Vurdering av personvernkonsekvenser (DPIA)

Navn på system/prosjekt:	Tilgjengelig språkmodell for NTNU / implementere Microsoft Copilot som verktøy ved NTNU
DPIA-en utføres av:	Strategisk rådgivningsgruppe, IT-strategi og -styring (Ansvarlig Heine Skipenes)
Dato:	27.02.2024

Innholdsfortegnelse

Merknader til den gjennomførte personvernkonsekvensvurderingen:

- Microsoft Copilot har byttet navn fra Bing Chat Enterprise. Det er den samme tjenesten i bunn, og denne DPIAen erstatter DPIAen på Bing Chat Enterprise datert 21. september 2023
- Vi har hentet sitat og utklipp fra Microsoft sine nettsider som beskriver verktøyet. Disse vurderingene finnes ikke på norsk og vi har ikke prioritert å oversette innholdet, men heller å fokusere tilgjengelige ressurser på selve personvernkonsekvensvurderingen.
- Tidsspennet verktøyet har vært tilgjengelig for NTNUs ansatte siden september 2023. Det er ikke mulig å hente ut bruksstatistikk, men IT-avdelingen har fått veldig få feilmeldinger på verktøyet og ingen kjente avvik. Verktøyet antas å fungere som tiltenkt.
- Bruk av språkmodeller og kunstig intelligens er utfordrende, og det er viktig med bevissthet rundt temaene som er belyst i denne vurderingen. For å gjøre lesinga lettere har vi markert særlig utfordrende områder med gult

1. Systematisk beskrivelse av behandlingen

I denne fasen er målet at den behandlingsansvarlige skal ha en fullstendig oversikt over behandlingen, og sørge for at beskrivelsene som er gjort er komplette og tydelige.

1. Overordnet oversikt

***Presenter systemet/prosjektet**, og på et overordnet nivå forklar hvilken behandling av personopplysninger den involverer. Her kan man gjerne referere/linke til andre dokumenter, som f.eks. en prosjektskisse. Forklar hvorfor du har identifisert et behov for en DPIA, jf. art. 35 nr. 1.*

IT-avdelingen skrudde i september 2023 på Microsoft sitt verktøy «Bing Chat Enterprise» (https://www.bing.com/chat) for alle ansatte på NTNU. Bing Chat Enterprise er en samtalerobot og en språkmodell som ligner på andre kjente verktøy som for eksempel ChatGPT. I motsetning til mange andre verktøy var sikkerhetsnivået høyere og løsningen var lett tilgjengelig for NTNU. Verktøyet er integrert i nettleseren og innlogging skjer automatisk for alle som er pålogget (Microsoftkonto). Informasjon om verktøyet finnes på innsida: https://i.ntnu.no/wiki/-/wiki/Norsk/Bing+Chat+Enterprise

Tjenesten har etter lansering for ansatte høsten 2023 blitt oppgradert flere ganger. Det er nå mulig å generere tekst, generere bilder via Dall-E, laste opp filer (enkelte typer filer) og bilder, samt ta bilde med kamera på enheten og laste dette direkte opp i tjenesten.

I september 2023 var Bing Chat Enterprise ikke gjort tilgjengelig for studentlisensene, og IT-avdelingen har siden dette jobbet med å tilby et KI-verktøy for studentene. IT-avdelingen har vurdert både Sikt sin Sikker KI-Chat, GPT.UIO og utvikling av en egen NTNU-løsning. IT-avdelingens ledergruppe falt til slutt ned på å jobbe videre med UiO sin løsning. For å kunne tilby UiO sin løsning på NTNU, var det nødvendig med noe utvikling som tidligst kunne være ferdig i februar 2024. Like før jul meldte Microsoft at de kommer til å tilgjengeliggjøre verktøyet Bing Chat Enterprise også for studentlisensene under et nytt navn: «Microsoft Copilot». Verktøyet tilbys som en såkalt «opt out»-løsning, det vil si at Microsoft skrur det på og NTNU må i så fall aktivt skru det av for at det ikke skal bli gjort tilgjengelig for brukerne. Det medfører ingen kostnad for NTNU å ta løsningen i bruk, men institusjonen må sørge for at alle vurderinger av informasjonssikkerhet og personvern er ivaretatt. Når et samtalerobotverktøy med generativ kunstig intelligens skal tilbys alle brukere anbefales det å gjennomføre en personvernkonsekvensvurdering (DPIA) jf Personvernforordningens artikkel 35 1: *«Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.»)*

Hovedformålet med å tilgjengeliggjøre Bing Chat Enterprise var å kunne tilby et språkmodellverktøy for behandling av informasjon med litt høyere informasjonssikkerhetsklassifiseringsnivå (intern) enn det som anbefales for åpne verktøy på nett (åpen). Ved å tilby verktøy hvor ansatte kan legge inn interne data så reduserer vi risiko for at åpne plattformer som ChatGPT brukes til å behandle informasjon som NTNU ønsker å holde internt i virksomheten. IT-avdelingen ønsket også å tilby en lett tilgjengelig og trygg

språkmodell der ansatte kan gjøre seg kjent med fordeler og ulemper med denne typen verktøy og teknologi. Språkmodeller er ny teknologi for mange, og mange har aldri turt å prøve. Ved å tilby en trygg «sandkasse» for testing ønsket IT-avdelingen å bidra til at alle ansatte skal få større kjennskap om hva denne typen verktøy kan bidra med av positive og negative effekter på måten ansatte kan jobbe på. I tillegg har IT-avdelingen ønsket å tilby et verktøy hvor vi er åpne om hvordan vi har tenkt risikovurdering, informasjonssikkerhet og personvern. IT-avdelingen håper at dette skal kunne bidra til økt forståelse for hvorfor og hvordan vi alle bør tenke på informasjonssikkerhet i hverdagen.

IT-avdelingen har tatt utgangspunkt i følgende behandlingsformål i vurderingen av om det skal tilbys et felles KI-verktøy for studenter og ansatte (samtalerobot / språkmodell):

1. Tilby en språkmodell for behandling av gule/interne data (ikke personopplysninger).
    a. Å tilby og anbefale et sikrere alternativ til studentene enn åpne tjenester på nett (for eksempel ChatGPT)
2. Tilby en lett tilgjengelig og trygg språkmodell der våre ansatte og studenter kan gjøre seg kjent med fordeler og ulemper med ny teknologi.
    a. Å tilby det samme verktøyet til både studenter og ansatte slik at fagspesifikk opplæring kan gis i ordinær undervisning
    b. Å tilby et verktøy raskt nok til at det kan inngå i undervisningsplanleggingen for våren 2024
3. Tilby en teknisk løsning hvor vi samtidig tilgjengeliggjør informasjon om hvordan vi har tenkt risikovurdering og personvern

IT-avdelingen ønsker ikke at betegnelsen «sikker» skal knyttes til dette verktøyet. Dette kan gi et feilaktig inntrykk av at løsningen kan brukes til å behandle data med et høyere informasjonssikkerhetsnivå enn åpen og intern og til å behandle personopplysninger.

Hvilke personopplysninger skal behandles?

