

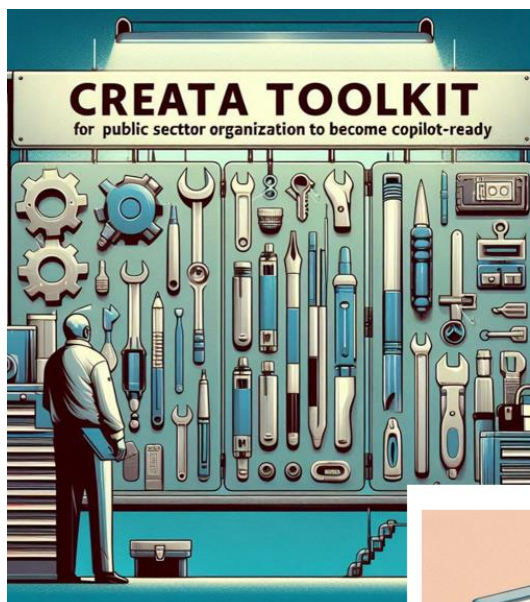
Heine Skipenes, Silje Reiten Blichfeldt,
Bodil Åberg Mokkelbost, Hanne Jensen Moe

PILOTERE COPILOT FOR MICROSOFT 365

Funnrapport fra NTNUs prosjekt i Datatilsynets
regulatoriske sandkasse våren 2024

Trondheim/Gjøvik, 17. juni 2024

NTNU
Norges
teknisk-naturvitenskapelige
universitet
IT-avdelingen/
Avdeling for utvikling og
virksomhetsstyring



Rapport

PILOTERE COPILOT FOR MICROSOFT 365

Datatilsynets regulatoriske sandkasse for personvernvennlig innovasjon og digitalisering våren 2024

VERSJON

Versjonsnummer 1.0

DATO

17. juni 2024

FORFATTERE

Heine Skipenes, Silje Reiten Blichfeldt,
Bodil Åberg Mokkelbost, Hanne Jensen
Moe

ANTALL SIDER OG VEDLEGG

161 sider
Hovedrapport (side 5-26)
Seks vedlegg (side 27-160)

OPPDRAGSGIVER

Datatilsynet

Hvordan blir en organisasjon «Copilot ready»?

Rapporten omhandler NTNUs erfaringer med å teste Copilot for Microsoft 365 våren 2024, og presenterer de åtte hovedfunnene som spilles inn til Datatilsynets prosjekt i den regulatoriske sandkassen for personvernvennlig innovasjon og digitalisering. Funnene inkluderer at Copilot er effektivt når brukeren allerede har god kunnskap om oppgaven, men kan påvirke utøvelsen av offentlig myndighet. Copilot behandler store mengder personopplysninger på nye måter, ikke bare brukernes personopplysninger. Rapporten påpeker også at Microsoft 365 er utfordrende å forvalte, at Copilot fortsatt er tidlig i utviklingsløpet og at det tidvis fungerer veldig bra. Copilot kan påvirke organisasjonen på ulike måter, og systemet kan brukes til å overvåke og måle prestasjoner og adferd. Rapporten understreker viktigheten av opplæring, gode personvernkonsekvensvurderinger og aktiv stillingstaken til hvilke data Copilot skal ha tilgang til. Rapporten anbefaler også å se på Copilot primært som et organisasjonsutviklingsprosjekt (ikke et IT-prosjekt), og anbefaler at organisasjoner bruker prosjektresultatene for å komme raskt inn i kjernen av utfordringene som gjelder for egen virksomhet.

I tillegg inneholder rapporten overordnede anbefalinger til hva en organisasjon bør vurdere før verktøy med innebygd kunstig intelligens tas i bruk, informasjon om hvordan testene har blitt gjennomført og opplæringsprogram, samt NTNUs forslag til personvernkonsekvensvurderinger for både Copilot with commercial data protection og Copilot for Microsoft 365, og utkast til retningslinjer for bruk av generativ kunstig intelligens.

Sammendraget er laget av KI-verktøyet Copilot with commercial data protection. Innholdet er kvalitetssikret av et menneske.

Dette dokumentet er funnrapporten fra NTNUs prosjekt i Datatilsynets regulatoriske sandkasse for personvernvennlig innovasjon og digitalisering våren 2024. Rapporten beskriver NTNUs erfaringer med å teste Copilot for Microsoft 365. Rapporten er basert på data og erfaringer fra en begrenset gruppe av testere i en avgrenset periode, og gir et øyeblikksbilde av prosjektets funn. Verktøyet Copilot for Microsoft 365 er i kontinuerlig utvikling, og kan endre seg over tid. Rapporten er ikke en vitenskapelig rapport, men et dokument som oppsummerer våre erfaringer og er utarbeidet som NTNUs innspill til Datatilsynets sluttrapport fra sandkasseprosjektet (kommer høsten 2024). Rapporten er skrevet fra NTNUs perspektiv, og representerer ikke synspunktene til Datatilsynet, Microsoft eller andre samarbeidspartnere. Rapporten er ikke en anbefaling eller en kritikk knyttet til et konkret verktøy, men en beskrivelse av våre observasjoner og refleksjoner i løpet av en begrenset prosjektperiode. Rapporten er ment som et innspill til andre organisasjoner når de gjør sine egne vurderinger. NTNU understreker viktigheten av at alle organisasjoner bør gjøre egne vurderinger, og NTNUs mål har vært å levere en rapport som kan hjelpe til med å komme så raskt som mulig inn i kjernen av muligheter og utfordringer som kunstig intelligente verktøy gir.

Gjennomgående i dokumentet er det listet opp refleksjonsspørsmål som kan være nyttig å ta stilling til når en organisasjon gjør egne vurderinger. Spørsmålene er satt opp på følgende måte, etter inspirasjon fra malverket til EDUCAUSE sin modenhetsvurdering beskrevet i NTNUs verktøykasse:

	Ja	Nei	Vet ikke
Er organisasjonen din klar for å ta i bruk Copilot for Microsoft 365?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Som en del av NTNUs egen læringsprosess er rapporten så langt det er mulig skrevet ved hjelp av verktøyene Copilot with commercial data protection (<https://copilot.microsoft.com/>) og Copilot for Microsoft 365. Kvalitetssikring er alltid gjort av et menneske. NTNU anbefaler at du leser rapporten med det i bakhodet, så du kan se hva som er mulig å få til med relativt enkle og tilgjengelige verktøy. Hvis du ønsker med informasjon om hvordan dette er gjort i praksis, se vedlagte eksempelbeskrivelse av fremgangsmåte («Steg for steg beskrivelse: Eksempel på bruk av Copilot»).

Kildehenvisninger og referanser er bakt inn i teksten. Vedleggene har egne kildelister relevant for vedlegget.

Alle illustrasjoner er generert av kunstig intelligens (Copilot with commercial data protection), med unntak av der skjermbilder er brukt.

Alt innhold utarbeidet av prosjektet kan gjenbrukes fritt av alle til ikke-kommersielle formål og er lisensiert som CC BY-NC 4.0 (<https://creativecommons.org/licenses/by-nc/4.0/>)



Alle samarbeidspartnere har dekt sine egne utgifter i forbindelse med prosjektet. Microsoft har gjort tilgjengelig intern utrullingsstøtte for programvareleverandøren Crayon sitt arbeid opp mot NTNU (Copilot readiness workshop). NTNU har godkjent Crayons arbeid hos Microsoft og dokumentert dette i NTNUs arkivsystem (sak 2023/37288)

Prosjektet har mottatt støtte fra EUs DIGITAL EUROPE program (nr 101083966)

This project has received funding from the European Union's DIGITAL EUROPE programme, under Grant Agreement n° 101083966.



Innholdsfortegnelse

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

Innledning

Hvordan blir en organisasjon «Copilot ready»? Dette spørsmålet har vært NTNUs hovedproblemstilling i prosjektet i Datatilsynets «regulatoriske sandkasse for personvernvennlig innovasjon og digitalisering våren 2024».

Med Copilot sine egne ord: «Copilot for Microsoft 365 er et produktivitetsverktøy som er drevet av kunstig intelligens og som kombinerer store språkmodeller med innhold fra egne data i Microsoft 365 for å hjelpe deg med å skape, redigere og kommunisere mer effektivt». For å forstå hvordan man kan bli «Copilot ready» må man også skape en grunnleggende forståelse i egen organisasjon for hva verktøy med innebygd kunstig intelligens faktisk er, hva man kan bruke det til og hva man ikke kan bruke det til. I tillegg er det viktig å forstå hva det å ta i bruk kunstig intelligens vil si for organisasjonen både menneskelig og maskinelt. Til grunn for alt arbeidet har vi tatt utgangspunkt i følgende arbeidshypotese: *Hvis det er mulig å gjøre, så vil det bli gjort*. Dette setter strenge krav til systemene og verktøyene våre og hvordan vi skal tenke. I en organisasjon med mer enn 70 000 brukere vil tiltak av typen «du må bare få brukerne til å [...]» være utopisk.

Kunstig intelligens kan bidra til å løse mange samfunnsutfordringer, forbedre offentlige tjenester og skape nye muligheter for innovasjon og verdiskaping. Kunstig intelligens er også en teknologi som reiser en rekke etiske, juridiske, tekniske og organisatoriske spørsmål som må håndteres på en ansvarlig måte. Hvordan kan offentlige organisasjoner bruke KI på en smart, sikker og trygg måte? Hvordan sikre at bruken av KI er i samsvar med egne verdier og mål, og i tillegg overholde regulatoriske krav?

NTNU har gjennom prosjektet med Datatilsynet sett nærmere på disse problemstillingene, og prosjektet har hatt som mål å vurdere om og hvordan en offentlig organisasjon kan bli «Copilot ready». Prosjektet har blitt organisert med tre delprosjekt som til sammen har hatt som mål å utarbeide en verktøykasse med innhold som kan hjelpe offentlige organisasjoner til å bli «Copilot ready», i tillegg til å gjøre en organisasjon bedre rustet til å ta i bruk KI på et mer generelt grunnlag. NTNUs overordnede visjon er «Kunnskap for en bedre verden». Vi mener det er viktig å dele funn og erfaringer så åpent som mulig, og så lukket som nødvendig. Innholdet i verktøykassen på NTNUs nettsider er i tillegg i størst mulig grad lagt ut i et gjenbrukbart format.

Hvorfor vurdere om man er «Copilot ready» nå?

Gjennom prosjektet har vi forsøkt å belyse ulike sider av muligheter, problemstillinger og utfordringer som KI gir, og som kan påvirke en organisasjon. Veldig forenklet har prosjektet identifisert en rekke tema som påvirker NTNUs mulighets- og handlingsrom når det kommer til å ta i bruk KI-verktøy på en god måte. Eksempler på hva som er viktig for NTNU:

- **Rask teknologisk utvikling:** Etter lanseringen av ChatGPT i november 2022 har NTNU opplevd en endret hverdag som påvirker hvordan universitetet må forholde seg til en ny type teknologi som både er veldig tilgjengelig, og veldig forskjellig sammenlignet med tidligere. KI er ikke ett verktøy, det er mange, og gjennom prosjektet har vi omtalt dette som et «teknologisk taktskifte» for å løfte diskusjonen opp fra enkeltverktøyperspektivet.

- **Brukerbehov:** NTNUs ansatte, undervisere, studenter og forskere har et behov for å kunne teste og ta i bruk kunstig intelligens i ulike former i forskning, undervisning, studier, formidling og i arbeidshverdagen generelt. NTNU har et klart og tydelig ønske om å være «fremme i skoa» teknologisk sett.
- **Konkurransefortrinn:** NTNU opplever strammere finansieringsrammer enn tidligere, og har derfor behov for et enda større fokus på effektivitet og produktivitet.
- **Markedsutviklingen:** Leverandører av programvare med integrert KI-funksjonalitet har et ønske om å selge flere og nye verktøy og tjenester. NTNU blir jevnlig kontaktet av forskjellige leverandører fra inn- og utland, og det er vanskelig å holde oversikt over feltet.
- **Regulatoriske krav og endringer:** Personvernforordningen omfatter personopplysninger behandlet av kunstig intelligens, og tidligere gjennomførte vurderinger må revurderes. KI-forordningen er vedtatt i EU og vil snart bli implementert i norsk lov, og andre gjeldende lover som er skrevet teknologinøytralt må forstås og tolkes i en ny teknologisk kontekst.

