



1. NTNU (stor/offentlig)

- Teste Microsoft KI-assistent «Microsoft 365 Copilot», med fokus på å vurdere verktøyets muligheter og utfordringer, samt etablering av et robust rammeverk for forvaltning, drift, vedlikehold og utvikling.

2. Helsedirektoratet (stor/offentlig)

- Forenklet tilgang til informasjon gjennom generative språkmodeller.

3. JuridiskABC (liten/privat)

- Bruk og videreutvikling av juridisk chatbot basert på KI/språkmodeller. Tjenesten er rettet mot virksomheter, særlig HR og ledere med fokus på arbeidsrettslige spørsmål.

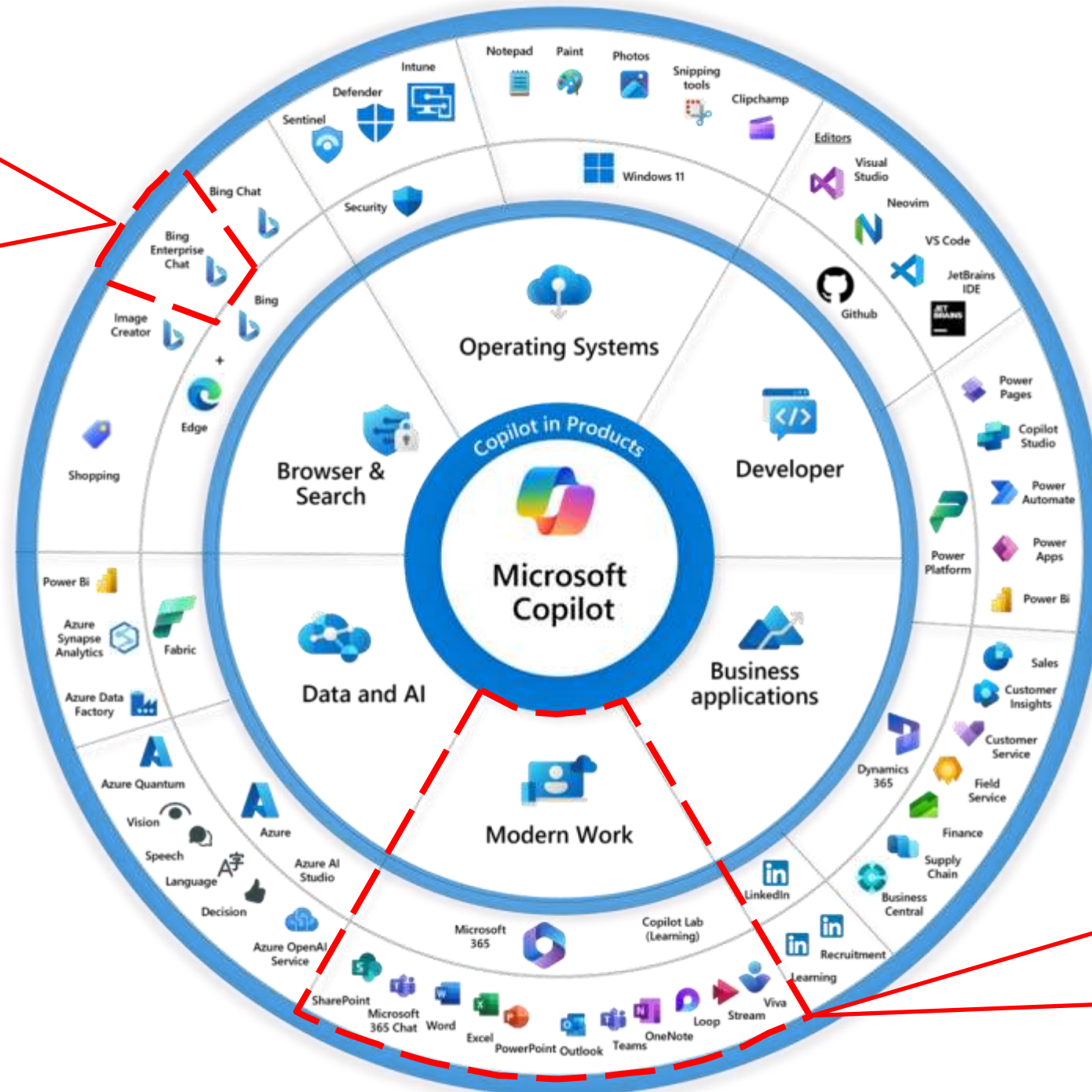
Microsoft Copilot - KI-verktøy for studenter og ansatte