- Brukernavn
- Personopplysninger som finnes åpent på nett
- Personopplysninger som brukeren selv legger inn (prompts/kommandoer/input)

Antallet brukere (51 000), klassifiseringsnivå (intern/gul) på behandlingen av informasjonsverdier og at dette er ny teknologi for NTNU tilsier at personvernkonsekvensvurdering bør gjøres jf. art. 35 nr. 1.

Behandlingsansvarlig

- NTNU er behandlingsansvarlig som organisasjon, og IT-direktør ved IT-avdelingen har den operative rollen som behandlingsansvarlig.

Databehandler

- Microsoft

Referanser:

- All dokumentasjon og informasjon om tjenesten er hentet fra denne siden (med undersider) https://learn.microsoft.com/en-us/bing-chat-enterprise/overview

2. **Behandlingens art**

Behandlingens iboende karakteristikk og hvordan behandlingsaktivitetene skal foregå. Beskrivelser av hva dere planlegger å gjøre med personopplysningene.

Hvordan skal personopplysningene samles inn?	Hentet fra leverandørens nettsider: "Copilot is a generative AI service grounded in data from the public web in the Bing search index only. It doesn't have access to organizational resources or content within Microsoft 365, such as documents in OneDrive, emails, or other data in the Microsoft 365 Graph. Copilot for Microsoft 365 is required if your organization wants a chat experience grounded in work data inside your tenant boundary. Copilot can access organizational content in the chat only when it's provided by users. This can be done in one of two ways: 1. Users explicitly type or paste this information directly into the chat. 2. Users type a prompt into Copilot in Edge after enabling the 'Allow access to any webpage or PDF' setting, and an intranet page is open in the browser. In this scenario, Copilot may use this content to help answer questions. In both cases, when commercial data is enabled, Copilot doesn't retain any of this data after the chat session is over".
Hvordan skal personopplysningene lagres?	Hentet fra leverandørens nettsider: "When organizations and employees use generative AI services, it's important to understand how these services handle user and chat data. Because employee chats may contain sensitive data, Copilot is designed to protect this information. • Copilot uses Microsoft Entra ID (formerly known as Azure Active Directory) for authentication and only allows users to access Copilot with commercial data protection using their work account.

	• An Entra ID user's tenant and user information is removed from chat data at the start of a chat session. This information is only used to determine if the user is eligible for commercial data protection. Search queries triggered by prompts from an Entra ID user aren't linked to users or organizations by Bing. • Microsoft doesn't retain prompts or responses from Entra ID users when using Copilot. Prompts and responses are maintained for a short caching period for runtime purposes. After the browser is closed, the chat topic is reset, or the session times out, Microsoft discards prompts and responses. • Chat data sent to and from Copilot with commercial data protection is encrypted in transit (TLS 1.2+) and at rest (AES-128) during the chat session. Microsoft has no 'eyes-on' access to it. • Because Microsoft doesn't retain prompts and responses, they can't be used as part of a training set for the underlying large language model. "Commercial data protection means user and organizational data are protected, prompts and responses are not saved, Microsoft has no eyes-on access, and chat data isn't used to train the underlying large language models. Unlike Copilot for Microsoft 365, Copilot has no access to organizational data in the Microsoft 365 Graph".
Hvordan skal personopplysningene brukes?	Den registrertes brukernavn brukes kun til pålogging og bekreftelse på autentisering. Personopplysninger som en bruker selv legger inn, blir kun brukt i den chatsesjonen som gjennomføres. Personopplysningene lagres ikke.
Hvem skal ha tilgang til personopplysningene?	Microsoft
Hvem skal det samles inn personopplysninger om?	Ansatte og studenter som tar i bruk løsningen. De må logge seg på med brukernavn (ikke aktiv pålogging, det går av seg selv når du er logget på andre Microsoft-tjenester).
Hvordan kan den registrerte utøve sine rettigheter?	Den registrerte har rett til å se/få innsyn i alle personopplysninger som er registrert om seg ved NTNU. Den registrerte har rett til å få utlevert en kopi av personopplysninger om seg selv. Utfyllende informasjon på https://innsida.ntnu.no/wiki/-

	/wiki/Norsk/Personvernerklæring+NTNU Det blir i tillegg utviklet en egen modul for innsyn etter GDPR gjennom prosjektet NTNU Sak, og tilgangen til Copilot inngår i datagrunnlaget med personopplysninger som Microsoft vet om NTNUs brukere.
Vil det være systematisk behandling av personopplysninger?	Nei
Brukes det ny teknologi eller ny bruk av eksisterende teknologi hvor personvernkonsekvenser ikke har blitt vurdert?	For sektoren er dette ny teknologi. Verktøyene som er valgt er ikke nye «for verden», men ganske tidlig i utviklingsløpet og teknologien utvikler seg fortløpende.

3. **Behandlingens omfang**

Kategorier av personopplysninger som behandles	Tjenesten skal behandle data av typen åpen og intern informasjon. Løsningen blir ikke godkjent til fortrolig og strengt fortrolig. Om brukere selv legger inn vanlige og/eller særlige kategorier personopplysninger blir dette behandlet i chatsesjonen.
Antall registrerte involvert i behandlingen	Maks antall brukere er 51 000 (forutsatt at alle ansatte og studenter tar løsningen i bruk).
Datavolum	Det kan legges inn mye data, men det slettes fortløpende når sesjonene avsluttes.
Behandlingsfrekvens	Kontinuerlig.
Lagringstid for personopplysningene	Midlertidig. Hentet fra leverandørens nettsider: «Copilot doesn't support the chat history feature. It doesn't retain chat prompts or responses". "It also offers no usage reporting or auditing capabilities to organizations".
Geografisk omfang	NTNUs ansatte og studenter er hovedsakelig lokalisert i Trondheim, Gjøvik og Ålesund, men løsningen blir tilgjengelig uavhengig av lokasjon, så fremt brukeren er logget på Microsoft-kontoen de har hos NTNU.

4. **Behandlingens formål**

Behandlingens formål	Formålet med løsningen er: 1. Tilby en språkmodell for behandling av gule/interne data (ikke personopplysninger). a. Å tilby og anbefale et sikrere alternativ til studentene enn åpne tjenester på nett (for eksempel ChatGPT)

	2. Tilby en lett tilgjengelig og trygg språkmodell der våre ansatte og studenter kan gjøre seg kjent med fordeler og ulemper med ny teknologi. a. Å tilby det samme verktøyet til både studenter og ansatte slik at fagspesifikk opplæring kan gis i ordinær undervisning b. Å tilby et verktøy raskt nok til at det kan inngå i undervisningsplanleggingen for våren 2024 3. Tilby en teknisk løsning hvor vi samtidig tilgjengeliggjør informasjon om hvordan vi har tenkt risikovurdering og personvern Formålet med behandlingen av personopplysningene er å identifisere brukere av løsningen, slik at brukeren kan få tilgang. Ytterligere behandling av personopplysninger gjøres ikke systembasert. Den enkelte bruker kan legge inn, bearbeide og laste ned personopplysninger den selv har lagt inn i løsningen.
Vil det være kontrollformål?	Nei
Er formålet å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personlige aspekter?	Nei
Har behandlingen av personopplysninger som mål å ta beslutninger som får betydning for den registrerte?	Nei.
Skal opplysningene brukes til å profilere den registrerte?	Nei
Brukes personopplysninger for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte?	Nei
Vil personopplysningene viderebehandles til nye eller andre formål?	Nei

5. Sammenhengen behandlingen utføres i (kontekst)

Her er målet å se behandlingen i et større bilde og vurdere alle interne og eksterne faktorer som kan påvirke forventninger eller konsekvenser.

