

## Forslag til personvernkonsekvensvurdering «Copilot for Microsoft 365» (Driftsfase)

Navn på system/prosjekt:	Copilot for Microsoft 365 ved NTNU (driftsfase)
DPIA-en utføres av:	Seksjon for virksomhetsstyring, Avdeling for utvikling og virksomhetsstyring Silje Reiten Blichfeldt (Kvalitetsikring Heine Skipenes)
Dato:	14.06.2024

### Merknader til den gjennomførte personvernkonsekvensvurderingen:

- Denne DPIAen er utformet etter metodikken skissert av WP29 i «Guidelines on Data Protection Impact Assessment». DPIAen vurderer personvernkonsekvensene av teknologiproduktet «Copilot for Microsoft 365», og må derfor anses som en overordnet DPIA som vurderer teknologien, og ikke personvernkonsekvensene pr. behandling av personopplysninger. Det anbefales at alle organisasjoner gjennomfører en egen DPIA som anses å være passende til sitt bruk av M365 Copilot.
- Denne DPIAen gjelder utelukkende en driftsfase for verktøyet Copilot for Microsoft 365, og er levert som del av prosjektet Pilotere Copilot for Microsoft 365 i Datatilsynets regulatoriske sandkasse. Det er utviklet en egen DPIA for testfasen av verktøyet (datert 07.02.2024): <https://www.ntnu.no/adm/it/copilot/verktoykasse/m365-copilot-test>
- NTNU har også skrudd på et KI-verktøy for studenter og ansatte som også heter «Microsoft Copilot». Copilot for Microsoft 365 og KI-verktøyet for studenter og ansatte er to forskjellige tjenester, og det er utviklet en egen DPIA for utrulling av Microsoft Copilot for studenter og ansatte fra (datert 27.02-2024): <https://www.ntnu.no/web/adm-it/microsoft-copilot-ki-verktoy-for-studenter-og-ansatte>
- Definisjonen på «Copilot for Microsoft 365» som brukes gjennom hele DPIAen er «**M365 Copilot**» og kan defineres både som verktøy og KI-funksjonalitet. Dette prosjektet har ikke testet andre copiloter enn M365 Copilot.
- I DPIAen for testfasen ble det identifisert 22 problemstillinger vi ikke kunne svare på. Disse problemstillingene er vurdert i en rekke utfyllende vurderinger som er bakt inn i denne DPIAen.
- 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.
- DPIAen er utarbeidet med utgangspunkt i styringssignaler gitt i NTNUs Sentrale samarbeidsorgan (SESAM) 06.11.2023. Saken «Verktøy med kunstig intelligens ved NTNU» ble behandlet som sak 81/23 med overordnet 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 DPIAen.

- 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 lesingen lettere har vi markert særlig utfordrende områder med **gult**. Vi har i tillegg presisert en del temaer, spørsmål og områder som man bør ha spesielt oppmerksomhet på i egen organisasjon. Disse temaene er markert med **grønt**.

# 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 våren 2024 gjennomført prosjektet «Pilotere Microsoft 365 Copilot» i Datatilsynets regulatoriske sandkasse for personvernvennlig innovasjon og digitalisering våren 2024. M365 Copilot er neste generasjons KI-verktøy, og pilotprosjektet skulle teste om Microsofts kunstige intelligente assistent kan bli tatt i bruk i en stor offentlig organisasjon. Det som er spesielt med M365 Copilot er at KI-funksjonaliteten blir integrert i allerede eksisterende Microsoft-tjenester som Word, Excel, Powerpoint, Teams, Sharepoint, Outlook osv, og kan derfor 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, og kan derfor defineres som en «klone» av brukeren med identiske tilganger. Brukeren vil ikke få tilgang til data med M365 Copilot, som brukeren ikke hadde tilgang til fra før. Forskjellen er at M365 Copilot bringer mer av dataen brukeren allerede har tilgang til, til overflaten.

**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 utstyrt med en egen fysisk Copilot-knapp. Samtaleroboten som før het Bing Chat Enterprise har blitt omdøpt til Microsoft Copilot og er gjort tilgjengelig for alle brukere.

M365 Copilot er kostnadskrevende og NTNU har tatt utgangspunktet i at M365 Copilot vil koste ca. 5000 kr pr bruker pr år i økte lisensutgifter. Dette kommer i tillegg til eksisterende kostnader og annen prisutvikling.

NTNU må sørge for at alle vurderinger av informasjonssikkerhet og personvern er ivarettatt når digitale verktøy benyttes. Når KI verktøy som samtaleroboter med innebygget generativ kunstig intelligens skal tilbys alle brukere, har NTNU lagt til grunn at det er riktig å gjennomføre en full personvernkonsekvensvurdering (DPIA) jf. Personvernforordningens artikkel 35, nr. 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.*»)

#### **Behandlingsansvarlig**

- NTNU er 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/>  
NB: Dokumentasjonen på nettsidene endrer seg jevnlig, så det er viktig å følge med på hva som gjelder for egen organisasjon.
- Se lenkesamling til slutt i dokumentet

## **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?	Personopplysningene samles inn på ulike måter: <ul style="list-style-type: none"><li>• fra kjernesystemer (navn, epostadresse, brukernavn osv)</li><li>• at den registrerte selv oppgir sine egne personopplysninger (for eksempel direkte i epost eller dokumenter)</li><li>• andre har oppgitt personopplysninger om den registrerte (lager dokumenter med andre sine opplysninger)</li><li>• Opptak av møter i Teams og transkripsjon av gjennomførte møter (kan også være fysiske møter i rom hvor Teams lytter inn)</li><li>• Samhandling med M365 Copilot ved prompts. Svar fra M365 Copilot kan føre til innsamling av personopplysninger da en bruker kan skrive inn personopplysninger i prompten og be M365 Copilot om å få personopplysninger i svaret.</li></ul>
--	--

	<p>Personopplysninger kan da genereres i M365 Copilot sin respons.</p> <p>Det vil i tillegg samles inn indirekte personopplysninger via de registrertes bruk av verktøyene i Microsoft 365, disse samles inn via deling av personopplysninger i for eksempel chat i Teams, lagring av filer som inneholder personopplysninger eller deling av personopplysninger i Outlook.</p> <p>M365 Copilot vil lage nye personopplysninger om de registrerte ved å sammenstille informasjon som finnes i Teams chat, epost, filer og samhandling mellom personer.</p> <p><i>Se utfyllende vurdering: Punkt 1.2 og 1.3 «Behandlingens art og behandlingens omfang»</i></p>
<p>Hvordan skal personopplysningene lagres?</p>	<p>Personopplysningene som behandles av M365 Copilot lagres på ulike måter:</p> <ul style="list-style-type: none"> <li>• Brukerdata lagres direkte i et Microsoft-verktøy sin kobling til NTNUs Microsoft tenant</li> <li>• Filer som kan inneholde personopplysninger kan være lagret i en brukers OneDrive, SharePoint, på en epostkonto, i chatlogger i Teams</li> <li>• Chatlogger etter prompting og svar fra M365 Copilot i hver enkelt brukers logg ligger lagret i en mappe i Exchange som brukeren selv ikke har tilgang til</li> </ul> <p>Listen er ikke uttømmende, men det er en fellesnevner at noder/verktøy og koblinger som blir gjort tilgjengelig for Graph blir behandlet av M365 Copilot og indeksert.</p> <p><i>Se utfyllende vurdering: Punkt 1.2 og 1.3 «Behandlingens art og behandlingens omfang»</i></p>
<p>Hvordan skal personopplysningene brukes?</p>	<p>Personopplysninger i Microsoft 365 brukes på mange måter. Personopplysninger vil bli brukt til identifisering ved pålogging, samhandling, filbehandling etc. All bruk av personopplysninger i Microsoft applikasjoner vil deretter bli indeksert og behandlet av Graph'en.</p> <p>Når M365 Copilot får tilgang til personopplysninger via Microsoft Graph kan opplysningene bli behandlet, men det er ikke forutsigbart hvordan personopplysningene vil bli behandlet og i hvilken kontekst. M365 Copilot beskriver selv hvordan dette gjøres på følgende måte:</p> <p><i>«Microsoft Graph er en API som gir utviklere tilgang til data og tjenester i Microsoft 365, inkludert brukerprofiler, e-post, kalendere, filer, kontakter, grupper, sikkerhet, enheter og mer. Den tilbyr en enhetlig måte å programmere mot data fra ulike</i></p>

	<p><i>Microsoft-tjenester og indekserer innhold og signaler fra de fleste Microsoft 365-applikasjoner i organisasjonen din. Når du søker etter noe, bruker Microsoft Graph indeksen til å rangere de mest relevante resultatene basert på personlige forbindelser og sosiale relasjoner.</i></p> <p><i>Semantic Index er en ny funksjon i Microsoft 365-søk som bruker Microsoft Graph for å bedre samhandle med dine personlige og organisatoriske data. Den skaper en ny indeks som muliggjør fremtidige søke- og Copilot-opplevelser og følger sikkerhets- og policyreglene til Microsoft Graph. Bare innhold som en bruker har tilgang til, vises i søket eller i Microsoft Copilot. Den semantiske indeksen forbedrer funksjonene i Microsoft 365 som lar deg finne relevant innhold basert på nøkkelord, personlige preferanser og sosiale forbindelser.</i></p> <p><i>Den oppretter vektoriserte indekser som muliggjør konseptuell forståelse og hjelper deg med å finne det du leter etter og få tilgang til organisatorisk innhold. En vektor er en numerisk representasjon av et ord, bildepiksel eller annet datapunkt, ordnet eller kartlagt med nærliggende tall for å representere likhet.</i></p> <p><i>Se utfyllende vurdering: Punkt 1.2 og 1.3 «Behandlingens art og behandlingens omfang»</i></p>
Hvem skal ha tilgang til personopplysningene?	Microsoft som databehandler NTNU som behandlingsansvarlig
Hvem skal det samles inn personopplysninger om?	<p>Ansatte Studenter Eksterne (for eksempel via shared channels) Forskningsdeltakere Potensielle studenter Personer som henvender seg til NTNU (via epost eller skjemaverktøy som videresender til epostlister)</p> <p>Den store mengden registrerte som NTNU på et tidspunkt tidligere har behandlet personopplysningene til. Dette kan være uklassifiserte/ukrypterte filer som ikke er slettet og som ligger på en brukers lagringsområde/epost osv.</p>
Hvordan kan den registrerte utøve sine rettigheter?	<p>Retten til informasjon vil bli ivaretatt ved å informere om behandling av personopplysninger i personvernerklæringen til NTNU.</p> <p>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 <a href="https://innsida.ntnu.no/wiki/-/wiki/Norsk/Personvernerklæring+NTNU">https://innsida.ntnu.no/wiki/-/wiki/Norsk/Personvernerklæring+NTNU</a></p>

	<p>Det blir i tillegg utviklet en egen modul for innsyn etter GDPR gjennom prosjektet NTNU Sak. <b>Tilgangene som M365 Copilot har inngår i datagrunnlaget med personopplysninger som Microsoft vet om NTNUs brukere.</b></p> <p>Den registrerte kan henvende seg til NTNU som behandlingsansvarlig for å be om sletting, retting og begrensning. NTNU vil da gjøre en vurdering om hvorvidt dette kan la seg gjøre etter personvernforordningen og jf. lovverk som arkivloven, forvaltningsloven og regnskapsloven m.fl.</p>
Vil det være systematisk behandling av personopplysninger?	<b>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.</b>
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	<p>M365 Copilot vil behandle samme data som Microsoft 365 plattformen i tråd med NTNUs lagringsguide (<a href="https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide">https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide</a>) og er godkjent for klassifiseringene åpen, intern og fortrolig informasjon med de forbehold som gjelder. Løsningen blir ikke godkjent til strengt fortrolig.</p> <p>M365 Copilot vil behandle vanlige og personopplysninger av særlig kategorier jf. Personvernforordningens artikkel 9. M365 Copilot behandler alle personopplysninger som både tilgjengeliggjøres via prompts, men også personopplysninger som hver enkelt bruker har tilgang til via sine filer, alle eposter som ligger lagret i alle postkasser, chatter etc. <b>M365 Copilot kan også behandle data fra web og M365 Copilot sin kommando ut mot web kan inneholde personopplysninger.</b> Kategorisering av personopplysninger som kan bli hentet fra web er vanskelig, men man bør anta at M365 Copilot kan behandle alle kategorier personopplysninger i det den henter innhold fra web.</p>
Antall registrerte involvert i behandlingen	<p><b>Antall brukere (dvs. personer ved NTNU med M365 Copilot-lisens) av tjenesten er ikke definert for driftsfasen da dette henger sammen med oppfølging av DPIAens tiltaksliste, hvem som har tjenstlig behov osv.</b></p> <p>Antall registrerte involvert i behandlingen vil avhenge av hvorvidt NTNU tilgjengeliggjør tjenesten for eksempelvis 10,</p>

	<p>50, 100 brukere, alle ansatte (8000) eller alle ansatte og studenter (tilsvarende 43 000 studenter og 8000 ansatte).</p> <p>Antall registrerte avhenger av hvor mange brukere som har tilgang til M365 Copilot og hvem dette er. Antallet avhenger av brukernes tilgang til personopplysninger i sine filer, epostkasser, chatmeldinger, samhandling etc. Alle personopplysninger en bruker har tilgang til i Microsoft 365 vil bli behandlet av M365 Copilot, og derav vil antallet registrerte være høyt, men vanskelig å tallfeste eksakt.</p> <p>Uansett tilnæringsmåte bør antallet registrerte regnes som høyt da dette vil påvirke risikobildet.</p>
Datavolum	<p>Det er avhengig av hva brukerne har tilgang til i sine filer, chatter, epostkasser etc. og hva brukerne har tilgang til ved bruk av applikasjoner i M365 og via prompting med M365 Copilot.</p>
Behandlingsfrekvens	<p><b>Kontinuerlig.</b> Personopplysninger vil behandles kontinuerlig ved bruk av M365 Copilot. Dette gjelder både de brukerne som har M365 Copilot lisens (påloggingsinfo etc), og de registrertes personopplysninger som behandles i applikasjonene i M365 (Teams, Word, Outlook etc) og som er tilgjengelig for brukerne.</p>
Lagringstid for personopplysningene	<p>Personopplysningene som behandles av M365 Copilot lagres på ulike måter:</p> <ul style="list-style-type: none"> <li>• Brukerdata lagres direkte i et Microsoft-verktøy sin kobling til NTNUs Microsoft tenant</li> <li>• Filer som kan inneholde personopplysninger kan være lagret i en brukers OneDrive, Sharepoint, på en epostkonto, i chatlogger i Teams</li> <li>• [...]</li> </ul> <p>Listen er ikke uttømmende, men det er en fellesnevner at noder/verktøy og koblinger som blir gjort tilgjengelig for Graph blir behandlet av M365 Copilot og indeksert.</p> <p>Ved å samhandle med M365 Copilot ved at en registrert legger inn prompts og mottar svar, vil Microsoft lagre data om samhandlingen. Hva som er skrevet, hvilket svar M365 Copilot har gitt, og informasjon som brukes til å forankre M365 Copilots svar.</p> <p><i>Se utfyllende vurdering: Punkt 1.2 og 1.3 «Behandlingens art og behandlingens omfang»</i></p> <p>Innstillinger for lagring, mellomlagring og sletting er tilgjengelig for organisasjonens administratorer. Microsoft</p>

	<p>opererer med «retention policies» (retningslinjer for oppbevaring) som kan administreres på ulike måter for de ulike appene innenfor «Modern work»-programvarene i Microsoft 365. «Retention policies» kan implementeres for å bestemme hvor lenge data skal behandles (lagres), og hva som skal skje med dataene når de ikke lenger er nødvendige.</p> <p><i>Se utfyllende vurdering: Punkt 1.8 – Dataflyt, lagring og mellomlagring»</i></p>
Geografisk omfang	<p>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.</p> <p>Dette innebærer at M365 Copilot på NTNUs tenant kan bli benyttet fra hvor som helst i verden der brukerne er.</p>

#### 4. **Behandlingens formål**

Behandlingens formål	<p>Det er komplisert å definere ett eller flere klare og tydelige formål for bruk av M365 Copilot i tråd med Personvernforordningens artikler 5 og 6. M365 Copilot er bygd som en tilleggsfunksjonalitet inni allerede eksisterende verktøy som tekstbehandling, epost, regneverktøy osv. Behandlingens formål må derfor ses i direkte sammenheng med bruken av allerede eksisterende verktøy hvor M365 Copilot blir en "forsterker" både med tanke på effektivitet, behandlingsomfang av personopplysninger og risiko.</p> <p>Bruken av M365 Copilot kan direkte relateres til NTNUs egne retningslinjer for behovet for vurdering av personvernkonsekvenser: <i>Punkt "8. Innovativ bruk eller anvendelse av ny teknologisk eller organisatorisk løsning [...] bruk av ny teknologi som defineres «i samsvar med det oppnådde nivået av teknisk kunnskap» kan medføre behov for å gjennomføre en vurdering av personvernkonsekvenser. Grunnen til dette er at anvendelse av ny teknologi kan medføre nye former for innsamling og bruk av personopplysninger, eventuelt med høy risiko for den enkeltes rettigheter og friheter. De personlige og sosiale konsekvensene ved anvendelsen av ny teknologi kan være ukjente. En vurdering av personvernkonsekvenser hjelper den behandlingsansvarlige å forstå og håndtere slike risikoer. For eksempel kan visse «tingenes internett»-applikasjoner få betydelige konsekvenser for den enkeltes dagligliv og privatliv, og kan derfor kreve en vurdering av personvernkonsekvenser.»</i></p>
----------------------	--



	<p><a href="https://i.ntnu.no/wiki/-/wiki/Norsk/Vurdere+personvernkonsekvenser">https://i.ntnu.no/wiki/-/wiki/Norsk/Vurdere+personvernkonsekvenser</a></p> <p>På bakgrunn av dette må konklusjonen være at beskrivelse av behandlingens formål for bruk av M365 Copilot må ses i direkte sammenheng med bruk av allerede eksisterende Microsoft-verktøy. Dette kan gjøres gjennom eksisterende rammeverk og oversikt over saksprosesser i protokoll/behandlingsoversikt. Bruk av verktøy med innebygd kunstig intelligens og M365 Copilot særskilt må kartlegges, dokumenteres og vurderes pr saksprosess av den prosessansvarlige.</p> <p><b>NB: Bruk av verktøy med innebygd kunstig intelligens må følges opp kontinuerlig. Det blir viktig med gode interne prosedyrer og retningslinjer. NTNU har valgt å se dette i sammenheng med oppfølging av protokoll/oversikt over behandling av personopplysninger.</b></p>
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?	<p>Da NTNU testet M365 Copilot ble funksjoner som kan brukes til å profilere de registrerte identifisert. Det er uklart hvorvidt dette er formålet til de aktuelle funksjonene, og om utfallet av denne behandlingen regnes som profilering, men NTNU vurderer det dithen at ved bruk av de aktuelle funksjonene vil profilering sannsynligvis skje.</p> <p><i>Se utfyllende vurdering: Punkt 1.4 – Behandlingens formål» og «Punkt 2.2 – De registrertes rettigheter</i></p>
Brukes personopplysninger for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte?	<p>NTNUs formål er ikke å bruke personopplysningene til å avdekke ukjente sider eller gjenkjenne mønstre ved den registrerte.</p> <p>Da NTNU testet M365 Copilot ble funksjoner som kan brukes til å avdekke ukjente sider eller gjenkjenne mønstre ved den registrerte identifisert.</p>

	<p>Eks: En bruker kan spørre M365 Copilot om hvilken sinnsstemning en navngitt person er i, basert på samhandling i bl.a. chat. M365 Copilot responderer med å analysere innhold i samhandling mellom brukerne, og gi en vurdering av gitte brukers «mood».</p> <p><i>Se utfyllende vurdering: Punkt 1.2 og 1.3 – Behandlingens art og behandlingens omfang</i>  <i>og</i>  <i>utfyllende vurdering: Punkt 1.4 – Behandlingens formål</i></p> <p>Selv om NTNUs formål ved å ta verktøyet i bruk ikke er å avdekke ukjente sider eller gjenkjenne mønstre, må NTNU anta at så lenge funksjonen er tilgjengelig for brukere, vil behandlingen skje. Det er derfor nødvendig å vurdere tekniske og organisatoriske tiltak fortløpende for å motvirke feilaktig bruk.</p>
<p>Vil personopplysningene viderebehandles til nye eller andre formål?</p>	<p>Da NTNU testet M365 Copilot ble det identifisert funksjoner som gjør at personopplysninger samlet inn for ett formål vil bli viderebrukt til nye eller andre formål.</p> <p>I og med at M365 Copilot bruker personopplysninger som kan ligge lagret i epostkasser, Teams chat og annen samhandling mellom brukere, kan man anse at personopplysningene vil bli viderebehandlet til nye eller andre formål.</p> <p>Det er derfor nødvendig å vurdere tekniske og organisatoriske tiltak fortløpende for å motvirke feilaktig bruk.</p>

## 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.

<p>Hvilke kilder brukes for innhenting av personopplysninger?</p>	<p>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»</p> <p>Alle personopplysninger vil behandles på tvers av de ulike tjenestene.</p> <p>Eksempler på kilder som brukes for innhenting av personopplysninger er: Profiler, dokumenter, eposter (innboks, sendte eposter, slettede elementer etc), Teams, samhandling som chatlogger etc.</p>
---	--