Disse endringene setter organisasjoner i en posisjon hvor man må ta stilling til nåsituasjonen, og vurdere eget modenhetsnivå for å ta i bruk verktøy med kunstig intelligens, inkludert Copilot for Microsoft 365. NTNU har gjennom dette prosjektet forsøkt å ta stilling til hvorvidt vi er «Copilot ready», og hva som skal til for å kunne bli det. Det viktigste arbeidet for NTNU sin del har utvilsomt vært prosessen fram til der vi er i dag.

Åtte hovedfunn

I denne rapporten presenterer vi våre åtte hovedfunn som beskriver ulike aspekter ved Copilot for Microsoft 365. Funnene presenteres på en gjennomgående måte for å forenkle lesingen, og skape et levende dokument som kan brukes som et arbeidsdokument for andre. Hvert av de åtte funnene presenteres med påfølgende problemstillinger og spørsmål det anbefales å ta stilling til i egen organisasjon, samt noen anbefalinger.

I tillegg til de åtte hovedfunnene har vi samlet vurderinger, metoder, forslag til rammeverk og anbefalinger som er utarbeidet i løpet av prosjektet. Dette legges i en «verktøykasse» som kan være til hjelp for andre virksomheter for å kunne ta i bruk KI på en smart, sikker og trygg måte.

Vi håper at denne rapporten kan bidra til at andre organisasjoner som ønsker å ta i bruk Copilot for Microsoft 365 og KI generelt, kan vurdere om egen organisasjon er eller kan bli «Copilot ready». Vi anbefaler også at du ser særlig på vedleggene i rapporten, da de inneholder mer detaljert informasjon om vårt arbeid og vurderinger.

Vi vil gjerne takke alle som har bidratt til prosjektet, og til våre samarbeidspartnere i Sikt, Microsoft og Crayon som virkelig har stilt opp. Takk til Statens vegvesen, Vestland fylkeskommune og NAV for at dere har delt deres erfaringer og innspill med oss. Vi vil også takke alle våre testere ved IT-avdelingen, deltakere og samarbeidspartnere på NTNUs institutter, fakulteter og avdelinger som har deltatt i gjennomføringen av prosjektet.

En spesiell takk til Datatilsynet for muligheten til å være med i sandkassa, og for at dere har hatt trua på prosjektet vårt. Tusen takk for utrolig gode innspill, hjelp, støtte og råd underveis i prosessen. Dere har gjort oss på NTNU bedre.

God lesning!

«Vi har ansvar for å styre teknologien i riktig retning, teknologien skal ikke styre oss.»

- Eirik Gulbrandsen, Datatilsynet

FUNN 1: Copilot er helt glimrende når du allerede kan det du vil at den skal hjelpe deg med

Copilot fungerer best når brukeren allerede har en solid forståelse av det de ønsker hjelp med. Dette funnet er delt inn i tre hovedpunkter som belyser forskjellige aspekter av denne observasjonen. Disse punktene gir innsikt i hvordan Copilot kan være et kraftig verktøy for de som allerede har en god forståelse av oppgaven de skal løse, men også hvordan det kan være utfordrende for de som prøver å løse en oppgave for første gang.

Når du har en dyp forståelse av informasjonen Copilot bruker, og du vet hva du ville ha gjort selv, kan du raskt identifisere når Copilot gjør feil. Dette gir deg muligheten til å korrigere feilene og gi mer presise instruksjoner til Copilot for å oppnå det ønskede resultatet. Med andre ord, din ekspertise og kunnskap om emnet kan hjelpe deg med å styre Copilot mer effektivt.

Copilot kan hjelpe deg med å komme raskere i gang med oppgaven du skal løse. Den kan gi deg et utgangspunkt, foreslå løsninger, og hjelpe deg med å strukturere arbeidet ditt. Som en sparringspartner kan Copilot bidra med ideer, foreslå forbedringer, og hjelpe deg med å se problemet fra forskjellige vinkler. Dette kan føre til en mer effektiv og bedre oppgaveløsning.

Når du gjør en oppgave for første gang, kan situasjonen være helt annerledes. Uten tidligere erfaring eller kunnskap om oppgaven, kan du ende opp med å bruke mer tid på å kvalitetssikre arbeidet enn på selve oppgaveutførelsen. Det er en betydelig risiko for å gjøre feil, siden du kanskje ikke er kjent med alle aspekter av oppgaven. I slike tilfeller kan Copilot fortsatt være nyttig, men det er viktig å være ekstra oppmerksom på viktigheten av kvalitetssikring.

	Ja	Nei	Vet ikke
Har brukeren en dyp forståelse av informasjonen Copilot bruker?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kan brukeren gi presise instruksjoner til Copilot for å oppnå det ønskede resultatet?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er brukerne gjort i stand til å kvalitetssikre arbeidet når de bruker Copilot?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er det en betydelig risiko for at brukeren gjør feil når de prøver å løse en oppgave for første gang med Copilot?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Anbefaling

- Prioriter opplæring! Kompetanseheving, -sikring og -utvikling for alle parter er en nøkkel til suksess

FUNN 2: Copilot kan påvirke utøvelse av offentlig myndighet

Dette funnet er av stor betydning, da det berører kjernen i hvordan vi forstår og gjennomfører offentlig myndighet i en digital tidsalder. Innbyggerne i Norge har stor tiltro og tillit til det offentlige Norge, og det er viktig at våre verktøy og metoder ikke undergraver dette tillitsforholdet. Verktøyene våre må gjøre oss bedre, ikke dårligere. Når det offentlige tar i bruk nye digitale verktøy skal dette gjøres på en ansvarlig og informert måte.

I den norske grunnloven er maktfordelingsprinsippet nedfelt. Statsmakten skal fordeles på tre uavhengige institusjoner: en lovgivende, en utøvende og en dømmende makt. Offentlige organisasjoner har utøvende myndighet til å gjennomføre politiske vedtak og håndheve gjeldende lover, og i dag har vi klare og tydelige regler for hvordan dette skal gjøres. Prosessene skal være rettferdige og gjennomsiktige, da må også verktøyene være det.

Det offentlige har et ansvar for å unngå feil, og vi må alltid være 100 % sikre på at vi har full kontroll på hvordan vi har kommet fram til en beslutning. Vi skal kunne redegjøre for data- og vurderingsgrunnlaget, og prosessen skal være gjennomsiktig. Vi skal ta vare på informasjonen for ettertiden slik at vi kan ettergå feil og svakheter. Dette sikrer at offentlige myndigheter klarer å opprettholde tilliten i befolkningen.

Copilot kan gi feilaktige svar eller gjøre feilslutninger. Dette gjelder særlig når den ikke har nok informasjon å jobbe med, men kan også forekomme når den tilsynelatende har tilgang til god nok informasjon. Det er viktig å være klar over dette og ha mekanismer på plass for å identifisere og korrigere slike feil. Det er stor risiko for at det offentlige gjør feil om vi tar alt Copilot foreslår som sannhet.

Det er visse områder innenfor utøvelse av offentlig myndighet hvor man bør være ekstra forsiktig med å bruke Copilot. Dette gjelder spesielt der risikoen er for stor. Foreløpig bør terskelen for bruk av Copilot i disse områdene være veldig høy. Det betyr imidlertid ikke at det ikke finnes mange arbeidsområder der Copilot kan brukes helt eller delvis, for eksempel for språkforbedring, oversettelse og analyse av åpne informasjonskilder.

	Ja	Nei	Vet ikke
Har dere tilstrekkelig forståelse av hvordan Copilot fungerer og tar beslutninger?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere etablert klare retningslinjer for hvor og når Copilot kan brukes?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere identifisert områder hvor bruk av Copilot er for risikabelt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere identifisert områder der Copilot kan påvirke utøvelse av offentlig myndighet positivt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Anbefaling

- Ta aktivt stilling til hvilke data Copilot skal ha tilgang til (dette gjelder alle verktøy, også Microsoft 365).
- Arbeid systematisk med å sikre god regelverksforståelse og forvaltningskompetanse ved institusjonen.
- Prioriter å ha «Orden i eget hus».
- Sørg for at den menneskelige kontrollen fungerer.

FUNN 3: Copilot behandler enorme mengder personopplysninger på nye og ukontrollerte måter

Det er lett å bli registrert! Offentlige organisasjoner er i dialog med mange mennesker hver dag, og både kontaktinformasjon og informasjon som gjelder enkeltpersoner blir behandlet i stor skala. Personvernforordningen gjelder for all behandling av personopplysninger, og Copilot kan gi utfordringer knyttet til bruk, ivaretagelse av den registrertes rettigheter og friheter, registrering, forvaltningsmessige hensyn og ukjente behandlinger.

Copilot er en klon av deg og har de samme tilgangene og rettighetene som du har i Microsoft-økosystemet. Dette betyr at alt du kan gjøre, kan Copilot også gjøre. Det er viktig å være klar over dette når du gir Copilot tilgang til informasjon.

Hvis en organisasjon gir Copilot tilgang til all informasjonen den har, vil denne informasjonen bli behandlet og kan bli satt sammen på nye måter. For eksempel kan du be Copilot om å sammenstille to eller flere filer for å lage et nytt dokument. Hvis du gir en upresis kommando til Copilot, vil den selv velge hva den mener er den beste måten å løse oppgaven på. Copilot skiller ikke på kvalitetssikrede, endelige dokumenter og utkast. Den bruker den informasjonen den har tilgang til.

For store organisasjoner som behandler mange menneskers personopplysninger, er det lett at dokumenter som inneholder personopplysninger mellomlagres utenfor fagsystemer, ikke blir klassifisert ordentlig eller deles internt via samhandlingsplattformer. Copilot får da tilgang til disse dokumentene og kan bruke dem i en annen sammenheng, eller til andre formål, enn det som opprinnelig var tenkt.

For organisasjoner som NTNU er den "store mengden" registrerte ikke ansatte, men studenter og deltakere i forskningsprosjekter. Disse personopplysningene bør NTNU behandle ekstra varsomt. Det er mange mennesker, store mengder særlige kategorier av personopplysninger og skjeve maktforhold mellom behandlingsansvarlig og den registrerte. Dette gir skjerpede krav til ivaretagelse av personvernet.

Hvis du sender en e-post til det offentlige; Hvilke forventninger har du til hvordan informasjonen du har sendt blir behandlet? Vet du at du automatisk blir en registrert, og en del av datagrunnlaget som Copilot bruker? Å sende en e-post er en ensidig transaksjon, og det øyeblikket du trykker på «send» er innholdet i e-posten utenfor din kontroll. Det er lite sannsynlig at du vil gå til en personvernerklæring (eller ringe opp en saksbehandler) på forhånd for å sjekke om e-posten din blir behandlet av kunstig intelligens eller ikke.

Det offentlige må ivareta en rekke forvaltningsmessige hensyn. Hvis du for eksempel søker på to forskjellige jobber på NTNU, skal du forvaltningsmessig regnes som to forskjellige individer i to forskjellige saker. Du skal behandles likt, men vurderingene fra den ene saken skal ikke påvirke den andre. Personvernmessig er du ett individ/en registrert, men forvaltningsmessig kan du være flere. Vi må være helt sikre på at vurderinger ikke flyter på tvers av saker.

Copilot kan vurdere og lage nye personopplysninger basert på det du har tilgang til. Copilot kan basere disse nye personopplysningene på for eksempel privat chat, epost og

samhandling i Teams, humør og deltakelse i møter som transkriberes og tas opp. Copilot klarer ikke å fange opp nyanser og verdier hos enkeltmennesker som et menneske ville gjort. Modellene kan være trent på andre mennesker, kulturer, verdier og normer enn du er kjent med, og da kan det være vanskelig å forstå hvordan og hvorfor Copilot gir sine svar. Det er viktig å være klar over dette og ha mekanismer på plass for å identifisere og korrigere eventuelle feil.

