

Vurdering av personvernkonsekvenser (DPIA)

Navn på system/prosjekt:	Microsoft 365 Copilot Chat med Enterprise Data protection (EDP)
DPIA-en utføres av:	Seksjon for digital sikkerhet, NTNU
Dato:	31.10.2025

Innholdsfortegnelse

1. Systematisk beskrivelse av behandlingen.....	4
2. Behandlings art	7
3. Behandlings omfang	10
4. Behandlings formål	11
5. Sammenhengen behandlingen utføres i (kontekst)	13
6. Identifisering og oversikt	17
7. Mottakere av personopplysninger	17
8. Dataflyt, lagring og mellomlagring.....	19
9. Informasjonssikkerhet	21
10. Nødvendighet og proporsjonalitet	23
Personvernprinsippene.....	Error! Bookmark not defined.
11. Vurdering av risiko for de registrertes rettigheter og friheter, og planlagte tiltak for å håndtere risikoene	29
12. Ledelsens validering av personvernkonsekvensvurderingen (DPIA)	35
Vedlegg til personvernkonsekvensvurdering Microsoft Copilot with enterprise data protection...	37
Vedlegg 2 - Kildeliste:.....	39

Merknader til den gjennomførte personvernkonsekvensvurderingen:

Microsoft 365 Copilot Chat er en KI-chat for studenter og ansatte ved NTNU. Den ble opprinnelig lansert under navnet Bing Chat Enterprise i 2023, og har endret både navn og funksjonalitet siden den gang. Verktøyet har vært tilgjengelig for ansatte siden september 2023 og for studenter siden februar 2024.

Opprinnelig personvernkonsekvensvurdering av Bing Chat Enterprise fra høst 2023 finnes her: <https://www.ntnu.no/documents/10507/1359912/2024-02-27+DPIA+Microsoft+copilot.pdf/436d8f4f-6142-d33c-c1df-6769750d7d9a?t=1709887086495>

Microsoft 365 Copilot Chat har fått ny funksjonalitet siden den første personvernkonsekvensvurderingen ble utført.

Én av endringene består i at spørringer nå lagres. Lagring av spørringer endret noen av de grunnleggende forutsetningene for forrige personvernkonsekvensvurdering, og en ny vurdering er derfor utført nå.

Spørringene som hver bruker utfører, er å betrakte som lagring av personopplysninger om brukeren selv. Dette gjelder altså alle spørringer. Spørringer er alltid tilknyttet den brukeren som har lagt dem inn i utgangspunktet, og selv om brukeren ikke bevisst legger inn egne eller andres personopplysninger i selve spørringen. Interaksjonene kan for eksempel fortelle noe om hvem brukeren er, og hva vedkommende er opptatt av for tiden. I tillegg kan hver bruker legge inn personopplysninger om andre. Selv om dette altså ikke er meningen, har vi ingen måte å kontrollere og begrense hva brukere legger inn i spørringer.

Lagringen av spørringer utfordrer prinsippet om dataminimering og lagringsbegrensning. Det var nettopp den automatiske slettingen av utførte spørringer som ved forrige DPIA ble vurdert som en god funksjonalitet som ville ivareta disse prinsippene.

En annen omfattende endring fra juli 2025 er innføringen av Copilot Memory i Microsoft 365 Copilot Chat. Copilot Memory er en funksjon som lar Copilot Chat huske visse detaljer som hver bruker deler med chatten. Det kan være hva slags språk brukere ønsker svar på, om det er formell eller uformell stil på svaret chatten skal gi, hvilke interesser bruker har, samt fakta bruker deler med chatten, for eksempel hva man jobber med og hvor man jobber.

Funksjonen skal gi brukere mer relevante svar i Copilot Chat. Minner opprettes ved at bruker legger inn sine preferanser, for eksempel: "Husk at jeg foretrekker punktlister", "Jeg jobber med sikkerhet". Det er ikke enkeltord som «husk» alene, men kombinasjonen av verb (husk, glem, foretrekker) samt personlig eller fremtidig kontekst som oppretter et minne.

Hver bruker kan skru av Copilot Memory, hvert minne kan slettes av bruker selv eller bruker kan be Copilot Chat glemme et minne. Minnene blir lagret som en spørring på hver bruker. Hvis et minne slettes vil det følge gjeldende retention policy i Microsoft 365 som per dags dato er 30 dager, før det slettes helt.

Microsoft har varslet endringer som vi velger å omtale i denne DPIAen, da dette er funksjonalitet som kommer snart:

I løpet av høsten 2025 vil Microsoft 365 Copilot Chat bli tilgjengelig fra applikasjoner som word, excel etc i M365. Chatten vil da bli tilgjengelig med Copilot-symbolet i de ulike

applikasjonene. Chatten vil da kunne brukes i det gjeldende dokumentet, og spørringene lagres i Microsoft 365 Copilot Chat på samme måte som ellers.

En annen funksjon som er under utrulling i Microsoft 365 Copilot Chat er muligheten for å koble opp tredjepartsagenter til chatten. En agent er en instans av Copilot som er konfigurert med spesifikke instruksjoner og datatilganger for å utføre avgrensede oppgaver. I motsetning til standard Microsoft 365 Copilot Chat som primært bruker webdata, kan agenter aksessere data fra SharePoint, OneDrive, Exchange, Teams og eventuelle eksterne systemer som er konfigurert av organisasjonen. Agenter opererer alltid med brukerens egen identitet og tilgangsnivå, noe som betyr at agenten ikke gir brukeren tilgang til data vedkommende ikke allerede har. Brukeren må gi samtykke første gang en agent ber om tilgang til en datakilde. Når en agent brukes, henter den relevant organisasjonsdata, kombinerer dette med brukerens spørringer og sender det til språkmodellen for å generere svar. Organisasjonsdata forblir i kilde-systemene – agenten lager ikke permanente kopier av dataen den leser. Samtalehistorikk med agenter lagres i Brukerens Exchange-postboks for revisjon og eDiscovery på samme måte som standard Copilot Chat. IT-administratorer kontrollerer hvilke agenter som er tilgjengelige for organisasjonen. Per oktober 2025 er ingen agenter aktivert ved NTNU. Fremtidig aktivering av agenter vil kreve godkjenning fra IT-avdelingen, og egenutviklede agenter må godkjennes før de kan tas i bruk.

Bruksstatistikk over Microsoft 365 Copilot Chat har vært tilgjengelig siden oktober 2024. Her får man oversikt over AI-interaksjoner siste måned. En AI-interaksjon er en utveksling mellom brukeren og AI-systemet. Dette inkluderer å stille spørsmål, motta svar, få hjelp til oppgaver eller ha en samtale. Organisasjonen kan ta ut rapporter for bruksstatistikk 30 dager tilbake i tid. Fra 9. november til 9. desember 2024 var det utført 285.183 AI-interaksjoner. For 31. august til 29. september 2025 er det utført 251.698 AI-interaksjoner. Dette viser at Microsoft 365 Copilot Chat blir jevnlig brukt over tid.

Angående terminologi: På engelsk brukes ordet «prompts» for det innholdet som legges inn av brukerne av tjenesten, og «response» for det innholdet som Copilot genererer og returnerer til brukeren som svar på et «prompt». I denne DPIA'en oversetter vi «prompt» med spørring, og «response» med svar.

Det er viktig med høy bevissthet rundt bruken av verktøy med kunstig intelligens.

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.

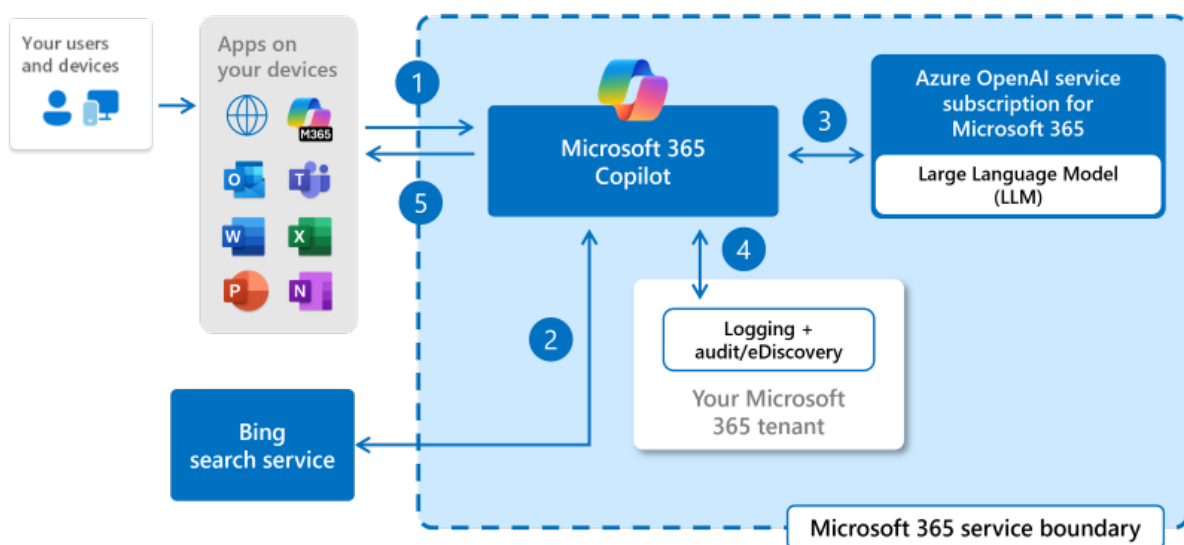
Overordnet oversikt

Microsoft 365 Copilot Chat er et KI-drevet verktøy. Det fungerer som en språkmodell integrert med Bing (Microsofts søkemotor) og bruker kunstig intelligens fra OpenAI, samme teknologi som ChatGPT. Microsoft 365 Copilot Chat har vært tilgjengelig for ansatte og studenter ved NTNU fra henholdsvis september 2023 og februar 2024.

