Vurdering av personvernkonsekvenser (DPIA)

Navn på system/prosjekt:	Teste Microsoft 365 Copilot ved NTNU
DPIA-en utføres av:	Strategisk rådgivningsgruppe, IT-strategi og -styring (Ansvarlig Heine Skipenes)
Dato:	07.02.2024

Innholdsfortegnelse

Merknader til den gjennomførte personvernkonsekvensvurderingen:

- Microsoft Copilot har byttet navn fra Bing Chat Enterprise, og det er utviklet en egen DPIA for utrulling av Microsoft Copilot for studenter og ansatte fra februar 2024. Denne DPIAen gjelder utelukkende testfase for verktøyet Microsoft 365 Copilot. Definisjonen som brukes gjennom hele DPIA er «**M365 Copilot**»
- 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.
- Utvikling av KI-verktøy er behandlet i Sesam 06.11.2023 med konklusjon: *«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.»* Hele referatet ligger til slutt i dokumentet
- 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 har søkt og fått opptak i Datatilsynets regulatoriske sandkasse for personvernvennlig innovasjon og digitalisering våren 2024 med prosjektet «Pilotere Microsoft 365 Copilot». M365 Copilot er neste generasjons KI-verktøy, og **NTNU gjennomfører et pilotprosjekt for å teste om Microsofts kunstige intelligente assistent kan bli tatt i bruk i en stor offentlig organisasjon.** Det som skiller de to forskjellige «copilotene» ligger i at M365Copilot blir integrert i allerede eksisterende Microsoft-tjenester som Word, Excel, Powerpoint, Teams, Sharepoint, Outlook osv, og at verktøyet kan potensielt få tilgang til lokale filer og organisasjonsintern informasjon. Dette vil innebære et «teknologisk taktskifte» som kan gi NTNU mange muligheter, men også en del nye utfordringer. M365 Copilot jobber i kontekst av brukeren og dens rettigheter. Du vil ikke få tilgang til data med M365 Copilot, som du ikke hadde tilgang til fra før. Forskjellen er at M365 Copilot bringer mer av dataen du allerede har tilgang til til overflaten. Testingen skal sjekke at tilganger til datakildene er sjekket grundig før "frislipp" i resten av organisasjonen (ansvarsoppgave som administratorer har i dag).

NB: Det er viktig å bemerke at Microsoft bygger en kraftig merkevare rundt begrepet «Copilot», og det er ulike tjenester som operer med samme navn. For eksempel blir de fleste tastaturer på Windows11 PCer snart utstyr med en egen fysisk Copilot-knapp. Samtaleroboten som før het Bing Chat Enterprise omdøpes til Microsoft Copilot og gjøres tilgjengelig for alle brukere, og her er det en egen DPIA-prosess på gang (februar 2024) for å tilgjengeliggjøre verktøy for studentene. Testing av andre copiloter enn M365 Copilot er utenfor scopet til denne testingen.

M365 Copilot er en kostnadskrevende løsning, ca 4733 kr pr bruker pr år. Dette tilsvarer 394,44 pr bruker pr måned. Vi gjør avtaler pr år, så kostnadsforpliktelse går fram til 31. august 2024.

Prosjektperioden og varighet på DPIA-vurdering er fra 1. februar til 31. august. Vi må fornye lisenser ved videreføring, og da må vi også utarbeide en ny DPIA. **Dette må skje innen 15. august 2024.**

Institusjonen må sørge for at alle vurderinger av informasjonssikkerhet og personvern er ivaretatt. Når verktøy som samtaleroboter med innebygget 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.»)

IT-avdelingen har tatt utgangspunkt i følgende behandlingsformål i prosjektet «Pilotere Microsoft 365 Copilot»:

1. Teste M365Copilot på en begrenset gruppe brukere med kompetent personell for å se om tjenesten kan bli tatt i bruk i en stor offentlig organisasjon
2. Fremskaffe erfarings- og datagrunnlag for å kunne ta gode og fornuftige valg om denne tjenesten skal kunne tilbys til flere.
3. Tilgjengeliggjøre informasjon om hvordan vi har tenkt risikovurdering, informasjonssikkerhet og personvern.

Hvilke personopplysninger skal behandles?