Tidligere navn Bing Chat Enterprise.
Tilgjengelig for studenter og ansatte ved NTNU

(Teknisk løsning «Copilot with commercial data protection»)

Saksdokumentasjon:

<https://www.ntnu.no/web/adm-it/microsoft-copilot-ki-verktoy-for-studenter-og-ansatte>



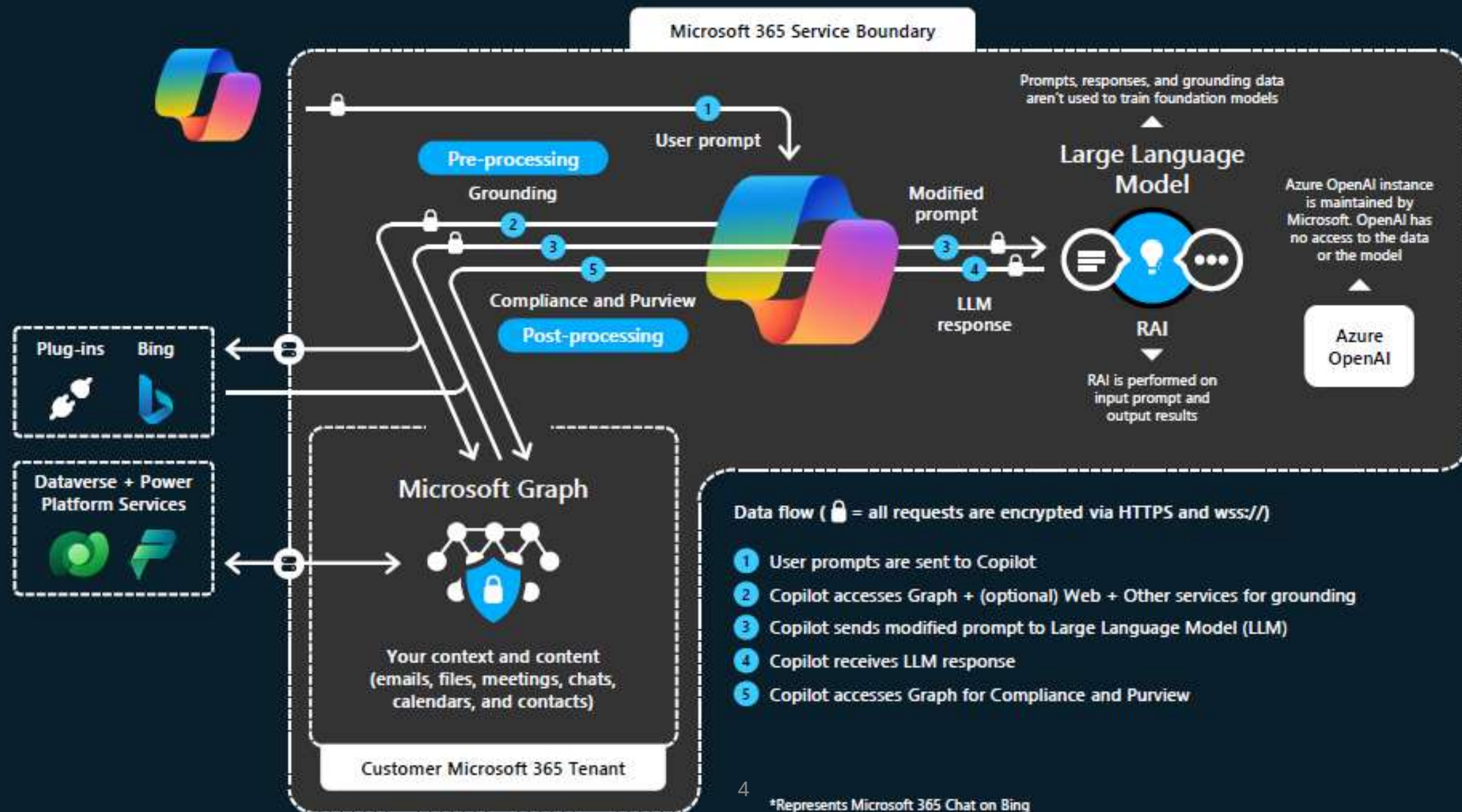
Testing av Copilot for Microsoft 365

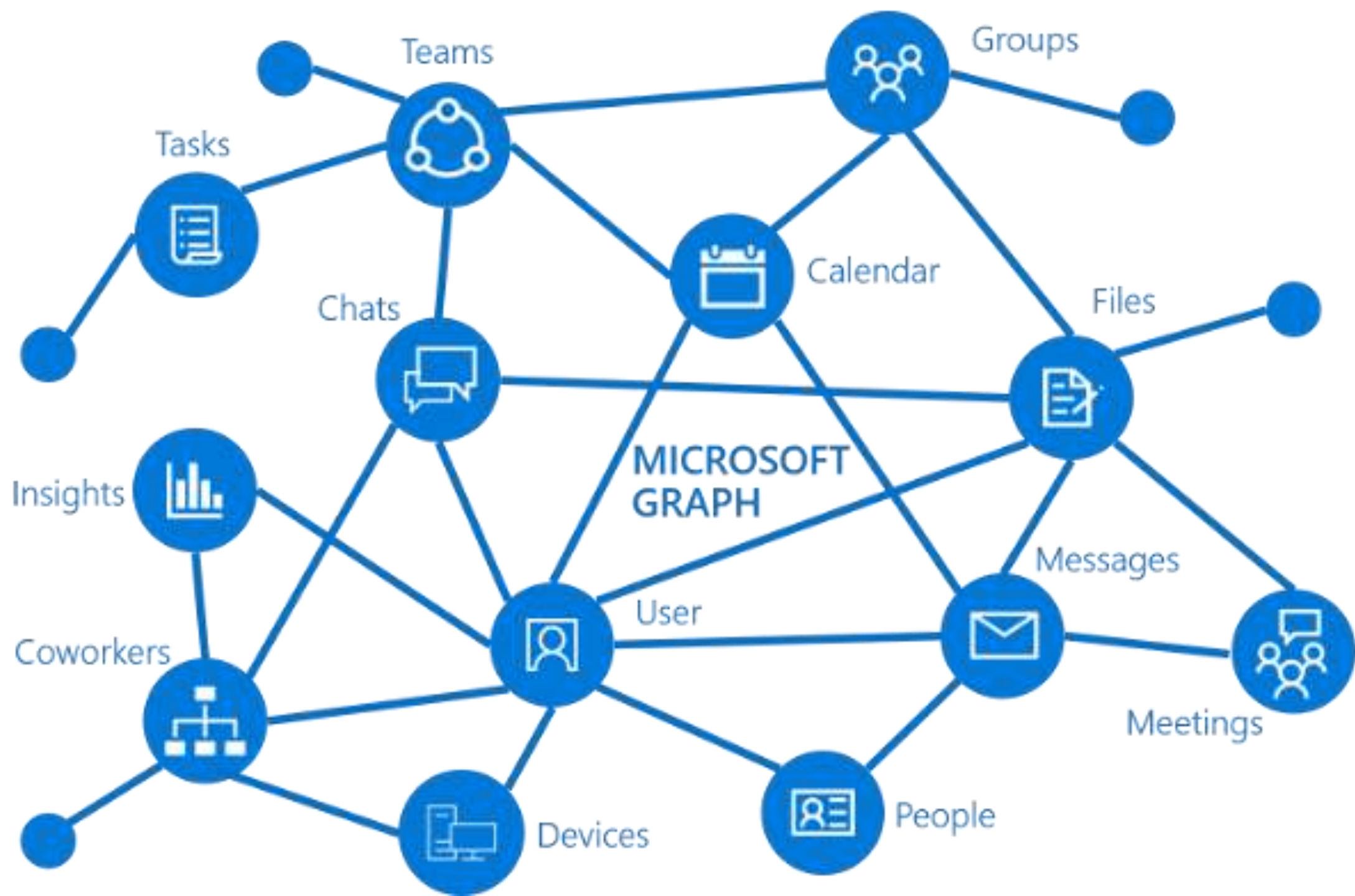
Åpnet for teknisk test i IT-avdelingen 5-10 brukere

Saksdokumentasjon:

<https://www.ntnu.no/adm/it/copilot/verktoykasse/m365-copilot-test>

Microsoft Copilot for Microsoft 365 architecture





Copilot finner alt du har tilgang til

(enten er er intensjonen eller ikke)

To sider av saken...



På den ene siden:

En fantastisk assistent som hjelper, avlaster, automatiserer, rådgir osv osv OSV...



