

Prosjekt: ***Tilgjengelig språkmodell for NTNU***

*(tidligere forslag hadde arbeidstittel NTNU-GPT)*

Dokument: **Prosjektforslag**

Prosjekteier: *Heine Skipenes, faggrupeleder arkitektur og rådgivning*  
Kontaktperson: *Heine Skipenes*  
Forfatter:  
Dato: *02.09.2023*  
Versjon: *0.1*

### **Hva handler prosjektforslaget om?**

KI- klynga har gjennom sommeren testet ut om det er mulig å tilby en egen språkmodell for NTNUs brukere som er «sikrere» enn det som finnes tilgjengelig gratis på nett. Det har noen uker blitt jobbet med en enkel GTP-tjeneste på Azure-plattformen, men når Microsoft nå har bekreftet lansering av Bing chat enterprise som blir gratis for våre ansattlisenser (ikke studenter) blir dette vurdert som den letteste veien til målet. Løsningen gir inntrykk av å være en løsning som kan sidestilles sikkerhetsmessig med andre tjenester fra Microsoft, og vil ikke kreve like mye FDVu-ressurser som en egenprodusert løsning. Microsoft skrur løsningen på 21. september 2023 og vi ønsker å ta i bruk løsningen fra dag 1.

Formålet med prosjektet er:

1. Tilby en språkmodell for behandling av gule/interne data.
2. Tilby en lett tilgjengelig og trygg språkmodell der våre ansatte kan gjøre seg kjent med fordeler og ulemper med ny teknologi.
3. Tilby en teknisk løsning hvor vi samtidig tilgjengeliggjør informasjon om hvordan vi har tenkt risikovurdering og personvern

Prosjektforslaget er skrevet med støtte av språkmodellen som IT-avdelingen har testet sommeren 2023.

### **Anbefaling:**

*SRG anbefaler at prosjektforslaget godkjennes og at IT-avdelingen gjør tilstrekkelig med forberedelser til å skru på funksjonen Bing Chat Enterprise ved første anledning. IT-avdelingen må prioritere ressurser til å gjennomføre ROS, personvernkonshevsvurdering og FDVu-forberedelser. Den nye tjenesten skal behandles og godkjennes av Driftsmøtet før løsningen kan skrur på. Seksjonsleder for IT-drift foreslås som ansvarlig for gjennomføring.*

## 1 Bakgrunn

Kunstig intelligens brer om seg i verden, og det som får mest oppmerksomhet er den økende bruken av språkmodeller som ChatGPT, Bing chat osv. Til dags dato har ikke NTNU tatt stilling til hvor vidt vi skal tilby egne tjenester eller ikke, og dette prosjektforslaget legges fram som beslutningsgrunnlag med anbefaling om hvorfor IT-avdelingen bør prioritere å gjøre dette.

Men hvorfor skal vi tilby en egen språkmodell?

*Prompt: «Kan du skrive en forklaring for hvorfor vi skal foreslå et prosjekt som innfører en språkmodell på NTNU?»*

*Svar: «En språkmodell er en type kunstig intelligens som kan forstå og produsere naturlig språk. NTNU er en av de ledende universitetene i Norge innenfor teknologi og datavitenskap, og ved å innføre en språkmodell kan universitetet dra nytte av den siste teknologien innenfor dette feltet.*

*En språkmodell kan ha mange praktiske anvendelser innenfor forskning, undervisning og administrasjon. For eksempel kan en språkmodell brukes til å analysere store mengder tekst og trekke ut nyttig informasjon, eller til å automatisere oppgaver som å svare på vanlige spørsmål fra studenter eller ansatte.*

*En språkmodell kan også være nyttig i undervisningen ved å gi studentene tilgang til en virtuell assistent som kan hjelpe dem med å forstå vanskelige konsepter eller svare på spørsmål om pensum. På denne måten kan en språkmodell bidra til å forbedre læringen og opplevelsen for studentene.*

*I tillegg kan en språkmodell også være nyttig i administrasjonen ved å automatisere oppgaver som å svare på vanlige spørsmål fra besøkende eller å håndtere henvendelser fra studenter eller ansatte. Dette kan frigjøre tid og ressurser som kan brukes til andre oppgaver.*

*Alt i alt vil innføringen av en språkmodell på NTNU kunne bidra til å forbedre forskningen, undervisningen og administrasjonen ved universitetet, og dermed styrke NTNU sin posisjon som et av de ledende teknologiske universitetene i Norge.»*