- Potensielt alle registrerte personopplysninger som NTNU har om en bruker
- Personopplysninger som brukeren selv legger inn (prompts/kommandoer/input)

Antallet brukere (5), omfang av personopplysninger, klassifiseringsnivå (fortrolig) på behandlingen av informasjonsverdier og at dette er ny teknologi for NTNU tilsier at personvernkonsekvensvurdering bør gjøres jf. art. 35 nr. 1. a. Antallet brukere vil øke i løpet av prosjektperioden, til maks 100.

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/microsoft-365-copilot/

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?	Allerede samlet inn
Hvordan skal personopplysningene lagres?	Hvordan lagring skjer er et av de temaene som testfasen skal avklare
Hvordan skal personopplysningene brukes?	Dette er en av de temaene som testfasen skal avklare
Hvem skal ha tilgang til personopplysningene?	Microsoft
Hvem skal det samles inn personopplysninger om?	Testpersonell - Alle er administratorer i M365, så uttesting av M365 Copilot for disse betraktes som en

	behandlingsaktivitet med begrenset omfang og risiko sammenlignet med å gi tilgang til alle brukere. NB: M365 Copilot skal testes på testernes vanlige brukerkontoer (ikke privilegierte admin-kontoer).
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 M365Copilot inngår i datagrunnlaget med personopplysninger som Microsoft vet om NTNUs brukere.
Vil det være systematisk behandling av personopplysninger?	Ja! - M365 Copilot vil kontinuerlig bearbeide og analysere brukernes data. Den vil bearbeide de dataene den får tilgang til, og en bruker vil ikke kunne merke at behandlingen skjer.
Brukes det ny teknologi eller ny bruk av eksisterende teknologi hvor personvernkonsekvenser ikke har blitt vurdert?	For UH-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, intern og fortrolig informasjon. Løsningen blir ikke godkjent til strengt fortrolig. Om brukere selv gjør tilgjengelig vanlige og/eller særlige kategorier personopplysninger blir dette behandlet.
Antall registrerte involvert i behandlingen	Maks antall brukere er 5. Antallet brukere vil øke i løpet av prosjektperioden, til maks 100.
Datavolum	Avhengig av hva brukerne gjør tilgjengelig. Kan være alt fra små til store mengder.
Behandlingsfrekvens	Kontinuerlig.
Lagringstid for personopplysningene	M365 Copilot bearbeider en brukers allerede lagrede datafiler gjennom å indeksere innholdet og gjøre dette tilgjengelig for Graph. Det er ikke kjent hvor lenge dataene blir liggende der, og om de noensinne slettes. M365 Copilot opererer med ulike typer indeksering av innhold, deriblant en ny semantisk indeks: https://learn.microsoft.com/en-us/MicrosoftSearch/semantic-index-for-copilot

	Dette gjelder dataene M365 CoPilot har tilgang til. Historikk kan styres ved retention policies: https://learn.microsoft.com/en-us/purview/retention-policies-copilot og det ser ut til at det samme også styrer hvor lenge vi tar vare på "loggdata" for eDiscovery. Det ser ut til at dersom en bruker ved en feiltagelse limer "sensitive data" inn i et M365Copilot chat-vindu, kan man ved hjelp av eDiscovery, finne og slette disse dataene (https://learn.microsoft.com/en-us/purview/ediscovery-search-and-delete-copilot-data) eDiscovery vil gi administratorer tilgang til å kunne få se andre brukeres prompts. Dette er en av de temaene som testfasen skal avklare
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	IT-avdelingen har tatt utgangspunkt i følgende behandlingsformål i prosjektet «Pilotere Microsoft 365 Copilot»: 1. Teste M365Copilot på en begrenset gruppe brukere med kompetent personell for å se om tjenesten kan bli tatt i bruk i en stor offentlig organisasjon 2. Fremskaffe erfarings- og datagrunnlag for å kunne ta gode og fornuftige valg om denne tjenesten skal kunne tilbys til flere. 3. Tilgjengeliggjøre informasjon om hvordan vi har tenkt risikovurdering, informasjonssikkerhet og personvern.
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?	Ja – det er formålet med prosjektet å avklare om verktøyet kan gjøre dette. For eksempel kan M365 Copilot lære seg skrivestilen til en bruker for å foreslå et første utkast til en svar-epost.
Vil personopplysningene viderebehandles til nye eller andre formål?	Ja – det er formålet med prosjektet å avklare om verktøyet kan gjøre dette. For eksempel kan et datasett settes sammen med et annet datasett for å kunne finne hittil ukjente sammenhenger. Vi kan ikke utelukke at datasettene inneholder personopplysninger