På den andre:

«Bare» en ny tilleggsfunksjon som ikke endrer noe (vi forutsetter du har jo alt på plass for å ha full kontroll)



(Microsoft: «vi forutsetter du har jo alt på plass for å ha full kontroll»)

Hva er språkmodeller IKKE...



- **Skaper ikke original kunnskap:** De genererer språk basert på mønstre i data, men oppfinner ikke ny kunnskap eller fakta.
- **Forstår ikke betydningen av tekst:** De forutsier tekst basert på statistiske mønstre, uten å forstå dypere mening eller kontekst.
- **Bruker ikke logikk eller resonnement:** LLM-er etterligner resonnement, men driver ikke med faktisk logisk tenkning eller problemløsning med mindre det er styrt av treningsdataene deres.
- **Er ikke selvbevisste eller bevisste:** De har verken tanker, følelser eller bevissthet om sine svar eller beslutninger.
- **Er ikke beslutningstakere eller etiske agenter:** De har ikke evnen til å ta moralske vurderinger eller forstå de etiske konsekvensene av sine svar.
- **Har ingen reelle erfaringer fra den virkelige verden:** De mangler levde erfaringer og sanseoppfatninger som ligger til grunn for menneskelig forståelse.
- **Kan ikke verifisere faktakorrekthet:** De faktasjekker ikke eller har tilgang til sanntidsdata med mindre de spesifikt er programmert til å hente eksterne kilder.