Sitat 30.08.2023 fra språkmodell i test ved NTNUs IT-avdeling: <https://gs-chatgpt.azurewebsites.net/>

### 1. Hovedmål og gevinst

Hovedformålet med prosjektet er å:

**Tilby en språkmodell for behandling av gule/interne data.** Pr i dag anbefaler IT-avdelingen at kunstig intelligens og språkmodeller ikke benyttes på noe annet enn grønne/åpne data. Ved å tilby en plattform eller tjeneste som kan behandle data på klassifiseringsnivå **intern** blir dette et mer anvendbart verktøy, og risiko for at ikke godkjente (åpne) plattformer brukes til den type data blir redusert.

**Tilby en lett tilgjengelig og trygg språkmodell der våre ansatte kan gjøre seg kjent med fordeler og ulemper med ny teknologi.** Mange av NTNUs brukere har aldri turt å prøve en språkmodell, og i hvert fall ikke i jobbsammenheng. Ved å tilby et trygt teststed/sandkasse der du kan prøve deg fram kan vi gjøre brukerne bedre i stand til å forstå hva språkmodeller og kunstig intelligens dreier seg om. Rent pedagogisk er det stor forskjell på teknologi som du bare lærer på et teoretisk plan, kontra det å prøve det ut i virkeligheten. Tiltaket vil kunne bidra til økt kompetanse, øke bevissthet om hvorfor det er viktig å være kritisk til innhold fra en språkmodell, og tydeliggjøre behovet for å identifisere bruk hvor manuell kontroll blir viktig.

**Tilby en teknisk løsning hvor vi samtidig tilgjengeliggjør informasjon om hvordan vi har tenkt risikovurdering og personvern.** Ved å publisere informasjon om risiko- og sårbarhetsvurderinger, personvernkonsekvensvurdering, tekniske valg og utfordringer i utviklingsarbeidet sammen med navn på hvem du kan spørre om «hvordan har dere tenkt informasjonssikkerhet?» kan være en viktig kilde til informasjon for alle på NTNU. I tillegg kan innholdet brukes sammen med den obligatoriske opplæringa informasjonssikkerhet som alle ansatte og studenter skal gjennom denne høsten.

## 2. Strategiske mål som understøttes

Å lære seg hvordan en språkmodell fungerer, hvilke fordeler og ulemper som finnes vil bli viktig for å øke den generelle kompetansen på området. Riktig bruk av en språkmodell kan bidra til en rekke fordeler, på samme tid kan feil bruk få katastrofale følger. Brukere av språkmodeller må for eksempel ha god kjennskap til viktigheten av manuell kontroll, referansebruk osv. Kompetanse er stikkordet og vi ønsker med dette forslaget å bidra til den absolutt nødvendige diskusjonen.

Fra rektors tale til NTNUs nye studenter i 2023 (<https://nyheter.ntnu.no/velkommen-til-ntnu-og-et-nytt-studiear/>):

*«Hvis jeg sier Chat GPT – hva tenker dere da? Er kunstig intelligens, forkortet KI, en stor trussel eller utallige muligheter? Jeg mener absolutt det siste. Kunstig intelligens og digitale løsninger generelt spiller en nøkkelrolle for bærekraftig omstilling og for å løse oppgaver vi ikke har folk nok til å fylle.*

*Men vi trenger alle kunnskap om temaet. Vi trenger å forstå hva kunstig intelligens er og hva det ikke er. – Og hvilke muligheter og utfordringer denne teknologien gir. Det har vår egen førsteamanuensis Inga Strømke tatt på seg å bidra til – blant annet gjennom boka «Maskiner som tenker». Jeg er sikkert ikke den eneste her som har lest denne.*

*Sett dere inn i temaet – kunstig intelligens påvirker en rekke fagfelt og endrer måter å jobbe på. Jeg vet at mange av våre undervisere nå planlegger hvordan problemstillinger knyttet til KI kan tas inn i undervisningen.»*

Ved å tilby en egen tjeneste kan IT-avdelingen være med på at NTNU når denne ambisjonen, og tjenesten er i tråd med [NTNUs strategi 2018 – 2025](#):

- «... har en nasjonal rolle i å utvikle det teknologiske grunnlaget for fremtidens samfunn.»