Hvilke kilder brukes for innhenting av personopplysninger?	Brukernavn hentes fra brukerdatabase «Active directory» (AD)/Entra ID.

	Andre personopplysninger er det enten bruker selv som har lagt inn i chatsesjonen, eller de finnes tilgjengelig på internett.
Relasjon mellom behandlingsansvarlig og den registrerte	De registrerte er ansatte og studenter hos behandlingsansvarlig.
I hvilken grad har den registrerte kontroll over sine opplysninger?	Den registrerte må selv legge inn egne personopplysninger i løsningen om disse skal bli behandlet, og den registrerte har da full kontroll på egen behandling. Den registrerte har rett til å se/få innsyn i alle personopplysninger som er registrert om seg ved NTNU. Den registrerte har rett til å få utlevert en kopi av personopplysninger om seg selv. Utfyllende informasjon på https://innsida.ntnu.no/wiki/-/wiki/Norsk/Personvernerklæring+NTNU. Personopplysningene til Copilot (Bing chat enterprise) inngår i datagrunnlaget med personopplysninger som Microsoft vet om våre brukere og vil bli synlig ved innsyn i Microsoft sin verktøyportefølje.
Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel	Bruk av brukernavn for tilgang til tjenesten vil oppleves som positivt fordi det er det som gir deg tilgang til tjenesten. Det ligger i en språkmodells natur å fremstille informasjon som sann selv om den både er usann og feilaktig. Språkmodellen kan også finne informasjon om personer fra åpent nett som du som bruker ikke visste at fantes «der ute». Det kan oppleves som både negativt og skremmende dersom en bruker selv legger inn personopplysninger som blir feilaktig sammensatt med informasjon fra internett.
Vil den registrerte ha en særskilt forventning om konfidensialitet?	Nei
Vil den registrerte ha en særskilt forventning om at personopplysningene er nødvendige og korrekte?	Nei
Vil den registrerte ha en særskilt forventning om privatliv?	Nei
Vil det behandles personopplysninger om barn, pasienter eller andre kategorier av personer som defineres som sårbare?	Nei
Finnes det tidligere erfaring med tilsvarende type behandling?	Ja og nei. Forskningsmiljø ved NTNU er ledende kompetansemiljø nasjonalt og har jobbet med problemstillinger knyttet til bruk av språkmodeller og kunstig intelligens i en

	årrekke allerede. Tilgjengelige tjenester som ChatGPT og Grammarly har vært kjent og flittig i bruk samfunnet en stund, og NTNU har tidligere laget retningslinjer for spesielle områder allerede (eksamen og undervisning) https://i.ntnu.no/wiki/-/wiki/Norsk/Kunstig+intelligens+i+undervisning+og+vurdering
Beskriv eventuelle relevante fremskritt innen teknologi eller sikkerhet	Utdrag fra https://snl.no/språkmodell: **«Nyere språkmodeller** *Med fremveksten av dyplæring og store mengder tilgjengelige data, som oftest fra internett, har moderne språkmodeller basert på maskinlæring blitt den vanligste måten å modellere språk på. I stedet for å bare telle ordforekomster, bruker man i dag nevrale nettverk.* *Oppgaven nettverket får, er typisk å gjette neste ord gitt en foregående sekvens. Til å begynne med vil modellen gjette helt tilfeldig, men etter hvert som den har gjettet nok ganger, og har sett enormt store tekstmengder, vil den begynne å danne seg et godt bilde av hva som typisk følger en gitt kontekst. Denne typen modellering er kjent som autoregressiv språkmodellering, og det er vanligvis dette som ligger til grunn for de mest allment kjente språkmodellene, som for eksempel de vi finner i chatbots.* *Moderne språkmodeller basert på maskinlæring har mange fordeler. De har evnen til å fange opp komplekse språklige nyanser fra store mengder data, og de kan generere tekst som er sammenhengende og virker naturlig. De kan også tilpasses til ulike språk og domener. Imidlertid krever de også store mengder data, og de er ofte komplekse å implementere og forstå.»*
Finnes det noen nåværende tilfeller av allmenn bekymring for den beskrevne måten å behandle personopplysninger på?	Ja, i aller høyeste grad. Dette gjelder særlig i forbindelse med utøvelse av offentlig myndighet: • Dutch scandal (diskriminerende algoritmer) • Eksamensjuks • Forvaltningsrevisjon fra Riksrevisjonen: Bruk av kunstig intelligens i staten • Diskriminering, manglende likebehandling osv osv. For eksempel https://www.bufdir.no/aktuelt/ny-rapport-lite-kunnskap-og-kompetanse-om-kunstig-intelligens-og-diskriminering/ Den beskrevne måten å behandle personopplysninger på i denne tjenesten tilsier ikke at dette skal være en direkte bekymring, men problemstillingene fra eksemplene over gjelder bruk av kunstig intelligens og utøvelse av offentlig

	myndighet generelt som det er viktig at er godt kjent i organisasjonen. Dette er et verktøy som kan **gjøre det lettere for studentene å jukse**. Det kan brukes til å «koke oppgaver», henvise til feil referanser og tolke innhold helt feil. «Gode formuleringer» fra verktøyet kan være direkte sitat fra kjente og ukjente kilder, og studenter kan bli tatt for plagiat/tekstlikhet selv om de aldri en gang har lest den faktiske teksten.
Vil dere behandle personopplysninger fra ulike datasett, som er innsamlet for ulike formål og fra ulike behandlingsansvarlige?	Nei
Kobles ulike registre for å gi ny type informasjon om den registrerte?	Nei. Men sammenstilling av informasjon fra ulike kilder tilgjengelig på åpent nett vil kunne gi en ny fremstilling av en person.