~~Analysierer...~~

~~Vurderer...~~

~~Foreslår...~~

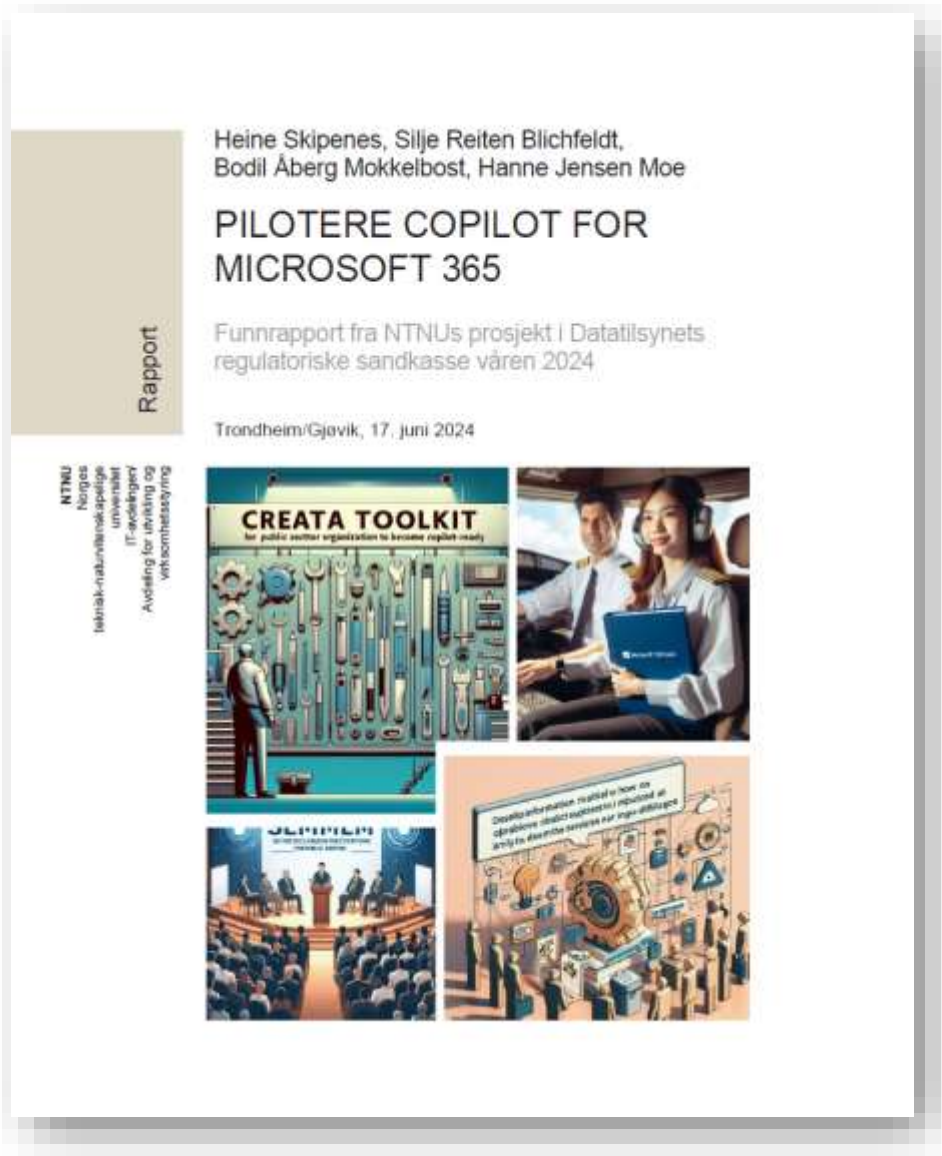
~~Finner...~~

Oppsummerer...

Gjenskaper...



- ✓ **Kunnskap om praktiske anvendelse av språkmodeller**
- ✓ **Kunnskap om store aktørers «integrert KI»-løsninger**
- ✓ **Bidra til å identifisere og strukturere personvern-problemstillinger**
- ✓ **Bidra til å finne gode regulatoriske og praktiske tilnærminger til ansvarlig bruk = tillitt**
- ✓ **Bidra til å utvikle gode råd, veiledning og verktøykasse**



Innholdsfortegnelse

Innledning	5
FUNN 1: Copilot er helt glimrende når du allerede kan det du vil at den skal hjelpe deg med.....	8
FUNN 2: Copilot kan påvirke utøvelse av offentlig myndighet	9
FUNN 3: Copilot behandler enorme mengder personopplysninger på nye og ukontrollerte måter ..	10
FUNN 4: Microsoft 365 er utfordrende å forvalte	12
FUNN 5: Copilot er tidlig i utviklingsløpet	14
FUNN 6: Copilot påvirker organisasjonen	16
FUNN 7: Copilot kan brukes til å overvåke og måle prestasjoner og adferd	18
FUNN 8: Copilot fungerer tidvis skikkelig bra.....	20
NTNUs verktøykasse.....	21
<i>NTNUs «KI-reise»</i>	<i>21</i>
<i>Gjør modenhetsvurdering av egen organisasjon</i>	<i>22</i>
<i>Sats på opplæring og kompetanseheving</i>	<i>23</i>
<i>Lag retningslinjer for bruk av kunstig intelligens</i>	<i>25</i>
<i>Test before you invest.....</i>	<i>25</i>
<i>Gjør gode nok personvernkonsekvensvurderinger.....</i>	<i>26</i>
Vedlegg	27
<i>KI-reisen.....</i>	<i>29</i>
<i>Testing av Copilot for Microsoft 365</i>	<i>37</i>
<i>Forslag til retningslinjer for generativ kunstig intelligens</i>	<i>52</i>
<i>Forslag til personvernkonsekvensvurdering «Copilot for Microsoft 365» (Driftsfase)</i>	<i>58</i>
<i>NTNUs personvernkonsekvensvurdering «Copilot with commercial Data protection»</i>	<i>132</i>
<i>Steg for steg beskrivelse: Eksempel på bruk av Copilot</i>	<i>157</i>



1

«Copilot er helt glimrende når du allerede kan det du vil at den skal hjælpe deg med»



2

*«Copilot kan påvirke utøvelse
av offentlig myndighet»*

2

«Copilot kan påvirke utøvelse av offentlig myndighet»

*Anbefaling: Vi må alle ta aktivt stilling til hvilke data
Copilot skal ha tilgang til (dette gjelder alle verktøy, også
Microsoft 365). Prioriter å ha Orden i eget hus, og sørg for
at den menneskelige kontrollen fungerer.*

3

«Copilot behandler enorme mengder personopplysninger på nye og ukontrollerte måter»



4

*«Microsoft 365 er utfordrende å
forvalte»*



5

*«Copilot er tidlig i
utviklingsløpet»*

6

«Copilot påvirker organisasjonen»

Anbefaling: Tenk Copilot først og fremst som et organisasjonsutviklingsprosjekt, sekundært som et IT-prosjekt. Involver relevante parter (for eksempel fagforeninger) tidlig i utviklingsløpet.



7

*«Copilot kan brukes til å
overvåke og måle prestasjoner
og adferd»*

NTNU vil neppe innføre Copilot – frykter overvåkning av ansatte

Det er lite sannsynlig at NTNU vil ta i bruk Copilot for Microsoft 365, forteller IT-direktøren etter fersk rapport om en pilot med løsningen.