- «Vi må gjennom gode og inkluderende prosesser være i stand til å utnytte våre samlede ressurser bedre gjennom tydelige prioriteringer og i større grad ta i bruk ny teknologi.»
- «Store teknologiske endringer gir utfordringer, men kan også gi nye muligheter og styrket konkurransekraft. NTNU må lede an i dette.»
- Utviklingsmål (Utdanning): «prioritere innovative og utforskende læringsprosesser»

Tjenesten understøttes også av IT-avdelingens prioriterte mål i periodeplan “Jobbe smart”, og utnytter Microsoftplattformen som IT-avdelingen allerede sitter på.

## 2.1. Hva sier språkmodellen om strategiske mål som understøttes?

*Prompt: «Kan du angi hvilke mål som understøttes innen områdene forskning, undervisning og læringsmiljø, formidling, innovasjon og nyskaping, kunst eller organisasjonen for øvrig ved bruk av KI?»*

*Svar: «Her er noen eksempler på mål som kan understøttes av bruk av kunstig intelligens (KI) i ulike områder ved NTNU:*

*Forskning:*

- Å utforske og utvikle nye metoder for å analysere store mengder data
- Å identifisere mønstre og sammenhenger i komplekse datasett
- Å utvikle nye algoritmer for maskinlæring og dyp læring
- Å forbedre nøyaktigheten og effektiviteten til eksisterende modeller og metoder
- Å bidra til å utvikle nye fagområder som kunstig intelligens og maskinlæring

*Undervisning og læringsmiljø:*

- Å tilby studentene en mer tilpasset og personlig læringserfaring
- Å gi studentene tilgang til virtuelle assistenter som kan hjelpe dem med å forstå vanskelige konsepter eller svare på spørsmål om pensum
- Å utvikle nye metoder og verktøy for å evaluere og forbedre studentenes læring og prestasjoner
- Å bidra til å utvikle nye fagområder og studieprogrammer som fokuserer på kunstig intelligens og relaterte emner

*Formidling:*

- Å utvikle nye verktøy og teknologier for å presentere og visualisere data på en mer engasjerende og tilgjengelig måte
- Å gjøre informasjon og kunnskap mer tilgjengelig og forståelig for publikum gjennom bruk av språkmodeller og andre KI-verktøy

*Innovasjon og nyskaping:*

- Å utvikle nye produkter og tjenester som er basert på kunstig intelligens og maskinlæring

- *Å utforske og utvikle nye forretningsmodeller som tar i bruk kunstig intelligens og relaterte teknologier*
- *Å samarbeide med næringslivet og andre institusjoner for å utvikle og implementere nye KI-løsninger*

Organisasjonen for øvrig:

- *Å automatisere og effektivisere interne prosesser og rutiner ved bruk av KI-verktøy*
- *Å forbedre kvaliteten og nøyaktigheten av beslutningsprosesser gjennom bruk av dataanalyse og modellering*
- *Å bidra til å utvikle NTNU som en ledende institusjon innen teknologi og innovasjon ved å ta i bruk nye og avanserte teknologier som KI.»*

Sitat 30.08.2023 fra språkmodell i test ved NTNUs IT-avdeling: <https://gs-chatgpt.azurewebsites.net/>

### 3. Hovedfunksjon

IT-avdelingen ønsker å aktivisere funksjonen Bing Chat Enterprise som lanseres av Microsoft 21. september 2023. Dette er en første tjeneste på vei mot Microsoft Co-pilot som lanseres på et senere tidspunkt. Løsningen skal være sikrere enn ordinære språkmodeller som finnes åpent på nett, og sikkerhetsnivået skal være på samme nivå som for resten av Microsoft (M365-plattformen.)

Hvordan vil tjenesten se ut for brukerne:

1. Gå til lenke på nettside eller trykk på knapp via Microsoft 365.
2. Vær så god og bruk, lim inn informasjon og klipp ut det du trenger.

All data slettes når bruk opphører. Den logger seg selv ut etter en tid med inaktivitet. Den husker ikke fra dag til dag.

### 4. Prosessforbedring

I utgangspunktet kan løsningen være et støtteverktøy i alle prosesser som baserer seg på språklig og tekstlig innhold. Det kan være til hjelp til å forstå mer om hvordan du selv kan produsere tekstlig innhold, og hvordan andre kan bruke slike verktøy i både positiv og negativ forstand.