6. Identifisering og oversikt

Behandlingsansvarlig:	IT-avdelingen ved NTNU (IT-direktør)
Felles behandlingsansvarlig:	Nei
Databehandler(e):	Microsoft

7. Mottakere av personopplysninger

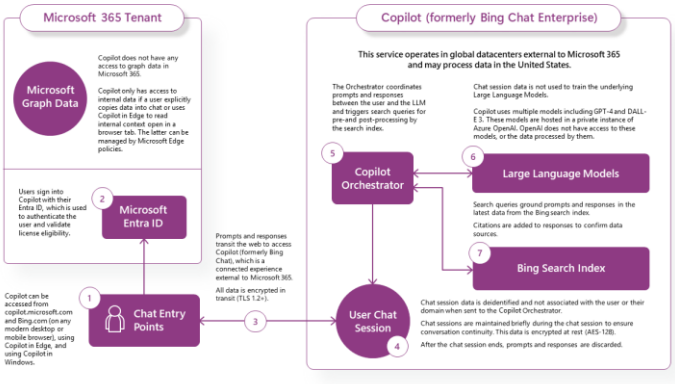
Beskriv alle mottakere/kategorier av mottakere av personopplysninger	Det er kun den registrerte selv som ser personopplysningene sine. Ansatte og studenter som tar i bruk verktøyet, ser kun resultater som er skapt på bakgrunn av informasjon som de selv har lagt inn satt sammen med informasjon som finnes på internett.
Hvordan deles personopplysningene mellom avdelinger **internt** i virksomheten?	Informasjon blir ikke delt internt i virksomheten.
Hvilke **eksterne** virksomheter deles personopplysningene med? Hvis ja, for hvilke formål og med hvilke rettslige grunnlag?	Personopplysningene deles med databehandler når løsningen brukes. Databehandler beskriver at dataene slettes hos dem når bruk opphører (når chatsesjon avsluttes, du klikker på x på nettleservinduet).
Overføres personopplysningene til land utenfor EU/EØS-området (tredjestater), jf. art. 44-49? Hvis ja, hva er det rettslige grunnlaget for det?	Ja. Databehandler garanterer ikke at dataene utelukkende skal behandles i EU/EØS-området. Hentet fra leverandørens nettsider: «Copilot is a connected service where Microsoft is the data controller. Users' prompts leave your organization's

	Microsoft 365 tenant boundary to reach the Copilot service. When commercial data protection is enabled, Microsoft doesn't retain this data beyond a short caching period for runtime purposes. After the browser is closed, the chat topic is reset, or the session times out, Microsoft discards all prompts and responses". "To provide chat responses, Copilot uses global data centers for processing and may process data in the United States. Optional, Bing-backed connected experiences don't fall under Microsoft's EU Data Boundary (EUDB) commitment. Learn more: Continuing Data Transfers that apply to all EU Data Boundary services. They also don't fall under the terms of Enterprise Subscription Agreements (EAS) or Campus and School Agreements (CASA) which may require company data to remain inside geographic or tenant boundaries. As a reminder, Copilot has no access to organizational data inside your tenant boundary, and chat conversations aren't saved or used to train the underlying models. Organizations with strict requirements that data must remain inside tenant or geographic boundaries should instead consider Copilot for Microsoft 365 or Azure Open AI to provide generative AI services. Copilot with commercial data protection is intended as a more secure alternative for organizations than using consumer-oriented generative AI services. For more information, see Microsoft 365 Data Residency and the Microsoft Privacy Statement».
Beskriv hvilke forholdsregler som tas for å beskytte personopplysninger	Forholdsregler for ansatte med tilgang til NTNUs systemer: Alle ansatte med tilgang til systemet skal være ansatt ved NTNU og er dermed underlagt gjeldende regelverk som til enhver tid gjelder for statens ansatte (Forvaltningslovens regler for inhabilitet, taushetsplikt osv). Alle skal gjennomføre nødvendig opplæring, signere IKT-reglement og følge styringssystem for informasjonssikkerhet. IT-avdelingens ansatte med administratortilganger er underlagt egne retningslinjer og rammeverk for sikker drift, tilgang osv. Alle studenter med tilgang til systemet skal være tatt opp som studenter ved NTNU og er dermed underlagt gjeldende regelverk https://i.ntnu.no/wiki/-

	/wiki/Norsk/Generelle+lover+og+regler+-+studier. Alle skal gjennomføre nødvendig opplæring, signere IKT-reglement og følge styringssystem for informasjonssikkerhet.
Er alle databehandlere identifisert, og er forholdet til dem avklart gjennom avtaler, jf. art. 28 nr. 3?	Ja. NTNU har ved å innføre sektoravtalen med Microsoft, godkjent Microsofts sine «Terms and conditions». Microsoft som leverandør opplyser her om hvordan data behandles, oppbevares og slettes. NTNU har ikke inngått en egen databehandleravtale med Microsoft.
Gir databehandleren tilstrekkelige garantier for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen, vil gjennomføres?	Hentet fra leverandørens nettsider: "Microsoft as the data controller Copilot is a connected service where Microsoft is the data controller. Users' prompts leave your organization's Microsoft 365 tenant boundary to reach the Copilot service. When commercial data protection is enabled, Microsoft doesn't retain this data beyond a short caching period for runtime purposes. After the browser is closed, the chat topic is reset, or the session times out, Microsoft discards all prompts and responses. To provide chat responses, Copilot uses global data centers for processing and may process data in the United States. Optional, Bing-backed connected experiences don't fall under Microsoft's EU Data Boundary (EUDB) commitment. Learn more: Continuing Data Transfers that apply to all EU Data Boundary services. They also don't fall under the terms of the Data Protection Addendum (DPA) which requires company data to remain inside geographic or tenant boundaries. As a reminder, Copilot has no access to organizational data inside your tenant boundary, and chat conversations aren't saved or used to train the underlying models. Organizations with strict requirements that data must remain inside tenant or geographic boundaries should instead consider Copilot for Microsoft 365 or Azure Open AI to provide generative AI services. Copilot with commercial data protection is intended as a more secure alternative for organizations than using consumer-oriented generative AI services. For more information, see Microsoft 365 Data Residency and the Microsoft Privacy Statement."

	"Chat data sent to and from Copilot with commercial data protection is encrypted in transit (TLS 1.2+) and at rest (AES-128) during the chat session. Microsoft has no 'eyes-on' access to it. » **"GDPR** The May 21, 2018, blog post from Microsoft outlines our commitment to GDPR compliance and how Microsoft helps businesses and other organizations meet their own GDPR obligations. You can find more details in the Microsoft Trust Center FAQ. Copilot aligns with GDPR principles. Customers who wish to submit a right to be forgotten request to remove information from the Bing search index can do so here: Bing - Request Form to Block Search Results in Europe"

8. Dataflyt, lagring og mellomlagring

Hvordan overføres og tilgjengeliggjøres personopplysningene?	Når den registrerte ønsker å bruke verktøyet går hen til et nettsted som kjører en spørring mot NTNUs brukerdatabase (Active directory) for å bekrefte at bruker er ansatt eller student ved NTNU. Da skjer dette: 1. Hvis bruker ikke finnes avvises forespørselen og løsningen starter ikke 2. Hvis bruker finnes gis det tilgang til tjenesten og brukernavnet slettes. 
Hvor og hvor lenge lagres personopplysningene ulike steder?	Microsoft beskriver at de kun tar vare på personopplysninger i «kort» tid. Hentet fra leverandørens nettsider: An Entra ID user's tenant and user information is removed from chat data at the start of a chat session. This information is only used to determine if the user is eligible

	for commercial data protection. Search queries triggered by prompts from an Entra ID user aren't linked to users or organizations by Bing".
Hvor lenge lagres personopplysningene etter at formålet ved behandlingen er over, før de slettes? Når skal opplysningene slettes? Er det utarbeidet sletterutiner?	Hentet fra leverandørens nettsider: "Microsoft doesn't retain prompts or responses from Entra ID users when using Copilot. Prompts and responses are maintained for a short caching period for runtime purposes. After the browser is closed, the chat topic is reset, or the session times out, Microsoft discards prompts and responses".
Er personopplysningssikkerheten tilstrekkelig ivaretatt?	Ja, for klassifiseringsnivå «åpen» og «intern» i henhold til styringssystem for informasjonssikkerhet.