8

*«Copilot fungerer tidvis
skikkelig bra»*

*Anbefaling: Ikke vurder tilbakemeldingene fra prosjektet
som en showstopper for egen utvikling. Bruk
prosjekresultatene for å komme raskere inn i kjernen av
utfordringene for egen virksomhet.*

Noen oppsummerende observasjoner rundt Copilot...



- Copilot har (ukritisk) tilgang til alt du har tilgang til (Graph)
 - Vanskelig å kontrollere hva man ønsker den skal bruke / slå av-på
 - Tilgang til din epost; innboks/utboks
 - Forutsetter (urealistisk) god kontroll på tilgangsstyring på virksomhetsnivå
 - Svakheter i den digitale grunnmuren forsterkes
 - Krevende å klassifisere dokumentunderlag (også for kvalitet)
- Copilot kan automatisk transkribere dialog (Teams-møter)
 - Produserer omfattende tekst/referater «uten filter» fra «ny» kilde (tale)
- Copilot prompts/ledetekster kan generere svært komplekse søk (også i dokumenter)
 - Selv tilsynelatende enkle forespørsler kan generere omfattende behandlinger
 - Vanskelig å ha kontroll på behandlingsgrunnlag og formål
 - Tilsynelatende få begrensninger for «kreative» søk om f.eks. «hvordan har Per det», «hva jobbet Anne med i går»
 - Prompts kan lede til eksterne søk som via Bing eller 3dje part plug-ins eksponerer intern informasjon eksternt
- Å utforme prompts/ledetekster er en ferdighet og krever kompetanse og bevissthet
 - Vanskelig å vurdere kvalitet på svar (ingen andre hjelpemidler enn selve teksten som er generert)
 - Kan være krevende å kontrollere kvalitet på kilder / utøve kildekritikk generelt
 - Små justeringer av ledetekster kan gi veldig forskjellige svar
 - Persondata og opphavsrett... (produseres det tekst basert på opphavsrettsbeskyttede underlagsdokumenter?)





- **Få kontroll på begrepene**
 - Hva er en direkte og indirekte personopplysning, behandling, formål, midler, behandlingsprotokoll og tilgang
- **Dataforvaltning / «orden i eget hus» / innebygget personvern**
 - Kontroll på hvilke data løsningen har tilgang til, kvalitet på data, klassifisering av data, tilgangsstyring, brukerkontroll, åpenhet
- **Ha oversikt over behandlinger (behandlingsprotokoll)**
- **DPIA skal gjøres i kontekst av de enkelte behandlinger (NTNU...)**
- **Vurdering av hvilke arbeidsroller som gir muligheter**
 - Eks. kommunikasjon, veiledning
- **Vurdering av hvilke arbeidsroller som gir utfordringer**
 - Eks. ledelse, personalansvar, HR
- **Sterkt fokus på enkeltbrukeres verktøyforståelse- og kompetanse**
 - Bevisstgjøring, opplæring, kunnskapsutveksling
- **Løpende etterkontroll på alle nivåer**



1. NTNU (stor/offentlig)

- Teste Microsoft KI-assistent «Microsoft 365 Copilot», med fokus på å vurdere verktøyets muligheter og utfordringer, samt etablering av et robust rammeverk for forvaltning, drift, vedlikehold og utvikling.

2. Helsedirektoratet (stor/offentlig)

- Forenklet tilgang til informasjon gjennom generative språkmodeller.

3. JuridiskABC (liten/privat)

- Bruk og videreutvikling av juridisk chatbot basert på KI/språkmodeller. Tjenesten er rettet mot virksomheter, særlig HR og ledere med fokus på arbeidsrettslige spørsmål.



EG

Du

hvor mange nasjonalparker er det i norge



LawAi

Beklager, men jeg kan kun svare på spørsmål relatert til norsk arbeidsrett. Hvis du har spørsmål om arbeidsmiljøloven eller andre juridiske spørsmål knyttet til arbeidslivet i Norge, er jeg her for å hjelpe deg.

Kopier svar 

Lag utskriftsvennlig versjon 

Hva synes du om svaret du fikk?