	<p><i>Se utfyllende vurdering: Punkt 1.5 – Sammenhengen behandlingen utføres i (kontekst)</i></p>
<p>Relasjon mellom behandlingsansvarlig og den registrerte</p>	<p>De registrerte er alle som har fått sine personopplysninger behandlet i Microsoft applikasjonene som brukerne av verktøyet har tilgang til, jf. punkt 2. Ved NTNU vil det si at det er ansatte, studenter, potensielle studenter som samhandler med organisasjonen, forskningsdeltakere, eksterne/gjestbrukere etc.</p> <p>Relasjonen mellom behandlingsansvarlig og de registrerte kan i mange av disse tilfellene anses som et skjevt maktforhold (for eksempel arbeidstaker – arbeidsgiver, student-veileder osv).</p> <p>Det er derfor nødvendig å vurdere tekniske, organisatoriske og pedagogiske tiltak fortløpende for å motvirke feilaktig bruk og for å sikre god informasjon til alle involverte parter.</p>
<p>I hvilken grad har den registrerte kontroll over sine opplysninger?</p>	<p>De registrerte har til en viss grad kontroll over egne personopplysninger som de selv deler i epost utvekslinger og Teams chat meldinger og interaksjoner/reaksjoner på innlegg i Teams-kanaler. Eksempelvis kan en bruker slette sin kommentar til et innlegg, slik at denne ikke lenger er synlig for andre brukere i Teams.</p> <p>En bruker med M365 Copilot-lisens kan også slette egen historikk i M365 Copilot via Settings &amp; Privacy innstillinger. Dette kan inkludere sletting av egne og andre registrertes personopplysninger.</p> <p>En registrert kan be om 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 <a href="https://innsida.ntnu.no/wiki/wiki/Norsk/Personvernerklæring+NTNU">https://innsida.ntnu.no/wiki/wiki/Norsk/Personvernerklæring+NTNU</a></p> <p>Den registrerte har ikke mulighet til å ha full kontroll over all behandling av sine personopplysninger i M365 Copilot. Gjennom de tekniske mekanismene i M365 Copilot kan en registrert ha delvis kontroll over personopplysninger den selv legger inn i verktøy som har M365 Copilot tilkoblet, men den registrerte har ikke kontroll over hvordan andre brukere/registrerte behandler ens personopplysninger.</p> <p>NTNU som behandlingsansvarlig vil kunne ha en viss grad av kontroll over de registrertes personopplysninger ved bruk av M365 Copilot, men dette forutsetter at de saksprosessene som tillater bruk av M365 Copilot i oppgaveutførelsen også kartlegger bruk og registrerer dette i NTNUs behandlingsprotokoll. Det er viktig med gode internkontrollrutiner for systematisk oppfølging av dette området.</p>

	<p><i>Se utfyllende vurdering: Punkt 1.5 – Sammenhengen behandlingen utføres i (kontekst)</i></p>
<p>Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel</p>	<p>Behandlingen av personopplysninger i M365 Copilot vil kunne oppfattes ulikt av de registrerte, avhengig av deres rolle, forventninger, kunnskap og erfaring med Copilot-verktøy og KI-funksjonalitet for øvrig. NTNU antar at de færreste vil ha direkte erfaring eller høy kunnskap om bruk av M365 Copilot, men mange vil kunne ha både høy og lav generell kunnskap og erfaring med bruk av språkmodeller (LLM/LMM) generelt.</p> <p>De registrerte vil også ha ulike forventninger til hvordan deres personopplysninger blir behandlet av M365 Copilot, avhengig av hvilken informasjon de har fått, hvilket formål behandlingen har, og hvilken nytte eller risiko de opplever med NTNUs bruk av M365 Copilot.</p> <p>De registrerte vil også ha ulike nivåer av kunnskap og erfaring med M365 Copilot, som kan påvirke hvordan de oppfatter behandlingen av sine personopplysninger. For eksempel vil en registrert som har god kunnskap om hvordan M365 Copilot fungerer, hvilke data den bruker, og hvordan den kan styres, kanskje oppleve behandlingen som mer forutsigbar og håndterbar enn en registrert som har liten eller ingen kunnskap om dette. Den registrerte kan i ytterste fall ikke ha kunnskap om at den blir «en registrert» ved at hen har tatt kontakt med organisasjonen (gjennom f.eks gjennom å sende en epost.)</p> <p>NTNU har gjennom prosjektets gang diskutert denne problemstillingen med ulike aktører, og en gjentagende tilbakemelding er: For de registrerte som ikke har god kunnskap om hvordan M365 Copilot fungerer, kan behandlingen fremstå som uoversiktlig og uklar, og man er avhengig av tillit til behandlingsansvarlig og til systemleverandøren.</p> <p>NTNU må gjennomgå og tilgjengeliggjøre informasjon til de registrerte, og informere om hvordan behandlingen foregår, og hvilke personopplysninger som behandles. Det vil være mange registrerte som har lite eller ingen kunnskap om hvordan kunstig intelligente verktøy behandler personopplysninger. Dette temaet må vurderes kontinuerlig for å sikre nødvendig kompetanse i organisasjonen og ivaretagelse av informasjonsplikten i tråd med teknologiutviklingen.</p>

<p>Vil den registrerte ha en særskilt forventning om konfidensialitet?</p>	<p>Den registrerte vil ha forventning om at NTNU behandler personopplysninger (spesielt særlige kategorier) og annen data av fortrolig karakter med konfidensialitet.</p> <p><a href="https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide">Office 365 (SharePoint, Teams, Onedrive)</a> er klassifisert opp til fortrolig jf. NTNUs lagringsguide <a href="https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide">https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide</a> så fremt innholdet er kryptert med AIP.</p> <p>Gitt M365 Copilots natur og funksjon, vil verktøyet kunne behandle personopplysninger (og annen informasjon) av fortrolig kategori, samt personopplysninger av særlig kategorier. Den registrerte vil forvente at NTNU behandler disse opplysningene trygt og konfidensielt (så lukket som nødvendig).</p>
<p>Vil den registrerte ha en særskilt forventning om at personopplysningene er nødvendige og korrekte?</p>	<p>Ja, i en del behandlinger som utføres i Microsoft 365 og M365 Copilot vil den registrerte ha en forventning om at personopplysningene som behandles er nødvendige og korrekte.</p> <p>Den registrerte kan også ha en viss forståelse for at personopplysningene som behandles nødvendigvis ikke er korrekte.</p> <p>Dette vil begrenses til en viss type behandling, da særlig ved prompting og svar fra Copilot som involverer personer. Dette ligger i naturen til en språkmodell. Det kan forekomme blant annet hallusinerer som gjør at personopplysningene nødvendigvis ikke er korrekte. <b>Det er sannsynlig at M365 Copilot vil kunne finne på ting som både er usann og feilaktig.</b></p> <p>Informasjon om dette vil inngå i informasjonen som gis de registrerte i form av personvernerklæring og tilgjengeliggjøring av DPIA, samt opplæring i organisasjonen.</p>
<p>Vil den registrerte ha en særskilt forventning om privatliv?</p>	<p><b>Ja, den registrerte vil i en del behandlinger ha en særskilt forventning om privatliv.</b></p> <p>Personopplysninger innhentes fra kilder som blant annet Teams chat og epost. Den registrerte vil ha en særskilt forventning om at informasjon i den enkeltes epostkasse og Teams chat er private, og vil derav kommunisere på en mer privat måte enn når man kommuniserer åpent i Teams.</p>
<p>Vil det behandles personopplysninger om barn, pasienter eller andre kategorier av personer som defineres som sårbare?</p>	<p><b>Ja, det kan forekomme behandling av personopplysninger om personer som defineres som sårbare, eksempelvis barn, pasienter, forskningsdeltakere etc.</b></p> <p>Selv om NTNUs hovedformål med bruk av M365 Copilot som verktøy ikke innebærer behandling av ovennevnte kategorier registrerte, vil det kunne forekomme behandling av dette, da Copilot og Graph'en har tilgang til eksempelvis all epost i epostkassene til brukerne, samt alle filer som brukerne har</p>

	<p>tilgang til. I disse områdene vil det kunne forekomme behandling av ovennevnte kategorier registrerte og særskilte kategorier personopplysninger.</p>
<p>Finnes det tidligere erfaring med tilsvarende type behandling?</p>	<p>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 verktøy som ChatGPT og Grammarly har vært kjent og flittig i bruk samfunnet en stund, og NTNU har tidligere laget generelle retningslinjer og retningslinjer for spesielle områder allerede (eksamen og undervisning) <a href="https://i.ntnu.no/wiki/-/wiki/Norsk/Kunstig+intelligens+i+undervisning+og+vurdering">https://i.ntnu.no/wiki/-/wiki/Norsk/Kunstig+intelligens+i+undervisning+og+vurdering</a></p> <p>NTNU har tilgjengeliggjort Microsoft Copilot (tidligere Bing Chat Enterprise) for alle studenter og ansatte. Bruk av denne versjonen av «Copilot-verktøy» vil anses som en forberedelse og en opplæring av organisasjonen i bruk av kunstig intelligens og språkmodeller. I den forbindelse vil både NTNU som behandlingsansvarlig og de registrerte erfare ansvaret som behandlingsansvarlig, og hvordan bruke et slik verktøy som registrert. Denne bruken vil til en viss grad kunne tilsi at både NTNU som behandlingsansvarlig og de registrerte har erfaring med en lignende behandling.</p>
<p>Beskriv eventuelle relevante fremskritt innen teknologi eller sikkerhet</p>	<p>Utdrag fra <a href="https://snl.no/språkmodell">https://snl.no/språkmodell</a> (05.06.2024):  <b>«Nyere språkmodeller</b></p> <p><i>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 telle forekomster av ordkombinasjoner eksplisitt, bruker man i dag nevrane nettverk for å lære sammenhengen mellom ord implisitt.</i></p> <p><i>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.</i></p> <p><i>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.»</i></p>

<p>Finnes det noen nåværende tilfeller av allmenn bekymring for den beskrevne måten å behandle personopplysninger på?</p>	<p>Ja, i aller høyeste grad. Dette gjelder særlig i forbindelse med utøvelse av offentlig myndighet:</p> <ul style="list-style-type: none"> <li>• Dutch scandal (<u>diskriminerende algoritmer</u>)</li> <li>• Eksamensjuks</li> <li>• Forvaltningsrevisjon fra Riksrevisjonen: <u>Bruk av kunstig intelligens i staten</u></li> <li>• Diskriminering, manglende likebehandling osv osv. For eksempel <a href="https://www.bufdir.no/aktuelt/ny-rapport-lite-kunnskap-og-kompetanse-om-kunstig-intelligens-og-diskriminering/">https://www.bufdir.no/aktuelt/ny-rapport-lite-kunnskap-og-kompetanse-om-kunstig-intelligens-og-diskriminering/</a></li> </ul> <p>Den beskrevne måten å behandle personopplysninger på i M365 Copilot 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.</p> <p>Dette er et verktøy som kan <b>gjøre det lettere for studentene å jukse</b>. 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.</p>
<p>Vil dere behandle personopplysninger fra ulike datasett, som er innsamlet for ulike formål og fra ulike behandlingsansvarlige?</p>	<p>Ja. Et datasett settes sammen med et annet datasett for å kunne finne hittil ukjente sammenhenger. Vi kan ikke utelukke at datasettene inneholder personopplysninger.</p> <p>Grunnet måten M365 Copilot er bygd opp på, vil en slik behandling forekomme kontinuerlig ved bruk av M365 Copilot i ulike applikasjoner i Microsoft 365. M365 Copilot vil samle inn data, inkludert personopplysninger fra alle filer, epost, chatmeldinger, kalenderoppføringer, etc, en bruker har tilgang til, uavhengig av formålet de har blitt innsamlet for, og sammenstille disse og kunne finne nye sammenhenger.</p> <p>Ved forskningsprosjekt i samarbeid med andre forskningsinstitusjoner er ofte NTNU databehandler. Det kan forekomme datautlevering fra behandlingsansvarlig i forskningsprosjekt, som deretter vil bli behandlet i NTNUs Microsoft 365-tenant. M365 Copilot vil dermed kunne behandle personopplysninger som er innsamlet fra ulike behandlingsansvarlige og for helt andre formål. <b>Dette bør tas med i prosjektvurderinger.</b></p>
<p>Kobles ulike registre for å gi ny type informasjon om den registrerte?</p>	<p>Ja. Med utgangspunkt i SNL sin betegnelse om hva et register er (<a href="https://snl.no/register_-_IT">https://snl.no/register - IT</a>): «<b>Register som en samling av data</b> 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,</p>

	<p><i>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 [...]»</i></p> <p>Ut fra beskrivelsen vil det forekomme sammenkobling av ulike registre for å gi ny type informasjon om en registrert. Copilot i Teams kan blant annet lese og analysere hvordan en registrert har samhandlet i kanaler og chatmeldinger i Teams, i epostutvekslinger og i filer, og deretter analysere den registrertes humør.</p>
--	---

## 6. Identifisering og oversikt

Behandlingsansvarlig:	NTNU
Felles behandlingsansvarlig:	<p><b>Nei</b></p> <p>NTNU har i denne DPIAen vurdert Microsoft kun som databehandler, og ikke felles behandlingsansvarlig. Dette bør på sikt revurderes, i tråd med EDPS sin undersøkelse av EU-kommisjonen sin bruk av Microsoft 365:</p> <p><a href="https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en">https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en</a></p>
Databehandler(e):	Microsoft

## 7. Mottakere av personopplysninger

Beskriv alle mottakere/kategorier av mottakere av personopplysninger	<p>NTNU som behandlingsansvarlig</p> <p>Microsoft som databehandler</p> <p>Microsofts underleverandører</p>
Hvordan deles personopplysningene mellom avdelinger <b>internt</b> i virksomheten?	<p>M365 Copilot får tilgang til akkurat det samme som brukeren har tilgang til. Ettersom ansatte jobber og deler informasjon og personopplysninger på tvers av enheter, vil personopplysninger som brukeren har tilgang til deles internt i organisasjonen. M365 Copilot bruker Microsoft Graph som fungerer slik at den sammen med M365 Copilot gir tilgang til organisasjonens data, men kun data som brukeren allerede har tilgang til. M365 Copilot har tilgang til alle åpne team og dokumenter, dette er informasjon inkludert personopplysninger som kan deles internt i organisasjonen, også på en utilsiktet måte.</p> <p><i>Se Utfyllende vurdering: Punkt 1.7 – Mottakere av personopplysninger</i></p>
Hvilke <b>eksterne</b> virksomheter deles	<p>Personopplysningene deles med databehandler og databehandlers underleverandører. Det kan også forekomme</p>



<p>personopplysningene med? Hvis ja, for hvilke formål og med hvilke rettslige grunnlag?</p>	<p>deling av personopplysninger til eksterne aktører via web plugin og tredjepartsapplikasjoner.</p> <p>Rettslig grunnlag: Personvernforordningen artikkel 6, nr. 1 bokstav f – <b>Berettiget interesse</b></p> <p><i>Se utfyllende vurdering: Punkt 1.4 – Behandlingens formål</i></p>
<p>Overføres personopplysningene til land utenfor EU/EØS-området (tredjestater), jf. art. 44-49? Hvis ja, hva er det rettslige grunnlaget for det?</p>	<p>Microsoft oppgir at data fra kunder i EU blir behandlet innenfor EU Data Boundary. EU Data Boundary er en geografisk definert grense som Microsoft behandler og lagrer kundedata og personopplysninger for sine skytjenester, inkludert Microsoft 365. Dette innebærer alle EU- og EFTA-land. Microsoft definerer kundedata som all data, inkludert all tekst, lyd, video, bildefiler og software, som er tilgjengeliggjort for Microsoft.</p> <p>Ifølge Microsofts dokumentasjon vil det i noen tilfeller bli overført kundedata (inkludert personopplysninger) utenfor EU Data Boundary. Dette kan skje i form av at teknisk personell fra Microsoft må aksessere kundedata eller pseudonymiserte personopplysninger. Data blir ikke lagret utenfor EU Data Boundary selv om dataen aksesseres utenfra, videre oppgir Microsoft at de benytter kryptering som sikkerhetstiltak for å beskytte data under overføring.</p> <p>M365 Copilot har tilgang til websøk for å forbedre svar på prompts fra brukeren. Copilot henter informasjon relatert til brukerens prompt fra Bing search index. Copilot bruker ikke den opprinnelige prompten til å søke, men lager en ny tekst. Microsoft oppgir at bruker-ID og tenant-ID ikke er koblet mot søket som er sendt til Bing Search API.</p> <p><b>Ved bruk av tredjepartsapplikasjoner, Dataverse + power platform og plug-ins kan overføring til tredjeland forekomme.</b> Dette må vurderes fortløpende i forvaltning av Microsoft 365.</p> <p><i>Se Utfyllende vurdering: Punkt 1.7 B – Mottakere av personopplysninger – overføring til tredjeland»</i></p>
<p>Beskriv hvilke forholdsregler som tas for å beskytte personopplysninger</p>	<p>Forholdsregler for ansatte med tilgang til NTNUs systemer:</p> <p>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.</p> <p>IT-avdelingens ansatte med administratortilganger er underlagt egne retningslinjer og rammeverk for sikker drift, tilgang osv:</p>

	<p><a href="https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-retningslinjer">https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-retningslinjer</a></p> <ul style="list-style-type: none"> <li>• Retningslinje for arbeid med sikkerhetskultur og opplæring</li> <li>• Retningslinje for avviksmelding og avvikshåndtering innen informasjonssikkerhet og personvern</li> <li>• Retningslinje for behandling av personopplysninger</li> <li>• Retningslinje for digital beredskap, hendelses- og krisehåndtering</li> <li>• Retningslinje for informasjonssikkerhet i leverandørforhold</li> <li>• Retningslinje for klassifisering av informasjonsverdier</li> <li>• Retningslinje for kryptografiske kontroller</li> <li>• Retningslinje for nettverks- og informasjonsoverføring</li> <li>• Retningslinje for operativ sikkerhet</li> <li>• Retningslinje for risikostyring for informasjonssikkerhet</li> <li>• Retningslinje for sikring av personlig IKT-utstyr</li> <li>• Retningslinje for tilgangskontroll</li> </ul>
<p>Er alle databehandlere identifisert, og er forholdet til dem avklart gjennom avtaler, jf. art. 28 nr. 3?</p>	<p>Microsoft er databehandler, og har egne avtaler med sine underleverandører (underdatabehandlere).</p> <p>NTNU har innført sektoravtalen med Microsoft og har dermed akseptert Microsofts «Terms and conditions». Ved å akseptere disse vilkårene, inngås også databehandleravtalen med Microsoft. Databehandleravtalen som er inngått er en standard databehandleravtale.</p>
<p>Gir databehandleren tilstrekkelige garantier for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen, vil gjennomføres?</p>	<p>Microsoft oppgir at de gir tilstrekkelige garantier for at tekniske og organisatoriske tiltak som sikrer behandlingen vil gjennomføres.</p> <p>NTNU må ha et bevisst forhold til data som behandles innenfor egen tenant. Vilårene fra Microsoft er i kontinuerlig endring, og både lokale, overordnede avtaler og sammenhengen mellom disse, må NTNU ha oversikt over. NTNU gjennomgår tilgjengelig dokumentasjon som også innebærer å få oversikt over hvilke tekniske og organisatoriske tiltak som er beskrevet i juridisk bindende avtaleverk. Dette er et pågående og kontinuerlig arbeid som er tidkrevende og resultatet vil ikke ferdigstilles innen prosjektslutt.</p>

## 8. Dataflyt, lagring og mellomlagring

<p>Hvordan overføres og tilgjengeliggjøres personopplysningene?</p>	<p>Data, inkludert personopplysninger, tilgjengeliggjøres via Microsoft Graph hvor innhold kobles sammen, for eksempel filer, chat-meldinger, epost, samhandlinger i Teams etc.</p>
---	---

	Se skisser over dataflyt i « <i>Utfyllende vurdering: Punkt 1.8 – Dataflyt, lagring og mellomlagring</i> » og i punkt 3 i DPIA
Hvor og hvor lenge lagres personopplysningene ulike steder?	<p>Innstillinger for lagring, mellomlagring og sletting er tilgjengelig for organisasjonens administratorer. Microsoft opererer med «retention policies» (retningslinjer for oppbevaring) som kan administreres på ulike måter for de ulike appene i «Modern work»-plattformen. «Retention policies» kan implementeres for å bestemme hvor lenge data skal behandles (lagres), og hva som skal skje med dataene når de ikke lenger er nødvendige.</p> <p><i>Se utfyllende vurdering: Punkt 1.8 – Dataflyt, lagring og mellomlagring</i></p>
Hvor lenge lagres personopplysningene etter at formålet ved behandlingen er over, før de slettes? Når skal opplysningene slettes? Er det utarbeidet sletterutiner?	<p>«Retention policies» kan implementeres for å bestemme hvor lenge data skal behandles (lagres), og hva som skal skje med dataene når de ikke lenger er nødvendige.</p> <p><i>Se utfyllende vurdering: Punkt 1.8 – Dataflyt, lagring og mellomlagring</i></p>
Er personopplysningssikkerheten tilstrekkelig ivaretatt?	<p>Ved bruk av M365 Copilot vil det totalt sett behandles store mengder personopplysninger i flere ulike applikasjoner innenfor Microsofts «Modern work»-plattform. For å vurdere hvorvidt personopplysningssikkerheten ved bruk av M365 Copilot er ivaretatt, har vi tatt utgangspunkt i følgende klassifisering av informasjon: «åpen», «intern», «fortrolig» og «strengt fortrolig».</p> <p>I kategorien «åpen informasjon» vurderes det dithen at det ikke er stor risiko om informasjon i denne kategorien deles eller tilgjengeliggjøres. Personopplysninger vil finnes i denne kategorien, men vil være av den karakter som er offentlig delt. I kategorien «intern informasjon» finnes informasjon som kun skal være tilgjengelig for ansatte med formålstjenlig behov. Eksempler kan være arbeidsdokumenter, informasjon som er unntatt offentlighet og mange typer personopplysninger. Behandling av interne data i NTNUs Microsoft-tenant anses som tilfredsstillende.</p> <p>Fortrolig informasjon er informasjon som kan skade offentlige interesser, enkeltpersoner eller samarbeidspartnere hvis informasjonen kommer på avveie. Personopplysninger under særlig kategori faller innunder denne kategorien.</p>

M365 Copilot er ikke godkjent for strengt fortrolig informasjon.