Verktøyet er integrert i nettleseren Edge samt vil bli tilgjengelig fra applikasjoner i M365. Innlogging skjer automatisk for alle som er pålogget sin Microsoftkonto ved NTNU. Informasjon om verktøyet finnes på Innsida: <https://i.ntnu.no/wiki/-/wiki/Norsk/Copilot>

Når et samtalerobotverktøy basert på generativ kunstig intelligens skal tilbys alle brukere anbefales det å gjennomføre en personvernkonsekvensvurdering (DPIA) jf Personvernforordningens artikkel 35, nr. 1.

Siden lanseringen av verktøyet, har det kommet mange oppdateringer. Bildet under viser hvordan behandlinger skjer i Microsoft 365 Copilot Chat:



Dataflyt i Microsoft 365 Copilot Chat

Brukere ved NTNU er tilknyttet Enterprise Data Protection (EDP) siden brukere er logget på med Microsoft Entra-konto ID tilknyttet NTNUs tenant (NTNUs dedikerte område i Microsoft-skyen). EDP innebærer at alle data som sendes mellom bruker og Copilot er kryptert både under overføring og lagring.

1. Prompt (Brukerinput)

Brukere får tilgang til Microsoft 365 Copilot Chat ved å logge på fra:

· Microsoft 365 applikasjonen

- Nettleseren Edge (øverst på høyre side)
- URL: m365.cloud.microsoft/chat
- M365 – applikasjoner som Word, Excel, Powerpoint, OneNote og Outlook

Brukere kan skrive inn spørringer og laste opp bilder og dokumenter. Spørringen sendes til Copilot orchestrator som koordinerer behandlingen, utfører Responsible AI-sikkerhetskontroller og logger interaksjonen for revisjon/eDiscovery.

2. Grounding (Nettsøk via Bing)

Før svar genereres, kan Copilot utføre web grounding via Bing-søket. Bing-søket består av noen få ord generert fra spørringen som sendes via en sikker tilkobling. Søket identifiserer ikke bruker eller tenant (NTNUs del av skyløsningen). Bing gir relevant informasjon fra det åpne internett når Copilot vurderer det nødvendig.

3. LLM (Språkmodell via Azure OpenAI)

Den grunnlagte spørringen sendes til Language Model (LLM) via Azure OpenAI-tjenesten for Microsoft 365. Copilot kan bruke ulike språkmodeller for å generere relevante svar. Spørringer og svar blir ikke brukt for å trene underliggende grunnmodeller.

4. Logging og revisjon.

Før svaret sendes tilbake til brukeren, logges og lagres både spørringen og svaret i brukerens egen postboks i Exchange (innenfor Microsoft 365 tenant) for revisjon/loggiong og eDiscovery-formål.

Filer eller bilder som lastes opp blir lagret midlertidig mens arbeidsøkten i Copilot Chat foregår. Når økten er over, slettes filer/bilder fra Copilot Chat. En kopi av filen/bildet lagres under OneDrive -> My files -> Microsoft 365 Copilot Chat -> Chat files. Status på filen settes til privat, slik at kun brukeren som lastet opp filen har tilgang til den i egen OneDrive.

5. Response (Svar til bruker).

Copilot utfører siste Responsible AI-sikkerhetskontroller og returnerer svaret til applikasjonen og brukeren. Svaret baseres på opplastede dokumenter og informasjon oppgitt i spørringen, kombinert med relevante kilder fra Internett der Copilot vurderer det nødvendig.

Lagringen av spørringer og svar i Microsoft 365 Copilot Chat er utfordrende fordi det ble satt som premiss at data som ble lagt inn i Microsoft 365 Copilot Chat ikke skulle bli lagret da NTNU valgte dette KI-verktøyet. Teknisk sett kan man sette opp en retention policy (hvor lenge skal data oppbevares) for å begrense lagringen. Microsoft har historisk kun tilbudt globale innstillinger for retention policy, slik at retention policy er like lang for alle applikasjoner i M365. Global retention policy betyr at hvis NTNU setter at data i Microsoft 365 Copilot Chat kun skal oppbevares i 2 dager, så vil denne regelen også gjelde for eksempel all e-post i Microsoft Outlook og chat-meldinger i Microsoft Teams. Dette vil bryte kraftig med hva NTNUs brukere forventer med tanke på tilgjengelighet av informasjon. Hvis brukeren sletter dataene (feks spørringer, e-post, eller teams chat), vil dataene bli lagret i inntil 30 dager før de blir permanent slettet.

Microsoft har varslet at retention policy er mulig å separere mellom ulike funksjoner i M365. Slik Microsoft beskriver dette, kan man både ha egen retention policy for data på funksjoner og hvor lang tid det skal ta før data blir slettet uavhengig hva bruker gjør.

Funksjonaliteten er ikke testet innen NTNUs instans av Microsoft, så det må gjøres før egne retention policies innføres. Se tiltak s. 29 for nærmere beskrivelse.

Formål

Hovedformålet for tjenesteeier (NTNU/IT-avdelingen) med å tilgjengeliggjøre Microsoft 365 Copilot Chat, er å tilby et språkmodellverktøy for behandling av informasjon med noe høyere [informasjonssikkerhetsklassifiseringsnivå](#) (intern, men uten personopplysninger) enn det som anbefales for åpne verktøy på nett (åpen). Ved å tilby verktøy hvor ansatte kan legge inn interne data, reduserer vi risiko for at åpne plattformer som ChatGPT brukes til å behandle informasjon som NTNU ønsker å holde internt i virksomheten. IT-avdelingen ønsket også å tilby en lett tilgjengelig og trygg språkmodell der ansatte kan gjøre seg kjent med fordeler og ulemper med denne typen verktøy og teknologi. Ved å tilby en trygg «sandkasse» for testing ønsket IT-avdelingen å bidra til at alle ansatte skal få større kjennskap til hva denne typen verktøy kan bidra med av positive og negative effekter på måten ansatte kan jobbe på. I tillegg har IT-avdelingen ønsket å tilby et verktøy hvor vi er åpne om personvernkonsekvensvurderinger, risikovurdering, informasjonssikkerhet og personvern. IT-avdelingen håper at dette skal kunne bidra til økt forståelse for hvorfor og hvordan vi alle bør tenke på personvern og informasjonssikkerhet i hverdagen.

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

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

I tillegg vil hver enkelt bruker (ansatte og studenter ved NTNU) ha ulike formål for sin behandling av informasjon i Microsoft 365 Copilot Chat. Hovedformålet vil sannsynligvis for de fleste være å øke effektivitet og produktivitet ved å automatisere oppgaver, få generert tekst og bilder, samt få forslag til nye ideer. Behandlingsformål for hver enkelt bruker er ikke beskrevet utfyllende i DPIAen. Her trengs det både retningslinjer og prosedyrer, opplæring og bevisstgjøring, rundt hva verktøyet kan brukes til og ikke brukes til. Per nå er det definert at personopplysninger, samt informasjon som er klassifisert som fortrolig og strengt fortrolig, ikke skal behandles i Microsoft 365 Copilot Chat, men det er ingen sjekk om hvorvidt dette blir gjort.

Etter oppdateringer av Copilot i 2024, er det blitt teknisk mulig å sette opp «automatiserte regler» i systemet, for å forsøke å avdekke om sensitiv informasjon blir lagt inn. Vi ser at det

er komplisert å vurdere hvorvidt slike regler for å sjekke etterlevelse vil fungere etter hensikten (altså for å avdekke feilaktig bruk av tjenesten), da tiltakene samtidig vil innebære problematikk rundt overvåking av ansattes og studenters aktivitet i verktøyet. Det er dermed ikke gjort en vurdering av det å eventuelt innføre slike regelsett.

Hvilke personopplysninger skal behandles?

- Brukernavn
- Personopplysninger som finnes åpent på nett
- Personopplysninger som brukeren selv legger inn (spøringer) og lagring av disse spørningene

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/copilot/overview>

2. Behandlingens art

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

Hvordan skal personopplysningene samles inn?	Personopplysninger samles inn på følgende måter: <ol style="list-style-type: none">1. Brukernavn for å autentisere NTNU-bruker med tilgang til tjenesten deles via virksomhetens IT-systemer ved hjelp av Entra-ID (dette skjer på samme måte som ved bruk av andre Microsoft-tjenester). Slik autentisering er en forutsetning for å bruke tjenesten.2. En bruker kan skrive inn eller lime inn personopplysninger direkte i chat-vinduet til Copilot.3. En bruker kan dele en fil i chatten som inneholder personopplysninger. Det kan for eksempel være et tekstdokument/regneark/etc.4. Copilot som produkt/tjeneste er basert på en stor språkmodell som er trent ved hjelp av informasjon som er publisert på det åpne
--	---

	<p>Internett. Copilot er altså et produkt som Microsoft har basert på data fra det offentlige nettet ved å bruke Bing-søketjenesten. Denne bruken av personopplysninger har ikke NTNU noen måte å kontrollere.</p> <p>5. Copilot chat benytter også personopplysninger som er delt på Internett i svar på spøringer. Dette skjer ved at Copilot gjør søk med Bing-søketjenesten og returnerer et svar til brukeren, som kan inkludere personopplysninger som er delt på Internett. Denne funksjonen fins det p.d.d. ingen måte å endre på (dvs skru av eller på) i Copilot.</p>
<p>Hvordan skal personopplysningene lagres?</p>	<p>Informasjon som brukere legger inn i chatsesjonen blir i utgangspunktet lagret i brukerens eget område i Microsoft 365 (forkortet M365) til brukerkonto avsluttes.</p> <p>Hvis brukere sletter spørningen sin fra Microsoft 365 Copilot Chat, blir interaksjonen lagret i M365 som en backup som den enkelte brukeren ikke kan se selv i 30 dager, før endelig sletting. Denne perioden kan eventuelt justeres av administrator for systemet.</p> <p>Minner i Copilot er en funksjon som gjør det mulig for Copilot å huske informasjon om brukerens preferanser og arbeidskontekst over tid. Formålet er å gi mer relevante og tilpassede svar i chatten, slik at brukeren slipper å gjenta instruksjoner. Brukeren har full kontroll over egne minner. Det er mulig å se, redigere eller slette enkeltminner, samt deaktivere hele funksjonen når som helst. Brukerne kan når som helst skru av og på funksjonen. Minner lagres på samme måte som en spørning.</p> <p>Spøringer (fra bruker) og svar (fra Copilot) blir lagret som alle andre data i M365, dvs i NTNUs tenant. Med Enterprise Data Protection er alle data kryptert, både under lagring og overføring. I tillegg lagres spøringer, svar og metadata (f.eks. tidspunkt, brukerkonto, etc) som en drifts- og sikkerhetslogg. Slike logger er til for at administratorer skal kunne overvåke den tekniske leveransen av, og sikkerheten på, tjenesten.</p>