Enklere tilgang til informasjon (ETI)



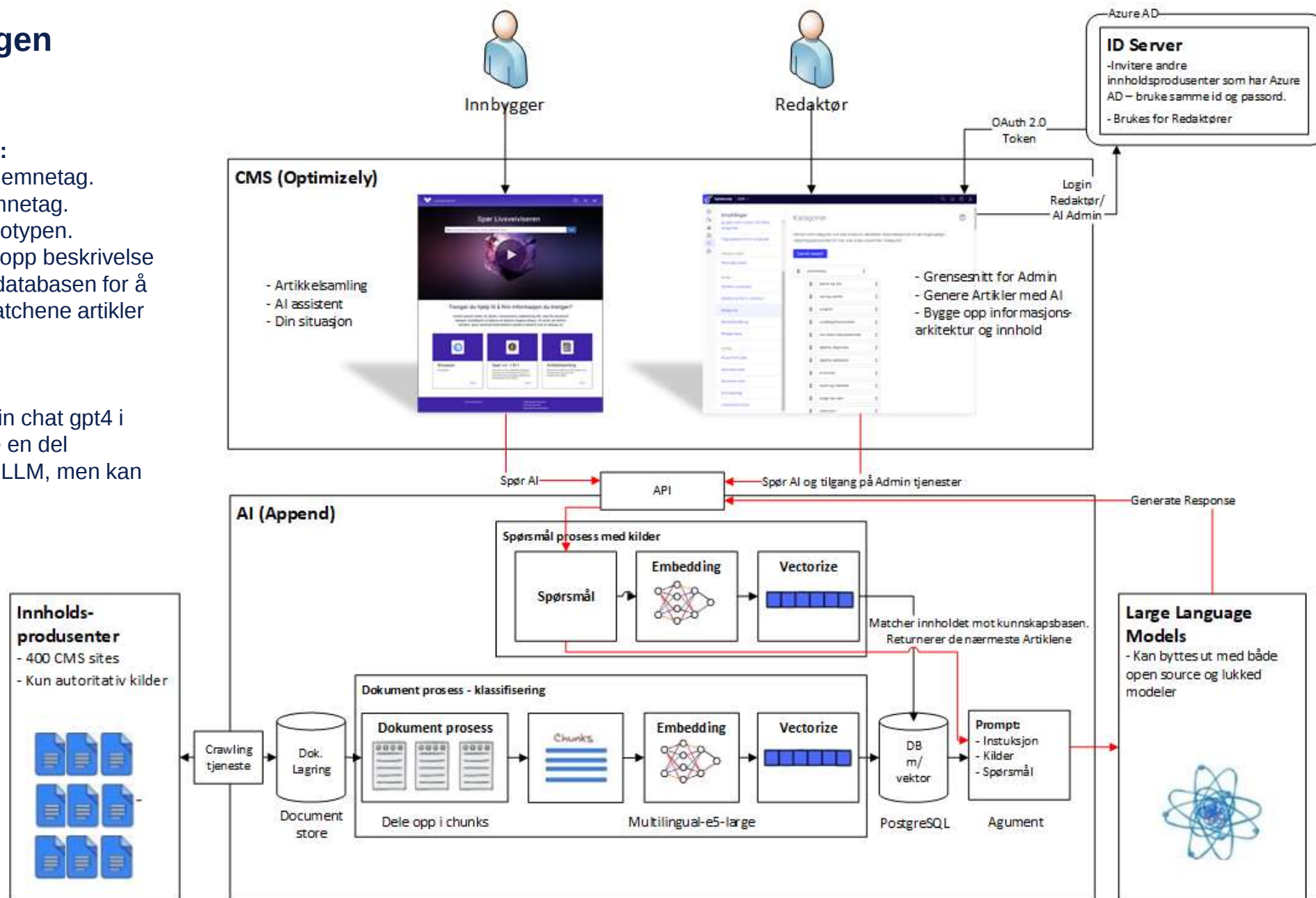
Prototype av løsningen

Uavklart ting som jobbes med:

- Autotagging av artikler med emnetag.
- Bruk av LOS termer som emnetag.
- Behov for Snomed CT i prototypen.
- Ser på om vi kan indeksere opp beskrivelse av LOS termer i kunnskapsdatabasen for å kunne koble det opp mot matchene artikler

Nye valg:

- Har valgt å bruke Open AI sin chat gpt4 i demonstratoren, for å slippe en del utfordringer med hosting av LLM, men kan lett byttes til en annen LLM



Kan kommunen ta i bruk Copilot?