*Se utfyllende vurdering: Punkt 1.8 B – Personopplysningssikkerhet»*

## 9. Informasjonssikkerhet

Gjennomgå den funksjonelle beskrivelsen av alle behandlinger og om alle aktiva som skal brukes er identifisert	<p>Microsoft 365 plattformen brukes i stor grad innenfor både forskning, utdanning og administrasjon. Plattformen brukes til behandling, lagring og kommunikasjon av informasjon og er godkjent for lagring og behandling av informasjon opp til Fortrolig, gitt at den krypteres.</p> <p>Ifølge dokumentasjonen, deler M365 Copilot data kun internt på egen «tenant». Systemet forholder seg til 'Semantic index' og brukere vil kun få tilgang til innhold de allerede har tilgang til ved søk eller sammenstilling av informasjon i M365 Copilot. Dette vil si at fra Microsoft sin side tilfører ikke M365 Copilot noen endring på informasjonssikkerheten i NTNU sin tenant, men hvordan dette oppleves fra NTNU sin side er ikke nødvendigvis likt. M365 Copilot utfordrer en del innstillinger i NTNUs tenant som tidligere er tenkt har vært tilstrekkelig, men med innføring av M365 Copilot ikke blir det.</p> <p>De viktigste områdene for NTNU å ha kontroll på i denne sammenheng er følgende:</p> <ul style="list-style-type: none"><li>• Tilganger/tilgangsstyring må være korrekte</li><li>• Klassifisering av informasjon (labels i M365 applikasjoner)</li><li>• Prompt injection attacks</li><li>• Sikkerhetskultur</li></ul> <p><i>Se utfyllende vurdering: Punkt 1.9 – Informasjonssikkerhet</i></p>
Tas ny teknologi i bruk, eller brukes eksisterende teknologi på en ny måte?	Ny teknologi tas i bruk, men tilgangsstyring og driftsteknologi gjenbraker samme teknologi som er godt kjent i Microsoftplattformen.
Har virksomheten bygget systemet fra grunnen av eller er det kjøpt ferdig (som hylleware) 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?	Leverandøren beskriver hvordan de mener personvern er ivarettatt i sin dokumentasjon. Microsoft oppgir at blant annet EU data boundary ivaretar EU-brukere, mulighet til sletting av Copilot chat log, informasjon om web plugin og

tilgangsstyring innenfor tenant som eksempler på innebygd personvern og personvern som standardinnstilling.

NTNU vurderer disse tiltakene m.fl. dithen at leverandøren har noen personverninnstillinger integrert i verktøyet som kan administreres av administratorer i organisasjonen, men det finnes funksjoner i verktøyet som overstyrer «personvernvennligheten». Eksempler på dette er

- Microsoft opplyser om at all data blir behandlet innenfor EU data boundary for EU-brukere, inkluderer dette ikke eksempelvis informasjon om at aksessering fra teknisk support kan forekomme fra land som kategoriseres som tredjeland, videre kan bruk av web plug-in medføre datalekkasje utenfor EU.
- Chat-loggen kan aksesseres av administratorer i organisasjonen via eDiscovery. Det er uklart for NTNU om sletting av egen logg også medfører sletting av loggen som administrator kan se
- For at tilgangsstyring skal fungere på tenkt måte er organisasjonen avhengig av et visst nivå på «orden i eget hus».

Det finnes ulike funksjoner man kan skru av og på som administrator, som da vil gjelde for hele tenant. Dersom listen over innstillinger utvides, og mulighet til å skru av Copilot i Outlook, vil dette bidra til å øke etterlevelsen etter personvernforordningen. Å forvalte Microsoft 365 innebærer kontinuerlig oppfølging av Microsoft sin roadmap for utvikling.

# Utfyllende vurderinger punkt 1.2 – 1.9

Utfyllende vurderinger til alle punkter følger nedenfor.

## Punkt 1.2 og 1.3 – Behandlingens art og behandlingens omfang

### **Hvordan skal personopplysningene samles inn:**

Personopplysningene som behandles av M365 Copilot samles inn på ulike måter, for eksempel:

- fra kjernesystemer (navn, epostadresse, brukernavn osv)
- at den registrerte selv oppgir sine egne personopplysninger (for eksempel direkte i epost eller dokumenter),
- andre har oppgitt personopplysninger om den registrerte (lager dokumenter med andre sine opplysninger)
- Opptak av møter i Teams og transkripsjon (kan også være fysiske møter i rom hvor Teams lytter inn)
- Samhandling med M365 Copilot ved prompts og svar kan føre til innsamling av personopplysninger da en bruker kan skrive inn personopplysninger, be om å få personopplysninger i svaret og personopplysninger kan genereres i M365 Copilots respons.

Listen er ikke uttømmende, men felles for de alle er at store deler av personopplysningene allerede er samlet inn.

I tillegg til direkte identifiserbare personopplysninger nevnt over vil det samles inn indirekte personopplysninger via de registrertes bruk av verktøyene i Microsofts «Modern work» plattform. Dette er personopplysninger som samles inn via bruk de registrerte selv utfører, som for eksempel deling av personopplysninger i chat i Teams, lagring av filer med personopplysninger eller deling av personopplysninger i filer og epost i Outlook.

Bruk av verktøyene fører til kontinuerlig fremtidig innsamling av personopplysninger.

### **Nye personopplysninger som lages eller sammenstilles av M365 Copilot**

Er det mulig at M365 Copilot lager nye personopplysninger eller sammensetning av informasjonskilder som kan bli direkte eller indirekte identifiserbare personopplysninger? For eksempel adferdsdata som kan identifisere kjønn.

- o *Vurdering: Ja! Du kan spørre M365 Copilot om hvilken sinnsstemning en navngitt person er i, og den vil kunne komme til å svare. I eksempelet nedenfor er Heine Skipenes sin samhandling med Silje Blichfeldt brukt av Silje. Heine Skipenes får ingen varsel eller mulighet til å vurdere at dette har skjedd. Vurdering av «mood» knyttet til faktisk person er å regne som en ny personopplysning og vurdering av tekstlig innhold.*

7. april 2024 kl. 12:53

what mood would you say heine skipenes was in last week?

Based on the interactions from last week, Heine Skipenes seemed to be in a positive and collaborative mood. They engaged in light-hearted exchanges, showed enthusiasm for various projects, and expressed interest in event participation and planning. For instance, they joked about using only the blue boxes they have access to and showed excitement about collaboration requests and artificial intelligence discussions. These interactions suggest a mood that is both professional and amiable. If you require more specific insights or have further questions, feel free to ask.

Kopier

3 av 30 svar Innhold generert av kunstig intelligens kan være feil

Figur – Skjerm bilde Testprompt fra 7. april – “mood”

### Hvordan og hvor lenge skal personopplysningene lagres:

Personopplysningene som behandles av M365 Copilot lagres på ulike måter:

- Brukerdata lagres direkte i et Microsoft-verktøy sin kobling til NTNUs Microsoft tenant
- Filer som kan inneholde personopplysninger kan være lagret i en brukers OneDrive, SharePoint, på en epostkonto, i chatlogger i Teams
- Chatloggen med M365 Copilot for hver enkelt brukers logg ligger lagret i en mappe i Exchange som brukeren selv ikke har tilgang til

Listen er ikke uttømmende, men det er en fellesnevner at noder/verktøy og koblinger som blir gjort tilgjengelig for Graph blir behandlet av M365 Copilot og indeksert.

Ved å samhandle med M365 Copilot ved at en registrert legger inn prompts og mottar svar, vil Microsoft lagre data om samhandlingen. Hva som er skrevet, hvilket svar M365 Copilot har reagert med og informasjon som brukes til å forankre M365 Copilots svar. Disse dataene behandles og lagres i samsvar med kontraktmessige forpliktelser i forbindelse med organisasjonens øvrige innhold i Microsoft 365. NTNU har pr. [02.04.2024] ikke klart for seg hva dette innebærer.

#### Merknader

- *Filer som inneholder personopplysninger gjort tilgjengelig for M365 Copilot kan bli behandlet når som helst så lenge filene ikke er slettet eller gjort utilgjengelig for M365 Copilot (flyttet til eget lagringsområde eller klassifisert/påført sensitivity label)*
- *En bruker kan slette filer og egne personopplysninger i input/output, men vi kan ikke garantere at informasjonen faktisk blir slettet hos Microsoft hvis ikke dette eksplisitt er omtalt i de kontraktmessige forpliktelsene.*

### Hvordan skal personopplysningene brukes:

Når M365 Copilot får tilgang til personopplysninger via Microsoft Graph kan opplysningene bli behandlet. M365 Copilot beskriver selv hvordan dette gjøres på følgende måte:

**«Microsoft Graph er porten til data og intelligens i Microsoft 365. Den gir en enhetlig programmeringsmodell for å få tilgang til data fra Microsofts skytjenester, Windows og Enterprise Mobility + Security, samt for å utvide opplevelser i Microsoft 365.**

### 1. Hva er Microsoft Graph?

- **Microsoft Graph** er en API (Application Programming Interface) som gir utviklere muligheten til å samhandle med data og tjenester i Microsoft 365.
- Den gir tilgang til en rekke funksjoner, inkludert brukerprofiler, e-post, kalendere, filer, kontakter, grupper, sikkerhet, enheter og mye mer.
- **Microsoft Graph** gir en enhetlig måte å programmere mot data fra ulike Microsoft-tjenester.

### 2. Hvordan fungerer Microsoft Graph?

- **Indeksering av data** er en viktig del av Microsoft 365, og det er også en del av hvordan **Microsoft Graph** fungerer.
- **Microsoft Graph** indekserer innhold og signaler fra de fleste Microsoft 365-applikasjoner i organisasjonen din. Dette inkluderer e-post, dokumenter og annet innhold.
- Når du søker etter noe, bruker **Microsoft Graph** indeksen til å rangere de mest relevante resultatene basert på signaler som personlige forbindelser og sosiale relasjoner.
- **Semantic Index** er en ny funksjon i **Microsoft 365-søk** som bruker **Microsoft Graph** for å bedre samhandle med dine personlige og organisatoriske data. Den skaper en ny indeks som muliggjør fremtidige søke- og Copilot-opplevelser. Den følger sikkerhets- og policyreglene til **Microsoft Graph**. Bare innhold som en bruker har tilgang til, vises i søket eller i Microsoft Copilot.

### 3. Hvordan hjelper den semantiske indeksen med å administrere dataene dine?

- Den semantiske indeksen forbedrer funksjonene i Microsoft 365 som lar deg finne relevant innhold basert på nøkkelord, personlige preferanser og sosiale forbindelser.
- Den oppretter vektoriserte indekser som muliggjør konseptuell forståelse. Dette hjelper deg med å finne det du leter etter og få tilgang til organisatorisk innhold.
- En vektor er en numerisk representasjon av et ord, bildepiksel eller annet datapunkt. Vektoren er ordnet eller kartlagt med nærliggende tall for å representere likhet.»

Microsoft oppgir at data ikke deles med tredjeparter, eller brukes til trening av M365 Copilot eller andre KI-funksjonalitet med mindre dette er godtatt av overordnet lokal administrator av tjenesten (hele tenant). M365 Copilot overvåker prompts og respons for å avdekke misbruk, for eksempel søk på bombeoppskrifter, men denne dataen lagres ikke.

#### Merknader:

- *Bruk av sensitivity labels gjør at M365 Copilot ikke bruker klassifisert data når den gir svar, men vi kan ikke garantere at dataene ikke blir lest eller behandlet av M365 Copilot (?)*



## Systematisk behandling av personopplysninger

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.

### Merknader:

- *Vi har ikke funnet grunnlag for å si noe annet enn at det er mulig at M365 Copilot kan behandle filer og personopplysninger selv uten at et menneske har instruert den om å gjøre det. Vil den reindexere innhold kontinuerlig for eksempel? Vil reindexering føre til endret oppfatning/tolkning av innhold i et dokument som igjen kan gi et annet svar seinere?*

### Innspill til risikoreducerende tiltaksliste i DPIA:

- Administrator ved NTNU skal gjennomgå alle innstillinger og tilse at disse er satt til mest personvernvennlig, slik at NTNU kan sikre de registrertes rettigheter og friheter, og etterleve personvernforordningen
- Gjennomgå kontraktsmessige forpliktelser i forbindelse med organisasjonens øvrige innhold i Microsoft 365
- Gjennomgå tilgangsstyringsrutiner
- Gjennomgå internkontrollrutiner informasjonssikkerhet.
- Opplæring av ansatte i lagring og forvaltning av data

## Punkt 1.4 – Behandlingens formål

### Behandlingens formål i driftsfasen:

Det er komplisert å definere ett eller flere klare og tydelige formål for bruk av M365 Copilot i tråd med Personvernforordningens artikkel 5 og 6. M365 Copilot er bygd som en tilleggsfunksjonalitet inni allerede eksisterende verktøy som tekstbehandling, epost, regneverktøy osv. Behandlingens formål må derfor ses i direkte sammenheng med bruken av allerede eksisterende verktøy hvor M365 Copilot blir en "forsterker" både med tanke på effektivitet, behandlingssomfang av personopplysninger og risiko.

Bruken av M365 Copilot kan direkte relateres til NTNUs egne retningslinjer for behovet for vurdering av personvernkonsekvenser: *«Punkt 8. Innovativ bruk eller anvendelse av ny teknologisk eller organisatorisk løsning [...] bruk av ny teknologi som defineres «i samsvar med det oppnådde nivået av teknisk kunnskap» kan medføre behov for å gjennomføre en vurdering av personvernkonsekvenser. Grunnen til dette er at anvendelse av ny teknologi kan medføre nye former for innsamling og bruk av personopplysninger, eventuelt med høy risiko for den enkeltes rettigheter og friheter. De personlige og sosiale konsekvensene ved anvendelsen av ny teknologi kan være ukjente. En vurdering av personvernkonsekvenser hjelper den behandlingsansvarlige å forstå og håndtere slike risikoer. For eksempel kan visse «tingenes internett»-applikasjoner få betydelige konsekvenser for den enkeltes dagligliv og privatliv, og kan derfor kreve en vurdering av personvernkonsekvenser.»* (<https://i.ntnu.no/wiki/-/wiki/Norsk/Vurdere+personvernkonsekvenser>)

På bakgrunn av dette må konklusjonen være at beskrivelse av behandlingens formål for bruk av M365 Copilot må ses i direkte sammenheng med bruk av allerede eksisterende

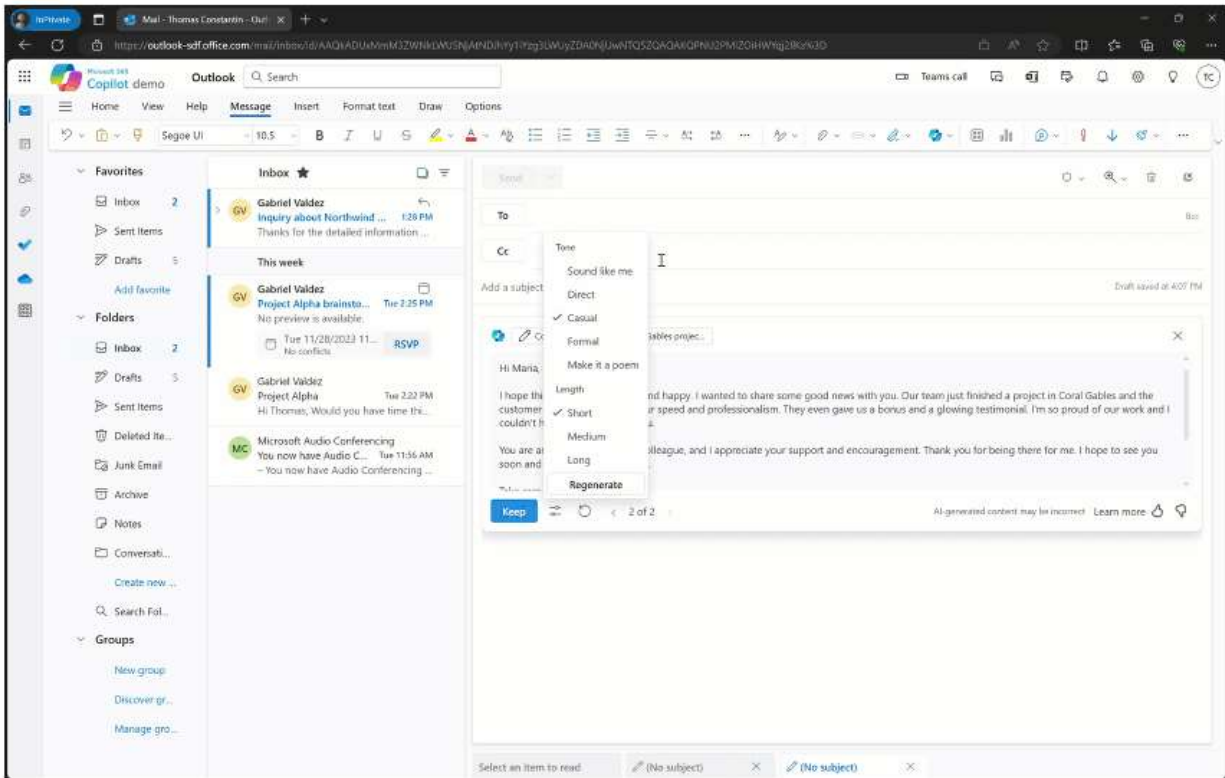
Microsoft-verktøy. Dette kan gjøres gjennom eksisterende rammeverk og oversikt over saksprosesser i protokoll/behandlingsoversikt. Bruk av verktøy med innebygd kunstig intelligens og M365 Copilot særskilt må kartlegges, dokumenteres og vurderes pr. saksprosess av den prosessansvarlige.

### **Brukes personopplysninger for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte?**

Gjennom testing av NTNU funnet funksjoner ved M365 Copilot som kan medføre bruk av personopplysninger for å avdekke ukjente sider, eller for å gjenkjenne mønstre ved den registrerte. For eksempel ved bruk av funksjonene Draft og Coach i Outlook, vil M365 Copilot kunne bruke personopplysninger som ligger i den enkeltes epostkasse. Dette kan være ens egne personopplysninger, men også andre registrertes personopplysninger som er omtalt i lagrede eposter. M365 Copilot kan analysere alle eposter i epostkassen, og eksempelvis gjenkjenne at en registrert har et mønster ved sin kommunikasjon, og deretter forslå endringer som kan gjøre at den registrerte endrer atferd. Eksempler på dette kan være at M365 Copilot gjenkjenner personer og tema som gjennomgående i en brukers epost, og foreslår endringer i brukerens atferd/samhandling med gitte person. Dette er funksjoner ved verktøyet som NTNU anses å brukes til å avdekke ukjente sider eller gjenkjenne mønstre ved den registrerte.

### **Draft**

Funksjonen «Draft» kombinerer LLMs med data i hver brukers Outlook som kilde. Funksjonen kan oppsummere lange epost-tråder og trekke ut viktige seksjoner og poenger fra flere eposter. Funksjonen kan også lage nye eposter eller besvare en epost via prompting, hvor man kan velge tonen i språket i eposten, eller man kan velge at M365 Copilot skriver eposten med utgangspunkt i hvordan brukeren selv skriver epost.

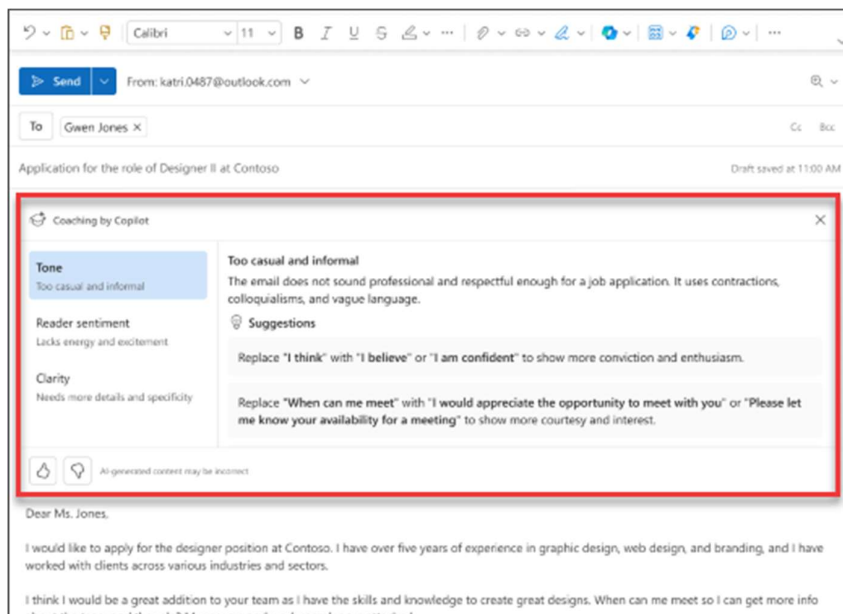


*Copilot helps you draft a message that sounds like you*

*Figur: Screenshot fra M365 Copilot Demo: Outlook (kilde: Microsoft)*

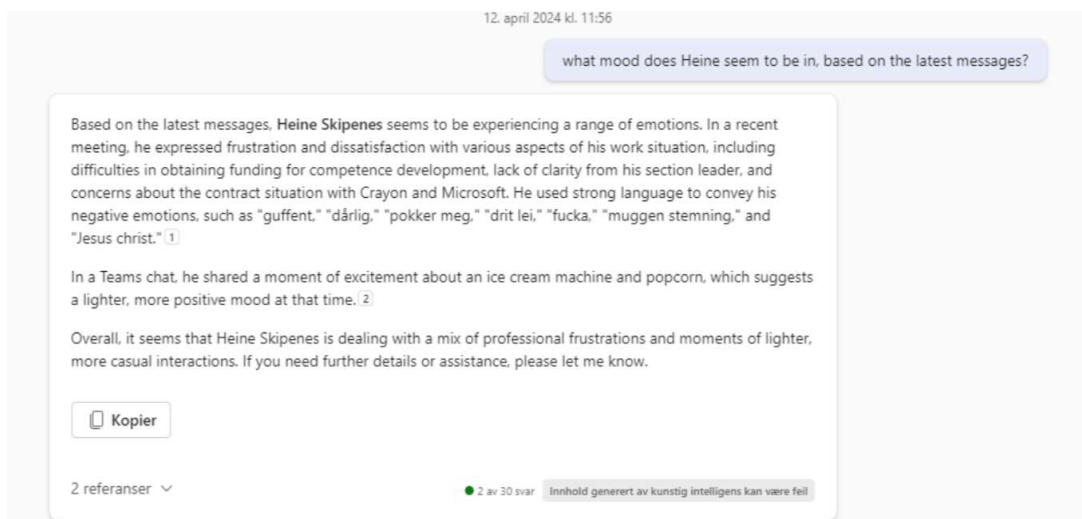
## Coaching

Med funksjonen Coaching i Outlook, kan M365 Copilot se gjennom en epost brukeren har skrevet, og komme med forslag til forbedringer av teksten i form av å endre språkets tone, klarhet og leserfølelsen. Eksempel på dette er at en epost som har et uklart språk med tegn på usikkerhet hos avsender, kan få forslag fra M365 Copilot på hvordan gjøre språket mer selvsikkert. Bruksområder for denne funksjonen kan for eksempel være når epost skal sendes til leder eller sende en epost med beslutning til potensielle søkere.