	Ja	Nei	Vet ikke
Har dere tilstrekkelig oversikt over hvilken informasjon Copilot har tilgang til?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er dere trygge på at Copilot ikke vil bruke personopplysninger på en måte som strider mot bestemmelsene i personvernforordningen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er dere i stand til å sikre at Copilot ikke får tilgang til dokumenter som inneholder personopplysninger, som ikke er ordentlig klassifisert eller mellomlagret utenfor fagsystemer?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere informert alle som kommuniserer med dere om at deres e-post kan bli behandlet av kunstig intelligens?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere mekanismer på plass for å sikre at Copilot ikke setter sammen informasjon på nye måter som kan være problematiske?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er dere i stand til å sikre at Copilot ikke vil bruke informasjon i en annen sammenheng eller til andre formål enn det som opprinnelig var tenkt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Anbefaling

- Gjør en grundig personvernkonsekvensvurdering (DPIA) og revider den oftere enn du hadde tenkt.
- Ha høy terskel for å godkjenne restrisiko når det gjelder personvern.

FUNN 4: Microsoft 365 er utfordrende å forvalte

Veldig mange offentlige organisasjoner benytter seg av Microsoft sine tjenester i større eller mindre grad til å gjøre jobben sin. Veldig mange har også tatt i bruk plattformen Microsoft 365, Microsoft sin skyløsning som binder sammen de mest brukte verktøyene som Outlook (epost), Word (tekstbehandling), Excel (regneark) og PowerPoint (presentasjonsverktøy). Copilot for Microsoft 365 er bygd oppå den digitale grunnmuren som Microsoft 365 utgjør, og for å forstå Copilot så må du forstå hvordan Microsoft 365 fungerer.

Microsoft 365 er et økosystem av tjenester og komponenter som stadig endrer seg. Det er en utfordring å holde seg oppdatert på utviklingen av de forskjellige tjenestene, sikkerhetsoppdateringer, informasjonsflyt, brukerdokumentasjon osv. Microsoft annonserer alle endringer, feil og feilrettinger og ny funksjonalitet på en ryddig måte i «Message center», men å følge med på denne regelmessig er utfordrende i en travel hverdag da det kan innebære å lese flere titalls sider med informasjon hver uke.

For å forvalte Microsoft 365, og da spesielt også Microsoft 365 med Copilot, på en forsvarlig måte, kreves det en robust infrastruktur av ansatte med spesialisert kompetanse. Disse ansatte må ha tilstrekkelig tid og ressurser til å holde seg oppdatert på hva som er gjeldende og hvilke funksjoner som kan og skal aktiveres eller deaktiveres til enhver tid. Microsoft tilbyr en rekke løsninger som kan tilpasses hver enkelt virksomhet, men det krever tid å sette seg inn i alternativene og tilpasse egen virksomhet for best mulig gevinst.

Microsoft opererer med en "opt out"-policy på mange av sine tjenester. Dette betyr at nye funksjoner, tillegg og utvidelser blir automatisk aktivert, og administratorer må aktivt deaktivere dem hvis de ikke skal være tilgjengelige for brukerne. Dette kan være en utfordring når det i liten grad er mulig å påvirke leverandørene til å tilpasse løsningen til sin egen organisasjon. Som bruker av løsningen må du akseptere leverandørens "terms & conditions" fullt ut, og du er avhengig av at leverandørene utvikler tjenesten i en retning som er i tråd med egne behov, forutsetninger, men ikke minst i henhold til egne retningslinjer og relevante lover og regler. Det er lett å havne i en "låst posisjon" hvor du blir avhengig av tjenesten, og det ikke finnes noe realistisk alternativ enn å akseptere leverandørens betingelser.

Å være avhengig av en enkelt leverandør kan være risikabelt, spesielt når det gjelder store og komplekse systemer som Microsoft 365. En exit-strategi er viktig for å sikre at organisasjonen har fleksibilitet og kontroll over egen teknologiske fremtid. Dette innebærer å ha en plan for hvordan man kan migrere data, funksjoner og tjenester til en annen løsning eller leverandør hvis det blir nødvendig. En slik strategi kan bidra til å redusere risikoen for driftsavbrudd, tap av data og høye kostnader ved en eventuell exit. Det gir også organisasjonen en sterkere forhandlingsposisjon overfor leverandøren, siden de ikke er låst til en enkelt løsning. Ved å ha en exit-strategi på plass, kan organisasjonen sikre at den er forberedt på alle eventualiteter og kan ta informerte beslutninger. Det er virksomhetens eget ansvar å styre teknologien i riktig retning og ikke la teknologien styre virksomheten.

Microsoft 365 og Copilot er dyre tjenester og funksjonaliteter, og kostnadsøkningen over tid har vært betydelig. Å tilby Copilot til alle brukere på NTNU vil være en stor investering

som kan være vanskelig å håndtere i en tid med økonomiske innstramminger i universitets- og høyskolesektoren.

Riktig bruk av KI-verktøy som Copilot krever en høy grad av opplæring for både brukere og administratorer. For å bruke tjenestene på en forsvarlig måte, kreves det et kontinuerlig fokus på å holde brukere og administratorer av tjenesten på et høyt kompetansenivå.

En realistisk vurdering av totalkostnadene er avgjørende for å sikre at alle kostnader er tatt med i betraktning når man vurderer å implementere og vedlikeholde systemer som Microsoft 365 og Copilot. Dette inkluderer ikke bare lisenskostnadene, men også indirekte kostnader som tid og ressurser til forvaltning, kursing av driftspersonell og opplæring av ansatte. En totalkostnadsvurdering kan også hjelpe organisasjonen med å identifisere potensielle kostnadsbesparelser, for eksempel gjennom mer effektiv bruk av ressurser eller redusert behov for ekstern støtte. Ved å ha en klar forståelse av alle kostnadene involvert, kan organisasjonen ta informerte beslutninger om implementering og forvaltning av disse systemene.

	Ja	Nei	Vet ikke
Har dere en exit-strategi på plass?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere vurdert alternative leverandører?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere vurdert alle direkte og indirekte kostnader som systemet medfører?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er dere komfortable med Microsofts "opt out"-policy, og har dere kapasitet til å håndtere de konsekvensene det kan medføre?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere tilstrekkelig med ressurser og kompetanse til å forvalte og oppdatere Microsoft 365 og Copilot på en god måte?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Anbefaling

- Ha oppdaterte risikovurderinger av plattformen som en helhet, men også mindre deler for å kunne avdekke ny risiko raskt.
- Lag en exit-strategi og gjør deg i stand til å avslutte bruken av verktøyet.
- Gjør en realistisk totalkostnadsvurdering for å sikre at alle kostnader er tatt med.

FUNN 5: Copilot er tidlig i utviklingsløpet

Når teknologiske fremskritt skjer i et raskt tempo, er det viktig for organisasjoner å være i forkant med utviklingen. Dette innebærer å forstå og tilpasse seg nye verktøy og teknologier som kommer på markedet, men også å erkjenne at verktøyene som kommer på markedet ikke nødvendigvis er ferdige. Der hvor vi før kunne kjøpe et ferdig og fulltestet produkt, må vi i større grad «være med på utviklingen» hos leverandøren og kontinuerlig følge med på alt det som det medfører av fordeler og ulemper.

Copilot er i mange henseender mer et konsept enn et ferdig produkt. Det representerer Microsofts innsats for å integrere kunstig intelligens, bruk av språkmodeller og smarte funksjoner i sin programvareportefølje og er fortsatt i en tidlig fase av utviklingen. Det er viktig for brukerne å forstå dette, slik at de ikke forventer samme grad av stabilitet og forutsigbarhet som de ville fått fra et mer «modent» digitalt verktøy.

Copilot er i dag et «bevegelig mål». Det vil si i konstant utvikling, og den versjonen av Copilot som vi har tilgang til nå, kan betraktes som en tidlig iterasjon på veien mot en mer fullverdig versjon. Dette betyr at funksjonaliteten kan endre seg fra dag til dag. Brukere og administratorer må derfor være forberedt på å tilpasse seg disse endringene og planlegge bruken, opplæring og informasjon om verktøyet deretter. Dagens Copilot kan sees på som en tidlig versjon av en lang rekke med versjonsoppdateringer.

Teknologiske fremskritt skjer i et raskt tempo, og vi må forvente og planlegge for teknologiske generasjonsskifter omtrent hvert andre år. Dette betyr at vi må være forberedt på å oppdatere og tilpasse våre systemer og prosesser regelmessig for å holde tritt med utviklingen. Dette kan innebære å lære nye ferdigheter, tilpasse arbeidsflyter, eller til og med bytte ut verktøy og teknologier etter hvert som nye alternativer blir tilgjengelige.

Når teknologien er i konstant utvikling, er det avgjørende for organisasjoner å være proaktive og tilpasse seg endringer. En effektiv måte å gjøre dette på er å aktivt bruke piloterings-, test- og prosjektmetodikk. Dette innebærer å prøve ut nye teknologier, som Copilot, i en kontrollert setting før de implementeres fullt ut. Ved å gjøre dette kan organisasjoner identifisere potensielle problemer og løse dem tidlig i prosessen. Det gir også mulighet til å tilpasse teknologien til organisasjonens spesifikke behov og arbeidsflyter, samt gjøre vurderinger om den nye funksjonaliteten er nødvendig eller ikke. Dessuten kan det bidra til å redusere risikoen for forstyrrelser i virksomheten og sikre en jevn overgang når nye systemer og prosesser implementeres. Det er viktig å huske på at det ikke finnes en "one-size-fits-all"-løsning når det kommer til teknologi. Hva som fungerer best vil variere fra organisasjon til organisasjon, og det er derfor viktig å prøve seg fram for å finne den beste løsningen.

	Ja	Nei	Vet ikke
Har dere en effektiv prosess for å prøve ut nye teknologier i en kontrollert setting før full implementering?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere ressursene, kapasiteten og kompetansen til å holde tritt med den raske teknologiske utviklingen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er dere forberedt på å «være med på utviklingen» hos leverandøren og kontinuerlig følge med på alt det som det medfører av fordeler og ulemper?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er dere villige til å investere tid og ressurser i å lære nye ferdigheter og tilpasse arbeidsflyter?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Anbefaling

- Planlegg egen bruk av verktøyet som et verktøy i kontinuerlig utvikling.
- Bruk piloterings-, test- og prosjektmetodikk aktivt. Viktig å prøve seg fram for å finne ut hva som fungerer for seg.
- Prioriter ressurser til egen utvikling og kompetanseløft for å holde interne oppdatert på verktøyet (teknologi, avtaleverk og bruk)

FUNN 6: Copilot påvirker organisasjonen

I vårt daglige arbeid er vi helt avhengige av digitale verktøy, og når det gjøres så store endringer på funksjonaliteten i våre mest brukte verktøy vil brukere oppleve endringer i både arbeidsmetoder, samhandling og organisatoriske effekter. Mennesker er forskjellige, og vi forholder oss til endringer på ulike måter. Dette vil også gjelde for Copilot.

Copilot er integrert i de mest brukte digitale verktøyene som ansatte bruker. Dette betyr at endringer i disse verktøyene fort kan føre til endringer på etablerte arbeidsmetoder. Det kan også påvirke måten vi samhandler og samarbeider på, ettersom nye funksjoner kan endre måten vi kommuniserer og deler informasjon på.

Nye funksjoner i etablerte verktøy kan skape reaksjoner blant brukere. For eksempel kan automatisk opptak av digitale møter med påfølgende transkripsjon og oppsummering/tolkning av innhold oppleves negativt hvis innholdet fremstilles feil. Det er ingen garanti for at verktøyet tolker innhold riktig, og dette kan føre til misforståelser eller feilinformasjon. Det er også risiko for nedkjølingseffekter som for eksempel at ansatte ikke ønsker å delta på møter der det blir tatt opptak, eller at de oppfører seg annerledes enn det de ellers ville gjort.

Copilot-funksjonaliteten er veldig lett tilgjengelig. Med bare ett trykk kan det tas opptak, og funksjonaliteten kan være satt opp slik at du samtykker ved å fortsette å delta i samtalen. Dette kan ha implikasjoner for personvern og reelt samtykke, og det er viktig at både brukere og organisasjonen tenker godt gjennom hvilke implikasjoner denne typen funksjonalitet kan ha på for eksempel arbeidsmiljøet.