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?	Alle Microsoft sine tjenester er koblet sammen gjennom kjernetjenesten i «Microsoft Graph»: «Microsoft 365 core services: Bookings, Calendar, Delve, Excel, Microsoft 365 compliance eDiscovery, Microsoft Search, OneDrive, OneNote, Outlook/Exchange, People (Outlook contacts), Planner, SharePoint, Teams, To Do, Viva Insights» Alle personopplysninger vil behandles på tvers av de ulike tjenestene. I tillegg vil M365Copilot ha tilgang til Dette er en av de temaene som testfasen skal avklare
Relasjon mellom behandlingsansvarlig og den registrerte	De registrerte er ansatte hos behandlingsansvarlig.
I hvilken grad har den registrerte kontroll over sine opplysninger?	Delvis ukjent. Det finnes noe info om uthenting og sletting av data. "To view and manage this stored data, admins can use Content search or Microsoft Purview." Permanent sletting skjer foreløpig ved å sende inn en support ticket med bruker-GUID og tenant-GUID. Finner ingenting om automatisk sletting, eller massesletting av mange brukere. Se mer her: https://learn.microsoft.com/en-us/microsoft-365-copilot/microsoft-365-copilot-privacy#data-stored-about-user-interactions-with-microsoft-copilot-for-microsoft-365 Dette er en av de temaene som testfasen skal avklare 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.

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?	Ja – det er formålet med prosjektet å avklare om verktøyet kan gjøre dette. For eksempel kan et datasett settes sammen med et annet datasett for å kunne finne hittil ukjente sammenhenger. Vi kan ikke utelukke at datasettene inneholder personopplysninger
Kobles ulike registre for å gi ny type informasjon om den registrerte?	Ja. Med utgangspunkt i SNL sin betegnelse om hva et register er (https://snl.no/register_-_IT): *«**Register som en samling av data** Register kan brukes om en fil eller en tabell bestående av objekter eller poster. Register kan også brukes om en samling av tabeller og filer. Da er register et synonym for en database. I dagligtale snakker vi om personregister, adresseregister, bilregister, båtregister, helseregistre, osv. Disse registrene er egentlig databaser som består av mange filer og tabeller. Det finnes en rekke registre som forvaltes av offentlige etater.*

	[…].» Det er formålet med prosjektet å avklare om verktøyet kan gjøre dette: Ulike registre skal kunne kobles sammen ulike registre for å gi ny type informasjon, ikke i hovedsak om den registrerte – men vi kan ikke utelukke at det kan komme til å skje

6. Identifisering og oversikt

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

7. Mottakere av personopplysninger

Beskriv alle mottakere/kategorier av mottakere av personopplysninger	Microsoft og den registrerte selv har tilgang til en brukers personopplysninger. Det er mulig at en bruker kan få tilgang til en annen brukers personopplysninger. Brukerne som i første omgang får tilgang til M365 Copilot har administratorrettigheter og vil kunne se opplysninger på tvers. De som nå får tilgang er godt kjent med og trent på å holde ulike brukeres informasjon fra hverandre. Det må presiseres at priviligert tilgang kun nås gjennom dedikerte brukerkontoer. Alle administratorer har også ordinære brukerkontoer, med ordinære tilganger. Testerne vil under testingen vurderere om de skal unngå bruk av priviligerte kontoer i første omgang. Det er risiko for at priviligerte kontoer kan ha tilgang til data som hverken "eies" av testerne, eller er relevant for testingen. Grenseoppgangen mellom «hva som ses av hvem» er et av de temaene som testfasen skal avklare. Testernes digitale kompetanse på plattformen er høy.
Hvordan deles personopplysningene mellom avdelinger **internt** i virksomheten?	Informasjon kan bli delt internt i virksomheten. Grenseoppgangen mellom hva som ses av hvem er et av de temaene som testfasen skal avklare.
Hvilke **eksterne** virksomheter deles personopplysningene med? Hvis ja, for hvilke formål og med hvilke rettslige grunnlag?	Personopplysningene deles allerede med databehandler. Rettslig grunnlag: Personvernforordningens artikkel 6 a) **Samtykke** - den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål
Overføres personopplysningene til land utenfor EU/EØS-området (tredjestater), jf. art. 44-49? Hvis	Ja. Vi kan ikke utelukke at personopplysninger ikke behandles utenfor EU/EØS-området, men Microsoft