<p>Hvordan skal personopplysningene brukes?</p>	<p>Den registrertes brukernavn brukes kun til pålogging og bekreftelse på autentisering.</p> <p>Personopplysningene tilknyttet spørringer fra bruker og svar fra Copilot brukes for å oppfylle selve formålet med tjenesten, beskrevet i punkt 4. Merk at dette formålet inkluderer vilkår for hvilke typer personopplysninger (og annen informasjon) som kan behandles i Copilot (kun intern og åpen informasjon).</p>
<p>Hvem skal ha tilgang til personopplysningene?</p>	<p>Brukeren selv har tilgang til sine spørringer (inkludert minner), svar fra Copilot (og kan eventuelt slette disse).</p> <p>Microsoft og et fåtall IT-ansatte har tilgang til brukerautentiseringsopplysninger, drifts- og sikkerhetslogger.</p>
<p>Hvem skal det samles inn personopplysninger om?</p>	<p>For autentisering: Ansatte og studenter som tar i bruk løsningen - da deles opplysninger om brukerkonto tilknyttet den enkelte person som logger seg på.</p> <p>I spørringer skal brukerne kun dele informasjon som kommer under kategorien åpne eller interne (uten personopplysninger). NTNU kan klassifisere tjenesten som kun åpen informasjon kan legges inn Microsoft 365 Copilot Chat, men da blir merverdien av tjenesten begrenset. Ved at behandlingsformålet kan klassifiseres som gule/interne data (uten personopplysninger) vil tjenesten ha en utvidet funksjonalitet for våre brukere sammenlignet med lignende tjenester. Samtidig fordrer dette en høyere bevissthet blant våre brukere. Tiltak som skal redusere risikoen for at personopplysninger blir lagt inn i Microsoft 365 Copilot Chat er lagt inn i risikolisten.</p>
<p>Hvordan kan den registrerte utøve sine rettigheter?</p>	<p>De registrerte får tilgang/innsyn i egne spørringer via Microsoft 365 Copilot Chat. De får ikke tilgang til spørringer andre brukere har gjort om deg/dine data. Sletting av brukerkonto innebærer sletting av alle de dataene som er lagt inn (inkludert data i Microsoft 365 Copilot Chat).</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 Personvernerklæring NTNU https://i.ntnu.no/wiki/-/wiki/Norsk/Personvernerkl%C3%A6ring+NTNU</p> <p>Den registrerte kan be om retting, sletting, begrenning og protestere mot bruk av personopplysninger ved å ta</p>

	<p>kontakt med behandlingsansvarlig. Informasjon om hvordan personopplysninger brukes vil tilgjengeliggjøres i personvernerklæringen, i tillegg til informasjon om hvordan den registrerte kan utøve sine rettigheter.</p>
<p>Vil det være systematisk behandling av personopplysninger?</p>	<p>Behandlingen av personopplysninger i verktøyet vil anses som systematisk behandling av personopplysninger. Spørringene som hver bruker utfører, er å betrakte som lagring av personopplysninger om brukeren selv. Dette gjelder altså alle spørringer. Minner (Memory) er også personopplysninger om brukernes preferanser. Minner blir lagret som en spørring i Copilot Chat.</p> <p>Spørringer og minner er alltid tilknyttet den brukeren som har lagt dem inn i utgangspunktet, og selv om brukeren ikke bevisst legger inn egne eller andres personopplysninger i selve spørringen. Interaksjonene og minner kan for eksempel fortelle noe om hvem brukeren er, og hva vedkommende er opptatt av for tiden. I tillegg kan hver bruker legge inn personopplysninger om andre.</p> <p>Behandlingen av personopplysninger i Copilot skjer regelmessig og kontinuerlig. Det innebærer et volum på over 200 000 interaksjoner i måneden.</p>
<p>Brukes det ny teknologi eller ny bruk av eksisterende teknologi hvor personvernkonsvenser ikke har blitt vurdert?</p>	<p>Teknologien utvikler seg i et relativt høyt tempo. For norsk UH-sektor er mange av verktøyene enda ganske tidlig i utviklingsløpet og bruken er lite systematisk innarbeidet i virksomhetene. Samtidig er det etter hvert flere virksomheter som har vurdert personvernkonsvenser i tilknytning til Copilot og lignende verktøy.</p> <p>Dette er andre versjon av NTNUs personvernkonsvensvurdering av Microsoft 365 Copilot Chat.</p>

3. Behandlingens omfang

<p>Kategorier av personopplysninger som behandles</p>	<p>Tjenesten skal behandle data av typen åpen og intern informasjon (uten personopplysninger). Løsningen er ikke godkjent til fortrolig og strengt fortrolig. Om brukere selv legger inn vanlige og/eller særlige kategorier personopplysninger vil disse i så fall bli behandlet i chatsesjonen, men behandling av personopplysninger på denne måten er altså ikke hensikten med å tilby</p>
---	---

	tjenesten. Det er ikke satt opp noen kontroller for denne eventualiteten.
Antall registrerte involvert i behandlingen	Maks antall brukere er 51 000 (forutsatt at alle ansatte og studenter tar løsningen i bruk). Antall registrerte kan være flere enn dette, dersom personopplysninger blir lagt inn i chatsesjonen.
Datavolum	Det er ingen begrensninger knyttet til datavolum. Brukerstatistikk for en måned i 2025 tilsier at det er over 250 000 interaksjoner med Copilot pr. måned, årlig vil man kunne nå over 2 000 000 interaksjoner, og antakeligvis økes volumet når flere vil ta i bruk verktøyet.
Behandlingsfrekvens	Kontinuerlig.
Lagringstid for personopplysningene	Permanent. Spøringer blir i utgangspunktet lagret fram til brukerkontoen avsluttes. Hvis brukeren selv sletter en spørring og det tilhørende svaret fra Copilot (disse lagres sammen), blir en backup bevart i M365 i maksimalt 30 dager.
Geografisk omfang	NTNUs ansatte og studenter er hovedsakelig lokalisert i Trondheim, Gjøvik og Ålesund, men løsningen blir tilgjengelig uavhengig av lokasjon, så fremt brukeren er logget på Microsoft-kontoen de har hos NTNU. Microsofts datasentre som benyttes i behandlingen befinner seg innenfor EU Data Boundary, men Microsoft kan benytte datasentre over hele verden til behandling av chatsesjoner, særlig når funksjoner i preview testes av Microsoft, eller det er behov for support.

4. Behandlingens formål

Behandlingens formål	<p>Formålet med tjenesten:</p> <ol style="list-style-type: none"> 1. Tilby en språkmodell for behandling av gule/interne data ved NTNU (uten personopplysninger) <ol style="list-style-type: none"> a. Å tilby og anbefale et sikrere alternativ til studentene enn åpne tjenester på nett 2. Tilby en lett tilgjengelig og trygg språkmodell der NTNUs ansatte og studenter kan gjøre seg kjent med fordeler og ulemper med ny teknologi. <ol style="list-style-type: none"> a. Å tilby det samme verktøyet til både studenter og ansatte slik at fagspesifikk opplæring kan gis i ordinær undervisning.
----------------------	---

	<p>3. Tilby en teknisk løsning hvor NTNU samtidig tilgjengeliggjør informasjon om hvordan vi har utført risikovurdering og personvernkonsekvensvurdering.</p> <p>I tillegg vil hver enkelt bruker (ansatte og studenter ved NTNU) ha ulike formål for sin behandling av informasjon i Microsoft 365 Copilot Chat. Hovedformålet vil sannsynligvis for de fleste være å øke effektivitet og produktivitet ved å automatisere oppgaver, få generert tekst og bilder samt få forslag til nye ideer. Behandlingsformål for hver enkelt bruker er ikke beskrevet i DPIAen. Her trengs det både retningslinjer og prosedyrer, opplæring og bevisstgjøring, rundt hva verktøyet kan brukes til og ikke brukes til. Per nå er det definert at informasjon som er klassifisert som fortrolig og strengt fortrolig ikke skal behandles i Microsoft 365 Copilot Chat, men det er ingen sjekk om hvorvidt dette blir gjort.</p> <p>Etter oppdateringer av Copilot i 2024, er det blitt teknisk mulig å sette opp «regler» for å forsøke å avdekke om sensitiv informasjon blir lagt inn, men det er ikke satt opp slike regler ved NTNU. Vi ser at det er komplisert å vurdere hvorvidt automatiske regler for å sjekke etterlevelse vil fungere etter hensikten (altså for å avdekke feilaktig bruk av tjenesten), da tiltakene samtidig vil innebære problematikk rundt overvåking av ansattes og studenter aktivitet i verktøyet. Det er dermed ikke gjort en vurdering av det å eventuelt innføre slike regelsett i denne DPIAen.</p>
Vil det være kontrollformål?	Nei NTNU skal ikke bruke tilgang til studenter og ansattes chatlogger til kontrollformål. Dette vil inngå i retningslinjene for bruken av Copilot og kommuniseres til de som bruker verktøyet.
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. NTNU skal ikke bruke tilgangen til personopplysninger i chatloggene til å fatte beslutninger som får betydning for den registrerte. Dette innebærer også å ikke under noen omstendighet å kontrollere om en student har

	brukt Copilot som et KI-verktøy til fusk. Dette vil inngå i NTNUs retningslinjer for bruk av Copilot.
Skal opplysningene brukes til å profilere den registrerte?	Nei
Brukes personopplysninger for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte?	Nei
Vil personopplysningene viderebehandles til nye eller andre formål?	Nei