#### 4.1. Hva sier språkmodellen om prosessforbedring?

*Prompt: «Hvilke arbeidsoppgaver berøres av ta i bruk KI, og hvilke arbeidsprosesser og tjenester berøres? På hvilke hvilken måte ønskes / tenkes det at prosessen(e) kan forbedres?»*

*Svar: «Bruk av kunstig intelligens (KI) kan berøre en rekke arbeidsoppgaver og arbeidsprosesser ved NTNU, avhengig av hvilke løsninger som blir implementert. Her er noen eksempler på arbeidsoppgaver og arbeidsprosesser som kan påvirkes positivt ved bruk av KI:*

- *Datainnsamling og analyse: KI kan brukes til å automatisere innsamlingen og analysen av store mengder data, noe som kan frigjøre tid og ressurser som kan brukes*

til andre oppgaver. På denne måten kan prosessen med å samle inn og analysere data bli mer effektiv og nøyaktig.

- *Beslutningsprosesser: KI kan brukes til å hjelpe beslutningstakere med å ta bedre og mer informerte beslutninger. For eksempel kan en KI-løsning analysere store mengder data og gi anbefalinger basert på resultatene. Dette kan bidra til å forbedre beslutningsprosessen og redusere risikoen for feil.*
- *Kundeservice og support: KI kan brukes til å automatisere og forbedre kundeservice og supporttjenester ved NTNU. For eksempel kan en språkmodell brukes til å svare på vanlige spørsmål fra studenter og ansatte, noe som kan frigjøre tid og ressurser som kan brukes til mer komplekse oppgaver.*
- *Undervisning og læring: KI kan brukes til å forbedre undervisning og læring ved NTNU på en rekke måter. For eksempel kan en språkmodell brukes til å gi studentene tilgang til en virtuell assistent som kan hjelpe dem med å forstå vanskelige konsepter eller svare på spørsmål om pensum. Dette kan bidra til å forbedre læringen og opplevelsen for studentene.*

*På hvilken måte prosessene kan forbedres avhenger av hvilken løsning som blir implementert. Generelt kan KI bidra til å forbedre prosessene ved å automatisere og effektivisere oppgaver, redusere risiko for menneskelig feil og gi bedre og mer informerte beslutninger. Dette kan frigjøre tid og ressurser som kan brukes til andre oppgaver, og bidra til å forbedre ytelsen og resultatene ved NTNU.»*

Sitat 30.08.2023 fra språkmodell i test ved NTNUs IT-avdeling: <https://gs-chatgpt.azurewebsites.net/>

## 5. Informasjonsinnhold

Bing Chat Enterprise er en generativ AI-tjeneste basert på data fra den offentlige weben i Bing-søkeindeksen. Den har ikke tilgang til organisatoriske ressurser eller innhold i Microsoft 365, som dokumenter i OneDrive, e-post eller annen data i Microsoft 365 Graph.

Bare organisatorisk innhold som brukes av brukerne i chatten, er tilgjengelig for Bing Chat Enterprise. Dette kan gjøres på to måter:

1. Brukere skriver eksplisitt inn denne informasjonen direkte i chatten.
2. Brukere skriver en forespørsel inn i chatten i Edge-sidebar etter å ha aktivert innstillingen 'Tillat tilgang til hvilken som helst nettside eller PDF', og et dokument eller en intranettside er åpnet i nettleseren. I dette scenariet kan Bing Chat Enterprise bruke dette innholdet for å hjelpe til med å besvare spørsmål.

I begge tilfeller beholder ikke Bing Chat Enterprise noen av disse dataene etter at chatten er avsluttet.

Informasjonsgrunnlaget er hentet fra <https://learn.microsoft.com/en-us/bing-chat-enterprise/privacy-and-protections> og oversatt 02.09.2023 ved hjelp fra språkmodell i test ved NTNUs IT-avdeling: <https://gs-chatgpt.azurewebsites.net/>



## 6. Brukerinvolvering

I første omgang er dette en tjeneste som vil tilbys til alle ansatte. Sammen med at tjenesten tilbys vil vi legge ut informasjon ut på Innsida om hvordan det er mulig å komme med tilbakemeldinger til oss som IT-avdeling, og komme med generelle tilbakemeldinger til verden om positive og negative ting med løsningen. For eksempel kan erfaringer deles på NTNUs Lærende fellesskap på [discourse.it.ntnu.no](https://discourse.it.ntnu.no)? Det blir opprettet en wikiside som det er mulig å finne informasjon om tekniske vurdering, risikovurderinger, personvernkonsekvensvurdering osv.

Det bør også vurderes om NTNU bør bidra mer aktivt med kompetansetiltak som kurs, seminar for erfaringsutveksling osv.