9. Informasjonssikkerhet

Gjennomgå den funksjonelle beskrivelsen av alle behandlinger og om alle aktiva som skal brukes er identifisert	Følger samme logikk som andre tjenester fra Microsoft. Det er gjennomført en egen risiko- og sårbarhetsvurdering av tjenesten fra Seksjon for Digital sikkerhet.
Tas ny teknologi i bruk, eller brukes eksisterende teknologi på en ny måte?	Ny teknologi tas i bruk, men tilgang og driftsteknologi gjenbruker samme teknologi som er godt kjent i Microsoftplattformen.
Har virksomheten bygget systemet fra grunnen av eller er det kjøpt ferdig (som hyllevare) fra ekstern leverandør og deretter installert hos dere?	Ekstern tjeneste i sky (SaaS – «Software as a service»).
Er programvaren utviklet med innebygd personvern og personvern som standardinnstilling?	Ja. Leverandøren har på sine nettsider beskrevet tydelig hvordan personopplysninger blir behandlet.

Forsikre deg om at alle aktuelle referanser som er relatert til og aktuelle for behandlingen er dokumentert. Kan omfatte eksterne og interne krav, policy mv. som er nødvendige eller som må etterleves, f.eks.:

- Godkjente atferdsnormer/bransjenormer (art. 40)
- Sertifiseringer relatert til personvern (art. 42)
- Forskrifter, rundskriv, mv.

2. Nødvendighet og proporsjonalitet

I denne fasen kvalitetssikres det at valgene oppfyller personvernprinsippene, dvs. at de er legitimert og utført for å bidra til at behandlingen er nødvendig. For å etterleve lovkravene, må man også sjekke at valgene står i et rimelig forhold til formålene.

2.1 Personvernprinsippene

2.1.1 Rettslig grunnlag

Rettslig grunnlag/behandlingsgrunnlag:	**For ansatte:** Personvernforordningen artikkel 6 b) «behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse» Vurdering: NTNU har arbeidsavtale med alle ansatte. For at den ansatte skal klare å gjøre jobben sin skal arbeidsgiver tilby gode nok verktøy. NTNU har valgt å tilby Microsoft-tjenester til sine ansatte. **For studenter:** Personvernforordningen artikkel 6 e) «behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt» Vurdering: Studenter skal gjennomføre et utdanningsløp hvor det forventes bruk og kunnskap om ulike IKT-verktøy i tråd med tidens teknologiske utvikling. NTNU har et ansvar for å gjøre teknologi tilgjengelig for studentene. I og med at behandlingsgrunnlaget er art. 6 nr 1 bokstav e) (oppgave i allmennhetens interesse eller utøve offentlig myndighet) kreves det etter art. 6 nr 3 i tillegg et supplerende rettsgrunnlag i nasjonal rett - normalt lov eller forskrift. I denne sammenheng er flere supplerende rettsgrunnlag i universitets- og høyskoleloven: - § 1-3 om universitetets oppgaver - § 4-2 om utdanningsplan - § 4-3 om studentenes læringsmiljø - § 4-15 om Innhenting og behandling av personopplysninger i studieadministrative systemer
Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem for de registrerte?	Nei, det er ikke direkte tydelig for den registrerte å se sammenhengen mellom det rettslige grunnlaget og dette konkrete verktøyet. Dette er en problemstilling som gjelder for tilgangen til alle IKT-tjenester på NTNU.

Omfatter rettslig grunnlag både egne formål og eventuell utlevering?	Det vil ikke være mulig å utlevere data.
Vurder hvordan åpenhet ivaretas i behandlingen	Generelt rett til innsyn i egne personopplysninger etter personopplysningsloven (GDPR-innsyn). I tillegg kommer NTNU til å være åpen med denne personvernkonsekvensvurderingen på egne informasjonssider og gjennom utsendt informasjon til alle ansatte og studenter.

2.1.2 Formålsbegrensning
Formål(ene) skal være spesifikt, uttrykkelig angitt og berettiget, jf. art. 5 nr. 1 bokstav b.

Er formålet klart definert? Er formålet definert slik at det samsvarer med forventningene til den registrerte?	Ja.
Vurder om formålet kan oppnås med en mindre inngripende behandling	Ikke mulig.
Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer	Ikke mulig.

2.1.3 Dataminimering
Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene, jf. art. 5 nr. 1 bokstav c.

Vurder om formålet kan oppnås med mindre datainnhenting	Nei. Det er kun brukernavn som brukes og det slettes med en gang. Systemeier må kontrollere at bruker finnes for å kunne gi tilgang til tjenesten, og dette skjer gjennom kontroll av brukernavnet.
Begrunn nødvendighet og relevans relatert til formål for hver enkelt variabel i et datasett	Det er bare 1 variabel og den er absolutt nødvendig for å kontrollere at bruker eksisterer i brukerdatabase.

2.1.4 Riktighet
Personopplysninger skal være korrekte og oppdaterte, jf. art. 5 nr. 1 bokstav d.

Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering	Todelt: - Brukernavn holdes korrekt og oppdatert i Active Directory/Entra ID, og kontrolleres gjennom andre kjernesystemer på IT-avdelingen. - Tolkning av personopplysninger som bruker selv legger inn er umulig å forutse resultatet av fra sesjon til

	sesjon. Det er stor sannsynlighet for at språkmodellen kan gi ulike og feilaktige svar
Vurder om dere har nødvendig funksjonalitet for å rette og slette uriktige opplysninger	Ja. Løsningen sletter data etter kort tid. I og med at hovedkilden til informasjon er «internett» vil det ikke være mulig å slette innhold uten å ta kontakt med eierne av nettsteder der informasjonen ligger.
Ut ifra den registrertes perspektiv, er det behov for kontradiksjon?	Nei. Det ligger i dette verktøyets natur å kunne gi uriktige opplysninger. Behandlingsansvarlig ønsker at den registrerte skal ta aktivt stilling til informasjonen løsningen gir, og være grunnleggende kritisk til informasjonen som en språkmodell gir.

2.1.5 Lagringsbegrensning
Personopplysninger skal slettes eller anonymiseres når formålet er oppnådd, jf. art. 5 nr. 1 bokstav e.

Vurder om personopplysninger lagres etter at formålet er oppnådd	Personopplysningene blir ikke lagret etter bruk.
Vurder hvilke garantier som må være på plass dersom personopplysninger skal lagres i lengre perioder grunnet arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål, jf. art. 89 nr. 1.	Personopplysningene blir ikke lagret etter bruk.