ja, hva er det rettslige grunnlaget for det?	beskriver at "EU traffic stays within the EU Data Boundary". Se mer: https://learn.microsoft.com/en-us/microsoft-365-copilot/microsoft-365-copilot-privacy#microsoft-copilot-for-microsoft-365-and-the-eu-data-boundary. Rettslig grunnlag: Personvernforordningens artikkel 6 a) **Samtykke** - den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål Hvor data behandles er en av de temaene som testfasen skal avklare.
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: https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+retningslinjer • Retningslinje for arbeid med sikkerhetskultur og opplæring • Retningslinje for avviksmelding og avvikshåndtering innen informasjonssikkerhet og personvern • Retningslinje for behandling av personopplysninger • Retningslinje for digital beredskap, hendelses- og krisehåndtering • Retningslinje for informasjonssikkerhet i leverandørforhold • Retningslinje for klassifisering av informasjonsverdier • Retningslinje for kryptografiske kontroller • Retningslinje for nettverks- og informasjonsoverføring • Retningslinje for operativ sikkerhet • Retningslinje for risikostyring for informasjonssikkerhet • Retningslinje for sikring av personlig IKT-utstyr

	• Retningslinje for tilgangskontroll
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?	Dokumentasjonen på leverandørens nettsider vil bli gjennomgått som ledd i prosjektet. Dette er et av de temaene som testfasen skal avklare

8. Dataflyt, lagring og mellomlagring

Hvordan overføres og tilgjengeliggjøres personopplysningene?	Dokumentasjonen på leverandørens nettsider vil bli gjennomgått som ledd i prosjektet. Dette er et av de temaene som testfasen skal avklare
Hvor og hvor lenge lagres personopplysningene ulike steder?	Dokumentasjonen på leverandørens nettsider vil bli gjennomgått som ledd i prosjektet. Dette er et av de temaene som testfasen skal avklare
Hvor lenge lagres personopplysningene etter at formålet ved behandlingen er over, før de slettes? Når skal opplysningene slettes? Er det utarbeidet sletterutiner?	Dokumentasjonen på leverandørens nettsider vil bli gjennomgått som ledd i prosjektet. Dette er et av de temaene som testfasen skal avklare
Er personopplysningssikkerheten tilstrekkelig ivaretatt?	Ja, for klassifiseringsnivå «åpen», «intern» og «fortrolig» i henhold til styringssystem for informasjonssikkerhet. Office 365 (SharePoint, Teams, Onedrive) er klassifisert opp til fortrolig jf NTNUs lagringsguide https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide så fremt innholdet er kryptert med AIP. Dette er et av de temaene som testfasen skal avklare

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 gjennomføres en egen risiko- og sårbarhetsvurdering av tjenesten fra Seksjon for Digital sikkerhet.

	NB: M365 Copilot forholder seg kun til "Semantic Index", og at alt foregår i brukerens egen sikkerhets-kontekst, og kun innhold brukeren allerede har tilgang til benyttes for å generere svaret. Det eneste "nye" er at vi nå får lagret brukerens dialog med copilot'en, og at man kan benytte eDiscovery for å fjerne evt. dialoginnslag av sensitiv karakter ved behov. Lenke til diri: KOMMER **Data deles kun internt på egen tentant: «**The stored data includes the user's prompt, how Copilot responded, and information used to ground Copilot's response. For example, this stored data provides users with Copilot interaction history in Microsoft Copilot with Graph-groundedc chat and meetings in Microsoft Teams. This data is processed and stored in alignment with contractual commitments with your organization's other content in Microsoft 365. The data is encrypted while it's stored and isn't used to train foundation LLMs, including those used by Microsoft Copilot for Microsoft 365." Les mer: https://learn.microsoft.com/en-us/microsoft-365-copilot/microsoft-365-copilot-privacy#data-stored-about-user-interactions-with-microsoft-copilot-for-microsoft-365 Dette er et av de temaene som testfasen skal avklare
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:	Personvernforordningen artikkel 6 a) «den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål» Vurdering: NTNU vurderer det som riktig å legge behandlingsgrunnlaget på samtykke i testfasen. Testerne må aktivt ta stilling til om dette er et prosjekt de ønsker å være med på eller ikke. Det kommer ikke til å ha noen konsekvens for de registrerte om de ikke ønsker å delta i pilotprosjektet, eller ønsker å trekke seg underveis. Hvis tjenesten settes i drift, vil ikke samtykke være rettslig grunnlag.
Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem for de registrerte?	Ja – NB dette gjelder kun i dette testprosjektet
Omfatter rettslig grunnlag både egne formål og eventuell utlevering?	Ja. NTNU skal ikke 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 nettsider.