5. Sammenhengen behandlingen utføres i (kontekst)

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

Hvilke kilder brukes for innhenting av personopplysninger?	<p>Brukernavn hentes fra brukerdatabase «Active directory» (AD)/Entra-konto ID.</p> <p>Andre personopplysninger er det bruker selv som legger inn i chatsesjonen.</p> <p>Spørringene, inkludert minner, som hver bruker utfører, er å betrakte som lagring av personopplysninger om brukeren selv. Dette gjelder altså alle spørringer. Spørringer er alltid tilknyttet den brukeren som har lagt dem inn i utgangspunktet, og selv om brukeren ikke bevisst legger inn egne eller andres personopplysninger i selve spørringen. Interaksjonene kan for eksempel fortelle noe om hvem brukeren er, og hva vedkommende er opptatt av for tiden.</p>
Relasjon mellom behandlingsansvarlig og den registrerte	De registrerte er ansatte og studenter hos behandlingsansvarlig. I tillegg kan de registrerte omfatte alle som brukere av verktøyet legger inn personopplysninger om i chatsesjoner. Selv om dette ikke er formålet med bruken av verktøyet, er risikoen for at det skjer fortsatt til stede.
I hvilken grad har den registrerte kontroll over sine opplysninger?	<p>Brukertilgangen til systemet styres på samme måte som alle andre tilganger gjennom M365, dvs via Active directory og Entra-konto ID. Brukertilgang reguleres på samme måte som alle andre tilganger til NTNUs IT-verktøy (IKT-reglement).</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</p>

	<p>om seg selv. Utfyllende informasjon på https://innsida.ntnu.no/wiki/-/wiki/Norsk/Personvernerklæring+NTNU.</p> <p>Personopplysningene til Microsoft 365 Copilot Chat inngår i datagrunnlaget med personopplysninger som Microsoft vet om våre brukere og vil bli synlig ved innsyn i Microsoft sin verktøyportefølje.</p>
<p>Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel</p>	<p>Brukere ved NTNU er tilknyttet Microsoft 365 Copilot Chat Enterprise Data protection (EDP) siden brukere er logget på med Microsoft Entra-konto ID. EDP innebærer at alle data som sendes mellom bruker og Copilot er kryptert. Krypteringen gjelder både under overføring og lagring.</p> <p>Lagring av spørringer og svar i Microsoft 365 Copilot Chat kan oppfattes både som en fordel og ulempe:</p> <ul style="list-style-type: none"> • Spørringene blir lagret til bruker sletter de, eller blir liggende frem til brukerkontoen avsluttes Dette kan oppfattes som en fordel ved at hver enkelt bruker har oversikt over spørringer vedkommende har gjort. Det vil gi kontinuitet og sporbarhet i bruken av verktøyet for den enkelte bruker. • Samtidig vil lagring av spørringer og lagringstiden dette har, kunne oppfattes som en ulempe med tanke på at data da lagres. Det kan for eksempel oppstå usikkerhet om hvorvidt NTNU kan få innsyn i den enkelte brukers data i verktøyet (overvåking av den registrerte). • Minner (Copilot Memory) blir lagret ut fra brukerens preferanser over tid. Minner skal gi mer relevante og tilpassede svar i chatten, slik at brukeren slipper å gjenta instruksjoner. Dette kan være en fordel for brukeren ved at Copilot Chat kjenner igjen hvordan brukeren ønsker respons. Hver enkelt bruker kan skru av minner helt, og de kan slette minner. Det hadde vært bedre innebygd personvern om Copilot Memory hadde vært avslått per default. • Minner blir lagret som spørringer og det kan oppstå usikkerhet om NTNU eller uvedkommende kan få innsyn i minnene som lagres.
<p>Vil den registrerte ha en særskilt forventning om konfidensialitet?</p>	<p>Nei</p>
<p>Vil den registrerte ha en særskilt forventning om at personopplysningene er nødvendige og korrekte?</p>	<p>Nei</p>

<p>Vil den registrerte ha en særskilt forventning om privatliv?</p>	<p>Hvis en registrert ikke er kjent med teknologien kan den registrerte tenke at interaksjonen mellom seg og Copilot ikke er tilgjengelig for andre, og dermed opptre på en privat måte som en ikke ønsker skal komme på avveie. Det bør derfor antas at en vanlig bruker av verktøyet anser dette som et privat område.</p>
<p>Vil det behandles personopplysninger om barn, pasienter eller andre kategorier av personer som defineres som sårbare?</p>	<p>Det kan forekomme behandling av personopplysninger om barn eller andre sårbare personer dersom noen legger inn dette i chatten.</p>
<p>Finnes det tidligere erfaring med tilsvarende type behandling?</p>	<p>Ja. Forskningsmiljø ved NTNU er ledende kompetansemiljø nasjonalt og har jobbet med problemstillinger knyttet til bruk av språkmodeller og kunstig intelligens i en årrekke.</p> <p>Tjenester som ChatGPT og Grammarly har vært i bruk samfunnet en stund, og NTNU har laget retningslinje for kunstig intelligens for eksamen og undervisning: https://i.ntnu.no/wiki/-/wiki/Norsk/Kunstig+intelligens+i+undervisning+og+vurdering</p> <p>I 2025 ble retningslinjen Bruk av IKT-verktøy med generativ kunstig intelligens ved NTNU ferdigstilt, denne gjennomgår jevnlig revisjon (halvårlig): https://i.ntnu.no/wiki/-/wiki/Norsk/Bruk+av+IKT-verkt%C3%B8y+med+generativ+kunstig+intelligens+ved+NTNU+-retningslinje</p> <p>Språkmodeller har blitt allemannseie de siste årene og mange bruker en eller annen form for kunstig intelligens i arbeidet eller studiene sine.</p> <p>Teknologien utvikler seg stadig, det er stadig forbedringer og ny funksjonalitet tilgjengelig i Copilot og tilsvarende verktøy.</p>
<p>Beskriv eventuelle relevante fremskritt innen teknologi eller sikkerhet</p>	<p>Utdrag fra https://snl.no/språkmodell: «Nyere språkmodeller</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 bare telle ordforekomster, bruker man i dag nevralt nettverk.</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</i></p>

	<p><i>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. For eksempel:</p> <ul style="list-style-type: none"> • Dutch scandal (<u>diskriminerende algoritmer</u>) • Eksamensjuks. Microsoft 365 Copilot Chat er et verktøy som kan gjøre det enklere å jukse på eksamen. Ved feil bruk kan referanser og tolkning av innhold bli feil. Studenter kan bli tatt for plagiat/tekstlikhet. • Forvaltningsrevisjon fra Riksrevisjonen: <u>Bruk av kunstig intelligens i staten</u> • Diskriminering og manglende likebehandling. For eksempel https://www.bufdir.no/aktuelt/ny-rapport-lite-kunnskap-og-kompetanse-om-kunstig-intelligens-og-diskriminering/ • Datatilsynets rapport etter sandkasse-prosjekt ved NTNU: https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/ntnu-sluttrapport-copilot-med-personvernbriller-pa/ • Tromsø kommune brukte kunstig intelligens i saksbehandling av skolestruktur. Chatloggene er nå frigitt med fullt innsyn: KI-Tromso-kommune-Kommunens-vedtak-omgiores-med-markeringer.pdf <p>Den beskrevne måten å behandle personopplysninger på i denne tjenesten tilsier ikke at dette skal være en direkte bekymring, men problemstillingene fra eksemplene over gjelder bruk av kunstig intelligens og utøvelse av offentlig myndighet generelt. Det er viktig at slike problemstillinger er godt kjent i organisasjonen.</p>
<p>Vil dere behandle personopplysninger fra ulike datasett, som er innsamlet for ulike formål og fra ulike behandlingsansvarlige?</p>	<p>Nei</p>

Kobles ulike registre for å gi ny type informasjon om den registrerte?	Nei. Men sammenstilling av informasjon fra ulike kilder tilgjengelig på åpent nett vil kunne gi en ny fremstilling av en person.
--	--

6. Identifisering og oversikt

Behandlingsansvarlig:	NTNU
Felles behandlingsansvarlig:	Nei
Databehandler(e):	Microsoft

7. Mottakere av personopplysninger

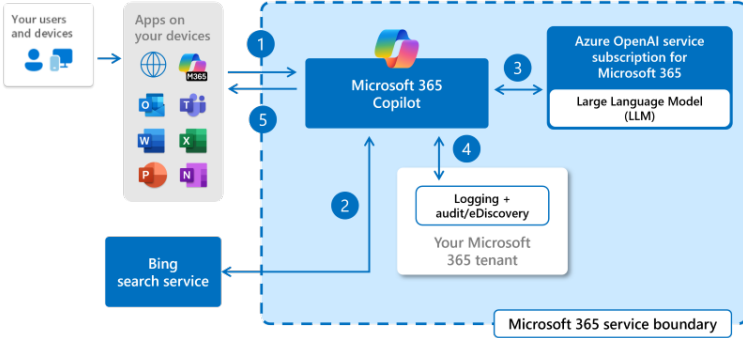
Beskriv alle mottakere/kategorier av mottakere av personopplysninger	<p>Den registrerte ser sine personopplysninger (man kan se dataene når man er innlogget i M365 og åpner Microsoft 365 Copilot Chat).</p> <p>De personopplysningene som hver enkelt bruker legger inn i spørringer blir lagret i Microsoft frem til konto avsluttes eller bruker sletter spørringer, eventuelt skrur av funksjonalitet, der dette er mulig (eks Copilot Memory). NTNU har tilgang til disse opplysningene, men NTNU kontrollerer ikke personopplysninger som legges inn av ansatte og studenter.</p> <p>Microsoft som databehandler, har tilgang til opplysningene som deles i verktøyet.</p>
Hvordan deles personopplysningene mellom avdelinger internt i virksomheten?	Informasjon blir ikke delt internt i virksomheten.
Hvilke eksterne virksomheter deles personopplysningene med? Hvis ja, for hvilke formål og med hvilke rettslige grunnlag?	Personopplysningene deles med databehandler (Microsoft) når løsningen brukes.
Overføres personopplysningene til land utenfor EU/EØS-området (tredjestater), jf. art. 44-49? Hvis ja, hva er det rettslige grunnlaget for det?	<p>Vi kan ikke utelukke at det er overføring av data til tredjeland.</p> <p>Som hovedregel vil ifølge Microsoft data fra chatlogger innenfor EU bli i EU Data Boundary. Når man har aktivert websøk i Copilot, vil websøkene bli behandlet på en annen måte enn innenfor EU data boundary. Microsoft</p>