Flere organisasjoner som har tatt i bruk opptaks- og transkripsjonsfunksjonaliteten forteller at det var mye diskusjon i starten, men at dette har gått seg til. Det er imidlertid viktig å merke seg at vi ikke har datagrunnlag for å si at nedkjølingseffekter da ikke har skjedd. For eksempel kan ansatte som ikke vil bli tatt opptak av, velge å ikke delta på møter eller ikke bli invitert. Drøft problemstillingene åpent.

Å ta i bruk og implementere nye digitale verktøy må skje hånd i hånd med utviklingen av organisasjonen i seg selv. Faktorer som fysiske arbeidsforhold, psykososiale faktorer, organisatoriske forhold, arbeid-liv balanse og muligheter for opplæring og utvikling er viktige elementer å ta med i vurderingen. Det kan lønne seg å tenke at implementeringen av nye verktøy som Copilot må være del av en større strategi for organisasjonsutvikling, ikke bare som et IT-prosjekt. Mens det tekniske aspektet ved implementeringen av Copilot er viktig, er det enda viktigere å tenke på hvordan det vil påvirke organisasjonen som helhet. Ved å se på Copilot som et organisasjonsutviklingsprosjekt, kan vi sikre at vi får mest mulig ut av denne nye og kraftige teknologien.

	Ja	Nei	Vet ikke
Har dere en plan for å sikre at implementeringen av Copilot støtter organisasjonens overordnede mål og visjon?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere en klar forståelse av hvordan Copilot vil påvirke arbeidsmetodene deres?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere vurdert og identifisert potensielle nedkjølingseffekter?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere en åpen diskusjon om denne typen problemstillinger?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere en plan for å håndtere eventuelle diskusjoner eller motstand som kan oppstå i organisasjonen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Anbefaling

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

FUNN 7: Copilot kan brukes til å overvåke og måle prestasjoner og adferd

Gjennom hele prosjektet har vi gjentatte ganger blitt presentert med påstanden om at Copilot ikke medfører noen ny risiko. Copilot har samme tilganger som deg, og i og med at den kun bruker informasjon du allerede har tilgang til må vi forstå argumentet som at Copilot kun kan gjøre det du som bruker allerede kan gjøre manuelt. Det er likevel en vesentlig forskjell: Selv om du som bruker i teorien kan lete gjennom alle eposter, teams-meldinger og kanaler der du har samhandlet med annet menneske og gjøre deg opp en mening om hvilket humør den andre personen er i, så vil dette være snakk om potensielt mange timers jobb. Copilot klarer det samme i løpet av sekunder. Det er mulig å spørre og få svar fra Copilot om for eksempel hvilken sinnsstemning eller humør et annet navngitt menneske er i. I og med at det er mulig, så vil det bli gjort.

Copilot kan gjøre oppgaver som ikke er mulig med Microsoft 365 alene. For eksempel kan Copilot stille vurderingsspørsmål basert på et mangfoldig innhold, noe som kan føre til såkalt "bossware-problematikk". Dette innebærer at arbeidsgivere kan vurdere ansattes prestasjoner og adferd basert på skriftlig innhold de har tilgang til, som filer, dokumenter, Teams-chatter, e-postkorrespondanse, Teams-innhold, følelsesreaksjoner (emojis), transkripsjoner fra møter med automatisk opptak, osv. Ansatte har ingen mulighet til å finne ut om en slik vurdering av dem selv har skjedd. Det er også uklart hvilke forutsetninger, parametre og verdier som er lagt til grunn for vurderingene som Copilot gjør. Det er lite sannsynlig at verdiene verktøyene er bygd på de arbeidslivsidealene vi er vant med i dag.

Når Copilot har for lite informasjon å jobbe med, kan det oppstå utfordringer med løgn og hallusinasjoner. Det er sannsynlig at Copilot kan "finne på" følelser for de ansatte, noe som gjør denne problemstillingen enda mer utfordrende.

Det er også observert at Copilot kan ha en tendens til å bekrefte spørsmålsstillerens påstand. For eksempel, hvis du spør Copilot "synes du ikke at Heine ser litt sur ut i dag?", vil den i stor grad søke å bekrefte dette. Dette kan potensielt forsterke eksisterende fordommer og misforståelser (bekreftelsesbias).

Det er viktig å ta hensyn til denne typen utfordringer for å sikre en etisk og ansvarlig bruk av Copilot i organisasjonen. Denne teknologien kan være et kraftig verktøy, men det må brukes på en måte som respekterer de ansattes menneskerettigheter som personvern og ytringsfrihet.

Merk: Det er mulig å håndtere denne problematikken. I tillegg til grundig opplæring av alle parter kan Copilot for eksempel begrenses til ikke å få tilgang til områder der mennesker er uformelle i tonen eller det de anser som sine private områder. Dette vil variere fra organisasjon til organisasjon. Å gi Copilot tilgang til for eksempel epost eller teams chat bør vurderes nøye. Et annet, og sannsynligvis mer kontroversielt alternativ, er å vurdere om for eksempel ledere med personalansvar ikke skal få tilgang til Copilot. Dette vil kunne føre til at lederne havner «teknologisk bakpå», men det vil kunne bidra til å beskytte ansattes personvern og hindre potensielt misbruk av verktøyet. Det ser også ut til å komme verktøy som kan plukke opp om man stiller slike spørsmål, men dette er ikke testet i denne omgang.

	Ja	Nei	Vet ikke
Bør Copilot ha tilgang til områder der de ansatte er uformelle i tonen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er det ok at Copilot gjør vurderinger av de ansattes adferd og prestasjoner?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere drøftet denne problematikken med fagforeninger, tillitsvalgte og verneinje?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Anbefaling

- Skru av tilgang til områder som ansatte anser som «uformelle» eller «private arenaer» (som Teams chat/Graph grounded Chat, epost osv).
- Prioriter opplæring og vurder ekstraordinære tiltak overfor arbeidsgivere og ansatte med personalansvar.
- Lag gode rutiner for internkontroll.

FUNN 8: Copilot fungerer tidvis skikkelig bra

Copilot fungerer ganske bra til veldig mye forskjellig, og ofte til oppgaver du ikke trodde var mulig.

Gjennom hele prosjektperioden har det vært flere «Aha!-opplevelser» hvor Copilot har vist seg å være et utmerket verktøy. Copilot er god til å trekke ut essensen fra store filer for å sette sammen til et nytt, mer fokusert dokument. Dette er en oppgave som fort ville tatt en person flere dager å gjøre, men Copilot kan utføre jobben på bare noen få minutter. Dette betyr at du kan komme raskere i gang med oppgaver, og du får umiddelbar hjelp der og da. Som et verktøy for å skrive et førsteutkast, kan Copilot være svært nyttig for mange. Dette gjelder særlig oppgaver som bare trenger å være «gode nok».

Copilot har evnen til å gi referanser, men det er viktig å merke seg at du ikke kan stole blindt på disse slik verktøyet fungerer i dag. Selv om verktøyet kan gi referanser, er det alltid lurt å sjekke disse selv for å sikre at informasjonen er korrekt og relevant. Det er forventet at denne funksjonen vil bli betydelig forbedret i fremtiden, noe som vil gjøre Copilot enda mer nyttig som et forsknings- og skriveverktøy. I prosjektet har vi også opplevd at internkontrolldelen på enkelte oppgaver av og til tar lenger tid enn å gjøre oppgaven helmanuelt.

Selv om Copilot er et kraftig verktøy, er det viktig å huske at du som bruker er piloten. Det er du som må stå ansvarlig for innholdet. Hvis du spør Copilot om «hvordan har du kommet fram til dette», vil verktøyet ofte ikke kunne gi et tilfredsstillende svar. Det er viktig alltid å dobbeltsjekke og verifisere informasjonen som Copilot gir.

	Ja	Nei	Vet ikke
Har dere en felles policy/retningslinje for hvordan man sier fra om at verktøy med kunstig intelligens er benyttet (referanse)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er brukerne gjort i stand til å være fullverdige «Copilot-piloter»?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har dere identifisert saksområder der behovet kun er «godt nok»?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er brukeren alltid i stand til å dobbeltsjekke og verifisere informasjonen som Copilot gir?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Anbefaling

- Ikke vurder tilbakemeldingene fra prosjektet som en showstopper for egen utvikling.
- Bruk prosjektresultatene for å komme raskere inn i kjernen av utfordringene for egen virksomhet.
- Bruk tida godt!

NTNUs verktøykasse

NTNU har gjennom prosjektet hatt som mål å utarbeide en verktøykasse bestående av sett med vurderinger, metoder, beskrivelse av rammeverk og anbefalinger som kan hjelpe offentlige organisasjoner med å bli «Copilot ready», og for å ta i bruk kunstig intelligens på en smart, sikker og trygg måte. Verktøykassen er basert på NTNUs erfaringer og funn fra prosjektet, og er ment som et bidrag til kunnskapsdeling og dialog i offentlig sektor om ansvarlig bruk av kunstig intelligens. Den inneholder både generell informasjon (verktøy) og vurderinger rundt Copilot for Microsoft 365. Vurderingene og rammeverk spesielt rettet mot Copilot for Microsoft 365 består blant annet av en personvernkonsekvensvurdering av teknologien og rammeverk for testmetodikk. Det er også mulig å bruke disse verktøyene som utgangspunkt for vurderinger og testmetodikk av annen KI-funksjonalitet.

I denne delen av rapporten presenterer vi «KI-reisen», anbefalinger rundt modenheitsvurdering, forslag til retningslinjer, opplæring og kompetanseheving, og personvernkonsekvensvurderinger. Vi vil også gi eksempler på hvordan vi har brukt Copilot til å lage deler av verktøykassen, og hvilke utfordringer og muligheter vi har møtt underveis.

Hele verktøykassen finnes på prosjektets nettside:

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

NTNUs «KI-reise»

Kunstig intelligens kan forenkle, forbedre og effektivisere ulike prosesser og oppgaver i en virksomhet. Copilot for Microsoft 365 er et av mange verktøy med KI-funksjonalitet som er tilgjengelig eller under utvikling for norske virksomheter. Hvordan bør en virksomhet forberede seg på å ta i bruk slike verktøy på en effektiv og hensiktsmessig måte? Hvilke vurderinger bør gjøres i forkant av anskaffelse, hvordan bør implementering og forvaltning følges opp, og hvordan bør organisasjonen forberedes på å integrere KI i arbeidshverdagen?

Å ha gjort grundige forberedelser vil gjøre virksomheten i bedre stand til å beslutte hvilke områder man ønsker å benytte KI og hvilke verktøy som skal tas i bruk. «KI-reisen» er innspill til en rekke vurderinger som bør gjøres som forberedelse, under anskaffelse og i forvaltning av slike verktøy. KI-reisen kan sammen med andre modenheitsverktøy være med på å forberede og verifisere at virksomheten er klar for å ta i bruk slik teknologi, og eventuelt hva som må gjøres eller bør prioriteres i forkant.

NTNU har gjennom dette prosjektet identifisert hvilke faktorer virksomheten må fokusere på for å kunne ta i bruk KI-verktøy på en effektiv måte. KI implementeres i nye og i allerede eksisterende produkter og verktøy i en hastighet det er vanskelig å følge opp. Det er derfor viktig å ta stilling til disse temaene som KI-reisen omhandler i forkant.

Under har vi listet noen spørsmål som er hentet fra KI-reisen og som kan være en første start med i en mulig modenheitsanalyse av virksomheten:

	Ja	Nei	Vet ikke
Har virksomheten avdekket relevante lovverk innenfor egen sektor?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har virksomheten avdekket hvilke gevinster de ønsker ved å ta i bruk KI?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har virksomheten avdekket hvilke områder det er aktuelt å ta i bruk KI?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har virksomheten avdekket hvilke områder de ikke skal ta i bruk KI?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har virksomheten avdekket nødvendige endringer i forvaltningsplan?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har virksomheten vurdert potensielt ressursbehov og totalkostnader for sikker forvaltning og oppfølging av KI-verktøy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har virksomheten vurdert exit-strategi for KI-verktøy og IT-systemer med integrerte KI-verktøy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har virksomheten vurdert behovet for opplæring av brukere og hvordan dette kan gjennomføres i praksis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har virksomheten avdekket hvordan bruken av KI skal reguleres og hvordan rutiner og retningslinjer dokumenteres?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Se vedlegg for den helhetlige KI-reisen.