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 pr i dag.

	Dette er et av de temaene som testfasen skal avklare
Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer	Ikke mulig. Dette er et av de temaene som testfasen skal avklare

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. Dette verktøyet får tilgang til alt som er registrert om den registrerte.
Begrunn nødvendighet og relevans relatert til formål for hver enkelt variabel i et datasett	Vi klarer ikke å gjennomføre testfasen uten å gi tilgang til personopplysningene.

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 brukerdatabase/Entra ID, og kontrolleres gjennom andre kjernesystemer på IT-avdelingen. - Tolkning av personopplysninger er det umulig å forutse resultatet av. Det er stor sannsynlighet for at språkmodellen kan gi ulike og feilaktige svar Dette er et av de temaene som testfasen skal avklare
Vurder om dere har nødvendig funksjonalitet for å rette og slette uriktige opplysninger	Dette er et av de temaene som testfasen skal avklare
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	Ukjent. Dette er et av de temaene som testfasen skal avklare. Det bør vurderes hvordan formålet bør beskrives/begrenses. Gitte datoer, vare helt til lisenser blir fjernet eller brukeren slettet osv. I dag er det slik at NTNU må årlig fornye alle lisenser (innen 31. august hvert år)
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.	Ukjent. Dette er et av de temaene som testfasen skal avklare