	<p>er tydelig i sin dokumentasjon på at websøk ikke er EU Data boundary compliant. Selv om instruks fra bruker vil reduseres før det sendes via Bing web søk, er det en risiko for at personopplysninger overføres til tredjeland.</p> <p>Vi kan ikke utelukke at Microsoft har tjenester i testfase (preview) eller ved for eksempel overbelastning av tjenester at data kan behandles utenfor EU/EØS. Dette forstår NTNU som en generell problemstilling for bruk av denne plattformen.</p> <p>Microsoft 365 Copilot Chat Privacy and Protections Microsoft Learn</p> <p>Beskrivelse av hvordan data behandles (11.06.2025):</p> <ol style="list-style-type: none"> 1. Alle de sentrale tjenestene i Microsoft - OneDrive, Sharepoint, Teams og Exchange, lagrer dataene på Microsofts datasenter i Norge. "Filtreringstjenesten" for e-post hos Microsoft (spam, phishing l.o.) kjører i Europa. 2. For logger, metadata o.l. blir det litt mer komplekst, men alle tjenester NTNU benytter hos Microsoft kjører innenfor vår geo-sone som er Europa/EU. <p>NTNU har muligheten til å se hvor de ulike Microsoft-tjenesten lagrer data og vi åpner ikke for bruk av tjenester ved NTNU som lagrer data i tredjeparts-land eller f.eks. USA. IT-avdelingen har prosesser for å sikre at de tjenestene vi tilbyr til enhver tid er innenfor gjeldene retningslinjer og lovverk.</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 rutiner og rammeverk for sikker drift og tilgangsstyring. For å få tilgang til for eksempel lagrede spørringer, må ansatte med administratortilgang aktivere</p>

	<p>roller for å få tilgang. Alt blir logget og varslet Sikkerhetsoperasjonssenteret (SOC).</p> <p>Det er i 2025 gjennomført en Risiko- og sårbarhetsanalyse (ROS) av Entra ID som gjelder logger og administratorrettigheter og ROS for hele M365-plattformen.</p> <p>Alle studenter med tilgang til systemet skal være tatt opp som studenter ved NTNU og er dermed underlagt gjeldende regelverk https://i.ntnu.no/wiki/-/wiki/Norsk/Generelle+lover+og+regler+-+studier. Alle skal gjennomføre nødvendig opplæring, signere IKT-reglement og følge styringssystem for informasjonssikkerhet.</p>
Er alle databehandlere identifisert, og er forholdet til dem avklart gjennom avtaler, jf. art. 28 nr. 3?	Ja. NTNU har ved å innføre sektoravtalen med Microsoft, godkjent Microsofts sine «Terms and conditions». Microsoft som leverandør opplyser her om hvordan data behandles, oppbevares og slettes.
Gir databehandleren tilstrekkelige garantier for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen, vil gjennomføres?	Ja. Mer informasjon er delt på leverandørens nettsider: https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection

8. Dataflyt, lagring og mellomlagring

Hvordan overføres og tilgjengeliggjøres personopplysningene?	<p>Når den registrerte ønsker å bruke verktøyet går hen til et nettsted for å åpne Copilot. Nettstedet vil da kjøre en spørring mot NTNUs brukerdatabase (Active directory – Entra-konto ID) for å bekrefte at bruker er ansatt eller student ved NTNU. Da skjer dette:</p> <ul style="list-style-type: none"> • Brukere ved NTNU er tilknyttet Enterprise Data protection (EDP) siden brukere er logget på med Microsoft Entra-konto ID. EDP innebærer at alle data som sendes mellom bruker og Copilot er kryptert. Krypteringen gjelder både under overføring og lagring. • Brukere får tilgang til Microsoft 365 Copilot Chat ved å logge på Microsoft 365 applikasjonen, eller
--	---

	<p>fra nettleseren Edge der den er lagt til øverst på høyre side.</p> 
<p>Hvor og hvor lenge lagres personopplysningene ulike steder?</p>	<p>Tilgangskontroll – persondata lagres slik: Brukere får tilgang til Microsoft 365 Copilot Chat ved å logge på Microsoft 365 applikasjonen, eller fra nettleseren Edge der den er lagt til øverst på høyre side, eller ved å skrive inn url direkte. Microsoft Entra-konto ID tilknyttet NTNUs tenant (NTNUs dedikerte område i Microsoft-skyen).</p> <p>Spørring og svar (interaksjoner) lagres slik:</p> <ul style="list-style-type: none"> • Copilot Orchestrator er den modulen i Microsoft 365 Copilot Chat som koordinerer spørringene mellom bruker, språkmodell og Bing-søket, samt sørger for at spørringene blir lagret. • Det er ulike språkmodeller som blir brukt for å gi svar på spørringene som bruker legger inn. Spørringer og svar blir ikke brukt for å trene underliggende grunnmodeller. Det er altså ingen lagring for dette formålet. • Før svaret sendes tilbake til chatten slik at brukeren ser den, logges og lagres spørringen og svaret i brukerens egen postboks i Exchange for revisjon/logging og eDiscovery. Spørringer og svar lagres og logges frem til brukerkonto avsluttes ved NTNU, eller brukeren sletter egne spørringer.
<p>Hvor lenge lagres personopplysningene etter at formålet ved behandlingen er over, før de slettes? Når skal opplysningene slettes? Er det utarbeidet sletterutiner?</p>	<p>Ved global retention policy gjelder pkt 1 og 2 under.</p> <p>Opplysninger for tilgangsstyring lagres ikke lenger enn normalt for slike opplysninger. Data slettes når brukerkonto slettes (for eksempel når ansatte/studenter slutter). Det er gode rutiner for dette.</p> <p>Personopplysninger som bruker skriver inn spørringer, og som Copilot returnerer som svar.</p>

	<ol style="list-style-type: none"> 1. Hvis bruker ikke sletter søket sitt, lagres opplysningene frem til brukerkontoen avsluttes (standardinnstilling). For ansatte betyr dette at søk blir lagret i hele perioden de er ansatt ved NTNU. For studenter vil søk bli lagret i hele studieperioden. Studentkontoer slettes permanent 4 måneder etter avsluttet studieperiode. Hvis studenten blir ansatt ved NTNU før permanent sletting trer inn, så vil studentkontoen endres til ansattkonto og alt kontoinnhold, inkludert søk i Copilot, beholdes. 2. Hvis bruker sletter spørringen og svaret, blir det lagret en backup av dataene i inntil 30 dager før alt er slettet.
Er personopplysningssikkerheten tilstrekkelig ivaretatt?	Ja, for klassifiseringsnivå åpen og intern (uten personopplysninger) i henhold til styringssystem for informasjonssikkerhet.

9. Informasjonssikkerhet

Gjennomgå den funksjonelle beskrivelsen av alle behandlinger og om alle aktiva som skal brukes er identifisert?	<p>Nei det vil ikke være mulig. Det er hver enkelt bruker som bestemmer hva verktøyet skal brukes til på egne vegne. Informasjonen (instruksen) som en bruker legger inn sendes til en språkmodell som gir svar avhengig av instruksen. Dette kan være fra språkmodellen eller fra Bing søk.</p> <p>For å møte dette er det gjort regulatoriske tiltak som generelle retningslinjer for bruk av generativ kunstig intelligens og organisatoriske tiltak. Ivaretagelsen av informasjonssikkerheten i Copilot følger samme administrative forvaltning som andre tjenester fra Microsoft:</p> <ul style="list-style-type: none"> • Det finnes et eget kjerneteam på IT-avdelingen som fortløpende vurderer tjenestenivå, endringer og oppgradering. • Det er gjennomført en egen risiko- og sårbarhetsvurdering av Copilot fra Seksjon for Digital sikkerhet. • Det planlegges en DPIA for Microsoft 365-plattformen med oppstart høsten 2025 • Risikovurderingen av Microsoft 365 (plattformen som Copilot jobber ut fra) er fulgt opp og forbedret
---	---