Gjør modenhetsvurdering av egen organisasjon

Informasjon er en av de mest verdifulle ressursene i offentlig sektor, og det har lenge vært et krav om at offentlig sektor må utnytte informasjonen sin på en bedre måte. Dette krever imidlertid en helhetlig forvaltning av informasjon på tvers av offentlige virksomheter, ikke minst også internt i den enkelte virksomheten. Dette arbeidet kalles ofte for "Orden i eget hus".

I denne sammenhengen kan modenhetsvurderinger være nyttige verktøy. Digitaliseringsdirektoratet har utarbeidet en egen modenhetsmodell for "Orden i eget hus" som fokuserer på å ha oversikt over og beskrivelse av egne datasett, men også som et internt hjelpemiddel til å kartlegge modenhet hos de enkelte virksomhetene i offentlig sektor (både store og små, statlige og kommunale virksomheter). Hensikten med en modenhetsmodell er å hjelpe en virksomhet å vurdere hvor langt den er kommet i henhold til gitte kriterier (aksene i modellen), og til "selvutvikling". Ved gjentatte målinger/vurderinger kan en følge sin egen utvikling fra en nullpunktmåling og videre fram mot ønsket mål.

I en tid der kunstig intelligens (KI) blir stadig mer integrert i offentlige tjenester, er det avgjørende at organisasjoner har en klar forståelse av deres egen modenhet når det gjelder dataforvaltning. KI-systemer er avhengige av store mengder data for å fungere effektivt, og evnen til å administrere og utnytte disse dataene er en nøkkelfaktor for suksess.

En modenhetsvurdering kan hjelpe organisasjoner med å identifisere styrker og svakheter i deres nåværende dataforvaltningspraksis, men også hvor klar organisasjonen er for verktøy som for eksempel Copilot, og gi veiledning om hvor de bør fokusere sine forbedringsinnsatser. Dette kan være spesielt verdifullt i organisasjoner der modenheten kan variere sterkt mellom ulike organisasjonsenheter.

På NTNU har vi gjennom prosjektet hatt god nytte av Digitaliseringsdirektoratets modenheitsvurderingsmaler, men vi har også hatt særlig god nytte av verktøyet «Higher Education Generative AI Readiness Assessment» som er utgitt av organisasjonen EDUCAUSE der NTNU er medlem.

Verktøyet gir brukere en liste med spørsmål som er designet for å gi et bilde av institusjonens beredskap for å ta i bruk generative KI-verktøy innenfor tre hovedområder: strategi og styring, kapasitet og kompetanse, og infrastruktur. Dette verktøyet er utviklet av representanter fra internasjonale høyere utdanningsinstitusjoner i samarbeid med teknologiselskapet Amazon Web Services. Verktøyet ligger åpent ute på nettsidene til EDUCAUSE under Creative Commons lisensen CC BY-NC-ND. NTNU har ikke hatt behov for å gjøre lokale tilpasninger til verktøyet.

Lenker:

- <https://library.educause.edu/resources/2024/4/higher-education-generative-ai-readiness-assessment>
- <https://www.digdir.no/>

Sats på opplæring og kompetanseheving

Gjennom prosjektperioden har det blitt tydelig hvor viktig det er at organisasjoner forbereder seg på det teknologiske taksiftet vi er en del av. Et av de viktigste områdene for forberedelse er opplæring og kompetanseheving. Det er nødvendig å tilegne seg mer KI-kompetanse, spesielt knyttet til generativ KI, for å skape forståelse for hva nye KI-systemer kan bety for de ansatte og for organisasjonen.

Det er viktig å forstå de grunnleggende trekkene i hvordan KI-systemer fungerer, og hvilke oppgaver slike systemer er gode på å løse. Det er spesielt viktig at medarbeiderne forstår hvilken rolle treningsdata spiller i slike systemer og hvilke utfordringer det kan være med tanke på skjevheter, forutinntatthet og partiskhet.

Det kan være nyttig å kartlegge den eksisterende kompetansen blant medarbeiderne og tilby opplæring i henhold til behov i hvert enkelt tilfelle. På NTNU har vi tatt utgangspunkt i en antakelse om at kompetansenivået er veldig varierende, men generelt sett lavere enn det det burde være.

NTNU har mange forskjellige typer medarbeidere, og det er mange behov som skal dekkes. Særlig undervisere har for eksempel behov for god kjennskap til:

- Hvordan KI kan bidra til læring: KI-systemer basert på store språkmodeller er et spennende verktøy brukt på en god, sunn og kritisk måte.
- Hvordan KI kan være til hinder for læring: En stor utfordring med slike KI-systemer er at det kan bli fristende å ta snarveier. Det kan bli søkelys på å finne raske svar og løsninger framfor å fremme læring og forståelse.

Kvaliteten til KI-systemer basert på store språkmodeller påvirkes i stor grad av de spørsmål som stilles. Det å utforme effektive instruksjoner – «prompt engineering» på engelsk – er en ferdighet i seg selv som kan være nyttig å lære seg og få god erfaring med. I fremtiden kan god kunnskap innen «prompt engineering» bidra til å bedre kunne utnytte mer spesifikke modeller innen snevrere områder.

Det er mange juridiske utfordringer man må ha kjennskap til ved bruk av KI. Prosjektet har hatt særlig oppmerksomhet på utfordringer knyttet til personvern og informasjonssikkerhet. De etiske utfordringene rundt trening av generative KI-systemer og bruken av materiale med opphavsrett bør også være i fokus.

Kompetanseheving

En rask kompetanseheving blant ansatte og studenter for å møte de muligheter og utfordringer de nye KI-systemene har gitt oss, er viktig. Hvilket ansvar har organisasjonen? Hva bør hver enkelt gjøre på egenhånd? Det er viktig å diskutere og avklare hvilke tiltak som skal igangsettes og hvilket nivå man bør legge seg på, slik at organisasjonen totalt sett får økt sitt generelle kompetansenivå. Det viktigste nå er «upskilling, ikke upscaling».

Opplæringsprogram

Prosjektet har utarbeidet et opplæringsprogram med tittelen «Hvordan bruke kunstig intelligens på en smart, sikker og trygg måte». Dette er et opplæringsprogram særlig myntet på offentlige organisasjoner, og inkluderer planverk, opplæringsmateriell og workshopinnhold. Følgende tema inngår:

- Hva er kunstig intelligens?
- Informasjonssikkerhet og personvern
- Behovet for økt informasjonskompetanse
- Bli kjent med verktøyene du har
- Rammer for kvalitet i saksbehandling
- Morgendagens rammeverk
- Hvilken teknologi er på trappene?

Prosjektet har i tillegg utarbeidet enkle opplæringsvideoer, presentasjoner og støttemateriell som kan gjenbrukes av andre. Alt er lagt ut på nettsidene til prosjektet www.ntnu.no/copilot

Opplæringspakke: Hva er generativ kunstig intelligens?

Inneholder opptak fra;

- Innlegg for NTNUs kommunikasjonsnettverk: "Kunstig intelligens - Hva har vi, og hva får vi NTNUs verktøykasse?" 07.06.2023
- Innlegg på Universitetsbibliotekets KI-dag 26.01.2024
- Innlegg på webinar om Copilot i IT-BOTT 06.02.2024

Opplæringspakke: Hva må jeg tenke på når jeg tar i bruk KI-verktøy?

Inneholder opptak og støttemateriell presentert gjennom prosjektets løypemelding 2 25. april 2024 med følgende tema:

- Informasjonskompetanse
- KI sett fra et HR-perspektiv
- Bærekraft
- Anskaffelser
- Informasjonssikkerhet

Opplæringspakke: Hvor lett er det å jukse med bruk av kunstig intelligens?

Inneholder opptak, støttemateriell og presentasjon hvor følgende tema diskuteres:

- Med dagens verktøy har det blitt mye lettere å jukse enn det det var tidligere. Vi må lære oss å tenke annerledes og derfor har vi laget støttemateriell for å forsøke å forklare de muligheter og utfordringer vi står overfor.
- «Men læll da doktrinen» gir et innblikk i hvordan man kan jukse ved bruk av kunstig intelligens. Dette er viktig for å øke bevisstheten på hvor lett dette faktisk er å få til.

Både opplæringsprogram og opplæringspakker kan tilbys og tilrettelegges for andre virksomheter gjennom prosjektet Nemonoor <https://nemonoor.no/> finansiert gjennom EUs Digital Europe program (Grant agreement No 101083966).

Lag retningslinjer for bruk av kunstig intelligens

I september 2023 innførte NTNU samtaleroboten Bing Chat Enterprise (nåværende navn er Copilot with commercial data protection). Som et oppfølgingstiltak etter innføringen har NTNU utarbeidet et forslag til generelle retningslinjer for bruk av generativ kunstig intelligens. Forslaget ligger vedlagt i sin helhet.

Som en del av arbeidet har forslaget til retningslinjer vært på høring i organisasjonen. Høringsrunden ga mange gode tilbakemeldinger som reflekterer et ønske om å utvikle et sett med klare, omfattende, og dynamiske retningslinjer for bruk av generativ KI ved NTNU. Høringssvarene legger vekt på en balansert tilnærming som både adresserer utfordringer og fremmer konstruktiv og innovativ bruk av KI, støttet av en robust organisatorisk struktur og kontinuerlig kompetanseutvikling. Tilbakemeldinger fra høringsrunder er innspill det er viktig og relevant å ta med i arbeidet med utarbeidelse av gode retningslinjer. Det fremmer en konstruktiv bruk av KI og øker tilliten.

De endelige retningslinjene er ikke ferdigstilt. NTNU har satt ned flere arbeidsgrupper som jobber med temaet fra utdannings-, forsknings-, og administrativ side. Forslaget til retningslinjer er vedlagt i sin helhet. De endelige retningslinjene blir gjort tilgjengelig på NTNUs nettsider når de er ferdige.

Test before you invest

NTNU har gjennomført en grundig test av generell funksjonalitet i Copilot for Microsoft 365 for å forstå hvordan verktøyet fungerer. Prosjektet har, i samråd med Datatilsynet, utviklet et sett med tester som dekker tre use case som er relevante for NTNU og andre offentlige organisasjoner. Vedlagte testgjennomgang gir innsikt i metodikken, hvordan Copilot ble brukt i hvert use case i tillegg til spørsmål og refleksjoner som er viktige når man skal bruke Copilot. Funnene fra testene er integrert i prosjektets åtte funn og personvernkonsekvensvurderinger.

Målet med testingen har vært å evaluere funksjonaliteten til Copilot med det bakteppet at produktet er et verktøy i utvikling. NTNU har valgt å ikke lage en egen testrapport, da resultatene kan være utdaterte etter kort tid på grunn av verktøyets kontinuerlige utvikling. Hensikten med å beskrive testingen har vært å øke kunnskapen om bruk av Copilot for M365 i offentlig sektor og skape dialog og diskusjon om ansvarlig og hensiktsmessig bruk av verktøyet (og andre liknende verktøy).

I vedlegget har vi inkludert fremgangsmåte, testbatteri, stegvis behandling i Copilot basert på dataflytskissen fra Microsoft, prosjektets arbeidshypoteser samt spørsmål og refleksjonspunkter til hvert use case. Spørsmålene er utarbeidet ved hjelp av Copilot.

Gjør gode nok personvernkonsekvensvurderinger

NTNU skal sørge for etterlevelse av Personvernforordningen og at alle vurderinger av informasjonssikkerhet og personvern er ivaretatt når digitale verktøy benyttes i organisasjonen. NTNU har lagt til grunn at ved bruk av verktøy basert på generativ kunstig intelligens, som samtaleroboter, skal det gjennomføres en personvernkonsekvensvurdering (DPIA) jf. Personvernforordningen artikkel 35 nr. 1:

«Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingsens 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.»

NTNU har utarbeidet en DPIA for Copilot for Microsoft 365 (driftsfase). Vurderingen er en sentral del av verktøykassen som NTNU har utarbeidet for å kunne vurdere om en stor offentlig organisasjon som NTNU kan bli «Copilot-ready».