2.2 De registrertes rettigheter

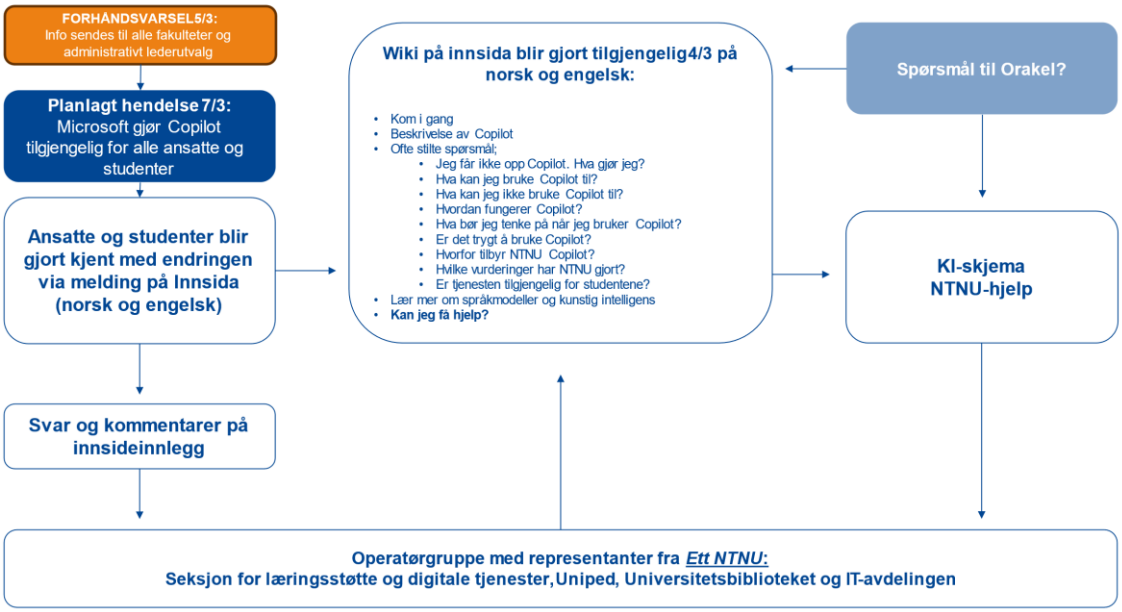
Vurder hvordan informasjon til de registrerte gis	Informasjon blir sendt ut til alle ansatte som melding til kanal «alle ansatte» og «studenter». Det er opprettet egne wikisider som beskriver verktøyet og behandlingen av personopplysninger:

	Norsk: https://i.ntnu.no/wiki/-/wiki/Norsk/Copilot Engelsk: https://i.ntnu.no/wiki/-/wiki/English/Copilot Se også NTNUs personvernerklæring
Vurder innhenting av samtykke, jf. art 7 og 8	**For ansatte:** Behandlingen er ikke direkte samtykkebasert med et dokument som «signeres/aksepteres før bruk», men gjennom å ta i bruk tjenesten hvor du har fått informasjon på forhånd bør dette kunne vurderes som en form for samtykke. Den registrerte kan velge å la være å bruke tjenesten, og ved å gå ut av tjenesten blir alle personopplysninger borte. Personopplysninger som bruker selv aktivt har hentet ut (klipp og lim) må behandles i tråd med øvrige retningslinjer og informasjonssikkerhetsregelverk i organisasjonen. **For studenter:** Samme vurderingsgrunnlag som for ansatte, men med unntak i undervisningssammenheng hvor faglærer sier at studentene skal ta verktøyet i bruk.
Vurder hvordan den registrertes rett til innsyn og til dataportabilitet ivaretas, jf. art. 15 og 20	Den registrerte har rett til innsyn i egne personopplysninger etter personopplysningsloven (GDPR-innsyn). I og med at opplysninger ikke lagres er det ikke behov for å vurdere dataportabilitet.
Vurder hvordan den registrertes rett til korrigering og sletting ivaretas, jf. 16 og 17	I og med at opplysninger ikke lagres er det ikke behov for å vurdere behov for korrigering og sletting.
Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas, jf. art. 18, 19 og 21	I og med at opplysninger ikke lagres er det ikke behov for å vurdere rett til innsigelser og begrensning av behandling. En bruker kan velge ikke å ta verktøyet i bruk
Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering, håndheves, jf. art. 22	Formålet med løsningen er at ansatte og studenter i virksomheten skal få tilgang til en språkmodell som kan benyttes for interne data. Det skal være en form for «sandkasse» hvor ansatte og studenter kan gjøre seg kjent med ny teknologi og dens fordeler og ulemper, og prøve ut løsningen på egne

	arbeidsoppgaver som de kan kjenne seg igjen i. Verktøyet skal ikke benyttes til noen form for automatiserte avgjørelser om individer. Dette vil løsningens brukere bli informert om i form av opplæring og retningslinjer for bruk. Verktøyet er en samtalerobot laget med kunstig intelligens, og kan brukes fritt av ansatte og studenter i virksomheten. Det er ikke mulig å sikre at ingen av løsningens brukere benytter løsningen til for eksempel å foreslå innhold til et beslutningsnotat, eller formulere et første utkast til et enkeltvedtak som er bestemmende for rettigheter og plikter. Hvis verktøyet benyttes til eksempler nevnt over, vil man ikke kunne spore alle ledd i en saksbehandlingskjede uten at saksbehandler eksplisitt informerer eller gjøre rede for at kunstig intelligens er benyttet. I retningslinjer og gjennom opplæring vil det påpekes at løsningen ikke skal benyttes til dette.

3. Vurdering av risiko for de registrertes rettigheter og friheter, og planlagte tiltak for å håndtere risikoene

Informasjonsskisse – Hvordan håndteres informasjon til og fra de registrerte i verktøyet



NTNU | Kunnskap for en bedre verden

Identifiser og vurder risikoer:

Beskriv risikoen behandlingen har for de registrertes rettigheter og friheter, og hvilke konsekvenser den har for de registrerte	**Alvorlighetsgrad for risikoen**	**Identifiser trusler som kan føre til hendelser**	**Sannsynlighet for at en hendelse oppstår**
En bruker tar usann informasjon som sann og bruker dette i en annen kontekst. For eksempel som del av interne utredninger, vurdering, begrunnelser som skal danne grunnlag for beslutninger eller som fakta i arbeid med oppgaver eller eksamen.	*Alvorlig*	Manglende opplæring eller lav kompetanse hos bruker	*Mulig*
Manglende samsvar mellom den registrertes rettigheter og den behandlingsansvarliges plikter etter Personvernforordningen (GDPR) For eksempel manglende rett til innsyn, sletting osv	*Minimal*	Manglende informasjon	*Liten*
En bruker legger inn noen andre sine personopplysninger som kommer på avveie	*Minimal*	Manglende opplæring eller lav kompetanse hos bruker	*Liten*
Tjenesten er ikke bra nok for våre brukere. Brukere ønsker seg verktøy som tar vare på data over tid og som kan «lære deg å kjenne». Denne funksjonaliteten kan ikke tilfredsstilles med krav til sletting, og det er risiko for at andre verktøy tas i bruk uten tilstrekkelig kunnskap om hva dette innebærer	*Minimal*	Manglende informasjon. Manglende opplæring eller lav kompetanse hos bruker	*Mulig*
Risiko for at studenter blir tatt i fjusk, (plagiat, tekstlikhet osv) ved bruk av dette verktøyet.	*Minimal (for organisasjon, men alvorlig for enkeltstudenten)*	Manglende informasjon. Manglende opplæring eller lav kompetanse hos bruker	*Mulig*