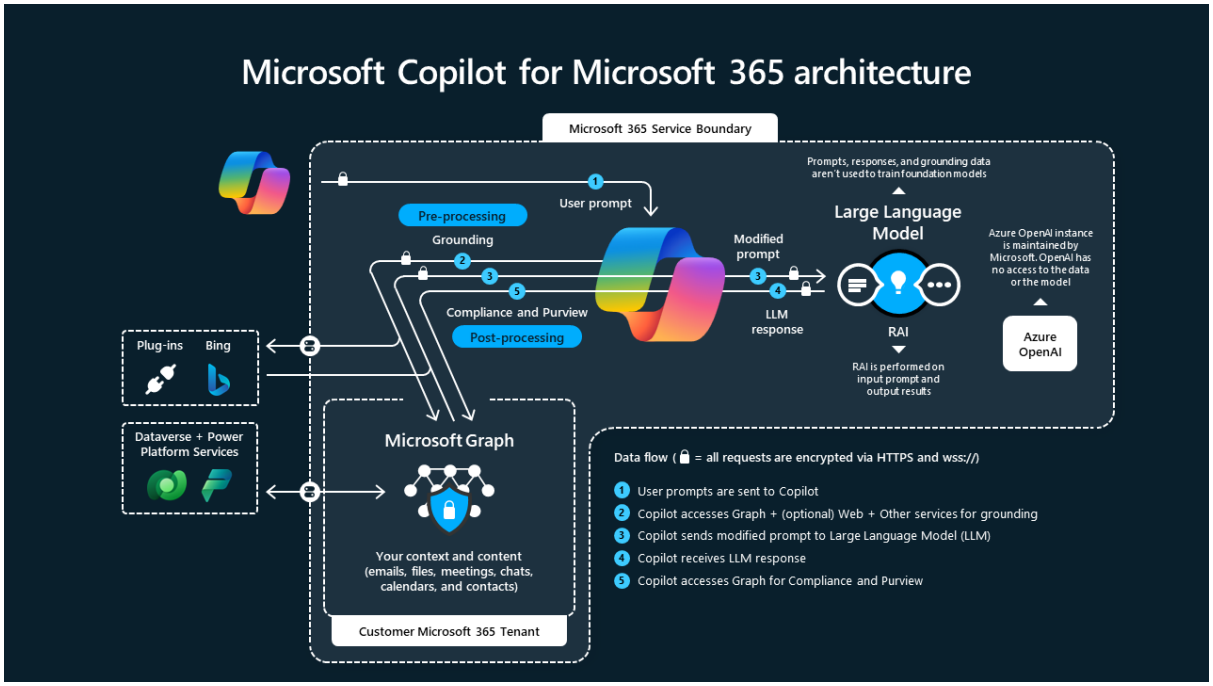
2.2 De registrertes rettigheter

Vurder hvordan informasjon til de registrerte gis	DPIA gjøres tilgjengelig for de registrerte. De må lese gjennom DPIA, og oppfordres til å komme med sine tilbakemeldinger. Deretter innarbeides tilbakemeldingene før DPIA godkjennes av IT-direktør. Se også NTNUs personvernerklæring
Vurder innhenting av samtykke, jf. art 7 og 8	Alle registrerte må aktivt samtykke til at innholdet i DPIA er lest og forstått. Dette gjøres via aktivt svar på epost som arkiveres på sak i ephorte fra prosjektleder. I epost gjøres det rede for at å trekke samtykke kan når som helst gjøres ved å sende epost til prosjektleder som vil iverksette tiltak for å stoppe behandlingen.
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. «"[…] we store data about [the user's] interactions. The stored data includes the user's prompt, how Copilot responded, and information used to ground Copilot's response." Se mer: https://learn.microsoft.com/en-us/microsoft-365-copilot/microsoft-365-

	copilot-privacy#data-stored-about-user-interactions-with-microsoft-copilot-for-microsoft-365
Vurder hvordan den registrertes rett til korrigering og sletting ivaretas, jf. 16 og 17	I og med at de registrerte har administratorrettigheter til M365 er det de registrerte som selv har mulighet til å rette/slette. Hvordan dette kan ivaretas for andre er et av de temaene som testfasen skal avklare.
Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas, jf. art. 18, 19 og 21	I og med at de registrerte har administratorrettigheter til M365 er det de registrerte som selv har mulighet til innsigelser og begrensning. Hvordan dette kan ivaretas for andre er et av de temaene som testfasen skal avklare.
Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering, håndheves, jf. art. 22	Verktøyet skal i testfasen 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. Dette er et av de temaene som testfasen skal avklare

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

Informasjonsskisse – Hvordan behandles informasjon



https://learn.microsoft.com/en-us/microsoftsearch/semantic-index-for-copilot

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**
Personopplysninger kommer på avveie	*Medium*	Teknologiutvikling i tidlig fase	*Liten*
Ikke mulig å sikre 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*

Manglende fokus på programvareutvikling med innebygd personvern	*Medium*	Manglende organisatorisk rammeverk for innebygd personvern	*Liten*

Identifiser risikoreduserende og skadebegrensende tiltak:

Risiko	Tiltak	Effekt på risiko	Restrisiko	Tiltak godkjent
Personopplysninger kommer på avveie **Teknisk perspektiv:** ***Ukontrollert spredning***	Direkte opplæring av de registrerte. Etablere rutiner og systematikk for innhenting av tilbakemeldinger og funn fra testerne. Funn gjennomgås jevnlig for å sikre at ikke ukontrollert behandling skjer. Rapportere til styringsgruppe og personvernombud regelmessig.	*Redusert*	*Lav*	
Personopplysninger kommer på avveie **Brukerperspektiv** En bruker legger inn noen andre sine personopplysninger som kommer på avveie. Generell risiko for at brukere legger inn informasjon som er klassifisert som fortrolig/strengt fortrolig i input/prompt til M365 Copilot. (I denne fasen er det kun 5 personer som skal ha tilgang og risiko vurderes som ytterst minimal)	Opplæring av brukere Gjennomgå funksjonalitet i verktøy eDiscovery til å fjerne denne data hvis uhellet. Search for and delete Microsoft Copilot for Microsoft 365 data | Microsoft Learn	*Redusert*	*minimal*	
Personopplysninger kommer på avveie **Organisatorisk** NTNU klarer ikke følge teknologisk utvikling på en sikker måte Problemstillingen er ikke unik for dette KI-verktøyet og NTNU er i dette tilfellet proaktiv i møte med KI. Dette vil også kunne føre til	Grundig testing av verktøyet	*Redusert*	*Lav*	