Ved prosjektets start utarbeidet vi en DPIA for testfasen av verktøyet som ligger tilgjengelig på prosjektets nettsider. I den versjonen av DPIAen ble det identifisert 22 problemstillinger vi ikke kunne svare på. Disse problemstillingene er særskilt undersøkt i arbeidet med vurderingen for driftsfasen, og resultatet er en rekke utfyllende vurderinger av problemstillingene som er innarbeidet i DPIAen for driftsfasen.

Personvernkonsekvensvurderingen 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 sin bruk av M365 Copilot.

I forbindelse med personvernkonsekvensvurderingene av både Copilot with commercial data protection og Copilot for Microsoft 365 har vi lagt til grunn styringssignaler for utvikling fra NTNUs Sentrale samarbeidsorgan (SESAM). I SESAM møtes fagforeningene og arbeidsgiver for informasjon, drøfting og forhandling av saker som er felles for hele NTNU, og når en sak berører flere enheter. SESAM behandlet saken «Verktøy med kunstig intelligens ved NTNU» 06.11.2023. og prosjektet har brukt konklusjonen aktivt i utviklingsarbeidet «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.» Å ha tydelige styringssignaler og tett samarbeid med student- og arbeidstakerorganisasjonene har vært viktig for å kunne gjøre gode vurderinger i prosjektet.

Vedlegg



KI-reisen



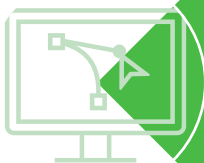
Testing av Copilot for Microsoft 365



Forslag til retningslinjer for generativ kunstig intelligens



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



NTNUs personvernkonsekvensvurdering «Copilot with commercial Data protection»



Steg for steg beskrivelse: Eksempel på bruk av Copilot



PROSJEKT

Pilotere Copilot for Microsoft 365 i Datatilsynets regulatoriske sandkasse



KI-reisen

NTNU har som mange andre i offentlig og privat sektor vurdert mulighetene for å ta i bruk kunstig intelligens (KI) i arbeidshverdagen. KI er en teknologi som kan bidra til å løse mange samfunnsutfordringer, effektivisere offentlige tjenester og skape nye muligheter for innovasjon og verdiskaping. Å ta i bruk KI i riktig form kan gi uante gevinster. Dette er derfor et teknologisk taktskifte man bør ta stilling til om man bør være med på, men det må skje i trygge rammer.

Bruk av KI også fører med seg noen problematiske områder. Prosjektgruppen har gjennom Copilot-prosjektet forsøkt å avdekke hvilke områder som er spesielt viktig å fokusere på før, under og etter anskaffelse av et informasjonssystem som anvender KI. Hva skiller seg fra tidligere informasjonssystemer og er det områder KI bør anvendes og ikke bør anvendes?

KI-reisen er et forsøk på å forberede ulike virksomheter på å kunne ta i bruk KI på en trygg måte. Den bygger på DFØ sin veiledning «Sky-reisen»¹ med momenter som er erfart fra prosjektet. KI-reisen består av flere trinn der det første trinnet omhandler KI-strategi og er det forberedende trinnet til å ta i bruk KI. Deretter kommer vurderinger av tjenester og anskaffelse som gjøres per informasjonssystem, før den tar for seg forvaltningen av systemet i dets levetid.

KI-strategi

Å utarbeide en KI-strategi er et naturlig første steg i prosessen for å klargjøre virksomheten for å ta i bruk KI. Ordet strategi kan for mange virke tungt og vanskelig og det er viktig å tenke på at dette er en del av en modningsprosess. Om det ender opp i et eget strategi-dokument eller dokumenteres på andre måter, for eksempel hektes på eksisterende strategier, retningslinjer og rutiner er opp til hver virksomhet, men å ha vært igjennom prosessen i forkant er viktig.

KI-strategien utarbeidet som forslag fra dette prosjektet består av syv trinn virksomheter bør være igjennom før den tar i bruk KI. Totalt sett utgjør strategien et flytskjema som også illustrerer hvilken rekkefølge disse trinnene bør gjennomføres i. I dette kapittelet vil hvert enkelt av punktene beskrives i større detalj.

Avdekke relevante lover

Første steget i prosessen er å avdekke hvilke lover og regler som er eller vil bli relevante for egen sektor. Listen kan være veldig varierende basert på hva systemet skal brukes til og hvilke informasjon som skal prosesserer, men å ha gjort denne jobben i forkant vil gjøre det lettere å avdekke hvilke områder KI kan anvendes på og ikke kan anvendes på.

Noen lover og regler vil være veldig generelle for alle sektorer. Dette gjelder for eksempel Personvernforordningen, Ligestillings- og diskrimineringsloven osv. I tillegg kommer det en rekke nye direktiver og forordninger fra EU som kan være med på å sette føringer for bruk av KI fremover. Både NIS-2 direktivet og KI-forordningen nærmer seg, og det er

¹ <https://markedsplassen.anskaffelser.no/veiledning/skyreisen>



viktig at virksomhetene setter seg godt inn i hva dette kan bety for egen virksomhet på et tidlig tidspunkt.

For offentlig sektor er det også en rekke ulike regelverk som kan være aktuelle ved bruk av KI. I tillegg skal virksomheter i offentlig sektor ta høyde for det til enhver tid gjeldende digitaliseringsrundskriv. Digitaliseringsrundskrivet er en sammenstilling av pålegg og anbefalinger om digitalisering i offentlig sektor². Rundskrivet refererer til relevant lovverk som er gjeldende, og til eksisterende veiledninger og kan være til hjelp i en slik prosess.

Hvilke områder kan KI brukes på

Hva skal KI hjelpe med, hvilke mål og gevinster ønsker man å oppnå ved å ta i bruk KI, og hvilke områder kan KI brukes eller ikke brukes på? Dette er viktige spørsmål å stille i forberedelsene for å ta i bruk KI. Ved å avdekke hvilke områder virksomheten ønsker hjelp fra KI vil gjøre det lettere å finne relevante KI-verktøy. Våre vurderinger er at KI er best på to ting: Det som ingen mennesker er gode på, altså analysere og sammenstille store datasett, og det som vi kan fra før, men som kan effektiviseres. På den måten kan vi som mennesker kontrollere utfall og forhindre eventuelle feil beslutninger.

Hvilke områder skal KI ikke anvendes?

KI har mange bruksområder og noen av disse områdene vil innebære høyere risiko for virksomheten, eller kan til og med være direkte ulovlig. Dette er helt avhengig av hvordan informasjonssystemet er bygget opp, hvilken informasjon systemet prosesserer, hvor den prosesseres osv. Det kan likevel være fint å avdekke disse områdene for å få gjort en ekstra vurderinger for bruk, om man ikke vurderer helt å droppe slik bruk.

Digdir har kommet med noen anbefalinger for hvor man bør være forsiktig ved bruk av KI³. De nevner blant annet at virksomheter bør være forsiktig ved bruk av KI mot innbyggere i tillegg til å være forsiktig å ta i bruk KI som oppslagsverk. I tillegg bør man være forsiktig med å legge inn sensitiv informasjon inn i «prompts» da denne informasjonen kan samles inn og gjenbrukes av andre.

Med bakgrunn i Digdirs anbefalinger og erfaringer og diskusjoner i løpet av prosjektet har vi kommet frem til noen anbefalinger:

- KI skal ikke brukes til å erstatte kompetanse. Vi må kunne avdekke feil som gjøres av verktøyet vi bruker.
- Skal KI brukes til å prosessere personopplysninger må man være ekstra varsom slik at relevant regelverk overholdes. For eksempel; lages det nye sammenstillinger av personopplysninger der man ikke kan kontrollere hvilke opplysninger som er brukt i sammenstilling? Eller kan tilfeldige sammenhenger brukes til å fatte beslutninger som ender med å diskriminere brukere?
- KI skal ikke brukes for å på noen som helst måte overvåke, sammenlikne eller vurdere egne ansatte.

² <https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id3025117/>

³ <https://www.digdir.no/kunstig-intelligens/bruk-av-generativ-kunstig-intelligens-i-offentlig-sektor/4670>



Utarbeid plan for forvaltning

De aller fleste virksomheter har allerede en forvaltningsplan, men hvordan forvalte informasjonssystemer som brukes allerede og som har endret seg drastisk de siste årene? Fra å være «on prem»-løsninger der det ble kjøpt inn lisenser og ikke gjort noe mer enn oppdateringer før lisenser måtte fornyes, krever sky-løsninger og også nå KI-verktøy at forvaltningen gjøres på en helt ny måte. Den teknologiske utviklingen har skjedd i eksponentiell hastighet de siste årene, og informasjonssystemene som anvendes i dag følger denne teknologiske utviklingen. Å forvalte slike typer informasjonssystemer stiller derfor strengere krav til deler av forvaltningen. Noen områder vil gjøre seg spesielt viktige for å følge opp nye IT-systemer og da spesielt med tanke på IT-systemer som anvender kunstig intelligens:

- Avtaleoppfølging
- Oppfølging av utvikling
- Oppdatert produktkunnskap
- Oppdaterte risikovurderinger
- Oppdatert opplæring og veiledning til brukere

Å henge bakpå i slik oppfølging kan føre til en situasjon der man står med et informasjonssystem med uante funksjonaliteter, men også uante risikoer og sårbarheter.

Utarbeid en exit-strategi

Ved å ta i bruk KI-verktøy er det også veldig viktig å ha tenkt over hvordan virksomheten kan avvikle bruken av verktøyet. Det kan være flere årsaker til at man ikke ønsker å bruke verktøyet lenger. Det kan for eksempel være økning i priser, en utvikling som går vekk fra opprinnelig ønske om å bruke verktøyet, en utvikling som gjør at bruk potensielt er ulovlig, økt risiko ved bruk av systemet eller andre årsaker. Exit-strategien bør ha avdekket disse linjene for akseptabel bruk slik at forvaltere kan oppdage og varsle beslutningsmyndighet hvis de overskrides. For virksomhetskritiske systemer bør man også ha vurdert hvilke exit-muligheter man har, er det alternative skyløsninger eller skal systemet tas ut av sky og tilbake til lokale løsninger.

Exit-strategi er også spesielt viktig i forbindelse med KI-verktøy for å kunne ta i bruk verktøy raskere. Da kan man ha lavere terskel for å ta i bruk et verktøy hvis virksomheten også har en plan for oppfølging og avvikling hvis verktøyet ikke gir ønsket gevinst eller hvis verktøyet har uønsket funksjonalitet/gir uønskede effekter.

Identifiser behov for opplæring

Bruk av informasjonssystemer som er i kontinuerlig utvikling krever oppdatert informasjon til brukere. KI-verktøy spesielt kan i noen tilfeller kreve en ny måte å arbeide på for størst mulig gevinst, for riktig bruk og ikke minst for å sikre informasjonsverdier tilstrekkelig. Bruk av KI krever også en annen bevissthet i forhold til informasjonskompetansen til hver enkelt bruker. Flere av de åtte funnene i prosjektet hadde anbefaling om opplæring av brukere på ulike områder. Hvordan dette skal realiseres og eventuelt verifiseres eller kontrolleres bør virksomhetene ha en plan på i forkant. Under har vi listet noen momenter som kan vurderes før virksomheten tar i bruk KI:

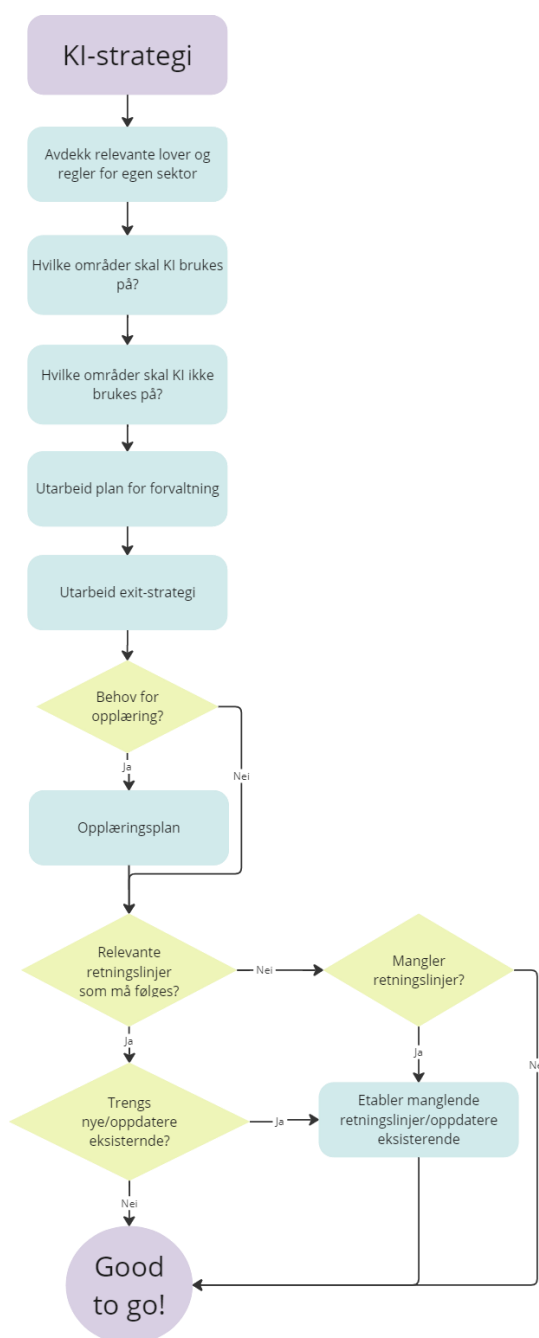
- Virksomheter bør ha tenkt igjennom hvilken type opplæring som kreves, skal noe være obligatorisk.