Identifiser risikoreduserende og skadebegrensende tiltak:

Risiko	**Tiltak**	**Effekt på risiko**	**Restrisiko**	**Tiltak godkjent**
Manglende samsvar mellom den registrertes rettigheter og den behandlingsansvarliges plikter etter Personvernforordningen (GDPR) For eksempel	Må gjennomgå NTNUs personvernerklæring for å kontrollere at informasjon til den registrerte er tydelig nok kommunisert	*Redusert*	*Lav*	*Må gjennomgås* *Ansvar for oppfølging Heine Skipenes*

manglende rett til innsyn, sletting osv				
Manglende opplæring eller lav kompetanse hos bruker og En bruker legger inn noen andre sine personopplysninger som kommer på avveie	Lage informasjonssider på nett norsk og engelsk om hva verktøyet er, og hva det kan brukes til Det blir opprettet en wikiside som det er mulig å finne informasjon om tekniske vurdering, risikovurderinger, personvernkonsekvensvurdering osv.	*Redusert*	*Lav*	*Dagens wikisider må oppdateres* *Ansvar for oppfølging Heine Skipenes*
Manglende opplæring eller lav kompetanse hos bruker	Legge ut melding til alle ansatte og studenter om at verktøyet nå er på plass med informasjon om hva det kan brukes til.	*Redusert*	*Lav*	*Må gjennomgås* *Ansvar for oppfølging Heine Skipenes*
Manglende opplæring eller lav kompetanse hos bruker	Tilby «å komme på besøk» til brukergrupper for å informere om verktøyet og bidra til økt bevissthet om bruk av kunstig intelligens	*Redusert*	*Lav*	*Gjennomføres kontinuerlig på forespørsel* *Ansvar for oppfølging Heine Skipenes*
Manglende opplæring eller lav kompetanse hos bruker	I informasjonsmateriellet er det gitt informasjon om hvordan det er mulig å komme med tilbakemeldinger til oss som IT-avdeling, og komme med generelle tilbakemeldinger og refleksjoner om positive og negative ting med løsningen.	*Redusert*	*Lav*	*Gjennomføres kontinuerlig. Kun sporadiske tilbakemeldinger så langt* *Følges opp fra KI-klynga i IT-avdelingen.* *Ansvarlig for oppfølging Ola Berntsen Huseby*
Manglende opplæring eller lav kompetanse hos bruker	NTNU bør lage retningslinjer for bruk av generativ kunstig intelligens	*Redusert*	*Lav*	*Under gjennomføring, endelig høringsfrist 1/2-24.* *Følges opp fra KI-klynga i IT-avdelingen.* *Ansvarlig for oppfølging Ola Berntsen Huseby*

Manglende opplæring eller lav kompetanse hos bruker	Tema «hvordan skal vi forholde oss til Kunstig intelligens?», «hva slags kjøreregler bør NTNU ha?» osv har blitt behandlet i til medvirknings- og medbestemmelsesorganer: - SESAM (06.11.2023) (* se referat fra møtet nedenfor) - Administrativt lederutvalg (24.11.2023) - Formøte Studenttinget (27.11.23) - Dekanmøtet (16.11.24)	*Redusert*	*Lav*	*Under gjennomføring,* *Ansvar for oppfølging Heine Skipenes*
Tjenesten er ikke bra nok for våre brukere. Brukere ønsker seg verktøy som tar vare på data over tid og som kan «lære deg å kjenne». Denne funksjonaliteten kan ikke tilfredsstilles med krav til sletting, og det er risiko for at andre verktøy tas i bruk uten tilstrekkelig kunnskap om hva dette innebærer	Alle tiltak på lista over vil bidra til risikoreduksjon: - Informasjonsmateriell på innsida om hva tjenesten kan brukes til, og hva det ikke kan brukes til - Retningslinjer - Opplæring I tillegg må det jobbes med videreutvikling og vurdere om NTNU også skal tilby verktøy som tilfredsstiller behovet for å ta vare på data over tid.	*Redusert*	*Lav*	*Under gjennomføring,* *Ansvar for oppfølging Heine Skipenes*
Risiko for at studenter blir tatt i fjusk, (plagiat, tekstlikhet osv) ved bruk av dette verktøyet.	Avdeling for utdanning har satt i gang et arbeid hvor en arbeidsgruppe med representanter fra alle fakultet skal se nærmere på klargjøring av rektorvedtaket om fjusk og skjema for redegjørelse for bruk av KI i arbeidet med besvarelser (deklarasjonsskjema). Gruppa vil også se på behovet for kompetanseutvikling knyttet til KI i utdanningsvirksomheten.	*Redusert*	*Lav*	*Under gjennomføring,* *Ansvar for oppfølging Morten Sørlie*

4. Ledelsens validering av personvernkonsekvensvurderingen (DPIA)

Moment	**Navn og dato**	**Kommentarer**
Tiltak godkjent av:	Rektor, 27. februar 2024	Håkon har godkjent forrige DPIA pr epost 21.09.2023, dokumentasjon i ephorte på sak 2023/32790
Restrisiko godkjent av:	Rektor, 27. februar 2024	*Dersom restrisiko med høy risikograd blir godkjent, ta kontakt med Datatilsynet før oppstart for forhåndsdrøfting, jf. art. 36 nr. 1.*
Personvernombudsbistand gitt:	Thomas Helgesen 21.09.2023, 01.02.2024	*Personvernombudet skal gi råd om regelverksoverholdelse, steg 6-tiltak og om hvorvidt behandlingsaktiviteter kan settes i gang, jf. art. 35 nr. 2 og art. 39 nr. 1 bokstav c.*
Sammendrag av personvernombudets råd: Innføring av Microsoft Copilot gjelder utprøving av ny teknologi, og det er viktig å ha fortsatt trykk på det som gjelder rettighetene til den registrere. Fortsette utvikling av informasjon, opplæringsmateriell, svare på spørsmål osv, og ha tilstrekkelig med ressurser for å kunne «være der» for brukeren. En stor utfordring er hva brukerne faktisk kommer til å bruke løsningen til, og det vil ikke være mulig å kontrollere eventuell feil bruk. God kontinuerlig informasjon blir derfor viktig. Personvernombudet anbefaler ikke at verktøyet brukes til å behandle personopplysninger. Dette må fremkomme av informasjonsmateriellet som skal utarbeides Personvernombudet ønsker at det blir gjennomført kontroll av at tjenesten blir benyttet som tenkt, systematisk gjennomgang av hva brukerne spør om og revidert tiltaksliste. Personvernombudet ber om å få delta i denne prosessen.		
Personvernombudets råd er akseptert eller overprøvd av:	Rektor, 27. februar 2024	
Kommentarer: Rektor aksepterer personvernombudets råd.		
De registrertes synspunkter er innhentet og gjennomgått av:	SESAM 06.11.2023, Høringsprosess KI-retningslinjer sendt ut til alle avdelinger, fakulteter og Studenttinget.	
Kommentarer:		
Denne personvernkonsekvensvurderingen vil følges opp av:	IT-avdelingen	.