generell økning av brukernes bevissthet rundt mulige negative konsekvenser og misbruk av slike verktøy i en tidlig fase. I tillegg er det rimelig å anta at ved å lansere et godt verktøy innenfor trygge rammer, reduserer man omfanget av "skygge-IT" blant brukerne, der personvern og sikkerhet ikke kan garanteres i samme grad.				
Ikke mulig å sikre samsvar mellom den registrertes rettigheter og den behandlingsansvarliges plikter etter Personvernforordningen (GDPR) For eksempel manglende rett til innsyn, sletting osv	Etablert konkrete oppfølgingspunkter i DPIA for å sikre samsvar mellom rettigheter og plikter. Alle funn i testperiode skal registreres. Full åpenhet om alle funn Datatilsynet skal bistå NTNU med å gjøre vurderinger i sandkasseprosjektet.	*Redusert*	*Medium*	*IT-direktør må eksplisitt godkjenne denne risikoen*
Manglende opplæring eller lav kompetanse hos bruker	NTNU utarbeider retningslinjer for bruk av generativ kunstig intelligens. Retningslinjer må oppdateres med innhold fra prosjektet hvis M365 Copilot skal settes i drift.	*Redusert*	*Lav*	
Manglende opplæring eller lav kompetanse hos bruker	Tema «hvordan skal vi forholde oss til Kunstig intelligens?», «hva slags kjøreregler bør NTNU ha?» osv behandles i medvirknings- og medbestemmelsesorganer: - SESAM (06.11.2023) (* se referat fra møtet nedenfor) med styringsparametre for utvikling - Administrativt lederutvalg (24.11.2023) - Formøte Studenttinget (27.11.23) - Dekanmøtet (16.11.24)	*Redusert*	*Lav*	*Under gjennomføring,* *Ansvar for oppfølging Heine Skipenes*
Manglende fokus på programvareutvikling med innebygd personvern	Opplæring av de registrerte i Datatilsynets veileder for Programvareutvikling med innebygd personvern https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-	*Redusert*	*Lav*	

	plikter/programvareutvikling-med-innebygd-personvern/			

4. Ledelsens validering av personvernkonsekvensvurderingen (DPIA)

Moment	Navn og dato	Kommentarer
Tiltak godkjent av:	Håkon Alstad IT-direktør, 02.02.2024	
Restrisiko godkjent av:	Håkon Alstad IT-direktør, 02.02.2024	*Dersom restrisiko med høy risikograd blir godkjent, ta kontakt med Datatilsynet før oppstart for forhåndsdrøfting, jf. art. 36 nr. 1.*
Personvernombudsbistand gitt:	Thomas Helgesen, Personvernombud 01.02.2024 og 02.02.2024	*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:

Personvernombudet har gitt sine råd gjennom behandling i personvernklynga 01.02.2024, og på telefon med Heine Skipenes 01.02.2024. Sammendraget er laget av Heine Skipenes og godkjent av personvernombud muntlig pr telefon 02.02.2024: «Dette er et ambisiøst prosjekt med mange potensielle risikoelementer, og DPIAen kunne med fordel vært tydeligere på at vurderingen kun gjelder selve testsituasjonen. Det er veldig viktig at både de registrerte er klar over hvilket prosjekt de er med på, og organisasjonen rundt må fungere godt for å fange opp problematiske forhold tidlig. I og med at dette kun er fem personer som vil få tilgang er det viktig at de har tenkt godt gjennom på forhånd hva verktøyet får tilgang til av data, og at prosjektet stiller tydelige forventninger om at testerne på forhånd har:

- «**Rydd egen bruker**»: Gå gjennom alle filer, dokumenter og lagringsområder (for eksempel teamsområder) som brukere har for å sikre at ikke verktøyet får tilgang til data den ikke skal ha tilgang til (særlig andre sine personopplysninger, eller annen skjermingsverdig informasjon)
- «**Gå gjennom alle tilganger**»: Det er viktig at det kun er NTNU sine data som blir behandlet, Hvis bruker har tilgang til for eksempel shared channels med andre institusjoner må disse holdes utenfor. Gå gjennom tredjeparts programvare, add-ons osv for å sikre at dataflyten inn og ut er kontrollert.
- «**Si fra på forhånd om du bruker KI i samhandling med andre**»: Om testerne skal bruke KI-verktøy på andre sine personopplysninger må dette opplyses om på forhånd slik at den andre parten kan motsette seg. For eksempel: Hvis testerne bruker verktøyet i et teamsmøte må man si fra på starten hva man har tenkt til å gjøre, hvordan og hvor lenge data skal behandles og når det blir slettet. Hvis ikke alle samtykker skal ikke behandlingen gjennomføres.