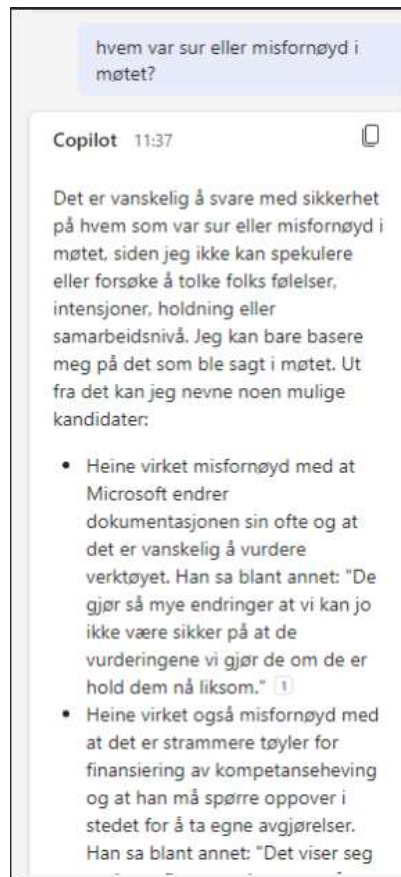


Figur: Skjerm bilde «Coaching by Copilot» (kilde: Microsoft)

Andre eksempler som avdekkes ved testing av funksjoner i M365 Copilot er verktøyets muligheter til å bruke en registrerts personopplysninger fra eksempelvis chat, filer og epost, for så å sammenstille disse opplysningene til å avdekke hvilket humør den registrerte er i basert på personopplysninger i disse kildene. M365 Copilot kan også bruke personopplysninger fra transkripsjoner og opptak av Teams-møter, oppsummere og sammenstille oppfølgingspunkter, men også avdekke hvem som snakket mest og minst i møtet, og hvilket humør de ulike deltakerne befant seg i under møtet.



Figur – Skjerm bilde Testprompt fra 12. april – “mood”



Figur - Skjerm bilde av testprompt 12. april "Hvem var sur eller misfornøyd i møtet"

## Vil personopplysningene viderebehandles til nye eller andre formål?

Da NTNU testet M365 Copilot ble det identifisert funksjoner som gjør at personopplysninger samlet inn for ett formål vil bli viderebrukt til nye eller andre formål.

I og med at M365 Copilot bruker personopplysninger som kan ligge lagret i epostkasser, Teams chat og annen samhandling mellom brukere, kan man anse at personopplysningene vil bli viderebehandlet til nye eller andre formål.

Det er derfor nødvendig å vurdere tekniske og organisatoriske tiltak fortløpende for å motvirke feilaktig bruk.

### Merknader:

- Se også vurdering med eksempel fra 1.2
- Formål må konsolideres med innspill og tilbakemeldinger fra arbeidsgrupper på NTNU som vurderer bruk av kunstig intelligens i forskning og utdanning
- Vi må ta utgangspunkt i at M365 Copilot vil komme til å gjøre det som brukerne ber den om å gjøre.

### **Innspill til risikoreduserende tiltaksliste i DPIA:**

- Administrator ved NTNU skal gjennomgå alle innstillinger og tilse at disse er satt til mest personvernvennlig, slik at NTNU kan sikre de registrertes rettigheter og friheter, og etterleve personvernforordningen
- Gjennomgå kontraktsmessige forpliktelser i forbindelse med organisasjonens øvrige innhold i Microsoft 365
- Gjennomgå tilgangsstyringsrutiner
- Gjennomgå internkontrollrutiner informasjonssikkerhet.
- Opplæring av ansatte i lagring og forvaltning av data

### Punkt 1.5 – Sammenhengen behandlingen utføres i (kontekst)

#### **Hvilke kilder brukes for innhenting av personopplysninger?**

NTNU som behandlingsansvarlig innhenter personopplysninger som kontinuerlig behandles i verktøyet M365 Copilot. Personopplysningene behandles i alle applikasjoner innenfor «Modern work»-plattformen, eksempelvis Teams, Word, Excel og Outlook.

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.

#### **Eksempler på kilder personopplysninger innhentes fra via M365 Copilot:**

**Profiler:** M365 Copilot henter personopplysninger fra de registrertes profiler. Dette inkluderer navn, brukernavn, e-postadresser, lokasjon, preferanser og interesser. Brukerprofilene er opprettet av administrator i organisasjonen når en bruker blir lagt til eller skal få tilgang.

**Dokumenter:** Ved bruk av verktøyet kan M365 Copilot få tilgang til personopplysninger som ligger i dokumenter som en bruker tar i bruk i verktøyet. Dokumenter som opprettes av brukerne selv kan inneholde persondata om brukeren selv, eller om andre registrerte. M365 Copilot kan opprette dokumenter som kan inneholde personopplysninger basert på input/ledetekst som en bruker legger inn, samt andre dokumenter som brukeren kan legge referanser til i ledeteksten.

**Eposter:** M365 Copilot har tilgang til eposter som kan inneholde personopplysninger. M365 Copilot leser og analyserer all epost i alle epostkasser en bruker har tilgang til. Dette innebærer potensiell behandling av store mengder personopplysninger om brukeren selv og om andre registrerte. Det kan antas at mange brukere i organisasjonen ikke har innarbeidet sletterutiner for epost som er mottatt og sendt.

**Nettsider:** M365 Copilot kan få tilgang til nettsider som inneholder personopplysninger, som navn, sosiale medieprofiler, kommentarer og anmeldelser. Nettsider besøkes og vises av brukerne eller av M365 Copilot basert på prompts/brukerinnndata.

**Teams:** M365 Copilot får tilgang til personopplysninger som stammer fra brukernes interaksjoner til eksempelvis innlegg eller meldinger i ulike Teams.

**Chatlogger:** Personopplysninger om selve brukeren og om andre registrerte i chatmeldinger blir behandlet av M365 Copilot. Verktøyet kan oppsummere meldinger fra navngitte personer.

*Merknader:*

- *Det kan virke som om M365 Copilot «sveiper» over tilgjengelige kilder hvis den mener selv at den har behov for det. Hvis ikke prompten som brukeren stiller er tydelig og presis vil M365 Copilot lete etter relevant informasjon andre steder, og vi klarer ikke å beskrive hvorfor eller hvordan den velger en kilde framfor en annen.*

### **I hvilken grad har den registrerte kontroll over sine opplysninger?**

De registrerte har til en viss grad kontroll over egne personopplysninger som de selv deler i epost utvekslinger og Teams chat meldinger og interaksjoner/reaksjoner på innlegg i Teams-kanaler, eksempelvis kan en bruker slette sin kommentar til et innlegg, slik at denne ikke lenger er synlig for andre brukere i Teams.

En bruker kan også slette egen historikk i M365 Copilot via Settings & Privacy innstillinger. Dette kan inkludere sletting av egne og andre registrertes personopplysninger.

En registrert kan be om 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>

Den registrerte har ingen mulighet til å ha full kontroll over all behandling av sine personopplysninger via M365 Copilot. Ved bruk av ovennevnte mekanismer kan en registrert ha delvis kontroll over personopplysninger den selv legger inn i verktøy som har M365 Copilot tilkoblet. Den registrerte har ikke kontroll over hvordan andre brukere/registrerte behandler ens personopplysninger.

NTNU som behandlingsansvarlig vil kunne ha en viss grad av kontroll over de registrertes personopplysninger ved bruk av M365 Copilot, men dette forutsetter at de saksprosessene som tillater bruk av M365 Copilot i oppgaveutførelsen også kartlegger bruk og registrerer dette i NTNUs behandlingsprotokoll. Det er viktig med gode internkontrollrutiner for systematisk oppfølging av dette området.

*Merknader:*

- *Hvilken risiko kan NTNU ta? Viktig å følge med på utviklingen og sikre at Microsoft gjør tilgjengelig oversikter og funksjonalitet som gjør at den registrerte kan ha kontroll på sine opplysninger*

### **Vil dere behandle personopplysninger fra ulike datasett, som er innsamlet for ulike formål og fra ulike behandlingsansvarlige?**

Ja. Et datasett settes sammen med et annet datasett for å kunne finne hittil ukjente sammenhenger. Vi kan ikke utelukke at datasettene inneholder personopplysninger.

Grunnet måten M365 Copilot er bygd opp på, vil en slik behandling forekomme kontinuerlig ved bruk av ulike applikasjoner i M365. M365 Copilot vil samle inn data, inkludert personopplysninger fra alle filer, epost, chatmeldinger, kalenderoppføringer, etc, en bruker har tilgang til, uavhengig av formålet de har blitt innsamlet for, og sammenstille disse og kunne finne nye sammenhenger.

Ved forskningsprosjekt i samarbeid med andre forskningsinstitusjoner er ofte NTNU databehandler. Det kan forekomme datautlevering fra behandlingsansvarlig i forskningsprosjekt, som deretter vil bli behandlet i NTNUs Microsoft 365-tenant. M365 Copilot vil dermed kunne behandle personopplysninger som er innsamlet fra ulike behandlingsansvarlige og for helt andre formål. Dette bør tas med i prosjektvurderinger.

*Merknader:*

- NTNU bør vurdere om dette også gjøres gjeldende for bruk av shared channels.

#### **Innspill til risikoreducerende tiltaksliste i DPIA:**

- Gjør en egen vurdering av situasjoner der NTNU er databehandler

#### **Kobles ulike registre for å gi ny type informasjon om den registrerte?**

SNLs 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 [...].»

Med utgangspunkt i ovennevnte betegnelse vil det forekomme sammenkobling av ulike registre for å gi ny type informasjon om en registrert. M365 Copilot i Teams kan blant annet lese og analysere hvordan en registrert har samhandlet i kanaler og chatmeldinger i Teams, i epostutvekslinger og i filer, og deretter analysere den registrertes humør.

## Punkt 1.7 – Mottakere av personopplysninger

### **Beskriv alle mottakere/kategorier av mottakere av personopplysninger**

Personopplysningene som behandles av M365 Copilot blir behandlet av:

- NTNU (behandlingsansvarlig)
- Microsoft (databehandler) med underleverandører

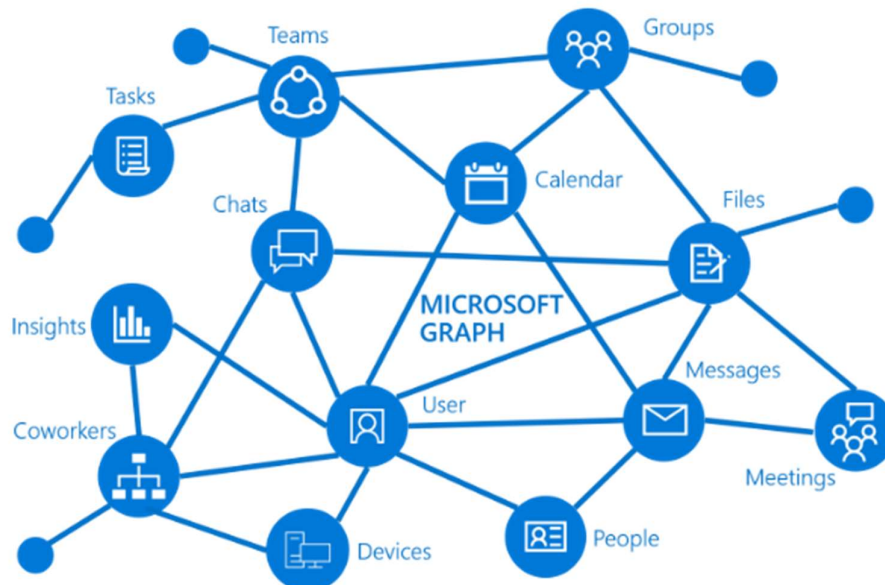
*Merknader:*

- *Ansatte har tjenstlig behov for behandling av personopplysninger (utøvelse av offentlig myndighet)*
- *Ansatte, studenter og gjestebukere har behov for samarbeid og samskriving*
- *Får Microsoft delt behandlingsansvar ut fra sin rolle? Dette må vurderes på et senere tidspunkt*



## Hvordan deles personopplysningene mellom avdelinger internt i virksomheten?

Ansatte jobber og deler personopplysninger på tvers av interne organisatoriske enheter (mellom for eksempel institutt og fakultet). Når M365 Copilot aktiveres får verktøyet tilgang til personopplysninger via Microsoft Graph og opplysningene kan bli behandlet. Copilot with commercial data protection beskriver selv hvordan dette gjøres på følgende måte: «Microsoft Graph er et verktøy som kan brukes til å dele personopplysninger og data internt i en organisasjon på en sikker og skalerbar måte. Microsoft Graph fungerer sammen med Copilot ved å gi tilgang til organisasjonsdata, noe som gjør det mulig for Copilot å gi mer relevante og kontekstuelle svar.»



Figur 1 Illustrasjon av Microsoft Graph

Personopplysninger kan deles enten aktivt eller utilsiktet, mellom ulike avdelinger, ulike grupper og ulike registrerte i organisasjonen. Ved prompting med M365 Copilot vil man ikke kunne være sikker på hvilken informasjon, filer eller dokumenter den henter opplysninger fra, og lenker til. M365 Copilot henter utelukkende informasjon fra kilder som brukeren allerede har tilgang til. Verktøyet får tilgang til alle åpne Team og dokumenter iblant annet den registrertes SharePoint, og kan dele dette med andre registrerte ved prompting og mottak av svar fra M365 Copilot.

### Eksempel:

- Personopplysninger kan deles internt i organisasjonen i Teams på følgende måte:
  1. Bruker legger inn prompt i chatvinduet i M365 Copilot i Teams. Prompt'en kan inneholde forespørsel om eksempelvis en navngitt person, men kan også inneholde en generell forespørsel om eksempelvis forbedring av tekst i Teams-meldinger.
  2. M365 Copilot analyserer alle tilgjengelige dokumenter, epost, chatlogger etc. jf. Graphskisse, som den brukeren har tilgang til. Dette innebærer også innhold fra personer som ikke har sikret sine filer riktig (filene må være gjort aktivt tilgjengelig). Alle tilgjengelige filer kan være blant kildene som M365 Copilot bruker for å kunne gi et svar på forespørselen som opprinnelig ble sendt.

#### **Merknader:**

- *M365 Copilot referer til dokumenter, men det er ukjent om også andre dokumenter er behandlet for å fremskaffe svar på prompt.*
- *Hvis du har tilgang til filer fra to institutt A og B og spør om noe som kun gjelder institutt A, kan også filer fra institutt B bli benyttet i utarbeidelsen av svar.*
- *Det er fri flyt mellom interne avdelinger i en organisasjon. Du som bruker må aktivt prompte (for eksempel «bruk bare datakilde fra «/filnavn» og kontroller svar manuelt). Du skal være veldig presis for ikke å behandle for mye data.*

#### **Innspill til risikoreduserende tiltaksliste i DPIA:**

- Alle registrerte må merke sine filer med «Sensitivity labels»
  1. Alternativt: kjøre script på alle filer i tenant'en og klassifisere alle uklassifiserte filer som intern/fortrolig/privat eller lignende (Vurder behov for «Tante Sofie»-tjeneste)
- Opplæring – deling og forvaltning av data, og spesifikk opplæring i hvordan prompte riktig.

### Punkt 1.7 B – Mottakere av personopplysninger

#### **Overføres personopplysningene til land utenfor EU/EØS-området (tredjestater), jf. art. 44-49? Hvis ja, hva er det rettslige grunnlaget for det?**

I henhold til personvernforordningen art. 45 kan en overføring av personopplysninger til tredjeland forekomme dersom tredjestaten har et tilstrekkelig beskyttelsesnivå. EU-kommisjonen har fattet adekvansbeslutninger for 10 land, og ytterligere 5 land med visse unntak, som tilsier at det aktuelle landet har tilstrekkelig med beskyttelsesnivå, og overføring til et av disse landene er å sammenligne med overføring av personopplysninger internt i EU/EØS. Noen land har visse unntak, deriblant USA, hvor aktuell leverandør må være på liste over sertifiserte virksomheter under EU-US Data Privacy Framework.

Dersom det skal overføres personopplysninger til en stat uten at det foreligger en adekvansbeslutning, kan overføringen kun skje dersom databehandleren kan gi nødvendige garantier, jf. personvernforordningen art. 46, nr. 2. Det mest brukte overføringsgrunnlaget er «Standard contractual clauses».

Microsoft oppgir at data fra kunder i EU blir behandlet innenfor EU Data Boundary. EU Data Boundary er en geografisk definert grense som Microsoft behandler og lagrer kundedata og personopplysninger for sine skytjenester, inkludert Microsoft 365. Dette innebærer alle EU- og EFTA-land. Microsoft definerer kundedata som all data, inkludert all tekst, lyd, video, bildefiler og software, som er tilgjengeliggjort for Microsoft.

Ifølge Microsofts dokumentasjon vil det i noen tilfeller bli overført kundedata utenfor EU Data Boundary. Dette kan skje i form av at teknisk personell fra Microsoft må aksessere kundedata eller pseudonymiserte personopplysninger. Data blir ikke lagret utenfor EU Data Boundary selv om dataen aksesseres utenfra, videre oppgir Microsoft at de benytter kryptering som sikkerhetstiltak for å beskytte data under overføring.

M365 Copilot har tilgang til websøk for å forbedre svar på prompts fra bruker. Dette tilgjengeliggjøres via «web content plugin». Når plugin er aktivert, kan M365 Copilot hente informasjon som er relatert til prompten brukeren har skrevet inn fra Bing search index, hvis M365 Copilot finner at den kan svare bedre ved hjelp av informasjon fra web. Prompten blir analysert og identifiserer uttrykk som brukes til web søk, og søker deretter via Bing Search API. M365 Copilot bruker ikke den opprinnelige prompten til å søke, men lager en ny ledetekst som brukes til søk. Bruker ID og tenant-ID er ikke koblet mot søk sendt til Bing Search API.

Ved bruk av tredjepartsapplikasjoner, Dataverse + power platform og plug-ins kan overføring til tredjeland forekomme. Dette må vurderes fortløpende i forvaltning av Microsoft 365.

I Microsofts databehandleravtale, oppgir Microsoft at behandlingsansvarlig (NTNU) godtar at Microsoft overfører blant annet kundedata til USA, eller hvilket som helst land Microsoft eller Microsofts underleverandører opererer.

*Merknader:*

- *Ved å bruke Microsoft sine tjenester aksepterer NTNU at Microsoft står fritt til å behandle personopplysninger der Microsoft selv eller noen av underleverandørene anser det som hensiktsmessig (hvor som helst).*
- *Uklart om det er gjort en god nok vurdering av rettslig grunnlag som står seg over tid. Dette bør revurderes på et senere tidspunkt.*

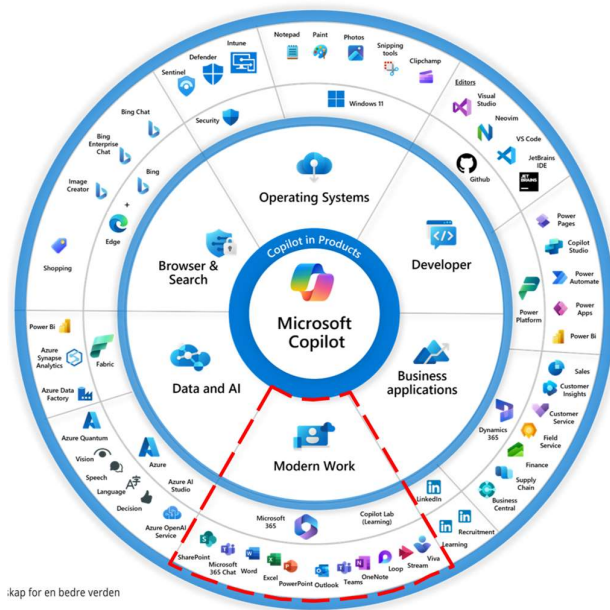
**Innspill til risikoreduserende tiltaksliste i DPIA:**

- Vurdere om plugin for web bør deaktiveres. Kan redusere funksjonaliteten av verktøyet for mange brukere.
- Gjør vurdering av rettslig grunnlag

## Punkt 1.8 – Dataflyt, lagring og mellomlagring

NTNU har gjennomgått dokumentasjon som finnes på Microsofts nettsider om dataflyt, lagring og mellomlagring. En merknad til denne dokumentasjonen er at den er utilgjengelig, i den form at det er veldig mye informasjon en registrert må sette seg inn i, mange dokumenter som må gjennomleses, og informasjonen er beskrevet på en måte som gjør at den faktiske behandlingen av data (inkludert personopplysninger) som gjennomføres er vanskelig å forstå ut ifra dokumentasjonen.

Denne vurderingen tar utgangspunkt i applikasjoner som faller innunder Microsofts beskrivelse av egne tjenester som «Modern work-plattformen» (se figur 1).