- Hvis man har kontroll på plattform (forvaltning → sky → M365)
- Hvis du har kontroll på datakvalitet, klassifisering og tilgangsstyring
- Hvis du har kontroll på behandlinger, behandlingsansvar og roller



Ta små steg:

- Identifiser roller med egnet risiko (2, 5, 15..)
- Identifiser behandlinger med egnet risiko (2-3)
- Fokuser på brukerkompetanse og opplæring (ledetekster er en ferdighet)
- Prosesser for etterkontroll og evaluering
- Gevinstrealisering
- Vurder også andre GKI-tilnærminger (spesifikke løsninger for spesifikke formål)

Eirik Gulbrandsen

Datatilsynets sandkasse

Datatilsynets seksjon for Teknologi, Sikkerhet og Tilsyn

eirik.gulbrandsen@datatilsynet.no



Datatilsynet

postkasse@datatilsynet.no

Telefon: +47 22 39 69 00

datatilsynet.no

personvernbloggen.no



Norwegian Large Language Models

Community

<http://norlm.nlpl.eu> [lrgoslo/norallm](https://github.com/lrgoslo/norallm)

AI & ML interests

Large Language Models

Team members 7



Organization Card

Community

About org cards

Norwegian Large Language Models

Welcome to the emerging collection of large-scale generative language models for the Norwegian language. [NorLM](#) (or, more recently, NORA.LLM) originated as a joint initiative of the projects [EOSC-Nordic](#) (European Open Science Cloud), [SANT](#) (Sentiment Analysis for Norwegian), and [HPLT](#) (High-Performance Language Technologies), in collaboration with the [AI Laboratory of the National Library of Norway](#) and the [National e-Infrastructure Services](#), coordinated by the [Language Technology Group](#) (LTG) at the University of Oslo.

We are working to provide these models and supporting tools for researchers and developers in Natural Language Processing (NLP) for the Norwegian language. We do so in the hope of facilitating scientific experimentation with and practical applications of state-of-the-art NLP architectures, as well as to enable others to develop their own large-scale models, for example for domain- or application-specific tasks, language variants, or even other languages than Norwegian.

Models 4

Sort: Recently updated

 **norallm/normistral-7b-warm**
Text Generation • Updated Jun 21 • 497 • 28

 **norallm/normistral-7b-warm-instruct**
Text Generation • Updated Jun 17 • 1.13k • 24

 **norallm/normistral-7b-scratch**
Text Generation • Updated Apr 17 • 78 • 8

 **norallm/norbloom-7b-scratch**
Text Generation • Updated Apr 17 • 91 • 2

CHAT GP-TOTEN: KAN VI DRIFTE EN NORSK SPRÅKMODELL?



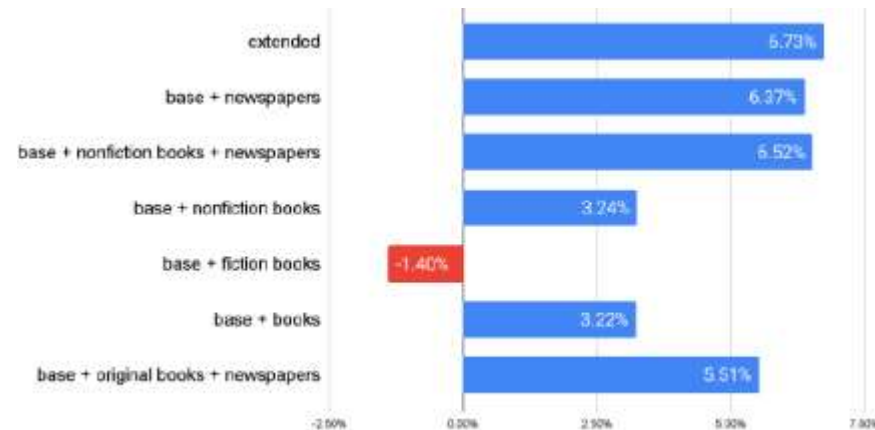
Nasjonalbiblioteket deler kunstig
intelligens som skjøner norske dialekter og
gjør tale om til tekst



Mímir-prosjektet



*Evaluering av virkningen av opphavsrettsbeskyttet materiale på generative
store språkmodeller for norske språk*



```
def parse_args():  
    parser = argparse.ArgumentParser(description="Makes the corpus more GDPR compliant by removing all email addresses and Norwegian personal identification numbers.")  
    parser.add_argument('--input_file', required=True, help='Path to input file.')  
    parser.add_argument('--output_folder', required=True, help='Path to output folder.')  
    args = parser.parse_args()  
    return args
```