Behandlingsansvarlig ønsker å bruke tjenesten på en måte som kan omfattes av vedlegg III, skal partene først avklare dette skriftlig.

7. Varighet og oppsigelse

7.1 Denne avtalen gjelder fra signeringsdato og så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig.

7.2 Begge parter kan si opp avtalen med samme oppsigelsestid som tjenesteavtalen.

7.3 Ved opphør gjelder bestemmelsene i punkt 4.7 om sletting eller tilbakelevering.

7.4 Bestemmelsene om taushetsplikt (punkt 4.2) og ansvar gjelder også etter avtalens opphør.

8. Kontaktpersoner

Behandlingsansvarlig:

Navn: [Fyll inn]

E-post: [Fyll inn]

Telefon: [Fyll inn]

Databehandler:

Navn: Gaute Thøgersen

E-post: kontakt@spraki.no

9. Signatur

Denne avtalen er utferdiget i to eksemplarer, ett til hver av partene.

Behandlingsansvarlig:

Sted/dato:

Signatur:

Navn:

Tittel:

Databehandler:

Sted/dato:

Signatur:

Navn: Gaute Thøgersen

Tittel: Daglig leder, Tilvo Tek Thøgersen

Vedlegg A: Instrukser fra Behandlingsansvarlig

Behandlingsansvarlig instruerer Databehandler om å behandle personopplysninger slik det er nødvendig for å levere tjenesten Språki, som beskrevet i punkt 2 og i tjenesteavtalen mellom partene.

Ytterligere instruksjoner kan gis skriftlig til kontakt@spraki.no.

Vedlegg B: Tekniske og organisatoriske sikkerhetstiltak (sammendrag)

Fullstendig sikkerhetsdokumentasjon (TOMs) er tilgjengelig som eget dokument og utleveres på forespørsel. Hovedtiltak:

Kryptering

- All kommunikasjon mellom brukerens enhet og servere er kryptert med TLS 1.2+ (HTTPS/WSS).
- Passord lagres med enveis kryptografisk hashing (bcrypt) og er ikke tilgjengelig i klartekst. Kontoer fra tidligere systemversjoner oppgraderes til bcrypt ved neste innlogging.
- Alle API-kall til underdatabehandlere skjer kryptert.

Tilgangskontroll

- Rollebasert tilgangskontroll (elev, lærer, administrator) med organisasjonsisolering: lærere ser kun elever i egne grupper, administratorer kun egen organisasjon.
- Innloggingsbegrensning mot automatiserte angrep, e-postverifisering av nye kontoer.
- Kun autorisert personell hos Databehandler har tilgang til servere og database.

Infrastruktur og lagring

- Server og database driftes i datasenter i Tyskland (EU) med fysisk adgangskontroll, redundant strøm og brannvern.
- Fillagring (bilder, lyd, dokumenter) i Cloudflare R2 konfigurert med EU-jurisdiksjon.
- Nattlig automatisk sikkerhetskopiering av databasen. Kopiene krypteres på serveren før de forlater den, og lagres innenfor EU. Krypteringsnøkkelen oppbevares ikke på serveren.

Logging og dataminimering

- Sikkerhetsrelevante hendelser logges. Innholdet i KI-forespørsler og -svar logges ikke; kun teknisk metadata (tidspunkt, tjeneste, tokenforbruk).
- Tekniske logger med IP-adresse slettes automatisk etter 90 dager.

Avvikshåndtering og vedlikehold

- Dokumentert prosedyre for hendelseshåndtering; varsling av Behandlingsansvarlig uten ugrunnet opphold og senest innen 48 timer.
- Operativsystem og programvare holdes oppdatert med sikkerhetspatcher.
- Sikkerhetstiltak og dokumentasjon gjennomgås minst årlig.

Vedlegg C: Liste over underdatabehandlere

Behandlingsansvarlig har godkjent bruk av følgende underdatabehandlere:

Selskap	Land	Formål	Data som behandles	Overføringsgrunnlag
Google LLC	USA	KI-prosessering (tekst, bilde, tale — Gemini API), e-postutsendelse (Google Workspace), innlogging (Google OAuth, valgfritt for bruker)	Elevtekst, opplastede bilder, taleopptak og sanntidsstrøm til KI-analyse (lagres midlertidig, inntil 55 dager, hos leverandør for misbrukskontroll); e-postadresse ved kontovarsler	EU-US DPF + SCCs
ElevenLabs Inc.	USA	Talesyntese (tekst-til-tale) og transkribering (tale-til-tekst)	Tekst for talesyntese; brukerens taleopptak for transkribering (behandles midlertidig, lagres ikke varig)	EU-US DPF + SCCs
OpenAI (OpenAI Ireland Ltd / OpenAI OpCo, LLC)	Irland / USA	Talesyntese (tekst-til-lyd) — hvilende fra 13.08.2026 : godkjent og avtalefestet, men ingen funksjon sender data hit	Tekst for talesyntese, uten direkte identifikatorer (misbrukslogg inntil 30 dager hos leverandør)	SCCs
Cloudflare Inc.	USA	Fillagring (R2, konfigurert med EU-jurisdiksjon), CDN/DDoS-beskyttelse og bildegenerering (Workers AI — FLUX)	Opplastede bilder, genererte bilder, lyd, dokumenter og presentasjoner; tekst-prompts for bildegenerering (normalt uten personopplysninger; brukes ikke til modelltrening og lagres ikke)	EU-US DPF + SCCs
netcup GmbH	Tyskland	Serverdrift og database	All brukerdata (lagring i EU)	EØS (ingen tredjelandsoverføring)