- Bør det være en generell opplæring som alle ansatte skal igjennom, og hvordan skal denne gis.
- Skal det være opplæring per system, skal nye oppdateringer eller endret bruk komme frem i dokumentasjon eller opplæring.

Dokumenter strategi

Det siste punktet omhandler å få dokumentert det som har kommet frem i prosessen. Hvor dette gjøres er opp til hver virksomhet. Å hekte det på allerede eksisterende dokumentasjon vil etter prosjektets mening være enklest å gjennomføre og også holde oppdatert i forhold til annen dokumentasjon.



Figur – Flytskjema «steg for steg» i KI-reisen



Vurderinger per tjeneste

Før man tar i bruk et KI-verktøy i en offentlig virksomhet, bør man gjøre en grundig vurdering av de potensielle fordelene og ulempene, samt de juridiske, etiske og praktiske konsekvensene ved å ta i bruk det spesifikke verktøyet. Vi ser på slike vurderinger som spesielt viktig å gjøre i forbindelse med bruk av KI da KI har mange fordeler, men verktøyet kan også brukes til andre formål enn opprinnelig tiltenkt. Prosjektet har kommet opp med spørsmål innenfor ulike kategorier som kan være med på å vurdere viktigheten av verktøyet eller systemet man vurderer å anskaffe.

Informasjonssikkerhet

Informasjonssikkerhet handler om å beskytte informasjonsverdiene våre mot uautorisert tilgang, endring, tap eller skade. Hva som har verdi, og hvilken verdi det har, er avhengig av tid, sted og person. Noe kan ha ulik verdi for ulike personer, organisasjoner, samfunn og nasjoner. Oversikt over hvilke verdier som eksisterer i informasjonssystemer der KI-verktøy skal anvendes er derfor grunnleggende for å kunne gjøre vurderinger rundt informasjonssikkerheten til verktøyet og om de er tilstrekkelig. Det henvises ofte til «Orden i eget hus» og er et ansvar hver enkelt ansatt må bidra med.

- Hvilke data prosesseres av KI-verktøyet, og hvor sensitive eller konfidensielle er de?
- Kan vi styre/begrense hvilke data som prosesseres?
- Hvem har tilgang til dataene, og hvordan kontrolleres og loggføres denne tilgangen?
- Hvordan sikres dataene mot uønskede hendelser som hacking, lekkasje, sletting eller manipulering?
- Deles dataene med noen andre aktører, som leverandører, samarbeidspartnere eller tredjeparter, og hvordan sikres dataene i disse tilfellene?

Personvern

Personvern går på mange områder hånd i hånd med informasjonssikkerhet, så flere av vurderingene som gjøres innenfor informasjonssikkerhet vil også være aktuelle for personvern.

Personvern handler om å respektere og beskytte de registrertes rettigheter og interesser når det gjelder deres personopplysninger. Dette blir av mange sett på som regulatoriske hindringer, men til syvende og sist handler det om å ivareta menneskerettigheter. Med det i bakhodet bør virksomheter gjøre noen ekstra vurderinger før KI-verktøy slippes løs på personopplysninger:

- Hvem blir registrert av KI-verktøyet, og hva slags personopplysninger samles inn, lagres og behandles?
- Hvor mye data lagres, og hvor lenge lagres de?
- Lages det nye sammensetninger av opplysninger, som profiler, segmenter eller prediksjoner, basert på dataene?
- Hvilket rettslig grunnlag har vi for å bruke KI-verktøyet, og hvordan informerer vi de registrerte om dette?
- Hvordan ivaretar vi de registrertes rettigheter, som innsyn, retting, sletting, begrensning, dataportabilitet og motstand?

I og med at KI er innovativ bruk eller anvendelse av ny teknologisk eller organisatorisk løsning, og hvis KI-verktøyet skal behandle personopplysninger, bør terskelen være lav



for å gjøre en full personvernkonsekvensvurdering (DPIA). Gjennom en DPIA-prosess vil du få svar på spørsmålene over, og du vil få et bedre helhetsbilde over verktøyet og hvordan den registrertes rettigheter og friheter best ivaretas.

Menneskelig perspektiv

Menneskelig perspektiv handler om å ta hensyn til de sosiale, kulturelle og etiske aspektene ved bruk av KI, og å sikre at KI bidrar til å fremme menneskelig verdighet, autonomi, rettferdighet og inkludering.

- Hvordan påvirker KI-verktøyet de ansatte, brukerne og andre berørte parter, både positivt og negativt?
- Hvordan sikrer vi at KI-verktøyet ikke diskriminerer, stigmatiserer eller utestenger noen grupper eller individer på grunnlag av deres personlige kjennetegn, som alder, kjønn, etnisitet, funksjonsevne, religion eller seksuell orientering?
- Hvordan sikrer vi at KI-verktøyet ikke undergraver de ansattes kompetanse, motivasjon, arbeidsmiljø eller arbeidsvilkår?
- Hvordan sikrer vi at KI-verktøyet ikke krenker brukernes integritet, selvbestemmelse, tillit eller forventninger?
- Hvordan sikrer vi at KI-verktøyet er forståelig, forklarlig og kontrollerbart for de ansatte og brukerne, og at de har mulighet til å gi tilbakemelding, klage eller anke på KI-baserte beslutninger?
- Hvordan sikrer vi at KI-verktøyet er i tråd med de etiske verdiene og prinsippene som gjelder for vår virksomhet og sektor?
- Kan bruk av verktøyet føre til digitalt utenforskap?⁴

Bærekraft

Bærekraft handler om å vurdere de økonomiske, miljømessige og samfunnsmessige konsekvensene av å bruke KI, og å sikre at KI bidrar til å oppnå bærekraftsmålene og redusere klima- og miljøavtrykket. Dette innebærer å stille spørsmål som:

- Hvordan påvirker KI-verktøyet vår virksomhets økonomi, effektivitet og innovasjonsevne?
- Hvordan påvirker KI-verktøyet miljøet, både lokalt og globalt, i form av energiforbruk, utslipp, avfall og ressursbruk?
- Hvordan påvirker KI-verktøyet samfunnet, både nasjonalt og internasjonalt, i form av demokrati, rettsstat, menneskerettigheter, likestilling og sosial utjevning?
- Hvordan sikrer vi at KI-verktøyet er i samsvar med de bærekraftsmålene og de klima- og miljømålene som gjelder for vår virksomhet og sektor?
- Hvordan sikrer vi at KI-verktøyet er basert på ansvarlig og transparent datainnsamling, -deling og -bruk, som respekterer menneskers og samfunns interesser og verdier?
- Hvordan sikrer vi at KI-verktøyet er utformet, utviklet og implementert på en måte som fremmer sirkulær økonomi, grønn innovasjon og digital inkludering?

Behov

Å vurdere KI-verktøyet opp mot hvilke behov man har omhandler å vurdere bruksområdet opp mot egen KI-strategi. I tillegg bør det gjøres vurderinger rundt om verktøyet kan brukes til andre formål eller andre områder som er uønsket og potensiell effekt av bruk av verktøyet. Spørsmål man kan vurdere her er:

- Hva er gevinsten ved å ta i bruk verktøyet?

⁴ <https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id3025117/>



- Har vi mulighet til å kontrollere utfallet av bruken?
- Strider verktøyet med KI-strategien til virksomheten?
- Kan verktøyet misbrukes?
- Hva er mulig utfall hvis verktøyet brukes feil?

Anskaffelse

Når man skal anskaffe et KI-verktøy i offentlig sektor, må man følge anskaffelsesloven og tilhørende forskrifter, som regulerer hvordan offentlige innkjøp skal gjennomføres. Anskaffelsesloven stiller allerede en del krav til ulike områder og hvordan disse skal vektlegges i en anskaffelsesprosess. Dette er områder som klima og miljøhensyn, menneskerettigheter, miljø og andre menneskehensyn, samt arbeidsforhold, sosiale forhold og arbeidslivskriminalitet.

I tillegg til å følge anskaffelsesloven er det viktig å få kravstilt annet relevant lovverk i forbindelse med den konkrete anskaffelsen. Dette kan være personvernforordningen eller andre lovverk som ble avdekket under arbeidet med en KI-strategi.

Når alle funksjonelle krav er stilt, skal man stille krav til den ikke-funksjonelle delen. Dette omfatter blant annet informasjonssikkerhet. Det er en balansegang mellom mengde A-krav og B-krav. For mange A-krav kan føre til få eller ingen tilbydere. For få A-krav kan føre til at man ender med et system eller verktøy som ikke er i henhold til egen virksomhet sine retningslinjer. A-krav innenfor ikke-funksjonell kategori bør derfor holdes til absolutte krav for virksomheten. Dette kan være sikring av data, hvem som skal ha tilgang til data osv.

Den teknologiske utviklingen gjør det ekstra vanskelig å stille krav til IT-systemer. Hvordan skal man stille krav til et system som er i kontinuerlig utvikling? Dette er viktig å ha med i betraktning i utforming av kravene som stilles slik at den fremtidige versjonen av systemet som anskaffes har samme teknologiske standard som ved anskaffelsestidspunkt. En offentlig anskaffelse kan også ta tid, så kravene som stilles må også ta høyde for utviklingen som skjer fra kravstillelse og til anskaffelse.

Hva som er relevante krav å stille i forbindelse med et KI-verktøy er per nå vanskelig å si. Vi har enda ikke så mye erfaring i anskaffelse av KI-verktøy eller IT-systemer som anvender KI eller på et tidspunkt kan anvende KI. Vi har laget noen forslag til krav som kan stilles under.

Krav	Type
KI-teknologi er godt dokumentert og tilgjengelig, inkludert formål og datakilder	A
Er det mulig å kontrollere/spore utfallet av KI	A
Beskriv eksisterende funksjonalitet som anvender KI eller annen automasjon og hva som er gevinsten av slik bruk	B
Beskriv planlagt utvikling av systemet og utvikling av KI spesielt.	B
Beskriv hvordan løsningen møter kravene fra kommende KI-forordningen	B
Beskriv hvordan KI-funksjonalitet er testet og godkjent før det implementeres i systemet	B
Beskriv hvordan bruker kan tilpasse, inkludert slå av/på, KI-funksjonalitet i løsningen	B
Beskriv hvordan løsningen håndterer dataene KI er trent på, spesielt med tanke på informasjonssikkerhet og personvern	B
<i>NB: Legg til spesielle krav for egen organisasjon (Hva er viktig for dere?)</i>	



Forvaltning

Hvordan forvalte IT-systemer på en god og forsvarlig måte er kanskje den største endringen fra tidligere IT-systemer og dagens IT-systemer. Utvikling av systemer og avtaler skjer kontinuerlig og krever derfor kontinuerlig oppfølging. Mangelfull forvaltning som tidligere har vært tilstrekkelig vil nå gi betydelige utfordringer. Dette er ikke nytt for kunstig intelligens, men har gradvis blitt mer gjeldende med sky-løsninger og hyppig teknologisk utvikling. I dette prosjektet har vi valgt å kalle det et forvaltningsmessig gap. Jo større dette gapet blir, jo mer ressurser vil kreves for å tette det. Nok ressurser fra start er derfor svært viktig når man går til anskaffelse av et slikt system. Derfor må kostnader til forvaltning av systemet synliggjøres sammen med kostnader til lisenser og eventuelt fysisk utstyr. Forvaltning vil innebære kursing og opplæring av forvaltere og driftspersonell, årsverk til oppfølging og drift, opplæring av brukere og liknende.