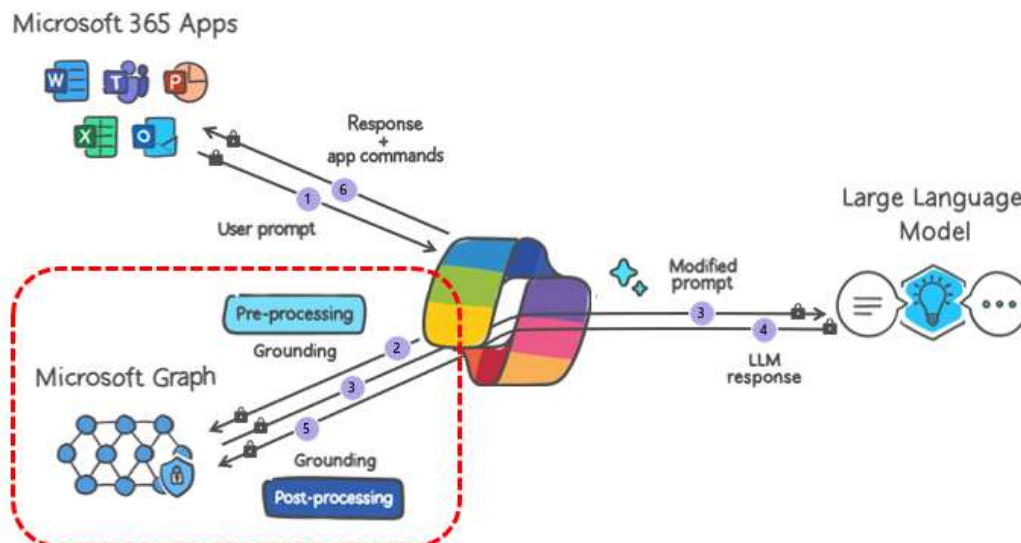


skap for en bedre verden

Figur 1: Microsoft sin oversikt over Copilot tjenester

## Hvordan overføres og tilgjengeliggjøres personopplysningene?

Personopplysningene som blir behandlet i M365 Copilot overføres og tilgjengeliggjøres på denne måten:



Figur - Bilde presentert av Microsoft i presentasjon Løypemelding 1 20. mars

Microsoft Copilot for Microsoft 365 fungerer slik (beskrevet av Copilot):

«Copilot mottar og forhåndsbehandler brukerens inndatamelding i en app som Word eller PowerPoint. Denne prosessen, kalt jording [grounding], forbedrer meldingens spesifisitet for å produsere relevante og praktiske svar. Copilot sender deretter meldingen til LLM for behandling, med tilgang begrenset til data brukeren allerede har tilgang til.

Etter å ha mottatt svaret fra LLM, etterbehandler Copilot det. Dette inkluderer ytterligere jordingskall til Microsoft Graph, KI-kontroller, sikkerhets-, samsvars- og personvern gjennomgang, og kommandogenerering.

Svaret returneres til appen for brukerens vurdering. Brukerens ledetekst og Copilots svar beskrives som "innholdet i samhandlingene", og disse samhandlingene utgjør brukerens Copilot-samhandlingshistorikk.

Microsoft Copilot for Microsoft 365 samkjører disse tjenestene for å produsere resultater som er relevante for organisasjonen, tilpasset konteksten og basert på organisasjonsdata.»

Data (inkludert personopplysninger) tilgjengeliggjøres via Microsoft Graph, hvor Microsoft kobler innhold som for eksempel filer, chat-meldinger, epost, samhandling i Teams mellom personer. Når en bruker av M365 Copilot søker etter noe i verktøyet, bruker Microsoft Graph indeksen til å rangere de mest relevante resultatene, noe som innebærer koblinger mellom personlige forbindelser og sosiale relasjoner (se illustrasjon av Graph under utfyllende vurdering punkt 1.7).

**Hvor og hvor lenge lagres personopplysningene ulike steder?**

**Hvor lenge lagres personopplysningene etter at formålet ved behandlingen er over, før de slettes? Når skal opplysningene slettes? Er det utarbeidet sletterutiner?**

Innstillinger for lagring, mellomlagring og sletting er tilgjengelig for organisasjonens administratorer. Microsoft opererer med «retention policies» (retningslinjer for oppbevaring) som kan administreres på ulike måter for de ulike appene i «Modern work»-plattformen. «Retention policies» kan implementeres for å bestemme hvor lenge data skal behandles (lagres), og hva som skal skje med dataene når de ikke lenger er nødvendige.

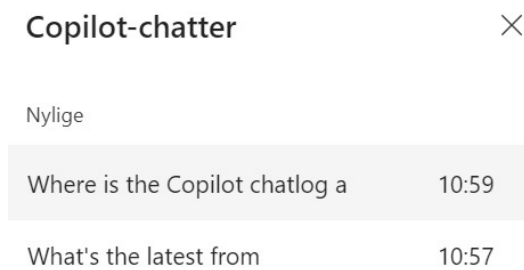
Organisasjonens «retention policies» (i Microsoft Purview) administreres av organisasjonens administratorer. I tillegg kan hver enkelt bruker administrere egne «retention policies» i enkelte applikasjoner, som for eksempel i Outlook, hvor man kan sette «retention labels» for en enkelt mappe eller epost.

Microsoft har utarbeidet fem prinsipper for bevaring og sletting av data. Prinsipp nr. 1 tilsier at bevaring av data alltid overgår policier for sletting. Det vil si, hvis eksempelvis en epost har flere «conflicting retention policies», vil alltid bevaringspolicyen overgå slettepolicyen.

Meldinger brukeren sender og mottar i samtaler med M365 Copilot er inkludert i «retention policy» for "Teams Chat and Copilot interactions". Administrator kan sette opp

en «retention policy» for å angi hvor lenge data skal beholdes i området for lagring. Data fra samhandling med M365 Copilot (som for eksempel den loggførte samtalen brukeren har med M365 Copilot) lagres i skjulte mapper i den enkelte brukers mailboks i Exchange. Den enkelte bruker av verktøyet, og organisasjonens administrator har ikke direkte tilgang til denne mappen med lagret data fra bruk av M365 Copilot. Mappen kan aksesserer av administratorer som har tilgang til eDiscovery. I mappen vil det også lagres data fra private Teams-kanaler.

En bruker med tilgang til M365 Copilot har en oversikt over sin egen chatlogg i Microsoft Copilot Graph-grounded chat (kan aksesserer via blant annet Teams). Denne oversikten gir brukeren mulighet til å slette oppføringen i loggen eller endre navn på chat-elementet. Det påpekes at dette ikke medfører at selve loggoppføringen og alt innhold (inkludert filer, oppgaver, epostmeldinger etc.) i den skjulte mappen i Exchange slettes. Chatoppføringen i loggen i Microsoft Copilot Graph-grounded chat er ikke lenger er synlig for brukeren. Meldingens innhold er slettet ikke permanent. Alle meldinger (inkludert innhold) som er lagret i skjulte mapper i Exchange, er søkbare for administratorer med tilgang til eDiscovery.



Figur – Skjerm bilde av brukers chatlog

#### Slette denne chatten?

Dette sletter Where is the Copilot chatlog a permanent og fjerner den fra listen over Copilot-chatter.

Innhold (filer, oppgaver, e-postmeldinger osv.) som det refereres til i denne chatten, slettes ikke.

Slett

Avbryt

Figur – Skjerm bilde av vindu når bruker vil slette chatlog

## Retention period og SubstrateHolds folder

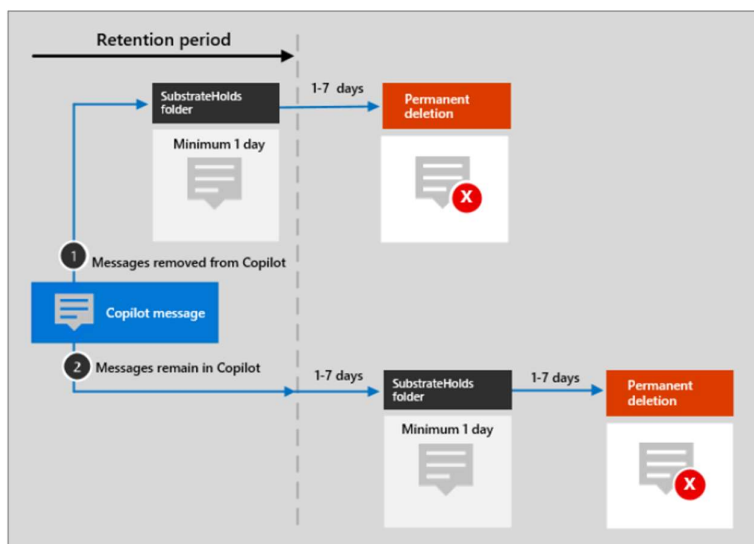
Brukere sletter (når denne muligheten er tilgjengelig) den tilknyttede chatten i Microsoft Copilot Graph-grounded chat. En forespørsel er sendt for å slette en brukers historie om alle interaksjoner med M365 Copilot.

Forklaring av de to veiene i diagrammet:

1. Hvis meldinger fjernes fra M365 Copilot, flyttes meldingen til SubstrateHolds-mappen der den forblir i minst 1 dag. Når oppbevaringsperioden utløper, blir meldingen permanent slettet neste gang timerjobben kjører (vanligvis mellom 1-7 dager).
2. Hvis meldinger forblir i M365 Copilot til oppbevaringsperioden utløper, kopieres meldingen til SubstrateHolds-mappen. Denne handlingen tar vanligvis mellom 1-7 dager fra utløpsdatoen. Når meldingen er i SubstrateHolds-mappen, lagres den

der i minst 1 dag, og deretter blir meldingen permanent slettet neste gang timerjobben kjører (vanligvis mellom 1-7 dager).

When the retention policy is to retain and then delete:



Figur – Skisse over dataflyt for bevaring og sletting av meldinger i Copilot (kilde: Microsoft)

Meldinger lagret i postkasser, inkludert de skjulte mappene, er søkbare via eDiscovery-verktøyet. Inntil meldingene blir permanent slettet fra SubstrateHolds-mappen, forblir de søkbare via eDiscovery-verktøyet.

Lagring av personopplysninger etter at formålet er oppnådd forekommer i en bestemt tidsperiode. NTNU har i IKT-reglementet definert tidsperiode for sletting av innhold i epost og personlige lagringsområder. Når en ansatt slutter, vil innhold i disse områdene slettes etter seks måneder. Når den ansattes brukerkonto tilknyttet Microsoft 365 slettes, vil Microsoft slette data etter 90 dager. NTNU har i tillegg egne backup-løsninger som kan lagre data i lengre perioder. Data i backup-løsninger er strengt definert i tråd med helhetlig styringssystem for informasjonssikkerhet.

#### Merknader:

- Behandling av personopplysninger forekommer i alle brukeres applikasjoner og lagringsenheter. Selv om administrator i organisasjonen kan sette bevarings- og slettepolicyer via Purview og eDiscovery, lagres personopplysninger kontinuerlig i filer lagret eksempelvis i brukeres OneDrive.
- Hvordan forholder dette seg til epostforskriften?
  - o <https://lovdata.no/pro/#reference/lov/2005-06-17-62/%C2%A79-5>  
*Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale*
- Vil det være mulig å avdekke snoking?
- En merknad til denne dokumentasjonen er at den er utilgjengelig, i den form at det er veldig mye informasjon en registrert må sette seg inn i, mange dokumenter som må gjennomleses, og informasjonen er beskrevet på en måte som gjør at

den faktiske behandlingen som gjennomføres er vanskelig å forstå ut ifra dokumentasjonen.

#### **Innspill til risikoreducerende tiltaksliste i DPIA:**

- Utarbeide nye og oppdatere eksisterende rutiner for sletting av personopplysninger
- Utarbeide rutiner for bruk av Microsofts verktøy for å administrere M365 Copilot – som for eksempel eDiscovery og Purview
- Opprette oversikt over alle apper i Microsoft «Modern work» med tilhørende retention policies
- Opprette internkontroll for å sjekke etterlevelse av nye rutiner og gjennomgang av administratorers bruk av eDiscovery og Purview
- Sikre åpenhet og informasjon til brukere om hvordan data behandles, lagres og slettes i form av å opprette (eller oppdatere) personvernerklæring

#### **Punkt 1.8 b – Er personopplysningssikkerheten tilstrekkelig ivare tatt?**

Ved bruk av M365 Copilot vil det totalt sett behandles store mengder personopplysninger i flere ulike applikasjoner innenfor Microsofts «Modern work»-plattform. I henhold til NTNUs styringssystem for informasjonssikkerhet er applikasjonene i Microsoft 365 (Modern work) klassifisert opp til «fortrolig» nivå, så fremt innholdet er kryptert med AIP. For å vurdere hvorvidt personopplysningssikkerheten ved bruk av M365 Copilot er ivare tatt, har vi tatt utgangspunkt i følgende klassifisering av informasjon: «åpen», «intern», «fortrolig» og «strengt fortrolig».

**Åpen informasjon** er tilgjengelig for alle uten særskilte tilgangsrettigheter, og er vurdert dertil at informasjonen ikke kan skade noe eller noen. Dette er for eksempel informasjon som legges ut på offentlige nettsider, kursoversikter og informasjon om pågående forskning (formidling). Det er ikke behov for å vurdere konfidensialitet. Tilgjengelighet og integritet i åpen informasjon (inkludert personopplysninger) delt av NTNU skal være høy. Åpen informasjon som NTNU behandler må være korrekt, og kan ikke endres på av uvedkommende. Om feil informasjon om for eksempel opptakskrav blir lagt ut på nett så kan det få store konsekvenser på søkermassen.

*Vurdering: NTNU vurderer at det ikke utgjør stor risiko om informasjon i kategorien «åpen» deles eller tilgjengeliggjøres. I kategorien kan det finnes personopplysninger, men disse er ansett å være offentlig delt (eks. informasjon om hvem som skal forelese i et studieprogrammer som skal offentliggjøres på NTNUs nettsider som typisk behandles i flere applikasjoner i Microsoft 365 før publisering).*

**Intern informasjon** er informasjon som er begrenset til å være tilgjengelig for ansatte med formålstjenlig behov for å kunne gjennomføre pålagte oppgaver. Eksterne med kontrollerte tilgangsrettigheter kan ha tilgang til informasjonen. Intern informasjon kan være arbeidsdokumenter, informasjon som er unntatt offentlighet og mange typer personopplysninger.



*Vurdering: NTNU vurderer at det kan være en betydelig risiko negative konsekvenser om informasjon i kategorien «intern» deles eller tilgjengeliggjøres. Behandling av interne data i NTNUs Microsoft-tenant anses som tilfredsstillende.*

**Fortrolig informasjon** er informasjon som kan skade offentlige interesser, enkeltindivider eller samarbeidspartnere hvis informasjonen kommer på avveie. Denne kategori informasjon skal kun være tilgjengelig for ansatte med formålstjenlig behov for informasjonen. Personopplysninger av særlig kategori faller innunder denne kategorien informasjon.

*Vurdering: Strengt fortrolig informasjon er informasjon som kan forårsake betydelig skade for offentlige interesser, NTNU, enkeltpersoner eller samarbeidspartnere skulle informasjonen gjøres kjent for uvedkommende. Store mengder personopplysninger av særlig kategori faller innunder denne kategorien informasjon. Data skal være kryptert jf. NTNUs lagringsguide <https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide>*

### **Bruk av M365 Copilot medfører økt risiko?**

I og med at Copilot kun har de samme tilgangene som bruker har kan det argumenteres for at bruk av Copilot ikke medfører økt risiko, for den har du allerede tatt ved å ta i bruk Microsoft 365 uten Copilot. NTNU anerkjenner argumentet, men velger likevel å vektlegge følgende som begrunnelse for hvorfor vi ikke kan akseptere argumentet fullt ut:

1. Der hvor bruker før aktivt måtte søke i filer etter for eksempel personopplysninger kan du spørre Copilot om den kan finne en bestemt type personopplysninger. M365 Copilot kan svare at «dette kan jeg ikke svare på», men det er relativt lett å omgå ved å stille spørsmål på en annen måte.
2. M365 Copilot motargumenterer. På spørsmål om den kan finne en fil kan den si at «det finnes ikke filer av denne typen», selv om det faktisk finnes. Du som bruker kan lettere akseptere «nei» fra en Copilot som du anser som en smart robot (bruk av ordet «jeg» feks)
3. M365 Copilot er en ko-pilot og du som bruker er piloten og ansvarlig for hva som skjer. I og med at M365 Copilot kan gjøre bruker mer effektiv og raskere, kan også menneskelige feil bli større og sterkere ved hjelp av M365 Copilot. En bruker som ikke kontrollerer et dokument «den fjerde gangen» like nøyaktig som de tre første fordi Copiloten «pleier å gjøre rett» kan medføre økt risiko for feil.

#### **Merknader:**

- Fokus på internkontroll, retningslinjer og endrede arbeidsformer er viktig

## **Punkt 1.9 – Informasjonssikkerhet**

### **Gjennomgå den funksjonelle beskrivelsen av alle behandlinger og om alle aktiva som skal brukes er identifisert**

*(Vurderingen er tatt med utgangspunkt for testresultatene for e-post i Outlook, Word og Teams)*

Microsoft 365 plattformen brukes i stor grad innenfor både forskning, utdanning og administrasjon. Plattformen brukes til behandling, lagring og kommunikasjon av

informasjon og er godkjent for lagring og behandling av informasjon opp til Fortrolig, gitt at den krypteres. Den totale informasjonsmengden og –verdien er derfor betydelig for NTNU.

Microsoft 365 tilbyr en rekke sikkerhetstiltak for sine kunder i skyen for å kunne beskytte dataene. Noen er “by default”, andre kan skrues på eller tilpasses egen “tenant”. For eksempel beskyttes dataene både “in transit” og “at rest” med ulik kryptering, de tilbyr Advanced Threat Protection (ATP) som for eksempel å søke gjennom lenker og vedlegg i epost og oppdage forsøk på phishing. I tillegg tilbyr de andre sikkerhetsmekanismer som Multi Faktor Autentisering (MFA), identitets- og tilgangsstyring og mange ulike innstillinger innenfor etterlevelse av regelverk og beskyttelse av data som for eksempel Data Loss Prevention (DLP). DLP dreier seg om å designe policyer som legger føringer for hvor filer av ulike klassifiseringer skal lagres og hvor de kan deles. Det vil si at mye av beskyttelsen av dataene er tilrettelagt for, men opp til brukeren selv å implementere.

Microsoft har tilgang til data som lagres i sky, men beskriver nøye hva som skal til og hvilke tilfeller dette gjøres. Dette er også mulig å unngå ved å administrere egen krypteringsnøkkel til skyløsningen. Denne vil ikke beskytte all data, men filer som lagres i skyen.

Det blir utarbeidet en egen risiko- og sårbarhetsvurdering for M365 Copilot. Denne er under utvikling ettersom testresultater blir kjent. Utisiktet avsløring av informasjon med ulike årsaker er den største risikoen sammen med ulike typer brudd på personvernlovgivning og en eventuell kommende KI-forordning.

Ifølge dokumentasjonen, deler M365 Copilot data kun internt på egen «tenant». Systemet forholder seg til ‘Semantic index’ og brukere vil kun få tilgang til innhold de allerede har tilgang til ved søk eller sammenstilling av informasjon i M365 Copilot. Dette vil si at fra Microsoft sin side tilfører ikke M365 Copilot noen endring på informasjonssikkerheten i NTNU sin tenant, men hvordan dette oppleves fra NTNU sin side er ikke nødvendigvis likt. M365 Copilot utfordrer en del innstillinger i NTNUs tenant som tidligere er tenkt har vært tilstrekkelig, men med innføring av M365 Copilot ikke blir det.

Det er helt avgjørende at dataene som legges inn og behandles i M365 Copilot er og forblir sikre. NTNU må sørge for etterlevelse av styringssystemet for informasjonssikkerhet både i en eventuell innføring av M365 Copilot og over tid. De viktigste områdene for NTNU å ha kontroll på i denne sammenheng er følgende:

### **Tilganger/tilgangsstyring må være korrekte**

Microsoft opererer med en rekke tilganger som er mulige feks: enkeltbrukere, gruppetilganger, lokale tilganger i Sharepoint med tilpassede nivåer, gjestetilganger etc. Tilgangsstyringen i Microsoft er komplisert, og sluttbrukere har i feks Sharepoint, styring på tilganger til grupper og sider.

Test av Teams Copilot viser at informasjon som ligger med tilgangen «Everyone except external users» i grupper i Sharepoint kommer opp i søkeresultatet ved bruk av Microsoft Copilot.

Et scenarie som må testes er hva som skjer med gjester som får tilganger ved NTNU og samtidig har tilgang til M365 Copilot fra en annen tenant.

## **Klassifisering av informasjon**

Labels kan brukes på alle Office-apper (Word, Excel, PowerPoint, Outlook, Publisher og Access) for å klassifisere filer og informasjon. Det er avgjørende at labels på filer/informasjon arver den høyeste klassifiseringen hvis dokumenter slås sammen eller sammenlignes.

Tester viser at sammenslåing av dokumenter klassifisert på ulike nivå (åpen, intern, fortrolig og strengt fortrolig) fungerer ved at det nye dokumentet arver den høyeste klassifiseringen.

En annen ting som det er avgjørende å få klarhet i, er om M365 Copilot klarer å identifisere hvilken informasjon som er hentet fra et fortrolig dokument, ved sammenslåing av flere ulike dokumenter. Foreløpige tester tyder på at det er vanskelig å få til, da Copilot klarer å referere utdrag fra tekst til riktig dokument, men ikke fortelle hva slags klassifisering referansene har.

Det er mulig å unnta teams og filer for tilgang til M365 Copilot. På denne måten kan ikke informasjonen fra disse kildene brukes til å lage ny eller sammenslått informasjon. Dette ser ut til å fungere godt i M365 Copilot. For at NTNU kan bruke funksjonaliteten er vi avhengig av at dette blir automatiserte prosesser og en kontinuerlig vurdering som gjøres av eier av teamet.