Vedlegg referat fra SESAM møte 06.11.2023

«Sak 81/23: Verktøy med kunstig intelligens ved NTNU (orientering)

NTNU trenger gode løsninger for kunstig intelligente (KI) verktøy for studenter og ansatte. Saken drøftes også i Utdanningsutvalget og Studenttinget. Heine Skipnes (IT) viste til utsendt notat med vedlegg. NTNU gjennomførte en personvernkonsekvensvurdering da man innførte Bing Chat Enterprise for ansatte. IE-fakultet ber om at vi også kan tilby et sikkert KI-verktøy for studenter og faglærere. IT-avdelingen er klar til å kunne tilby dette fra vårsemesteret (eks. løsningen som UiO tok i bruk våren 2023). Det kommer nye verktøy framover der kunstig intelligens får tilgang til alt vi har. Personvernombudet, Thomas Helgesen, påpekte at det er viktig å gjøre risikovurderinger. Det er heftige verktøy som kan innebære stor risiko for den enkeltes integritet om riktighet av opplysninger osv. Noen i sektoren har innført KI uten grundig vurdering. Ny KI-regulering vil bli strengere mht. risikovurdering og dokumentasjon.

OI-direktør tenker at NTNU må forventes å være framoverlent, men på en forsvarlig måte. KI har kommet for å bli. Spørsmålet er hvordan.

- NTL. KI har kommet for å bli. Det er en grunnleggende bekymring for hva som skjer med det som legges inn i ChatGPT. Løsningen for ansatte er tryggere, men hvordan skal vi ivareta sikkerheten for studentene? Det er viktig at vi har en god vurdering av personvern. Vi bør se utviklingen i sammenheng med NTNU sak. Vi må være med å påvirke den nasjonale utviklingen.
- Samfunnsviterne er bekymret for at en robot vil kunne få tilgang til alle typer informasjon ansatte produserer og uten noe filter.
- Tekna. Hva tenker man om Microsoft 365 Copilot? Hvis vi slår på hele Microsoft-systemet, hva skjer da? Det er ikke all informasjon som bør være søkbar og tilgjengelig for systemet.
- Studenttinget (Erik Johansen) er også opptatt av at systemet er trygt å bruke. Vi vet ikke hvilken informasjon studenter legger i åpne systemer. Jeg er redd for at studenter som sitter på person-sensitive forskningsdata, kan fristes til å legge det inn i åpne tilgjengelige verktøy. I forvaltnings-prosesser vil KI bli en svart boks som gjør at det ikke er klart hvilke prosesser som ligger bak beslutninger som fattes.
- FF. NTNU bør være i førersetet. Omfanget av hva som kan innhentes av opplysninger er skremmende; Det må lages gode rammer for hvordan data skal brukes av et KI-system. Det må være et reglement og retningslinjer for ansatte og studenter, med god opplæring i etikk.
- Parat. Enig i at vi må gjøre dette forsvarlig. Dersom dette verktøyet benyttes i saksbehandling, vil man ikke kunne spore alle ledd i en saksbehandlingskjede.

Rektor lurer på hva forskjellen vil være på systemet som NTNU har tatt i bruk og den som tenkes brukt for studenter. Hvilke språkmodeller skal vi velge? Må KI-verktøyene legges ut for alle eller kan vi prøve ut ved utvalgte enheter etter en kvalifisering (gjennomgått opplæring)? Ansatte og studenter som opptrer i god tro, må ikke risikere å gjøre noe fullstendig galt. Vi er NTNU, men vi må ikke være de første til å hoppe på bølgen, men heller gjøre det forsvarlig.

Heine Skipnes forklarte at den viktigste forskjellen på Bing Chat Enterprise og studentmodellen vil være at den siste vil være en ren språkmodell. Bing Chat Enterprise er mer avansert og er for eksempel ekstremt god til å oversette til nynorsk og skrive gode dokumenter. Alle data som legges inn slettes fortløpende. I det systemet som tenkes for studenter, vil data bli slettet etter 30 dager. NTNU ønsker å følge med på Microsoft 365 Copilot utviklingen, men vil ikke skru på noe vi ikke er sikre på at vi vil bruke. Microsoft teknologien kan lese alt man skriver, også epost, med mindre det er lagt inn en beskyttelse. Hvis man bruker AI-teknologi til opprettelse av et dokument, bør man opplyse om

hvordan AI har vært brukt (metode og sitat). Det er mulig å begrense tilgangen for studenter til en begrenset gruppe.

Arbeidsgiver konkluderte at småskala utprøving under kontrollerte former bør være veien videre. SESAM ønsker å få tilbake en sak om hvordan NTNU skal gripe dette an. Vi må gå runden i sentrale utvalg, dekanmøtet og studentdemokrati. Kostnadene ved innføring av KI-verktøy er ikke trivielle. Det vil bli behov for opplæring av alle ansatte og studenter.»

Vedlegg - Kildeliste:

- SESAM-notat 06.11.2023. Sak 81/23 «Verktøy med kunstig intelligens ved NTNU»
  - Lenke til referat fra møtet
- Wikiside på Innsida om Bing Chat Enterprise og alle vurderinger som er gjort
- Innlegg om Copilot og bruk av kunstig intelligens på KI-dagen 26.01.2024
- Melding til alle ansatte om ny kunstig intelligens chat (22. september 2023)
  Opptak av presentasjon fra møte i Kommunikasjonsnettverket 07.06.2023 (35 minutter). "Hva er kunstig intelligens? Hva har vi og hva får vi i NTNUs verktøykasse?"
  Hovedtema:
  - Smakebiter fra innsiden av teknologiutviklingen
  - Hvordan bruke kunstig intelligens på en sikker og trygg måte.
  - Hvordan jobber IT-avdelingen med å utvikle og tilpasse sine tjenester?
- Artikler i Khrono
  - NTNU med restriktive KI-retningslinjer: — Kan ikke kose på serveren

  Artikler i Universitetsavisa
  - 26. oktober 2023: Ny KI-chat på banen: - NTNU er i samtaler
  - 22. september 2023: Nå har NTNU KI-chat, men studentene får ikke
- Regjeringens strategi: «Nasjonal strategi for kunstig intelligens»
- Godt eksempel fra IE-fakultetet (18. oktober 2023):
  - «Fakultet for informasjonsteknologi og elektroteknikk ved NTNU (IE) etablerte våren 2023 en arbeidsgruppe for å vurdere hvilke konsekvenser den raske utviklingen innen kunstig intelligens vil ha innen fakultetets utdanningsvirksomhet. Arbeidsgruppen har nå ferdigstilt sin rapport. Rapporten inneholder en god del anbefalinger som det vil bli arbeidet videre med. Det vil om få dager komme en konkretisering fra fakultetet når det gjelder om og eventuelt hvordan rapportens anbefalinger vil ha direkte betydning for bachelor- og masteroppgaver samt det pågående emne- og studieplanrevisjonsarbeidet for neste studieår.»
  - Lenke til hele rapporten