<p>Tas ny teknologi i bruk, eller brukes eksisterende teknologi på en ny måte?</p>	<p>Relativt ny teknologi tas i bruk, men tilgangsstyring og annen driftsteknologi gjenbraker samme teknologi som er godt kjent i Microsoftplattformen. NTNUs brukere er kjent med verktøyet allerede og har hatt tilgang en god stund (ansatte siden september 2023 og studentene siden mars 2024)</p> <p>Sikkerhetslogging i Microsoft 365 er relativt ny og teknologien utvikles raskt. Se risikomatrix med tiltak: Det foreslås risikovurdering og forbedring av rutiner og prosedyrer.</p>
<p>Har virksomheten bygget systemet fra grunnen av eller er det kjøpt ferdig (som hyllevare) fra ekstern leverandør og deretter installert hos dere?</p>	<p>Ekstern tjeneste i sky (SaaS – «Software as a service»).</p>
<p>Er programvaren utviklet med innebygd personvern og personvern som standardinnstilling?</p>	<p>Microsoft skriver på sine nettsider at de har innebygd personvern som standardinnstilling. Microsoft 365 er et komplekst system som består av mange tjenester. Hver enkelt tjeneste kan ha ulike innstillinger enn "modersystemet", her er det en veg å gå for å kartlegge og gjennomføre innebygd personvern. For Microsoft 365 Copilot Chat er det vanskelig å finne konkrete tiltak som tilsier at applikasjonen faktisk har innebygd personvern. Det er opp til hver enkelt bruker å unngå at konfidensiell informasjon legges inn i Copilot-chatten. Hvis bruker prøver å laste opp et dokument som er merket med fortrolig eller strengt fortrolig avsluttes opplastingen av dokumentet, det er funksjonalitet som støttes så lenge NTNU har Enterprise Data Protection-versjonen av Copilot for studenter og ansatte. Microsoft tilbyr Microsoft Purview og Microsoft Priva som "enhetlig plattform for å hjelpe deg å overholde personvernforskriftene", NTNU har ikke lisens på Microsoft Priva og funksjonene oppfyller heller ikke tilstrekkelige tekniske og organisatoriske tiltak for oppfylle krav om innebygd personvern. For eksempel, så innebærer innebygd personvern at produksjonssetting og oversikt over funksjonalitet skal godkjennes. For NTNU ble dette godkjent da vi tok i bruk M365 på overordnet nivå, og denne godkjenningen gjøres dermed ikke per tjeneste under M365-paraplyen. Endringer i funksjonaliteten i tjenestene blir varslet på forhånd før utrulling starter. Denne varslingen er global og ikke tilpasset hver enkelt organisasjon når endringen faktisk skjer i hver organisasjon. Endringer kan derfor skje et halvt år etter varsling, og det må utarbeides manuelle rutiner for å sjekke når endringen faktisk skjer.</p>

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

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

10. 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.

Rettslig grunnlag

Rettslig grunnlag/behandlingsgrunnlag:	<p>For ansatte: Personvernforordningen artikkel 6 b) «behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse»</p> <p>Vurdering: NTNU har arbeidsavtale med alle ansatte. For at den ansatte skal klare å gjøre jobben sin skal arbeidsgiver tilby gode nok verktøy. NTNU har valgt å tilby Microsoft-tjenester til sine ansatte.</p> <p>For studenter: Personvernforordningen artikkel 6 e) «behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt»</p> <p>Vurdering: Studenter skal gjennomføre et utdanningsløp hvor det forventes bruk og kunnskap om ulike IKT-verktøy i tråd med tidens teknologiske utvikling. NTNU har et ansvar for å gjøre teknologi tilgjengelig for studentene.</p>
--	---

	<p>I og med at behandlingsgrunnlaget er art. 6 nr 1 bokstav e) (oppgave i allmennhetens interesse eller utøve offentlig myndighet) kreves det etter art. 6 nr 3 i tillegg et supplerende rettsgrunnlag i nasjonal rett - normalt lov eller forskrift. I denne sammenheng er flere supplerende rettsgrunnlag i universitets- og høyskoleloven:</p> <ul style="list-style-type: none"> - § 1-1 om formålet med universiteter og høyskoler - § 2-8 om Universiteters og høyskolars behandling av personopplysninger - § 10-1 om studentenes læringsmiljø - § 11-3 om utdanningsplan
Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem for de registrerte?	Nei, det er ikke direkte tydelig for den registrerte å se sammenhengen mellom det rettslige grunnlaget og dette konkrete verktøyet. Dette er en problemstilling som gjelder for tilgangen til alle IKT-tjenester på NTNU.
Omfatter rettslig grunnlag både egne formål og eventuell utlevering?	Ja.
Vurder hvordan åpenhet ivaretas i behandlingen	<p>Generelt rett til innsyn i egne personopplysninger etter personopplysningsloven (GDPR-innsyn).</p> <p>I tillegg er NTNU åpen med denne personvernkonsekvensvurderingen på egne informasjonssider og gjennom utsendt informasjon til alle ansatte og studenter. Prosessen rundt personvernkonsekvensvurderingen er også myntet på å ivareta åpenhet, blant annet ved at den er sendt på høring til Studenttinget og SESAM.</p>

Formålsbegrensning

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

Er formålet klart definert? Er formålet definert slik at det samsvarer med forventningene til den registrerte?	Ja.
--	-----

Vurder om formålet kan oppnås med en mindre inngripende behandling	Nei, ikke mulig. Gjelder bare åpne og interne data. Alternativet vil være å ikke bruke Copilot.
Vurder hvorvidt formålet kan oppnås med anonyme eller pseudonyme alternativer	Nei, ikke mulig.

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, ikke for å ivareta tilgangskontroll. Opplæring og bevisstgjøring av brukere mtp hva de legger inn i chatten er viktig som tiltak (se risikomatrix med tiltak, under).
Begrunn nødvendighet og relevans relatert til formål for hver enkelt variabel i et datasett	For å ivareta tilgangskontroll er det kun nødvendige og relevante data som er i bruk. Opplæring og bevisstgjøring av brukere mtp hva de legger inn i chatten er viktig som tiltak (se risikomatrix med tiltak, under).

Riktighet

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

Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering	Brukernavn holdes korrekt og oppdatert i Active Directory/Entra ID, og kontrolleres gjennom andre kjernesystemer på IT-avdelingen. Tolkning av personopplysninger som bruker selv legger inn er umulig å forutse resultatet av fra sesjon til sesjon. Det er stor sannsynlighet for at språkmodellen kan gi ulike og feilaktige svar. Opplæring og bevisstgjøring av brukere mtp hvor problematisk det er å bruke Copilot til faktaopplysninger er viktig som tiltak (se risikomatrix med tiltak, under).
Vurder om dere har nødvendig funksjonalitet for å rette og slette uriktige opplysninger	Ja. Løsningen har samme slettefunksjonalitet som andre tjenester i M365. Brukere kan slette hver enkelt chat i høyre panel, ved å trykke på tre prikker ved siden av chatten og deretter trykke Delete/Slett.

	Alternativt følge prosedyrer for sletting i NTNUs personvernerklæring.
Ut ifra den registrertes perspektiv, er det behov for kontradiksjon?	Nei. Det ligger i dette verktøyets natur å kunne gi uriktige opplysninger. Opplæring og bevisstgjøring av brukere mtp hvor problematisk det er å bruke Copilot til faktaopplysninger er viktig som tiltak (se risikomatrise med tiltak, under). Brukere må være kritisk til informasjonen som Microsoft 365 Copilot Chat gir. Microsoft 365 Copilot Chat kan ikke brukes til å medvirke til beslutninger.

Lagringsbegrensning

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

Vurder om personopplysninger lagres etter at formålet er oppnådd	<p>Som standardinnstilling: Hvis bruker legger inn personopplysninger i spørringer vil dette lagres permanent i M365, frem til brukerkontoen slettes (som skjer når en ansatt eller student slutter).</p> <p>Formålet med behandlingen er å:</p> <ol style="list-style-type: none"> 1. Tilby en språkmodell for behandling av gule/interne data ved NTNU (uten personopplysninger) <ol style="list-style-type: none"> a. Å tilby og anbefale et sikrere alternativ til studentene enn åpne tjenester på nett 2. Tilby en lett tilgjengelig og trygg språkmodell der NTNUs ansatte og studenter kan gjøre seg kjent med fordeler og ulemper med ny teknologi. <ol style="list-style-type: none"> a. Å tilby det samme verktøyet til både studenter og ansatte slik at fagspesifikk opplæring kan gis i ordinær undervisning. 3. Tilby en teknisk løsning hvor NTNU samtidig tilgjengeliggjør informasjon om hvordan vi har utført risikovurdering og personvernkonsekvensvurdering. <p>Det vurderes derfor dithen at</p>
--	--

	<p>personopplysninger ikke lagres etter at formålet er oppnådd, i og med at formålet er kontinuerlig mens en ansatt og student er i et aktivt arbeids-/studieforhold ved NTNU. Det betyr likevel ikke at det er tilstrekkelig behov for å ta vare på mer opplysninger enn nødvendig. Det er ikke behov for å ta vare på spøringer og svar til evig tid for å oppnå formålet. Automatisk sletting etter en periode er et risikoreduserende tiltak som skal utføres når det er teknisk mulig. Se tiltak s. 29.</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>Dette er ikke aktuelt i denne behandlingen.</p>

De registrertes rettigheter

<p>Vurder hvordan informasjon til de registrerte gis</p>	<p>Viktige oppdateringer om Copilot blir delt til alle ansatte og studenter som melding til kanal «Alle ansatte» og «Studenter».</p> <p>Proessen rundt personvernkonsekvensvurderingen av Copilot er også myntet på å ivareta åpenhet, blant annet ved at den er sendt på høring til Studenttinget og SESAM. Når DPIAen er ferdig vil den bli publisert på åpen nettside.</p> <p>Det er opprettet egen wikiside som beskriver verktøyet og behandlingen av personopplysninger https://i.ntnu.no/wiki/-/wiki/Norsk/Copilot På denne siden skal det legges inn oppdatert veiledning på hvordan slette og slå av funksjonalitet.</p> <p>Opplysninger om brukerkonto i NTNUs systemer generelt, er også delt i IKT-reglementet (relevant for tilgangskontroll).</p>
<p>Vurder innhenting av samtykke, jf. art 7 og 8</p>	<p>For ansatte: Innhenting av samtykke er ikke vurdert som behandlingsgrunnlag i denne behandlingen.</p>