## **Prompt injection attacks**

Det er fremdeles usikkerhet rundt hvilke ulike angrepsvektorer som kan utnyttes om man ønsker å misbruke M365 Copilot. Et eksempel på misbruk kan være det som på engelsk kalles «Prompt Injection Attacks». Dette handler om å på ulike måter manipulere verktøyet til å produsere feilinformasjon eller annen støtende informasjon, og faktisk også overstyre de instruksjonene som originalt gis av brukeren. Hvor stor risikoen ved dette er, og hvor krevende det eventuelt er å finne gode løsninger for å forhindre det, er det vanskelig å finne gode svar på per nå. For eksempel kan dette misbrukes for å lure brukere til å klikke på en phishinglenke, dersom man kan manipulere output av en brukerinitiert spørring til å peke mot en ondsinnet lenke.

## **Sikkerhetskultur**

Manglende kunnskap blant brukerne om hva systemet gjør med informasjonen brukere legger inn, kan føre til tap av konfidensialitet, integritet og tilgjengelighet av brukernes informasjonsverdier, hvis ikke de tre foregående punktene er oppfylt.

Opplæring av brukere er essensielt for å oppnå dette. M365 har mange gode funksjoner for å hjelpe til med å sikre dataen, men disse funksjonene er ikke bare avhengig av at administratorene har satt riktig innstillinger. De er også avhengig av at brukerne selv forstår meningen med f.eks. informasjonsklassifisering, og at de er i stand til å kartlegge og klassifisere rett i henhold til retningslinjer som er satt.

## 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:	<p>Personvernforordningen artikkel 6, nr. 1 bokstav f) berettiget interesse.</p> <p>Formålet med behandlingen omfattes ikke av organisasjonens utøvelse av offentlig myndighet jf. universitets- og høgskoleloven, forvaltningsloven osv, og behandlingsgrunnlag for den aktuelle behandlingen definert i formålet kan ikke dekkes av personvernforordningen artikkel 6, nr. 1 bokstav e).</p> <p>NTNU vurderer det som riktig å fastsette berettiget interesse som behandlingsgrunnlag for M365 Copilot i driftsfase. NTNUs interesser knyttet til å holde seg «digitalt oppdatert på teknologiutviklingen» skal veie tungt så fremt det gjøres i kontrollerte former.</p>
Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem for de registrerte?	<p>Nei. NTNU må kommunisere behandlingsgrunnlaget bedre til de registrerte i personvernerklæringen og denne må holdes oppdatert</p>
Omfatter rettslig grunnlag både egne formål og eventuell utlevering?	<p>Ja, rettslig grunnlag omfatter egne formål. NTNU skal ikke utlevere data.</p>
Vurder hvordan åpenhet ivaretas i behandlingen	<p>Generelt rett til innsyn i egne personopplysninger etter personopplysningsloven (GDPR-innsyn).</p> <p>Personvernerklæringen må beskrive behandlingen av personopplysninger.</p> <p>I tillegg kommer NTNU til å være åpen med denne personvernkonsjensvurderingen på egne nettsider, og gjennom opplæringstiltak.</p>

## 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?	<p>Nei, formålet kan fremstå uklart for den registrerte, da de registrerte ikke har innblikk i NTNUs vurderinger rundt bruk av M365-plattformen. NTNU må sikre at informasjon om formål m.m. formidles til de registrerte via personvernerklæring og tilgjengeliggjøring av vurderinger rundt personvernkonsekvenser.</p> <p><i>Se utfyllende vurdering: Punkt 2.1.2 – Formålsbegrensning</i></p>
Vurder om formålet kan oppnås med en mindre inngripende behandling	<p>Hvorvidt formålet kan oppnås med en mindre inngripende behandling vil komme an på hvordan verktøyet utvikles videre av Microsoft. Pr. i dag er eneste mulighet for å oppnå (delvis) fastsatte formål med en mindre inngripende behandling, å skru av Copilot i enkelte av verktøyene som utgjør «Modern work»-plattformen. Eksempelvis kan man skru av Copilot i enkelte applikasjoner, og på den måten redusere risikoen og minimere behandlingen av personopplysninger. Dersom man skrur av tilgangen for Copilot i epost (ikke mulig pr 01.06.24) eller Graph-grounded chat vil man kunne unngå at personopplysninger behandles i Teams, samt sammensettes for å gi nye personopplysninger.</p>
Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer	<p>Det er ikke mulig å oppnå formålet ved bruk av anonyme eller pseudonyme alternativer. Behandlingen av personopplysninger innen Microsoft 365 og M365 Copilot er omfattende og kontinuerlig, som medfører at anonymisering og pseudonymisering ikke er mulig med disse verktøyene. Du kan for eksempel pseudonymisere innholdet i wordfiler, men metadataene som registrerer hvem som er forfatter av dokumentet er knyttet til bruker og dermed direkte identifiserbare personopplysninger.</p>

### 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 er laget slik at det har tilgang til alt som en bruker har tilgang til. Verktøyet er en klon av brukeren selv, og alle tilganger brukeren har, vil M365 Copilot også ha.
Begrunn nødvendighet og relevans relatert til formål for hver enkelt variabel i et datasett	<p>Copilot for M365 i driftsfasen vil potensielt behandle veldig mange datasett med veldig mange variabler. Dette avhenger av hvor mange brukere som vil få lisens i en driftsfase, og hvordan man organiserer rammene rundt forvaltningen av verktøyet. Personinformasjon i form av kjernedata, som navn, brukernavn, epostadresse osv har NTNU god kontroll på. «Brukerinitierte» datasett som opprettelse av nye team på eget initiativ, teams-gruppechatter, filer som inneholder personopplysninger osv, har NTNU liten overordnet kontroll på og er avhengig av at brukerne gjør riktige valg.</p> <p>Det vil ikke være gjennomførbart for NTNU å kunne begrunne nødvendighet og relevans relatert til formål for hver enkelt av variablene i de datasettene som finnes i brukerens tilgang til Microsoft 365 plattformen, uten en mer grundig gjennomgang og systematisk oppfølging.</p> <p>Det påpekes at M365 Copilot som verktøy er laget for å behandle store mengder data som organisasjonen har tilgjengelig i form av brukernes filer, epost, chatter, kalenderoppføringer og annen samhandling i Teams etc.</p> <p>NTNU vil understreke at å inneha orden i eget hus vil kunne forenkle arbeidet med å overholde dataminimeringsprinsippet. Dette vil kunne bidra til å redusere antall datasett som inneholder personopplysninger som behandles i M365 plattformen, og som deretter tilgjengeliggjøres for M365 Copilot.</p>

## 2.1.4 Riktighet

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

<p>Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering</p>	<p>Todelt problemstilling:</p> <ul style="list-style-type: none"><li>- Administratorene i M365 teamet holder en korrekt og oppdatert oversikt over alle brukere i brukerdatatabasen i form av tilgangsstyring via Entra ID.</li><li>- Personopplysninger som behandles i applikasjonene i M365 deles på en måte som ikke tidligere har forekommet i organisasjonen. Hvis deling av feilaktige personopplysninger forekommer, vil behandlingsansvarlig ha lite kontroll på denne behandlingen, grunnet kompleksiteten i dataflyten og kontinuerlig behandling av personopplysninger.</li></ul> <p><i>Se utfyllende vurdering: Punkt 2.1.4 – Riktighet</i></p>
<p>Vurder om dere har nødvendig funksjonalitet for å rette og slette uriktige opplysninger</p>	<p>IT-avdelingen administrerer brukerkontoer i M365, og håndterer retting og sletting kontinuerlig tilknyttet brukerkontoer. Retting og sletting av personopplysninger som deles i M365 applikasjonene kan gjøres på ulike måter. Administrator kan slette data via eDiscovery og eier av dokumenter kan slette og rette personopplysninger i eget materiale.</p> <p><i>Se Utfyllende vurdering: Punkt 2.1.4 – Riktighet»</i></p>
<p>Ut ifra den registrertes perspektiv, er det behov for kontradiksjon?</p>	<p>Det ligger i dette verktøyets natur å kunne gi uriktige opplysninger. Behovet for kontradiksjon må derfor vurderes kontinuerlig, og det bør særlig vurderes om M365 Copilot bør benyttes i prosesser der det er naturlig med kontradiksjon.</p> <p>Behandlingsansvarlig ønsker at brukere skal kunne ta aktivt stilling til informasjonen løsningen gir, og være grunnleggende kritisk til informasjonen som en språkmodell gir nettopp for å motvirke faren for at uriktige opplysninger blir vurdert som riktige.</p>

### 2.1.5 Lagringsbegrensning

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

<p>Vurder om personopplysninger lagres etter at formålet er oppnådd</p>	<p>Innstillinger for lagring, mellomlagring og sletting er tilgjengeliggjort for organisasjonens administratorer. Microsoft opererer med «retention policies» som kan administreres på ulike måter for de ulike appene i «Modern work»-plattformen. «Retention policies» er retningslinjer som bestemmer hvor lenge data skal behandles (lagres), og hva som skal skje med dataene når de ikke lenger er nødvendig. Ved bruk av «retention policies» kan administratorer sikre at personopplysninger ikke lagres etter at formålet er oppnådd. Formålet er typisk oppnådd når for eksempel en ansatt slutter og ikke lenger er aktiv bruker i organisasjonens Microsoft-plattform.</p> <p>Gjeldende «Retention policies» må forvaltes på lik linje med alt annet, og det er behov for å vurdere informasjonsplikt overfor brukerne og å etablere internkontrollrutiner på området</p> <p><i>Se utfyllende vurdering: Punkt 2.1.5 – Lagringstidsbegrensning</i></p>
<p>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.</p>	<p>Bruken av Microsoft verktøy forutsetter en aktiv bruker og et aktivt avtaleforhold til NTNU (for eksempel arbeidsavtale). Når du ikke har en aktiv bruker blir data i Microsoft verktøyene slettet i tråd med policy. Arkivering/etterlagring av personopplysninger håndteres i andre fagsystemer (for eksempel HR-system).</p>

### 2.2 De registrertes rettigheter

<p>Vurder hvordan informasjon til de registrerte gis</p>	<p>NTNU vil oppdatere personvernerklæringen og inkludere informasjon som gjenspeiler informasjonen om bruk av M365 Copilot i behandlingsprotokollen.</p>
--	--



	<p>NTNU er i ferd med å endre hovedsystem for behandlingsprotokollen, og vil i løpet av høsten 2024 gjennomgå alle identifiserte saksprosesser hvor kunstig intelligens (deriblant M365 Copilot) er tatt i bruk.</p> <p>NTNU vil også tilgjengeliggjøre DPIA, og annen dokumentasjon fra prosjektet.</p>
<p>Vurder innhenting av samtykke, jf. art 7 og 8</p>	<p>Samtykke benyttes ikke som behandlingsgrunnlag.</p> <p>Det bør bemerkes at samtykke ble benyttet i testfasen av verktøyet. Dette var en vurdering som ble gjort i prosjektet for å få en utvetydig bekreftelse på at testerne forsto hva de var med på, og at de forsto hvordan egne personopplysninger kunne bli behandlet av verktøyet.</p>
<p>Vurder hvordan den registrertes rett til innsyn og til dataportabilitet ivaretas, jf. art. 15 og 20</p>	<p>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 <a href="https://innsida.ntnu.no/wiki/-/wiki/Norsk/Personvernerklæring+NTNU">https://innsida.ntnu.no/wiki/-/wiki/Norsk/Personvernerklæring+NTNU</a></p> <p>Det blir i tillegg utviklet en egen modul for innsyn etter GDPR gjennom prosjektet NTNU Sak, og tilgangen til M365 Copilot inngår i datagrunnlaget med personopplysninger som Microsoft vet om NTNUs brukere.</p> <p>Det må vurderes hvorvidt et innsynskrav kan besvares fullt ut, da NTNU som behandlingsansvarlig vil ha utfordringer med å identifisere alle steder personopplysninger kan bli behandlet i M365 Copilot (dette er også identifisert som et problem ved bruk av Microsoft 365 plattformen uten bruk av Copilot).</p> <p>M365 Copilot vil kunne skape nye personopplysninger basert på informasjon M365 Copilot har tilgang til via brukeren. Ved et innsynskrav vil det være vanskelig å oppgi kilden til personopplysningene</p>

	<p>som M365 Copilot har skapt basert på prompts fra brukeren.</p> <p>Personopplysninger kan også i visse tilfeller behandles av mottakere i tredjeland ved eksempelvis teknisk support hvor databehandler benytter underleverandører i tredjeland.</p>
<p>Vurder hvordan den registrertes rett til korrigerings og sletting ivaretas, jf. 16 og 17</p>	<p>De registrerte har rett til å få uriktige personopplysninger rettet eller slettet og ufullstendige personopplysninger komplettert. Informasjon om de registrertes rettigheter fremkommer i NTNUs personvernerklæring.</p> <p>Personopplysninger vil potensielt kunne være lagret hos alle brukere i organisasjonen, for eksempel i et dokument som kun er lagret hos en person. I disse tilfellene vil det være vanskelig for behandlingsansvarlig å tilrettelegge for håndheving av de registrertes rettigheter da oversikt over hvor aktuelle personopplysninger ligger lagret ikke finnes.</p> <p>Den registrerte kan selv rette og slette personopplysninger en har tilgang til, for eksempel ved samhandling med andre i Teams-kanaler.</p> <p>M365 Copilot kan skape nye personopplysninger basert på informasjon den har tilgang til. M365 Copilot bruker en LLM for å besvare prompts fra en bruker, og testing avdekker at hallusinerings forekommer på regelmessig basis om ikke prompten er presis nok. M365 Copilot vil dermed kunne skape personopplysninger om registrerte som er direkte feil. Dette vil være personopplysninger som er tilknyttet en person, men som vil kunne oppfattes som feil av den registrerte, men ikke nødvendigvis av andre som behandler personopplysningene. For eksempel om M365 Copilot selv har funnet på at navngitt person har mastergrad selv om vedkommende ikke har det, så vil det på</p>

	<p>NTNU være stor sannsynlighet for at ingen legger merke til det annet enn personen selv fordi det å ha mastergrad er vanlig.</p> <p>NTNU kan til en viss grad bistå i å rette og slette personopplysninger på bakgrunn av henvendelser fra de registrerte. Dette vil dog ikke garantere en fullstendig retting eller sletting av personopplysninger da det er utfordrende å holde oversikt over alle behandlinger i alle brukeres M365.</p> <p><i>Se utfyllende vurdering: Punkt 2.2 – De registrertes rettigheter»</i></p>
<p>Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas, jf. art. 18, 19 og 21</p>	<p>De registrerte kan be om at NTNU begrenser behandlingen av personopplysninger ved å bestride riktigheten, og har rett til å protestere mot behandling av sine personopplysninger hvis behandlingens rettslige grunnlag samsvarer med personvernforordningens art. 21 nr. 1. Artikkel 19 omfatter underretning av enhver mottaker om beslutning om retting, sletting eller begrensning.</p>
<p>Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering, håndheves, jf. art. 22</p>	<p>NTNUs formål med verktøyet er ikke å gjennomføre automatiserte avgjørelser, eller profilere brukere. NTNU etablerer systematiske internkontrollrutiner koblet til behandlingsprotokoll for å sikre at denne typen verktøy ikke blir benyttet til oppgaver som kan være i strid med artikkel 22.</p> <p>Verktøyet er en samtalerobot laget med kunstig intelligens. 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 saksbehandlingsskjede uten at saksbehandler eksplisitt informerer eller</p>

	<p>gjøre rede for at kunstig intelligens er benyttet.</p> <p>Det er uklart hvorvidt formålet med funksjoner som Microsoft har implementert i løsningen kan bidra til profilering av de registrerte. Funksjoner som har blitt oppdaget i testingen tilsier at sett med personopplysninger brukes til å sette sammen nye personopplysninger om de registrerte. Hvorvidt disse personopplysningene bør regnes som profilering er foreløpig uklart for NTNU, men for å være på sikre siden bør det regnes som sannsynlig at profileringsbehandling kan skje ved bruk av verktøyet.</p> <p>Gjennom retningslinjer og opplæring vil det være tydelig hvilke oppgaver M365 Copilot kan brukes til og ikke.</p> <p><i>Se utfyllende vurdering: Punkt 2.2 – De registrertes rettigheter (art. 22)»</i></p>
--	---

## Utfyllende vurderinger punkt 2.1.2 – 2.2

Utfyllende vurderinger til alle punkter følger nedenfor.

### Punkt 2.1.2– Formålsbegrensning

#### **Er formålet klart definert? Er formålet definert slik at det samsvarer med forventningene til den registrerte?**

Det er utfordrende å definere formålet med bruk av M365 Copilot i samsvar med Personvernforordningens artikler 5 og 6. M365 Copilot er en tilleggsfunksjonalitet innebygd i eksisterende verktøy som tekstbehandling, e-post og regneark. Formålet med behandlingen må derfor ses i sammenheng med bruken av disse verktøyene, hvor M365 Copilot fungerer som en "forsterker" med tanke på effektivitet, behandlingsomfang av personopplysninger og risiko.

Konklusjonen er at beskrivelsen av behandlingens formål for bruk av M365 Copilot må sees i sammenheng med eksisterende Microsoft-verktøy. Dette bør dokumenteres gjennom rammeverk og oversikt over saksprosesser, protokoll over behandling av

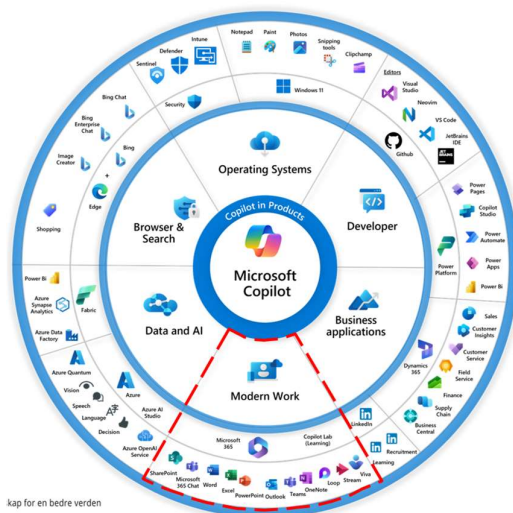
personopplysninger og bruken av verktøy med innebygd kunstig intelligens. M365 Copilot må vurderes for hver enkelt saksprosess av prosessansvarlige.

Med dette formålet som grunnlag, kan det fremstå uklart for den registrerte da de registrerte ikke har utdypende innblikk i NTNUs vurderinger rundt bruk av M365-plattformen. NTNU må sikre at informasjon om formål m.m. formidles til de registrerte via personvernerklæring og tilgjengeliggjøring av vurderinger rundt personvernkonsekvenser.

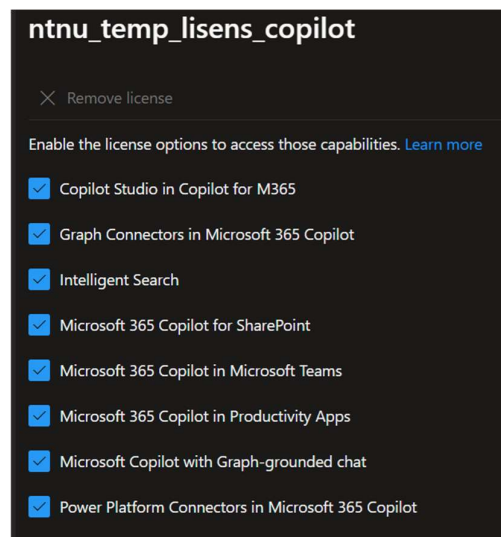
## Vurder om formålet kan oppnås med en mindre inngripende behandling

Hvorvidt formålet kan oppnås med en mindre inngripende behandling vil komme an på hvordan verktøyet utvikles videre av Microsoft. Pr. i dag er eneste mulighet for å oppnå (delvis) fastsatte formål med en mindre inngripende behandling, å skru av Copilot i enkelte av verktøyene som utgjør «Modern work»-plattformen. Eksempelvis kan man skru av Copilot i enkelte applikasjoner, og på den måten redusere risikoen og minimere behandlingen av personopplysninger. Dersom man skrur av Copilot med Graph-grounded chat vil man kunne unngå at personopplysninger behandles i Teams, samt sammensettes for å gi nye personopplysninger.

Hvorvidt du fortsatt oppnår fastsatt formål ved å skru av Copilot i ulike applikasjoner bør vurderes jevnlig.



Figur: Microsoft sin oversikt over Copilot tjenester



Figur: Oversikt over hvilke applikasjoner som kan skrur av pr. 21.05.24

## Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer

Det er ikke mulig å oppnå formålet ved bruk av anonyme eller pseudonyme alternativer. Behandlingen av personopplysninger innen Microsoft 365 og M365 Copilot er omfattende og kontinuerlig, som medfører at anonymisering og pseudonymisering ikke er mulig med

disse verktøyene. Du kan for eksempel pseudonymisere innholdet i wordfiler, men metadataene som registrerer hvem som er forfatter av dokumentet er knyttet til bruker og dermed direkte identifiserbare personopplysninger.

**Merknader:**

- Hvorvidt du fortsatt oppnår fastsatt formål ved å skru av Copilot i ulike applikasjoner bør vurderes jevnlig.

**Innspill til risikoreduserende tiltaksliste i DPIA:**

- Vurdere å ta i bruk Microsoft Priva portalen for administratorer
- Etablere rutiner for bruk av Purview for administratorer

## Punkt 2.1.4 – Riktighet

### **Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering**

Personopplysninger behandles i alle applikasjoner i Microsofts «Modern work»-plattform (Outlook, Teams, Word, OneDrive etc), i tillegg til å bli behandlet i bruker databasen/Entra ID. Å holde personopplysninger korrekte og oppdaterte er en flerdelt problemstilling. På den ene siden i form av tilgangsstyring og brukeradministrasjon som utføres av NTNUs administratorer, og på den andre siden i form av all annen behandling av personopplysninger i Microsoft-plattformen.

Administratorer holder en korrekt og oppdatert oversikt over alle brukere i bruker databasen i form av tilgangsstyring via Entra ID. Dette er en nødvendig behandling for å gi brukere tilgang til Microsoft-applikasjonene som ansatt/annen bruker. Disse personopplysningene kontrolleres, og holdes oppdaterte og korrekte gjennom kjernesystemer som styres av IT-avdelingen.