Merk: OpenAI er ikke sertifisert under EU-US Data Privacy Framework; for denne leverandøren er EUs standardkontraktsklausuler (SCCs), innarbeidet i leverandørens databehandleravtale, overføringsgrunnlaget.

Om «hvilende»: OpenAI er godkjent av behandlingsansvarlig og står i denne listen, men talesyntesen er erstattet av Google Gemini, og ingen funksjon sender data dit per 13.08.2026. Fordi leverandøren allerede er oppført og godkjent for det formålet som står i tabellen, utløser et eventuelt gjenopptak innenfor samme formål ikke ny varslingsplikt etter punkt 4.4 — det er ikke et tillegg til eller en erstatning i listen. Utvides formålet, gjelder varslingsplikten på vanlig måte.

Databehandler har inngått databehandleravtaler med alle oppførte underdatabehandlere.

Merknader:

- Betalingsformidler (Stripe Payments Europe Ltd / Stripe, LLC) benyttes kun for privatkunder og er ikke relevant for organisasjonsavtaler; fakturering av Behandlingsansvarlig skjer direkte fra Databehandler uten tredjepart.

- Dersom Databehandler ønsker å ta i bruk ytterligere KI-leverandører, varsles dette som endring i denne listen etter punkt 4.4 (minimum 30 dagers varsel) før noen personopplysninger behandles der.

Endringer i listen varsles skriftlig til Behandlingsansvarlig minimum 30 dager i forkant.

Sist oppdatert: august 2026. Den til enhver tid gjeldende listen, med endringslogg, finnes på spraki.no/underdatabehandlere.

Vedlegg D: Instrukser for KI-behandling

Følgende gjelder spesifikt for behandling av personopplysninger via kunstig intelligens (KI):

1. Alle KI-tjenester brukes via betalte API-er der leverandørene ved avtale er forpliktet til **ikke å bruke data til trening av KI-modeller**.
2. Databehandler praktiserer **dataminimering**: brukerens navn, e-postadresse, bruker-ID og organisasjonstilknytning sendes ikke til KI-tjenestene. Kun innholdet i selve læringsaktiviteten (tekst, taleopptak, bilde) og nødvendig pedagogisk kontekst (språknivå, oppgavetype) sendes.
3. Tekst, taleopptak og bilder fra brukeren sendes til KI-tjenester for prosessering (tilbakemelding, oversettelse, samtale, uttaleanalyse, tekstgjenkjenning). Slikt innhold kan inneholde personopplysninger brukeren selv velger å dele. Behandlingsansvarlig bør veilede deltakere om å unngå å dele sensitive opplysninger i fritekst og tale.
4. KI-leverandøren kan lagre innsendt innhold **midlertidig** for misbrukskontroll (hos Google Gemini API inntil **55 dager**), deretter slettes det. Innholdet brukes ikke til trening.
5. Elevens taleopptak ved uttaletrening analyseres av KI og forkastes; lydfilen lagres ikke hos Databehandler. Transkripsjon og vurderingsresultat lagres som læringsdata.
6. Sanntids KI-samtale (lyd, eventuelt video) strømmes til KI-tjenesten og behandles i sanntid; strømmen lagres ikke.
7. Samtaleinnhold i **elevrettet KI-chat** («Spør Språki», sanntidssamtale) lagres ikke permanent hos Databehandler — samtalehistorikken holdes kun i brukerens egen nettleser/app. Databehandler logger ikke innholdet i KI-forespørsler; kun teknisk metadata.
8. **Lærerassistenten** er et unntak fra punkt 7: en lærer kan lagre sine egne samtaler og genererte undervisningsmateriell i tjenesten, slik at de er tilgjengelige på tvers av enheter. Disse lagres i databasen i EU, er kun tilgjengelige for læreren som eide samtalen (ingen deling mellom kolleger eller innad i organisasjonen), kan slettes enkeltvis av læreren, og slettes automatisk **12 måneder** etter siste endring. Vedlegg (bilder, PDF, lyd) lagres ikke — kun teksten i samtalen. Fordi en lærer kan lime inn elevtekst (f.eks. i «Vurder elevtekst»), skal Behandlingsansvarlig veilede lærere om å anonymisere elevtekst før den limes inn.
9. **Transparens (AI Act art. 50)**: Brukere informeres om at de samhandler med et KI-system, og KI-generert innhold og KI-tilbakemeldinger merkes som dette i tjenesten.