	For studenter: Samme vurderingsgrunnlag som for ansatte.
Vurder hvordan den registrertes rett til innsyn og til dataportabilitet ivaretas, jf. art. 15 og 20	<p>Den registrerte har rett til innsyn i egne personopplysninger etter personopplysningsloven (GDPR-innsyn). Det vurderes dithen at den registrerte på enkelt vis kan få innsyn i sin egen chatlogg, enten i form av sin egen tilgang i selve verktøyet, eller ved å sende NTNU en innsynsbegjæring, som da vil bli behandlet på samme måte som alle innsynsbegjæringer ved NTNU. Innsyn vil kunne ivaretas ved at administrator kan hente ut chatlogg fra eDiscovery.</p> <p>Dataportabilitet vurderes som lite relevant for tjenesten, da interaksjoner uansett ikke kan gjentas i verktøy av denne typen. Bruker kan selv laste ned eller klippe ut spørringer med svar og lagre disse utenfor Copilot når de ønsker det.</p>
Vurder hvordan den registrertes rett til korrigerings og sletting ivaretas, jf. 16 og 17	Den registrerte kan slette egne spørringer med svar. Det blir da lagret en backup i bakgrunnen i opptil 30 dager. Den registrertes rett til korrigerings kan ikke ivaretas på samme måte, men det finnes heller ingen funksjon i verktøyet for å korrigere chatlogg.
Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas, jf. art. 18, 19 og 21	<p>En bruker kan velge å ikke ta verktøyet i bruk.</p> <p>Spørringene som hver bruker utfører, er å betrakte som behandling av personopplysninger om brukeren selv. Dette gjelder altså alle spørringer, inkludert minner i Copilot Memory. Spørringer er alltid tilknyttet den brukeren som har lagt dem inn i utgangspunktet, og selv om brukeren ikke bevisst legger inn egne eller andres personopplysninger i selve spørringen. Interaksjonene kan for eksempel fortelle noe om hvem brukeren er, og hva vedkommende er opptatt av for tiden.</p> <p>Når verktøyet tas i bruk i undervisning for alle studenter i et gitt fag, vil alle studenter måtte legge inn spørringer og motta svar ihht</p>

	<p>opplæringsopplegget som foreleser har laget. Gitt det skjeve maktforholdet mellom student og studiested/foreleser, kan det antas at det å protestere og å be om begrensning mot bruk av sine personopplysninger i opplæringsformål ikke er veldig enkelt for en student.</p> <p>Hvis ansatte blir pålagt å bruke Copilot for effektiviseringsformål i sin arbeidshverdag, kan man også anta at det skjeve maktforholdet mellom ansatt og arbeidsgiver medfører at den ansatte kan unngå å be om behandling av sine personopplysninger, all den tid NTNU har definert alle spørringer som behandling av personopplysninger.</p>
<p>Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering, håndheves, jf. art. 22</p>	<p>Verktøyet skal ikke benyttes til noen form for automatiserte avgjørelser om individer eller virksomheten. Dette vil løsningens brukere bli informert om i form av opplæring og retningslinjer for bruk.</p> <p>Det er ikke mulig å sikre at ingen brukere bruker tjenesten til saksbehandling, som grunnlag for beslutninger etc.</p> <p>I retningslinjer og gjennom opplæring/bevisstgjøringstiltak vil det påpekes at løsningen ikke skal benyttes til denne typen informasjon/arbeidsprosesser.</p>

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

Under følger en risikovurdering og tiltak for å håndtere de alvorligste risikoene i Microsoft 365 Copilot Chat. De registrerte (ansatte og studenter ved NTNU) har blitt informert om endringer i Microsoft ved en [Innsida-melding 26. November 2024](#).

Personvernkonsekvensvurderingen ble sendt til behandling i samarbeidsorganene og Studenttinget i januar/februar 2025.

Identifiserte og vurdering av 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	Lav	Manglende opplæring og generelt lav personvernkompetanse hos brukere.	Liten
4	Manglende opplæring av brukere øker risikoen og sannsynlighet for at øvrige risikoer inntreffer	Høy	Manglende opplæringsrutiner for ansatte	Medium
5	Feil bruk av verktøyet påvirker utøvelser av offentlig myndighet negativt. En part kan få en sak behandlet feil.	Høy	Verktøyet blir tatt ukontrollert eller feilaktig i bruk i saksprosesser.	Liten
6	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.	Medium	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.	Høy
7	Feilaktig bruk av verktøyet kan føre til overvåking av ansatte og studenters chatlogger. Brudd på lovverk kan føre til ulovlig adferd overfor ansatte og registrerte, og	Høy	Chatlogger lagres og kan aksesseres av administratorer.	Medium

	gi kraftige negative reaksjoner for en organisasjon/arbeidsgiver.		Manglende opplæring av brukere og administratorer.	
8	Brukere tar i bruk åpne, nettbaserte KI-verktøy i stedet for Copilot, og deler personopplysninger som da kommer på avveie. Alvorlighetsgraden avhenger av informasjonen som er lagt inn	Medium	Manglende informasjon til de registrerte om behandlingsansvarliges bruk/ikke bruk av chatlogger.	Høy
9	Verktøyet brukes til å fatte beslutninger som har påvirkning på den registrerte. Eksempel: Undersøke og fatte beslutning rundt hvorvidt en student har fusket på eksamen eller oppgaver.	Høy	Manglende informasjon om at NTNU ikke bruker chatloggen til overvåking av ansatte og studenter.	Liten

Identifiserte risikoreduserende og skadebegrensende tiltak:

Risiko-ID	Type tiltak (teknisk, organisatorisk, pedagogisk)	Tiltak	Effekt på risiko	Restrisiko	Ansvarlig enhet for tiltak
1-9	O	Utarbeide nye og oppdatere eksisterende rutiner for sletting av personopplysninger.	Redusert	Ja	IT og SoB
1,2,4,6,7,9	O	Opprette internkontrollrutiner for å sjekke etterlevelse av nye rutiner og gjennomgang av administratorers bruk eDiscovery.	Redusert	Ja	IT
1-9	O	Sikre åpenhet og informasjon til brukere om hvordan data behandles, lagres og slettes, både i NTNU-systemer og eksterne systemer. Utarbeide personvernerklæring og oppdatere veiledninger på wikisiden. Formidle dette i flere kanaler.	Redusert	Ja	IT og SoB
1-9	O	Lag en exit-strategi og gjør brukere ved NTNU i stand til å avslutte bruken verktøyet.	Redusert	Ja	IT-infrastruktur

1-9	P	Prioriter arbeidet med kompetanseheving for alle administratorer.	Redusert	Ja	IT
1-9	O, P	Gjennomgå og oppdatere informasjon om hvor registrerte kan henvende seg for å få personopplysninger rettet eller slettet.	Redusert	Ja	IT og AUV
1-9	O, T	Gjennomgå og sikre at rutiner for sletting av bruker og innhold følges når ansatte slutter eller endrer stilling.	Redusert	Ja	IT
9	T	Gjennomgå alle innstillinger og sørg for at disse er satt til mest mulig personvernvennlig og brukervenlig.	Redusert	Ja	IT
1-9	T	Gjennomgå og vurdere innstillinger på «retention policy» for verktøyet, slik at dette blir mest mulig personvernvennlig, brukervenlig og ivaretar krav om sletting. Veiledning og informasjon om retention policy og hva det har å si for hver enkelt bruker. Sammenfaller med tiltak "Sikre åpenhet og informasjon til brukere"	Redusert	Ja	IT
1-9	O, P	Opplæring av studenter og ansatte for å sikre forståelse av hvordan KI-verktøyet Copilot fungerer	Redusert	Ja	IT og AUV
7-9	O	Retningslinjer for å sikre at chatlogg ikke brukes til å undersøke fusk eller overvåke ansatte	Redusert	Ja	IT-digital sikkerhet

Restrisiko etter gjennomførte tiltak:

Risikonivå angis fra lav til høy: (● Høy / ● Middels / ● Lav)

Risiko-ID	Beskriv risikoen behandlingen har for de registrertes rettigheter og friheter, og hvilke konsekvenser den har for de registrerte	Alvorlighetsgrad for risikoen	Sannsynlighet for at en hendelse oppstår	Restrisiko per risiko etter gjennomførte tiltak
1	Personopplysninger kommer på avveie	Medium	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	Medium	
3	En bruker legger inn noen andre sine personopplysninger som kommer på avveie	Lav	Liten	
4	Manglende opplæring av brukere øker risikoen og sannsynlighet for at øvrige risikoer inntreffer	Høy	Medium	
5	Feil bruk av verktøyet påvirker utøvelser av offentlig myndighet negativt. En part kan få en sak behandlet feil.	Høy	Liten	
6	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.	Medium	Høy	
7	Feilaktig bruk av verktøyet kan føre til overvåking av ansatte og studenters chatlogger. Brudd på lovverk kan føre til ulovlig adferd overfor ansatte og registrerte, og gi kraftige negative reaksjoner for en organisasjon/arbeidsgiver.	Høy	Medium	
8	Brukere tar i bruk åpne, nettbaserte KI-verktøy i stedet for Copilot, og deler personopplysninger som da kommer på avveie. Alvorlighetsgraden avhenger av	Medium	Høy	

	informasjonen som er lagt inn			
9	Verktøyet brukes til å fatte beslutninger som har påvirkning på den registrerte. Eksempel: Undersøke og fatte beslutning rundt hvorvidt en student har fusket på eksamen eller oppgaver.	Høy	Liten	