## 7. Organisering

IT-avdelingen er ansvarlig for tjenesten, og prosjektforlaget legges fram til behandling i ledermøtet. Innføring av dette verktøyet håndteres som en normal change, og skal behandles av driftsmøtet før løsningen skrur på. Operativt ansvar når løsningen er i drift foreslås lagt til M365-teamet. Det er ikke behov for en styringsgruppe ved denne innføringen.

## 8. Forutsetninger

For at dette er en tjeneste som skal fungere er det viktig at IT-avdelingen er enige om at:

- Løsningen må kunne tilby å behandle data på intern (gult) nivå i henhold til NTNUs informasjonssikkerhetsklassifisering <https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonsklassifisering+-+informasjonssikkerhet> Løsningen er ikke godkjent for fortrolig eller strengt fortrolig nivå, og det vil ikke være tilrådelig å legge inn andres personopplysninger i løsningen.
- I denne omgang blir ikke løsningen åpnet for studenter, da tjenestemodellen fra Microsoft ikke åpner for løsningen i studentlisensene. Dette anses som forsvarlig på nåværende tidspunkt da studenter hovedsakelig skal behandle åpne data, og mange har tatt i bruk løsninger på nett (for eksempel <https://www.grammarly.com/>). Det er vanskelig å forhindre bruk av denne typen verktøy, og NTNU må i videre utviklingssteg ta stilling til dette.
- Tjenesten kan ha begrenset levetid, og er fra leverandørens ståsted en «innstegsløsning» til Microsoft Co-pilot.
- IT-avdelingen må rigge opp et organisatorisk apparat for å håndtere utviklingen av kunstig intelligens på en systematisk måte.
- Det må settes av tilstrekkelig med ressurser til å forhåndsvurdere løsningen med tanke på drift, sikkerhet, personvern og brukerinformasjon.
  - o Løsningen må ha ROS og DPIA
    - Løsningen må kunne slette alle data. Dette må være garantert. Både påloggings/bruksinformasjon og manuelt innputt.
    - Den må ikke være lærende av andres innputt, og du kan ikke få tilgang på andres informasjon (individseparasjon)
    - Må ha tilgjengelig samtykkeinformasjon for de som skal bruke løsningen. Samtykkeinformasjonen må kunne endre seg
- Det må settes av tilstrekkelig med ressurser og ansvar for å monitorere at tjenesten fungerer som den skal etter at den er satt i drift med tanke på drift, sikkerhet, personvern og brukerinformasjon. IT-avdelingen må også være i stand til å følge med

på om leverandøren gjør endringer på løsningen, og være i stand til å skru den av om det blir behov for det.

- Løsningen må harmonere med bruk i andre organisasjoner, og NTNU kan støtte seg på andres vurderinger i bruk av denne løsningen. Eksempler:
  - o <https://www.uio.no/tjenester/it/ki/gpt/personvern/>
  - o Nav – veileder kunstig intelligens
  - o [Digdirs veiledning for ansvarlig bruk og utvikling av kunstig intelligens.](#)

## 9. Omfang

Tjenesten blir skrudd på av Microsoft 21. september, og NTNU må aktivt skru av tjenesten om ikke den skal gjøres tilgjengelig for våre ansatte. Forslagsstiller oppfatter at IT-avdelingen har et ønske om å være «fremme i skoa» med å ta i bruk denne typen løsninger og jobber derfor etter følgende tidsplan:

- 28/8-23 – IT-direktør er orientert muntlig og har gitt godkjenning for iverksettelse av prosessen
- 6/9-23 – Prosjektforslag ferdig fra KI-klynga og sender til ledergruppa for behandling
- 11/9-23 – IT-direktør godkjenner forslaget formelt og iverksetter tiltak:
  - o ROS – Ansvarlig Digital sikkerhet
  - o DPIA og utvikling av brukerinformasjon – Ansvarlig SRG
  - o Teknisk forberedelse – Ansvarlig drift
  - o FDVu forberedelse – Ansvarlig forvaltning
- 19/9-23 Forslag behandles i Driftsmøtet
- 21/9-23 – Tjenesten lanseres og det legges ut melding på innsida til alle ansatte

Perioden fram til alle tiltak er på plass anses som arbeidsintensiv og innsatsen som må legges inn tidsmessig blant IT-avdelingens ansatte vurderes som betydelig, men ikke uoverkommelig. Prioritering av tilstrekkelig med ressurser er helt nødvendig.