Forventninger til prosjektet:

- **Etabler rutiner og systematikk** for innhenting av tilbakemeldinger og funn fra testerne. Dette må gjennomgås jevnlig for å sikre at ikke ukontrollert behandling skjer. Personvernombudet forventer å få tilgang til rapporter og funn.

- **Gjør ny vurdering hvis flere testere:** Denne DPIA er utarbeidet med en ytre grense på 5 testere. Viktig at prosjektet har fokus på skalerbarhet, og at nye vurderinger gjennomføres om flere skal ha tilgang. Flere registrerte inn i løsningen øker risikoen.
- **Avtalegjennomgang:** Prosjektet bør gjennomgå avtaler som er inngått med leverandøren, for å sikre at NTNU har full kontroll på avtaleverket og hvilke deler av «Microsoft-økosystemet» som påvirker hverandre. For eksempel kan prinsipper fra en selskapsgjennomgang (Due diligence) gjennomføres.

Så fremt tiltak og forventningene som fremkommer i dette dokumentet følges anses prosjektet å være innenfor akseptabelt risikonivå.»

Personvernombudets råd er akseptert eller overprøvd av:	Håkon Alstad IT-direktør, 07.02.2024	

Kommentarer:

Tilleggsvurdering til personvernkonsekvensvurdering datert 02.02.2024

Med utgangspunkt i Personvernombudets anbefalinger har de ansatte som skal teste løsningen (testerne) gitt følgende tilbakemeldinger som bør vurderes av behandlingsansvarlig. Merknader:

1. «Rydd egen bruker»: Det vil ikke være mulig å gjennomgå alle eposter/chatmeldinger før testing. Det er snakk om titusenvis av oppføringer, og er ikke realistisk før testing.
    1. Prosjektleders vurdering: Testerne har tilgang til store mengder data på sine personlige brukere gjennom mange års aktivitet, men det er veldig lite sannsynlig at det er snakk om annet enn arbeidsrelatert diskusjon, kommentarer og avklaringer. Ja det er personopplysninger, men det er snakk om navn/kontaktinformasjon knyttet til hvem som har sagt hva om et konkret tema. De ansatte behandler ikke særlige kategorier av personopplysninger og ingen har (eller har hatt) personalbehandling som en del av sine arbeidsoppgaver.
2. «Gå gjennom alle tilganger»: Tilgang til shared channels bør ikke holdes utenfor testfasen.
    1. Prosjektleders vurdering: Pr i dag er det kun ca 5-10 aktive shared channels på NTNU, og testerne jobber i dag med å rulle ut denne funksjonaliteten som en mer aktiv tjeneste for NTNUs brukere. Testerne bruker da egen bruker for å teste funksjonaliteten, og en begrensning i tilgangen vil ødelegge for annen aktivitet. I og med at det er veldig få eksisterende shared channels og det ikke deles skjermingsverdig informasjon i kanalene, anses risikoen for at noe skal skje som minimal.

Prosjektleder anbefaler at begge punktene aksepteres av behandlingsansvarlig og legges inn som tillegg til personvernkonsekvensvurderingen.

IT-direktør har godkjent endringer 07.02.2024

De registrertes synspunkter er innhentet og gjennomgått av:	Sendt ut på epost til alle de som skal ha tilgang. Deres tilbakemeldinger blir lagt ved her	*Hvis din avgjørelse avviker fra de registrertes synspunkter, bør du forklare bakgrunnen for at du velger å sette i gang/fortsette behandlingen*

Kommentarer:

Tilbakemeldinger mottatt fra de registrerte 06.02.2024, se tilleggsvurdering over

Denne personvernkonsekvensvurderingen vil følges opp av:	Heine Skipenes prosjektleder	*Personvernombudet bør også følge opp personvernkonsekvensvurderingen løpende, jf. art. 39 nr. 1 bokstav c.*

Vedlegg referat fra SESAM møte 06.11.2023 – STYRINGSSIGNALER FOR UTVIKLING

«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
    «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.»
- Wikiside på Innsida om Bing Chat Enterprise og alle vurderinger som er gjort
- 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