Personopplysninger vil bli behandlet i alle applikasjoner i «Modern work»-plattformen. Personopplysninger flyter mellom brukere (for eksempel står navnet ditt på teammeldingen du har sendt eller merknaden du har lagt igjen i et word-dokument), og deles på en måte som ikke tidligere har forekommet i organisasjonen. Utveksling av brukerinformasjon er en forutsetning for samhandling. Hvis det forekommer behandling av ukorrekte personopplysninger i brukeres applikasjoner (for eksempel at du skriver et navn feil), som deles videre med andre brukere, vil behandlingsansvarlig ha lite kontroll på denne behandlingen. Personopplysninger som oppfattes som uriktig og behandles på denne måten, vil kunne rettes hvis den registrerte selv opplyser om det. Uten involvering av den registrerte selv, vil behandlingsansvarlig ha problemer med å oppfatte og å rette feilaktige personopplysninger. Dette gjenspeiles i kompleksiteten i dataflyten, og hvordan personopplysninger kontinuerlig behandles.

### Copilot og LLM

En språkmodell (large language model – LLM) vil beregne sannsynligheten for hva det neste ordet i en sammenheng er, og dermed skape en tekst som kan bestå av personopplysninger som oppfattes som ukorrekt eller udaterte. Tolkning av personopplysninger i en slik tekst er det umulig å forutse resultatet av. Det er stor sannsynlighet for at språkmodellen kan gi ulike og feilaktige svar, og sannsynligheten øker om brukeren gir upresise kommandoer til språkmodellen. Bruk av Copilot i Teams Graph-grounded chat vil kunne medføre tolkning av personopplysninger og opprettelse av nye personopplysninger basert på en registrert sin

aktivitet. Det er umulig å si om disse personopplysningene er korrekte, de kan ikke holdes oppdatert og den registrerte selv vet ikke at disse personopplysningene skapes.

### Eksempel:



Figur – Skjerm bilde av mood-kommando til Copilot

### Har vi nødvendig funksjonalitet for å rette og slette uriktige opplysninger?

Retting og sletting av feil eller utgåtte brukerkontoer administreres av IT-avdelingen og gjennomføres kontinuerlig i form av oppdatering av kjernesystemet.

Copilot for Microsoft 365 har flere muligheter for å slette uriktige opplysninger.

Administratorer kan slette Copilot-data via eDiscovery. Hvis data involverer input/output prompts fra Copilot Graph-grounded chat, kan sletting gjennomføres via eDiscovery i brukerens Exchange mailboks. Dette kan kun gjennomføres av administratorer.

Dersom det oppdages at uriktige personopplysninger er lagret i filer i brukernes applikasjoner, må disse slettes eller rettes av noen som har eierrettigheter til dokumentet.

Sletting av ukorrekte personopplysninger som skapes av Copilot (jf. ovennevnte eksempel) kan gjøres gjennom administrator med eDiscovery-tilgang. Det er uklart om personopplysningene kan rettes.

Som behandlingsansvarlig kan NTNU legge til rette for enklere utøvelse av retting og sletting av uriktige personopplysninger ved å informere om hvordan dette kan gjøres, både fra administratorsiden og den registrerte selv.

### Merknader:

- M365 Copilot er en samtalerobot som bruker språkmodellteknologi. Det vil være umulig å gardere seg mot at en bruker stiller spørsmål ala «hvilket humør virker NAVN å være i».

### Innspill til risikoreducerende tiltaksliste i DPIA:

- Opprette rutiner som synliggjør ansvar for retting, og hvor registrerte kan henvende seg for å få personopplysninger rettet eller slettet
- Informasjon til de registrerte om hvordan retting og sletting av ukorrekte personopplysninger kan gjennomføres

## Punkt 2.1.5 – Lagringstidsbegrensning

### **Vurder om personopplysninger lagres etter at formålet er oppnådd**

Innstillinger for lagring, mellomlagring og sletting er tilgjengeliggjort for organisasjonens administratorer. Microsoft opererer med «retention policies» som kan administreres på ulike måter for de ulike appene i «Modern work»-plattformen. «Retention policies» er retningslinjer som bestemmer hvor lenge data skal behandles (lagres), og hva som skal skje med dataene når de ikke lenger er nødvendig. Gjeldende «Retention policies» må forvaltes på lik linje med alt annet, og det er behov for å vurdere informasjonsplikt overfor brukerne og å etablere internkontrollrutiner på området.

Ved bruk av disse «retention policies» kan administratorer sikre at personopplysninger ikke lagres etter at formålet er oppnådd. Formålet er typisk oppnådd når for eksempel en ansatt slutter og ikke lenger er aktiv bruker i organisasjonens Microsoft-plattform.

Videre må behandlingsansvarlig (NTNU) ha rutiner og systematisk oppfølging av brukere som slutter eller som ikke lenger skal ha tilgang til Microsoft-plattformen via NTNU. Dette reguleres etter NTNUs IKT-reglement. Brukeren til en ansatt som slutter settes inaktiv og ivaretas i 6 måneder etter sluttdato. Etter denne perioden vil brukeren og alt innhold (deriblant personopplysninger som har blitt behandlet av brukeren) slettes. Microsoft sletter alt innhold 90 dager etter at NTNU har slettet brukeren.

NTNU har i tillegg egne backup-løsninger som kan lagre data i lengre perioder. Data i backup-løsninger er strengt definert i tråd med helhetlig styringssystem for informasjonssikkerhet.

### **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.**

Bruken av Microsoft verktøy forutsetter en aktiv bruker og et aktivt avtaleforhold til NTNU (for eksempel arbeidsavtale). Når du ikke har en aktiv bruker blir data i Microsoft verktøyene slettet i tråd med policy, og eventuell lagring av personopplysninger håndteres i andre fagsystemer (for eksempel HR-system).

### **Innspill til risikoreducerende tiltaksliste i DPIA:**

- Sikre at rutiner for sletting av bruker og innhold følges

## Punkt 2.2 – De registrertes rettigheter

### **Vurder hvordan den registrertes rett til korrigerings og sletting ivaretas, jf. 16 og 17. Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas, jf. art. 18, 19 og 21?**

Den registrerte har etter personvernforordningens kapittel 3 ulike rettigheter som man kan kreve overholdt fra den behandlingsansvarlige. I dette dokumentet vurderes det hvordan NTNU som behandlingsansvarlig kan overholde de registrertes rettigheter etter art. 12 – 14, 16, 17, 18, 19 og 21.



- **Artikkel 12 – 14 – rett til informasjon**  
Den registrerte har rett til å få vite hvilke behandlinger som foregår, og hvilke rettigheter de har i forbindelse med behandlingene
- **Artikkel 15 – rett til innsyn**  
Den registrerte har rett til å få innsyn i hvilke personopplysninger som er lagret om seg selv.
- **Artikkel 16 – rett til retting**  
Den registrerte har rett til å få uriktig informasjon om seg selv rettet. Ufullstendige personopplysninger kan kreves gjort fullstendige.
- **Artikkel 17 – rett til sletting**  
Den registrerte har rett til at personopplysninger om seg slettes – artikkelen har visse unntak.
- **Artikkel 18 – rett til begrensning av behandling**  
Retten til begrensning innebærer at en registrert kan begrense måten en virksomhet bruker ens personopplysninger – kan kreve behandlingen stanset
- **Artikkel 19 - Underretningsplikt i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling**  
Den behandlingsansvarlige skal underrette enhver mottaker som har fått utlevert personopplysninger, om enhver retting eller sletting av personopplysninger eller begrensning av behandlingen utført i samsvar med artikkel 16, artikkel 17 nr. 1 og artikkel 18.
- **Artikkel 21 – rett til å protestere**  
Den registrerte kan protestere mot behandlingen av deres personopplysninger – kan be virksomheten stanse behandlingen

### **Artikkel 12 – 14 – rett til informasjon**

NTNU vil oppdatere personvernerklæringen og inkludere informasjon som gjenspeiler informasjonen om bruk av Copilot i behandlingsprotokollen. NTNU er i ferd med å endre hovedsystem for behandlingsprotokollen, og vil i løpet av høsten 2024 gjennomgå alle identifiserte saksprosesser hvor Copilot (kan) tas i bruk. NTNU vil også tilgjengeliggjøre personvernkonskvensvurderingen (DPIA), og annen dokumentasjon fra prosjektet.

### **Artikkel 15 – rett til innsyn**

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 M365 Copilot inngår i datagrunnlaget med personopplysninger som Microsoft vet om NTNUs brukere.

Det må vurderes hvorvidt et innsynskrav kan besvares fullt ut, da NTNU som behandlingsansvarlig vil ha utfordringer med å identifisere alle steder personopplysninger kan bli behandlet i Copilot for M365 (dette kan identifiseres som et problem med M365 plattformen uten bruk av Copilot også).

M365 Copilot vil kunne skape nye personopplysninger basert på informasjon Copilot har tilgang til via bruker. Ved et innsynskrav til det være vanskelig å oppgi kilden til personopplysningene som Copilot har skapt basert på prompts fra bruker.

Personopplysninger kan også i visse tilfeller behandles av mottakere i tredjeland ved eksempelvis teknisk support hvor databehandler benytter underleverandører i tredjeland.

### **Artikkel 16 – rett til retting og artikkel 17 – rett til sletting**

De registrerte har rett til å få uriktige personopplysninger rettet eller slettet og ufullstendige personopplysninger komplettert. Informasjon om de registrertes rettigheter fremkommer i NTNUs personvernerklæring.

Personopplysninger vil potensielt kunne være lagret hos alle brukere i organisasjonen, for eksempel i et dokument som kun er lagret hos en person. I disse tilfellene vil det være vanskelig for behandlingsansvarlig å tilrettelegge for håndheving av de registrertes rettigheter da oversikt over hvor aktuelle personopplysninger ligger lagret ikke finnes.

Den registrerte kan selv rette og slette personopplysninger en har tilgang til, for eksempel ved samhandling med andre i Teams-kanaler.

M365 Copilot kan skape nye personopplysninger basert på informasjon den har tilgang til. M365 Copilot bruker en LLM for å besvare prompts fra en bruker, og testing avdekker at hallusinerer forekommer på regelmessig basis om ikke prompten er presis nok. M365 Copilot vil dermed kunne skape personopplysninger om registrerte som er direkte feil. Dette vil være personopplysninger som er tilknyttet en person, men som vil kunne oppfattes som feil av den registrerte, men ikke nødvendigvis av andre som behandler personopplysningene. For eksempel om M365 Copilot selv har funnet på at navngitt person har mastergrad selv om vedkommende ikke har det, så vil det på NTNU være stor sannsynlighet for at ingen legger merke til det annet enn personen selv fordi det å ha mastergrad er vanlig.

NTNU kan til en viss grad bistå i å rette og slette personopplysninger på bakgrunn av henvendelser fra de registrerte. Dette vil dog ikke garantere en fullstendig retting eller sletting av personopplysninger da det er utfordrende å holde oversikt over alle behandlinger i alle brukeres M365.

### **Artikkel 18, 19 og 21**

De registrerte kan be om at NTNU begrenser behandlingen av personopplysninger ved å bestride riktigheten, og har rett til å protestere mot behandling av sine personopplysninger hvis behandlingens rettslige grunnlag samsvarer med personvernforordningens art. 21 nr. 1. Artikkel 19 omfatter underretning av enhver mottaker om beslutning om retting, sletting eller begrensning.

### **Vurdering**

NTNU har, som behandlingsansvarlig, ansvar for at de registrerte kan ivareta sine rettigheter ved framsatt krav. For at de registrerte kan håndheve sine rettigheter må

NTNU legge til rette for mottak av begjæringer om retting, sletting, begrensning etc. NTNU må også overholde informasjonsplikten ovenfor de registrerte, slik at utøving av rettigheter kan gjennomføres på en enkel og forståelig måte.

Personopplysninger som omhandler andre registrerte enn brukeren selv, vil potensielt kunne være lagret hos alle brukere i organisasjonen, for eksempel i et dokument som kun er lagret hos en person. I disse tilfellene vil det være vanskelig for behandlingsansvarlig å tilrettelegge for håndheving av de registrertes rettigheter da oversikt over hvor aktuelle personopplysninger ligger lagret ikke finnes.

NTNU kan til en viss grad bistå de registrerte med å utøve sine rettigheter, men det er vanskelig å kunne svare ut henvendelser rundt oppfyllelse av de registrertes rettigheter da verktøyet Copilot for M365 er oppbygd på en måte som gjør at fullstendig oversikt over hvor personopplysninger behandles.

NTNU som behandlingsansvarlig har også behov for bistand fra Microsoft som databehandler for å kunne oppfylle de registrertes rettigheter.

Microsoft vil tilgjengeliggjøre muligheten for at de registrertes rettigheter kan oppfylles, jf. Microsofts databehandleravtale (DPA pr. 02.02.24), dvs. tilgjengeliggjøre funksjonalitet i programvaren slik at behandlingsansvarlig kan bistå den registrerte i å oppfylle sine rettigheter. Microsoft kan motta og bistå behandlingsansvarlig i rimelige forespørsler, men det antas at det henvises til databehandleravtalen og behandlingsansvarliges ansvar.

**Merknader:**

- Å holde oversikt over alle personopplysninger i alle «kriker og kroker» kan være utfordrende, og det å holde oversikt kan også i seg selv være unødvendig inngripende overfor brukerne (overvåkingsmekanismer).

**Innspill til risikoreducerende tiltaksliste i DPIA:**

- Vurdere å ta i bruk Microsoft Priva portalen for administratorer. Mulighetsrom må utredes.
- Etablere rutiner for bruk av Purview for administratorer.
- Vurdere om bruk av Double Key Encryption (DKE) kan aktiveres for filer med personopplysninger som har fått innvilget begrensning.
- Slå av funksjonalitet i verktøyet som omfatter profilering
- Sørge for rutiner for lagring av data og internkontroll
- Opplæring av brukere
- Gjennomføre vurdering mot annet relevant lovverk som eksempelvis forvaltningsloven og arkivloven for å sørge for at arkivverdig informasjon blir lagret og annen informasjon blir slettet

## Punkt 2.2 – Særskilt om forbud mot automatiserte individuelle avgjørelser og profilering

### **Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering, håndheves, jf. art. 22**

Personvernforordningen definerer profilering i artikkel 4 nr. 4 som «enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelser».

NTNUs formål med verktøyet er ikke å gjennomføre automatiserte avgjørelser, eller profilere brukere. NTNU etablerer systematiske internkontrollrutiner koblet til behandlingsprotokoll for å sikre at denne typen verktøy ikke blir benyttet til oppgaver som kan være i strid med artikkel 22.

#### Vurdering av forbud mot automatiserte individuelle avgjørelser

Verktøyet er en samtalerobot laget med kunstig intelligens, og i en driftsfase vil det kunne brukes fritt av ansatte 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 eksemplene 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. Gjennom retningslinjer og opplæring vil det påpekes at løsningen ikke skal benyttes til dette.

Følgende beskrivelse (i kursiv) er skrevet av Copilot, formatert, redigert og kvalitetssikret av prosjektleder, og gir et godt bilde av problemstillingen:

*For å sikre at den registrerte har rett til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, inkludert profilering, som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende, er det viktig å huske på følgende:*

1. **Informer den registrerte:** Den registrerte skal informeres om at en avgjørelse kan bli tatt basert på automatisert behandling, og de skal gis informasjon om logikken bak, samt betydningen og de planlagte konsekvensene av slik behandling.
2. **Gi den registrerte en mulighet til å protestere:** Den registrerte skal ha rett til å protestere mot automatisert individuell beslutningstaking, inkludert profilering.
3. **Menneskelig inngripen:** Hvis en avgjørelse er tatt utelukkende på grunnlag av automatisert behandling, har den registrerte rett til å be om menneskelig inngripen, uttrykke sitt synspunkt og bestride avgjørelsen.
4. **Nøyaktighet av data:** Sørg for at dataene som brukes i den automatiserte beslutningsprosessen er nøyaktige og oppdaterte. Ukorrekte data kan føre til feilaktige avgjørelser.

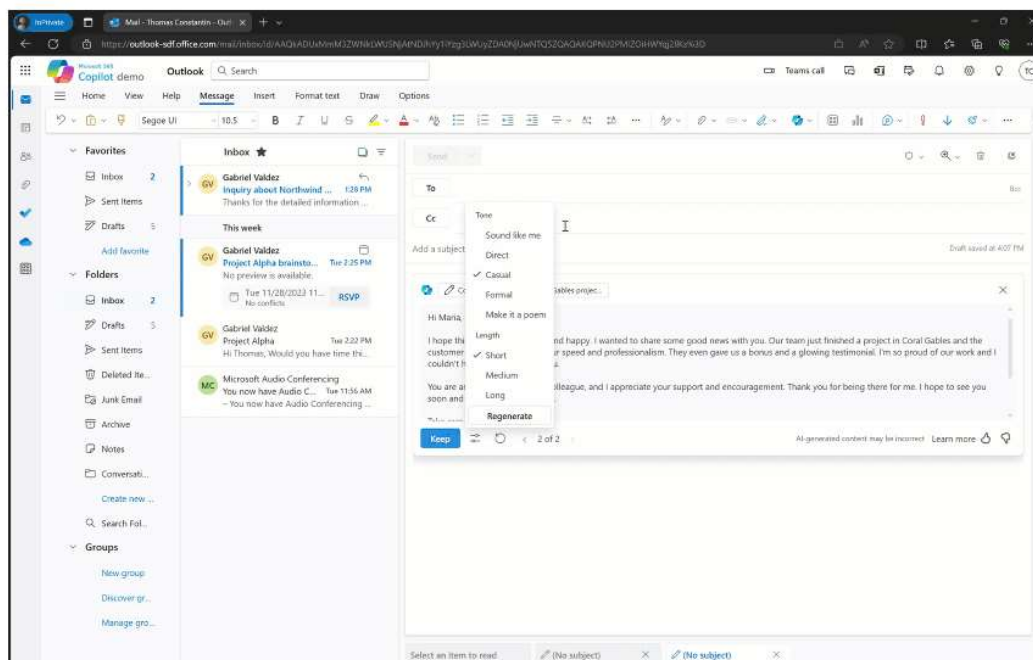
5. **Datasikkerhet:** Implementer passende tekniske og organisatoriske tiltak for å sikre datasikkerheten og beskytte den registrertes personopplysninger mot uautorisert tilgang, endring, sletting eller overføring.
6. **Regelmessig gjennomgang:** Gjennomgå regelmessig de automatiserte beslutningsprosessene for å sikre at de fortsatt er rettferdige, nøyaktige og respekterer den registrertes rettigheter.

NTNU kan ikke anbefale at Copilot tas i bruk i saksbehandling som er bestemmende for rettigheter og plikter for enkeltpersoner før totaliteten i saksbehandlingsskjeden, og hvordan kunstig intelligens påvirker saksbehandlingen, er «lest og forstått» av alle involverte parter.

### Vurdering av profilering av brukere

Det er uklart hvorvidt formålet med funksjoner som Microsoft har implementert i løsningen kan bidra til profilering av de registrerte. Funksjoner som har blitt oppdaget i den funksjonelle testfasen tilsier at sett med personopplysninger brukes til å sammensette nye personopplysninger om de registrerte. Hvorvidt disse personopplysningene bør regnes som profilering, er uklart for NTNU, men vi har valgt å regne det som høyst sannsynlig at profileringsbehandling skjer.

Eksempler på to slike funksjoner er "sound like me" i Microsoft 365, spesifikt i Microsoft Outlook. Denne funksjonen ble annonsert under et Surface-årsarrangement. Microsoft har uttalt at deres Copilot AI-assistentverktøy kan "personalisere enhver e-post for å matche din unike stil og tone i stemmen". Dette betyr at KI-verktøyet kan lære og tilpasse seg din skrivestil over tid både for å gjøre kommunikasjonen mer personlig og effektiv, men det er også et økt potensial og fare for misbruk gjennom for eksempel å etterligne mennesker.

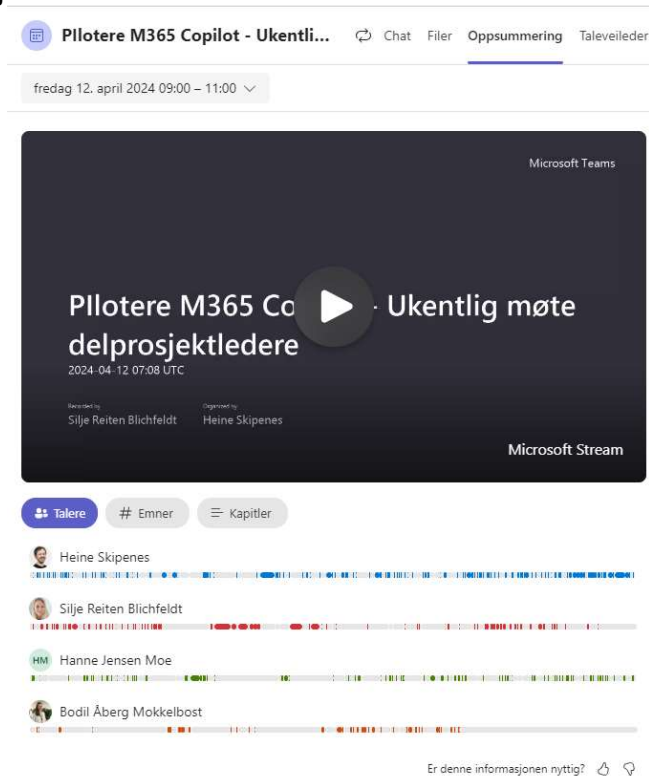


Copilot helps you draft a message that sounds like you

Figur 1: Skjerm bilde fra Copilot Demo: Outlook (kilde: Microsoft)

NTNUs testing har ikke funnet «sound like me» funksjonalitet i verktøyet, og har derfor ikke testet det.