12. Ledelsens validering av personvernkonsekvensvurderingen (DPIA)

Moment	Navn og dato	Kommentarer
Tiltak godkjent av:	<i>IT-direktør Håkon Alstad, 30.10.25</i>	<i>Godkjent per e-post 30.10.25. Blir også godkjent i Elements, sak 2023/32790</i>
Restrisiko godkjent av:	<i>IT-direktør Håkon Alstad, 30.10.25</i>	<i>Dersom restrisiko med høy risikograd blir godkjent, ta kontakt med Datatilsynet før oppstart for forhåndsdrøfting, jf. art. 36 nr. 1.</i>
Personvernombudsassistans gitt:	<i>Thomas Helgesen 28.10.25</i>	<i>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.</i>
<p>Sammendrag av personvernombudets råd:</p> <p>Personvernombudet har tidligere deltatt i DPIA-prosessen ved lansering av Copilot Chat for både ansatte og studenter. En ny DPIA er nå nødvendig som følge av vesentlige endringer i funksjonalitet, særlig knyttet til lagring av spørringer og innføringen av «Memory»-funksjonen, som påvirker behandlingen av personopplysninger.</p> <p>Overgangen fra automatisk sletting til lagring av spørringer utfordrer prinsippene om lagringsbegrensning og dataminimering. Spørringer kan inneholde personopplysninger, og det må gjøres en vurdering av om lagring gjennom hele studie- eller ansettelsesperioden er nødvendig. Personvernombudet stiller spørsmål ved om en lagringsperiode på flere år er for lang, og anbefaler at det vurderes en begrensning, for eksempel til ett år. Brukere har mulighet til å slette egne spørringer, men data forblir tilgjengelig for Microsoft og administrator i inntil 30 dager. Det forutsettes at brukerne får tydelig og lett tilgjengelig informasjon om lagring, sletting og konsekvenser av dette. Logging av administratorers innsyn vurderes som et positivt tiltak for å motvirke misbruk.</p> <p>Memory-funksjonen gir mulighet for tilpasning av verktøyet til brukerens preferanser, men innebærer samtidig en form for profilering. Brukeren kan se, slette og deaktivere lagrede preferanser. Personvernombudet ville foretrukket at funksjonen var basert på aktivt samtykke (opt-in), men forutsetter at det gis god informasjon og tydelige instruksjoner for deaktivering og sletting. Lagringstiden for Memory er oppgitt å være lik som for vanlige spørringer, og de samme vurderingene gjelder her.</p> <p>Copilot Chat skal gjøres tilgjengelig i applikasjoner på M365-plattformen, som for eksempel Teams. Personvernombudet har ingen innvendinger mot dette så lenge det ikke medfører automatisk behandling av dokumenter og data uten brukerens initiativ. Dersom slik behandling skulle bli aktuelt, må det foretas en ny vurdering opp mot personvernet.</p> <p>Det er også nevnt at oppsett og bruk av agenter vil bli en ny mulighet, men funksjonaliteten er foreløpig ikke tatt i bruk og ikke nærmere beskrevet. Personvernombudet gir derfor ingen merknad til denne funksjonaliteten på nåværende tidspunkt.</p> <p>Avslutningsvis har personvernombudet ingen innvendinger mot bruk av verktøyet, forutsatt at risikoreduserende tiltak som beskrevet i DPIAen følges opp og gjennomføres. DPIAen vurderes som grundig og tilfredsstillende, og har i det vesentlige adressert risikoene ved den nye funksjonaliteten. Personvernombudets kommentarer understreker forhold som bør prioriteres, men innebærer ikke nye innvendinger utover det som allerede er identifisert i DPIAen.</p>		

Personvernombudets råd er akseptert eller overprøvd av:	<i>IT-direktør, 30.10.25</i>	<i>Hvis overprøvd, må du forklare bakgrunnen for dette</i>
<i>Kommentarer: IT-direktør aksepterer personvernombudets råd.</i>		
De registrertes synspunkter er innhentet og gjennomgått av:	<i>SESAM 10.02.2025</i>	<i>Hvis din avgjørelse avviker fra de registrertes synspunkter, bør du forklare bakgrunnen for at du velger å sette i gang/fortsette behandlingen</i>
<i>Kommentarer: Vedlagt referat fra SESAM og tilbakemelding fra Studenttinget. Korrespondanse er arkivert på sak 2024/5301.</i>		
Denne personvernkonsekvensvurderingen vil følges opp av:	<i>IT-avdelingen</i>	<i>Personvernombudet bør også følge opp personvernkonsekvensvurderingen løpende, jf. art. 39 nr. 1 bokstav c.</i>

Vedlegg til personvernkonsekvensvurdering Microsoft 365 Copilot Chat with enterprise data protection

Vedlegg 1: Referat fra SESAM møte 10.02.2025

Sak 8/25: Kunstig intelligens – overvåking og personvern (orientering)

NTNU må ta stilling til hvordan vi skal ivareta personvern når nye datasystemer gir mulighet for lagring av personrelatert informasjon. Eksempel: Copilot Enterprise. NTNU innførte dette nye KI-verktøyet for ansatte og studenter i 2024. Fra november ble verktøyet endret slik at det tar ut en alarmlogg basert på søkeord og en logg over hvem som har brukt verktøyet. Etter ny personvern-vurdering, forslås det at NTNU ikke skal gjennomføre innsyn i logger eller overvåke bruken av verktøyet. Det skal alltid gjøres en personvernkonsekvensvurdering ved innføring av ny teknologi. Før personvernombudet gjør sine vurderinger må berørte gis mulighet til medvirkning? Hvordan skal vi ivareta medvirkning i slike personvernkonsekvensvurderinger ved innføring av ny teknologi framover?

- NTL. Takk for god presentasjon og gode spørsmål. NTL har tidligere etterlyst hvordan NTNU skal forholde seg til ulike datasystem som har innebygget ulike kontrollsystemer om bruk og bruker, som ikke er like akseptabelt i Norge og i vår type virksomhet. Iht. AML § 9 om kontrolltiltak i virksomheten, skal man ivareta medvirkning fra tillitsvalgte og informasjon til ansatte. Nye systemer kan også få ringvirkninger utenfor NTNU hvis PST eller andre kan be om innsyn i informasjon om ansatte. Det kan påvirke deres ytringsfrihet.
- Tekna. KI er eksempel på hvordan regelverk ofte kommer i etterkant av den raske teknologiske utviklingen. Hvilket ansvar skal ansatte ha til å sette seg inn i systemene og regelverket?
- NTL. Dette er en utfordring for alle typer virksomhet i regionen og ved andre universitet. Det er viktig at vi får hevet bevisstheten om personvern og at vi trykker ansatte på dette området. Kanskje vi skulle brukt SESAM-seminaret til opplæring og diskusjon om dette temaet?
- Parat. Det er viktig at ansatte er klar over hvordan KI-systemet fungerer i dag.

AUV-avdelingen hadde invitert Studenttinget til å delta på saken. Studenttinget forventer at de får medvirke framover ved innføring av systemer som berører studentenes personvern. De ønsker også åpenhet om hva NTNU har tilgang til av data om studentene.

NTNU må ha en føre-var-tilnærming. Vi må balansere mellom å gi ansatte tilgang til nye systemer så raskt som mulig og å sikre at vi ivaretar de ansattes personvern. Det tilsier at vi er forsiktige ved innføring av nye systemer. Vi har et like stort ansvar for å ivareta personvernet til studenter som til ansatte.

AUV inviteres til et møte med de tillitsvalgte om hvordan NTNU kan ivareta medvirkning / medbestemmelse i personvernkonsekvensvurderinger framover. Det er et stort behov for økt forståelse av personvern og ny teknologi i hele linjen - ansatte, ledere, tillitsvalgte. Tematikken følges opp på SESAM-seminaret i mars.

Vedlegg 2: Svar fra Studenttinget 05.02.2025:

«Studenttinget NTNU takker for moglegheita til å kome med innspel. Me ser viktigheita av at studentar og tilsette har tilgang til eit godt KI-verktøy. Studentar flest har allereie tatt i bruk KI-verktøy ukritisk til korleis sin eigen data vert behandla. Det er betre om NTNU tilbyr ein teneste med kjente svakheiter og gjer alle studentar eit likt utgangspunkt uavhengig av sosioøkonomisk bakgrunn.

Dersom det er mogleg for NTNU som arbeidsgivar å overvake aktiviteten til studentar og tilsette er dette svært problematisk. Studenttinget NTNU forventar at ein slik eventuell sårbarheit utgreiast, og løysast opp i så fort som mogleg. NTNU skal følge gjeldande lovverk og ivareta tilsette sine informasjonssikkerheitsrettigheitar. Denne kartlegginga skal ha vorte fullført 15. januar, og Studenttinget NTNU forventar at funna vert kommunisert vidare til både studentar og tilsette tydeleg og breidt. Om utfordringa skulle vise seg å vere reell og langvarig forventar me at tenesta lukkast for studentar og tilsette.

Dette er ein relativt uformell måte å gje tilbakemeldingar på, og Studenttinget NTNU etterspør ein meir formell høyringsinstans om utfordringa skulle vare ved.»

Vedlegg 2 - Kildeliste:

Første DPIA av Microsoft 365 Copilot Chat:

<https://www.ntnu.no/documents/10507/1359912/2024-02-27+DPIA+Microsoft+copilot.pdf/436d8f4f-6142-d33c-c1df-6769750d7d9a?t=1709887086495>

NTNUs personvernerklæring: <https://i.ntnu.no/wiki/-/wiki/Norsk/Personvernerkl%C3%A6ring+NTNU>

Generell informasjonsside om Copilot fra Microsoft: <https://learn.microsoft.com/en-us/copilot/overview>

Kunstig intelligens i undervisning og vurdering: <https://i.ntnu.no/wiki/-/wiki/Norsk/Kunstig+intelligens+i+undervisning+og+vurdering>

Dutch scandal: diskriminerende algoritmer

Forvaltningsrevisjon fra Riksrevisjonen: Bruk av kunstig intelligens i staten

Diskriminering og manglende likebehandling. For eksempel <https://www.bufdir.no/aktuelt/ny-rapport-lite-kunnskap-og-kompetanse-om-kunstig-intelligens-og-diskriminering/>

Datatilsynets rapport etter sandkasse-prosjekt ved NTNU:

<https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/ntnu-sluttrapport-copilot-med-personvernbriller-pa/>

Microsoft 365 Copilot Chat data movement: <https://learn.microsoft.com/nb-no/microsoft-copilot-service/copilot-data-movement-geos>

Generelle lover og regler - studier: <https://i.ntnu.no/wiki/-/wiki/Norsk/Generelle+lover+og+regler+-+studier>

Microsoft Enterprise Data Protection: <https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection>

Microsoft 365 Copilot Chat på Innsida: <https://i.ntnu.no/wiki/-/wiki/Norsk/Copilot>

Informasjon til ansatte og studenter 26. November 2024: [Innsida-melding 26. November 2024](#)

Jarbekk, E. I. E., & Sommerfeldt, Simen. (2019). *Personvern og GDPR i praksis* (1. utgave.). Cappelen Damm akademisk.

Lov om behandling av personopplysninger (personopplysningsloven) https://lovdata.no/dokument/NL/lov/2018-06-15-38/*#*