Et annet eksempel på en funksjon som bruker personopplysninger for å analysere de registrertes atferd og arbeidsprestasjon er opptak og transkripsjonsfunksjonen i Teams. Denne funksjonen kan ta opptak av møter og transkribere, samt identifisere hvem som sa hva og hvem som snakket mest. Man kan deretter spørre Copilot om hvem som gjorde en god jobb i møtet, hvem som bør bidra mer og få forbedringspunkter rundt deltakernes prestasjoner i møtet.



Figur – Skjerm bilde fra Teams – opptaksfunksjon

#### Merknader:

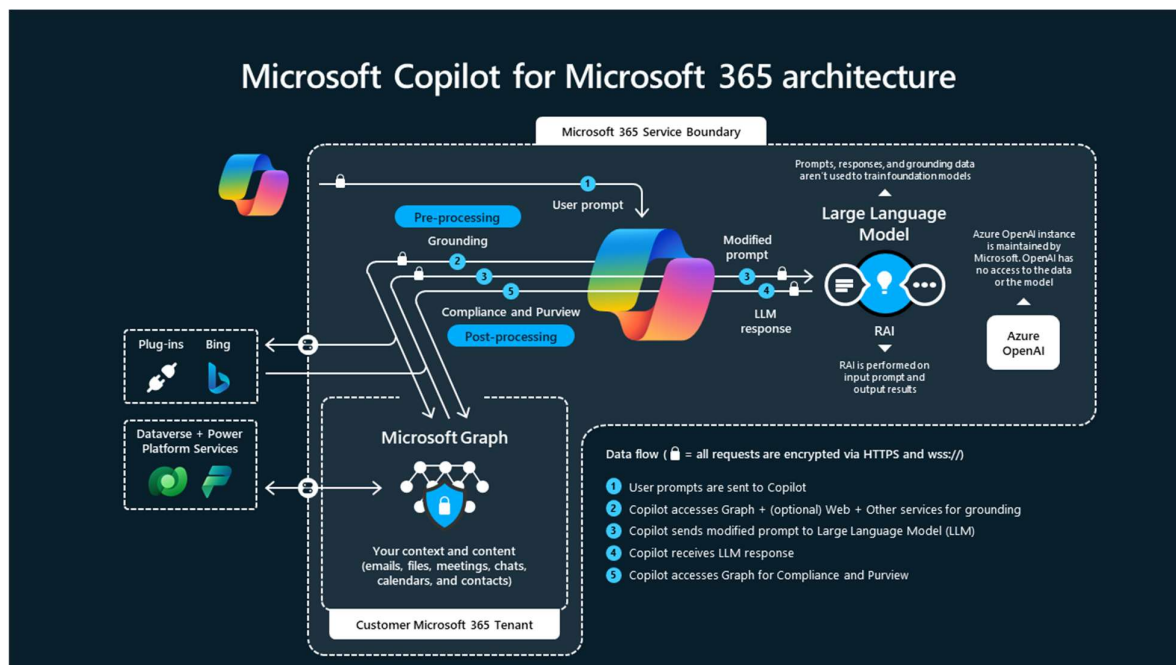
- NTNU kan ikke anbefale at Copilot tas i bruk i saksbehandling som er bestemmende for rettigheter og plikter for enkeltpersoner før totaliteten i saksbehandlingsskjeden, og hvordan kunstig intelligens påvirker saksbehandlingen, er lest og forstått av alle involverte parter.

#### Innspill til risikoreducerende tiltaksliste i DPIA:

- Etablere retningslinjer for bruk av Copilot i administrative oppgaver
- Opplæring i hvordan bruke kunstig intelligens på en trygg og sikker måte

### 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>

Identifiserte og vurderte risikoer:

Risiko-ID	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
1	Personopplysninger kommer på avveie	Medium	Teknologiutvikling i tidlig fase	Liten
2	Ikke mulig å sikre samsvar mellom den registrertes rettigheter og den behandlingsansvarliges plikter etter Personvernforordningen (GDPR). For eksempel manglende rett til innsyn, sletting osv	Høy	Manglende informasjon fra leverandør. Manglende funksjonalitet og åpenhet om behandling av personopplysninger i verktøyet.	Medium

3	En bruker legger inn noen andre sine personopplysninger som kommer på avveie	<i>Lav</i>	Manglende opplæring og generelt lav personvernkompetanse hos brukere.	<i>Liten</i>
4	Manglende opplæring av brukere øker risikoen og sannsynlighet for at øvrige risikoer inntreffer	<i>Høy</i>	Manglende opplæringsrutiner for ansatte	<i>Medium</i>
5	Verktøy-/programvareutvikling uten tilstrekkelig fokus på innebygd personvern	<i>Medium</i>	Manglende organisatorisk rammeverk for innebygd personvern.  For rask teknologiutvikling (løsninger gjøres tilgjengelig på markedet for tidlig)	<i>Liten</i>
6	Feil bruk av verktøyet påvirker utøvelser av offentlig myndighet negativt. En part kan få en sak behandlet feil.	<i>Høy</i>	Verktøyet blir tatt ukontrollert eller feilaktig i bruk i saksprosesser.	<i>Liten</i>
7	Verktøyet behandler store mengder personopplysninger på nye og ukontrollerte måter uten formål og grunn (overbehandling). Kan føre til konsekvenser for den registrerte som får sine personopplysninger behandlet uten formål, eller at personopplysningene blir brukt som grunnlag i andre vurderinger enn de skal bli brukt til.	<i>Høy</i>	Lav kompetanse hos brukere av verktøyet som behandler personopplysninger på en ikke-trygg måte.  Innebygd sikkerhetsfunksjonalitet som verktøyet forutsetter at brukes (som sensitivity labels) er ikke tatt i bruk eller brukes feil.	<i>Høy</i>
8	Manglende forvaltning av Microsoft 365-plattformen i bunn fører til at Copilot får for store tilganger. Risiko for overbehandling.	<i>Medium</i>	Microsoft 365 er tatt i bruk på et tidligere tidspunkt uten tilstrekkelig forvaltning, ROS, DPIA osv.	<i>Høy</i>
9	Underdimensjonert forvaltnings- og driftsapparat for å håndtere et verktøy som er tidlig i utviklingsløpet. Økt risiko for uønskede hendelser (øvrige risikoer) som kunne vært unngått.	<i>Medium</i>	Feilaktig oppfatning om at skyplattformen/-funksjonaliteten er «ut av boksen» og at leverandør håndterer «alt» på det offentliges vegne og i tråd med offentlige forvaltningsprinsipper.  Manglende oppfølging av meldinger fra leverandøren om for eksempel sikkerhetsrisikoer og trusselvurderinger som ikke blir fulgt opp i organisasjonen.	<i>Høy</i>



10	Bruk av verktøyet gir uheldige og ukontrollerte nedkjølingseffekter på organisasjonen. Registrerte som ikke ønsker å få sine personopplysninger behandlet kan få negative reaksjoner knyttet til egen arbeidssituasjon.	<i>Høy</i>	Verktøyet blir tatt ukontrollert eller feilaktig i bruk i interne arbeidsprosesser (for eksempel opptak og transkripsjon av digitale og fysiske møter)	<i>Medium</i>
11	Feilaktig bruk av verktøyet kan føre til overvåking og måling av ansattes prestasjoner og adferd. Brudd på lovverk kan føre til ulovlig adferd overfor ansatte og registrerte, og gi kraftige negative reaksjoner for en organisasjon/ arbeidsgiver.	<i>Høy</i>	Verktøyet får tilgang til for mye informasjon/data.  Verktøyet er trent på verdier og data som ikke er forenlig med norsk arbeidsliv.  Manglende opplæring av brukere.	<i>Høy</i>

### Identifiserte risikoreducerende og skadebegrensende tiltak:

- Effekt på risiko vurderes ut fra kriterier «eliminert, redusert eller akseptert»
- Restrisiko vurderes ut fra ja/nei
- Tiltak godkjent med merknad om hvilken enhet som har påtatt seg ansvar for gjennomføring av tiltak (Her eksempel VIS = Seksjon for virksomhetsstyring).

Risiko-ID	Type tiltak (teknisk, organisatorisk, pedagogisk)	Tiltak	Effekt på risiko	Restrisiko	Tiltak godkjent
1-11	○	All bruk av verktøy med innebygd kunstig intelligens forutsetter systematisk arbeid med å holde behandlingsoversikt/protokoll oppdatert og fullstendig. Etabler rutiner for hvor vidt kunstig intelligens blir benyttet i offentlige saksprosesser. <b>Hovedtiltak: Kan virke risikoreducerende på alle identifiserte risikoer.</b>	<i>Redusert</i>	<i>Ja</i>	<i>Godkjent VIS</i>
1-7	○	Gjennomgå rutiner og ansvarsroller for ivaretagelse av personvernrettigheter for de registrerte.	<i>[må vurderes]</i>	<i>[må vurderes]</i>	
1-7	○	Gjør juridisk vurdering av rettslig grunnlag for overføring av personopplysninger til tredjeland	<i>[må vurderes]</i>	<i>[må vurderes]</i>	
1-7	○	Gjennomgå og etabler egne rutiner for bruk av Microsofts verktøy for å administrere Copilot (som for eksempel eDiscovery og Purview)	<i>[må vurderes]</i>	<i>[må vurderes]</i>	

1-7	<input type="radio"/>	Etablere retningslinjer for bruk av Copilot til fagspesifikke oppgaver, for eksempel administrasjon.	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Utarbeide nye og oppdatere eksisterende rutiner for sletting av personopplysninger	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Opprette internkontrollrutiner for å sjekke etterlevelse av nye rutiner og gjennomgang av administratorers bruk av eDiscovery og Purview.	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Kartlegg hvilken funksjonalitet i Copilot som kan brukes til profilering i egen virksomhet og vurder om å skru det av.	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Gjennomføre vurdering av Copilot opp mot annet lovverk (eksempelvis Forvaltningsloven, Arkivloven osv). Vurder om bruk av Copilot er i tråd med lovverket.	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Gjennomføre utfyllende interesseavveining jevnlig (1 og med at berettiget interesse er behandlingsgrunnlag pr. saksprosess som skal benytte verktøyet. Må vurderes individuelt og i en helhet)	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Sikre åpenhet og informasjon til brukere om hvordan data behandles, lagres og slettes. Opprette (eller oppdatere) personvernerklæring for bruk av Copilot.	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Gjennomgå rutiner for lagring av data og internkontroll	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Gjennomgå kontraktsmessige forpliktelser i forbindelse med organisasjonens øvrige innhold i Microsoft 365	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Gjennomgå tilgangsstyringsrutiner	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Gjennomgå internkontrollrutiner informasjonssikkerhet.	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Gjør utfyllende vurdering av Microsoft som felles behandlingsansvarlig ved bruk av M365	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Iverksett systematisk arbeid med å sikre god regelverksforståelse og forvaltningskompetanse ved institusjonen (i tråd med forventning fra styrende myndigheter).	[må vurderes]	[må vurderes]	
1-7	<input type="radio"/>	Lag rutiner for menneskelig kontroll («Human in the loop»). Prioriter internkontroll av	[må vurderes]	[må vurderes]	

		internkontrollen for å sikre at den fungerer etter hensikten.			
1-7	O	Lag en exit-strategi og gjør deg i stand til å avslutte bruken av Copilot.	[må vurderes]	[må vurderes]	
1-7	O	Gjør en realistisk total kostnadsvurdering for å sikre at alle kostnader er tatt med. Gjør analyser av langsiktig kostnadsutvikling.	[må vurderes]	[må vurderes]	
1-7	O	Bruk piloterings-, test- og prosjektmetodikk aktivt. Gjør tilpasninger til egen organisasjon (bedre med litt enn ingenting).	[må vurderes]	[må vurderes]	
1-7	O	Gjennomføre utfyllende vurdering om bruk av Copilot i tilfeller der NTNU er databehandler (får utlevert data samlet inn for annet formål), og påvirkning på bruk av shared channels.	[må vurderes]	[må vurderes]	
1-7	P	Opplæring av brukere og administratorer i Datatilsynets veileder for Programvareutvikling med innebygd personvern	[må vurderes]	[må vurderes]	
1-7	P	Prioriter arbeidet med kompetanseheving, -sikring og -utvikling for alle parter	[må vurderes]	[må vurderes]	
1-7	P	Prioriter ressurser til egen utvikling og kompetanseløft for å holde interne oppdatert på verktøyet (teknologi, avtaleverk og bruk)	[må vurderes]	[må vurderes]	
1-7	P	Vurder ekstraordinære tiltak overfor arbeidsgivere og ansatte med personalansvar.	[må vurderes]	[må vurderes]	
1-11	T, O, P	Skrø av tilgang til områder som ansatte anser som «uformelle» eller «private arenaer» (som Teams chat/Graph grounded Chat, epost osv).	[må vurderes]	[må vurderes]	
1-7	O, P	Gjennomgå og oppdatere informasjon om hvor registrerte kan henvende seg for å få personopplysninger rettet eller slettet.	[må vurderes]	[må vurderes]	
1-7	O, P	Brukeropplæring med spesielt fokus på deling og forvaltning av data, og hvordan prompter riktig.	[må vurderes]	[må vurderes]	
1-7	O, P	Involver relevante parter tidlig i utviklingsløpet. Løft tema om hvordan Copilot og verktøy med innebygd kunstig intelligens påvirker arbeidsdagen til ansatte og studenter til behandling i medvirknings- og medbestemmelsesorganer som vernelinje, tillitsvalgte, studentorganisasjoner,	[må vurderes]	[må vurderes]	

		fagforeninger osv. (For eksempel «hva slags kjøreregler bør NTNU ha?») Eksempel på saksbehandling ved NTNU: <ul style="list-style-type: none"> <li>- SESAM (06.11.2023 - se referat fra møtet til slutt i dokument) med styringssignaler for utvikling</li> </ul>			
1-11	O, T	Gjennomgå og sikre at rutiner for sletting av bruker og innhold følges når ansatte slutter eller endrer stilling.	[må vurderes]	[må vurderes]	
1-11	O, T	Vurder hvorvidt Microsoft Priva portalen for administratorer kan benyttes i egen virksomhet.	[må vurderes]	[må vurderes]	
1-11	O, T	Etablere rutiner og oversikt over alle applikasjoner i Microsoft 365 med tilhørende retention policies.	[må vurderes]	[må vurderes]	
1-11	O, T	Gjennomfør regelmessig internkontroll av databehandlers tekniske og organisatoriske tiltak. Varsle databehandler på et tidlig tidspunkt at dette vil skje.	[må vurderes]	[må vurderes]	
1-11	O, T	Prioriter arbeidet med å holde Orden i eget hus.	[må vurderes]	[må vurderes]	
1-11	O, T	Oppdater risikovurderinger av Microsoft 365 plattformen som helhet. Vurder om det er hensiktsmessig med mer grundige vurderinger av mindre elementer for å kunne avdekke ny risiko raskt (for eksempel verktøy med «Copilot funksjonalitet», som Teams Premium).	[må vurderes]	[må vurderes]	
1-11	O, T	Planlegg egen bruk av verktøyet som et verktøy i kontinuerlig utvikling	[må vurderes]	[må vurderes]	
8-11	T	Vurder om plugin for web bør deaktiveres (kan redusere funksjonaliteten av verktøyet for mange brukere).	[må vurderes]	[må vurderes]	
8-11	T	Vurder om bruk av Double Key Encryption (DKE) bør aktiveres.	[må vurderes]	[må vurderes]	
8-11	T	Gjennomgå alle innstillinger og sørg for at disse er satt til «mest personvernvennlig».	[må vurderes]	[må vurderes]	
8-11	T	Ta aktivt stilling til hvilke data Copilot skal ha tilgang til (dette gjelder alle verktøy, også Microsoft 365).	[må vurderes]	[må vurderes]	

## 4. Ledelsens validering av personvernkonsekvensvurderingen (DPIA)

Moment	Navn og dato	Kommentarer
Tiltak godkjent av:	XXXX Må vurderes XX.XX.2024	Ikke gjennomført
Restrisiko godkjent av:	XXXX Må vurderes XX.XX.2024	Dersom restrisiko med høy risikograd blir godkjent, ta kontakt med Datatilsynet før oppstart for forhåndsdrøfting, jf. art. 36 nr. 1.
Personvernombudsassistans gitt:	XXXX Personvernombud  XX.XX.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.
<b>Sammendrag av personvernombudets råd for driftsfase:</b>		
<b>IKKE GJENNOMFØRT – MÅ GJENNOMFØRES I DIALOG MELLOM SYSTEMEIER OG PERSONVERNOMBUD</b>		
Personvernombudets råd er akseptert eller overprøvd av:	XXXX	
De registrertes synspunkter er innhentet og gjennomgått av:	DPIA bør behandles av SESAM (samarbeidsorgan med tillitsvalgte og fagforeninger)	Hvis din avgjørelse avviker fra de registrertes synspunkter, bør du forklare bakgrunnen for at du velger å sette i gang/fortsette behandlingen
Kommentarer:		
Denne personvernkonsekvensvurderingen vil følges opp av:	Må utpekes fra System-/verktøyeier	Personvernombudet bør også følge opp personvernkonsekvensvurderingen løpende, jf. art. 39 nr. 1 bokstav c.

## Vedlegg til personvernkonsekvensvurdering M365 Copilot

### Vedlegg 1: 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 personsensitive forskningsdata, kan fristes til å legge det inn i åpne tilgjengelige verktøy. I forvaltningsprosesser 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 førerretet. 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 saksbehandlingsskjede.

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 opptre 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 til SESAM-behandling - 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](#)

## Lenkesamling og kilder til personvernkonsekvensvurdering

I arbeidet med å lage DPIAen har vi benyttet oss av en rekke kilder. Vi har valgt ikke å referere direkte i teksten med utgangspunkt i at Microsoft sin dokumentasjon har endret seg mange ganger i løpet av prosjektets gang, og det har vært vanskelig å holde tritt med all informasjonen som finnes på Microsoft sine nettsider. Bruk derfor lenkesamlingen nedenfor til å gjøre egne vurderinger og kontrollsjekk at vurderingene stemmer opp mot oppdatert informasjon på Microsoft sine nettsider.

### Lenker til NTNU-nettsider

- <https://innsida.ntnu.no/wiki/-/wiki/Norsk/Personvernerklæring+NTNU>
- <https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide>
- <https://i.ntnu.no/wiki/-/wiki/Norsk/Vurdere+personvernkonsekvenser>
- <https://i.ntnu.no/wiki/-/wiki/norsk/office+365>
- <https://i.ntnu.no/wiki/-/wiki/Norsk/Kunstig+intelligens+i+undervisning+og+vurdering>
- <https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+retningslinjer>
- <https://learn.microsoft.com/en-us/microsoft-365-copilot/>

### Lenker til Microsoft-nettsider

- <https://mspoweruser.com/microsoft-outlook-sound-like-me-surface-2023-event/>
- <https://learn.microsoft.com/nb-no/microsoft-365-copilot/microsoft-365-copilot-privacy>
- <https://learn.microsoft.com/en-us/graph/overview>
- <https://learn.microsoft.com/en-us/microsoftsearch/semantic-index-for-copilot>
- <https://developer.microsoft.com/en-us/graph/graph-explorer>
- <https://developer.microsoft.com/en-us/graph>
- <https://learn.microsoft.com/en-us/graph/search-concept-overview>
- <https://support.microsoft.com/en-gb/office/draft-an-email-message-with-copilot-in-outlook-3eb1d053-89b8-491c-8a6e-746015238d9b>
- <https://learn.microsoft.com/en-us/training/modules/create-draft-content-with-microsoft-copilot-microsoft-365/4-draft-emails-replies-meeting-agendas-microsoft-copilot-outlook>
- <https://techcommunity.microsoft.com/t5/outlook-blog/copilot-in-outlook-helps-you-achieve-more/ba-p/3981033>
- <https://support.microsoft.com/en-us/office/delete-your-copilot-for-microsoft-365-interaction-history-76de8afa-5eaf-43b0-bda8-0076d6e0390f>
- <https://learn.microsoft.com/en-us/microsoft-365-copilot/microsoft-365-copilot-privacy#data-stored-about-user-interactions-with-microsoft-copilot-for-microsoft-365>
- <https://privacy.microsoft.com/nb-no/privacystatement>
- <https://learn.microsoft.com/en-us/graph/overview>
- <https://learn.microsoft.com/en-us/microsoftsearch/semantic-index-for-copilot>
- <https://developer.microsoft.com/en-us/graph/graph-explorer>
- <https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn?source=recommendations>
- <https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn>
- <https://learn.microsoft.com/en-us/microsoft-365-copilot/microsoft-365-copilot-privacy#microsoft-copilot-for-microsoft-365-and-the-web-content-plugin>
- <https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services?source=recommendations>
- <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>



- <https://learn.microsoft.com/en-us/purview/retention-policies-copilot>
- <https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-overview#how-does-microsoft-copilot-for-microsoft-365-work>
- <https://learn.microsoft.com/en-us/power-platform/faqs-copilot-data-security-privacy>
- <https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy#data-stored-about-user-interactions-with-microsoft-copilot-for-microsoft-365>
- <https://learn.microsoft.com/en-us/microsoftsearch/semantic-index-for-copilot>
- <https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn>
- <https://learn.microsoft.com/nb-no/microsoft-365-copilot/microsoft-365-copilot-privacy>
- <https://learn.microsoft.com/nb-no/compliance/regulatory/gdpr-data-subject-requests?view=o365-worldwide>
- <https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services?source=recommendations#fulfilling-gdpr-data-subject-rights-requests-worldwide>
- <https://learn.microsoft.com/en-us/purview/double-key-encryption>
- <https://learn.microsoft.com/en-us/microsoftsearch/semantic-index-for-copilot>

**Lenker til andre nettsider:**

- <https://lovdata.no/pro/#reference/lov/2005-06-17-62/%C2%A79-5>
- <https://snl.no/språkmodell>
- <https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/>
- <https://www.bufdir.no/aktuelt/ny-rapport-lite-kunnskap-og-kompetanse-om-kunstig-intelligens-og-diskriminering/>
- <https://snl.no/register - IT>
- [https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies\\_en](https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en)