Det ble i delkapittelet om forvaltningsplan nevnt områder som var spesielt viktig å følge opp i forbindelse med bruk av KI-verktøy. I tillegg til dette er det spesielt viktig å ha avklart ansvars- og beslutningsmyndighet. Dette er avgjørende for å kunne ta løpende vurderinger på risiko, utvikling og eventuelt når en exit-strategi skal iverksettes.

Oppsummering

Kunstig intelligens vil gi stor gevinst hvis det tas i bruk på riktig måte, men konsekvensene av feil bruk kan også være store. Å ha en gjennomarbeidet strategi for bruk er viktig underlag for å kunne gjøre gode vurderinger når et nytt system eller verktøy skal anskaffes. Flere av vurderingene har likhetstrekk med sky-teknologi, men det er likevel noen områder som skiller seg ut eller blir spesielt viktig i forbindelse med kunstig intelligens:

- Avdekk relevant lovverk og krav som stilles
- Avdekk hvor KI kan brukes og IKKE skal brukes
- Avdekk ansvars- og beslutningsmyndighet
- Sett kriterier for exit og gjør det til en realistisk mulighet.
- Følg opp produktet som anskaffes

A large graphic consisting of a light blue clipboard icon on the left, with a blue arrow pointing from it to a solid blue rectangular box on the right. The text 'Testing av Copilot for Microsoft 365' is written in white inside the blue box.

Testing av Copilot for Microsoft 365

PROSJEKT

Pilotere Copilot for Microsoft 365 i Datatilsynets regulatoriske sandkasse



Testing av Copilot for Microsoft 365

Copilot er et omfattende verktøy med mange muligheter. For å kunne teste verktøyet på en effektiv måte over en begrenset testperiode var vi avhengig av å strukturere testingen. Denne rapporten presenterer fremgangsmåten fra testingen av Copilot ved NTNU. NTNU har utviklet et testbatteri i samråd med Datatilsynet, som dekker tre ulike use cases som er relevante for NTNU og andre offentlige organisasjoner.

Testrapporten beskriver hvordan Copilot ble brukt i hvert use case, og eksempler på hvilke spørsmål og refleksjoner man kan stille seg hvis man skal bruke Copilot på disse områdene. Funn fra testingen er integrert i overordnet funnrapport og i personvernkonsekvensvurderingen.

Målet med testene har vært å avdekke gevinstene ved bruk av Copilot i offentlig sektor, samt mulige risikoer eller områder hvor virksomheter i offentlig sektor bør være forsiktige. Det ble tidlige i testingen tydelig at Copilot ikke var et ferdig produkt, men et verktøy i fortsatt stor utvikling. Dette var noe vi måtte ta høyde for i testingen og legge til grunn i evalueringen av resultatene. Copilot har hatt, og vil ha i tiden som kommer, en bratt utviklingskurve. NTNU legger derfor ikke frem en egen resultatsrapport, da resultatene allerede kan være utdaterte på grunn av verktøyets utviklingshastighet (NTNUs resultater er bakt inn i personvernkonsekvensvurdering (DPIA) og funnrapport). Denne testrapporten er ment som et bidrag til å øke kunnskapen og bevisstheten om KI-verktøy i offentlig sektor, og til å bidra til dialog og diskusjon om hvordan man kan bruke KI på en ansvarlig og hensiktsmessig måte.

For å kunne lære hvordan Copilot fungerer har det vært viktig å bruke og teste verktøyet ordentlig. Å balansere nok testere opp mot å holde risikoen på et akseptabelt nivå har derfor vært avgjørende for å få testet på en trygg måte. Vi ønsket å gjøre minst mulig begrensninger i selve Copilot, så både antall testere og utvalg av testere var nøye gjennomtenkt. God informasjonsflyt mellom testerne og mot prosjektgruppen for å få løpende resultater, funn og betraktninger rundt testene har også vært viktig for å avdekke nye tester og gjøre løpende vurderinger på risiko. Alle møter har blitt dokumentert gjennom en egen «loop». Det har vært nyttig med hyppige møtepunkter for å sikre fremdrift i testingen.

På grunn av usikkerheten rundt risikoen og ønske om å legge minst mulig begrensninger på testerne var det viktig for prosjektgruppen at alle testerne var innforstått med hva de var med på, hvilke risiko det innebar for dem og deres nærmeste kollegaer. Det ble lagt særlig vekt på Personvernombudets råd, og samtlige testere måttet aktivt samtykke til at de har forstått innholdet i DPIAen og at de har fulgt Personvernombudets råd når de har gjennomført testen.

Personvernombudets råd:

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



- «*Rydd egen bruker*»: Gå gjennom alle filer, dokumenter og lagringsområder (for eksempel teamsområder) som brukere har for å sikre at ikke verktøyet får tilgang til data den ikke skal ha tilgang til (særlig andre sine personopplysninger, eller annen skjermingsverdig informasjon)
 - *Tilbakemeldinger fra de registrerte: Det vil ikke være mulig å gjennomgå alle eposter/chatmeldinger før testing. Det er snakk om titusenvise av oppføringer, og er ikke realistisk før testing.*
 - *Prosjektleders vurdering: Testerne har tilgang til store mengder data på sine personlige brukere gjennom mange års aktivitet, men det er veldig lite sannsynlig at det er snakk om annet enn arbeidsrelatert diskusjon, kommentarer og avklaringer. Ja det er personopplysninger, men det er snakk om navn/kontaktinformasjon knyttet til hvem som har sagt hva om et konkret tema. De ansatte behandler ikke særlige kategorier av personopplysninger og ingen har (eller har hatt) personalbehandling som en del av sine arbeidsoppgaver.*
- «*Gå gjennom alle tilganger*»: Det er viktig at det kun er NTNU sine data som blir behandlet, Hvis bruker har tilgang til for eksempel shared channels med andre institusjoner må disse holdes utenfor. Gå gjennom tredjeparts programvare, add-ons osv for å sikre at dataflyten inn og ut er kontrollert.
 - *Tilbakemeldinger fra de registrerte: Tilgang til shared channels bør ikke holdes utenfor testfasen.*
 - *Prosjektleders vurdering: Pr i dag er det kun ca. 5-10 aktive shared channels på NTNU, og testerne jobber i dag med å rulle ut denne funksjonaliteten som en mer aktiv tjeneste for NTNUs brukere. Testerne bruker da egen bruker for å teste funksjonaliteten, og en begrensning i tilgangen vil ødelegge for annen aktivitet. I og med at det er veldig få eksisterende shared channels og det ikke deles skjermingsverdig informasjon i kanalene, anses risikoen for at noe skal skje som minimal.*
- «*Si fra på forhånd om du bruker KI i samhandling med andre*»: Om testerne skal bruke KI-verktøy på andre sine personopplysninger må dette opplyses om på forhånd slik at den andre parten kan motsette seg. For eksempel: Hvis testerne bruker verktøyet i et teamsmøte må man si fra på starten hva man har tenkt til å gjøre, hvordan og hvor lenge data skal behandles og når det blir slettet. Hvis ikke alle samtykker skal ikke behandlingen gjennomføres

Forventninger til prosjektet:

- **Etabler rutiner og systematikk** for innhenting av tilbakemeldinger og funn fra testerne. Dette må gjennomgås jevnlig for å sikre at ikke ukontrollert behandling skjer. Personvernombudet forventer å få tilgang til rapporter og funn.
- **Gjør ny vurdering hvis flere testere:** Denne DPIA er utarbeidet med en ytre grense på 5 testere. Viktig at prosjektet har fokus på skalerbarhet, og at nye vurderinger gjennomføres om flere skal ha tilgang. Flere registrerte inn i løsningen øker risikoen.
- **Avtalegjennomgang:** Prosjektet bør gjennomgå avtaler som er inngått med leverandøren, for å sikre at NTNU har full kontroll på avtaleverket og hvilke deler



av «Microsoft-økosystemet» som påvirker hverandre. For eksempel kan prinsipper fra en selskapsgjennomgang (Due diligence) gjennomføres.

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

Testfase 1: Teknisk test

Testing av Copilot har foregått i to faser. I første fase ble det gjennomført rene tekniske tester ved at 5 administratorer ved IT-avdelingen fikk tilgang til Copilot for å teste teknisk funksjonalitet og potensielle informasjonssikkerhetsutfordringer. Særlig tilfeller av overdeling ble ettergått, og det ble iverksatt en rekke tiltak for å stenge ned enkelte områder som Copilot ikke bør få tilgang til. Da verktøyet ble vurdert som «sikkert nok» for praktisk testing ble dette igangsatt ved at ytterligere 5 brukere fikk tilgang og fase to kunne igangsettes. De tekniske testene har i tillegg fortsatt gjennom hele fase 2, men med lavere forventninger til avrapportering og deling av funn. Det har vært nyttig for administratorene våre å ha tilgang gjennom hele perioden for å kunne bygge kompetanse på verktøyet og følge med på den raske utviklingen i verktøyet.

Testfase 2: Praktisk test

I den praktiske testfasen ble antallet testere utvidet til først 10 og deretter 15 brukere, med et mer etablert testregime for å vurdere konkrete bruksområder for Copilot på NTNU. Vi utviklet et eget testbatteri, men har måttet gjøre endringer og tilpasse oss underveis da det ikke var mulig å gjennomføre testen som vi hadde tenkt. Grunnen til dette var at Copilot ikke fikk norsk språkpakke før vi var nesten ferdig med den praktiske testfasen. Vi fikk likevel nok funn til å kunne gi et bilde av Copilot sin funksjonsevne. Resultatene av testene er bakt inn i DPIA for driftsfasen som er vedlagt, og de 8 overordnede funnene er presentert innledningsvis i rapporten.

Testbatteri

NTNU utvikler et nytt saksbehandlings- og arkivsystem sammen med andre universiteter og høyskoler i Norge. På NTNU heter dette arbeidet *NTNU Sak* og NTNU er pilotorganisasjon for å ta det nye systemet i bruk. For å få systemet til å fungere og for at man skal kunne holde saker fra hverandre er det nødvendig å forstå hvordan NTNUs virksomhetsområder med underliggende saksområder, og der igjen underliggende saksprosesser, henger sammen. I systemforstand omtales dette som Funksjon, Underfunksjon og Prosess (FUP). Det er identifisert 376 saksprosesser som igjen inneholder ulike sakstransaksjoner og -oppgaver hvor utveksling av informasjon, arkiv- og dokumentasjonsplikt er naturlige elementer. NTNU er en kunnskapsorganisasjon med mange studenter og ansatte, så særlig personopplysninger er veldig ofte en naturlig del av intern informasjonsutveksling. Liste over alle identifiserte saksområder:

<https://i.ntnu.no/wiki/-/wiki/Norsk/Saksområder+og+saksprosesser>

NTNU innfører våren 2024 Visma Drafit som protokollverktøy for å holde oversikt over behandling av personopplysninger etter Personvernforordningens artikkel 30. NTNU har valgt å ta utgangspunkt i oversikten over saksprosesser som grunnlag for å holde oversikt over behandling av personopplysninger i administrativ saksbehandling. I



forbindelse med dette arbeidet er alle saksprosesser forhåndsvurdert ut fra hvor vidt de inneholder skjermingsverdig informasjon og prosjektet har plukket ut 15 saksprosesser fra kjerne-/funksjonsområder utdanning, forskning, formidling og internadministrasjon for å gi et bilde av hva slags informasjon som er vanlig å behandle på NTNU. Disse 15 saksprosessene inneholder åpen informasjon og er de prosjektet har valgt å ta utgangspunkt i ved testing av hvorvidt Copilot for Microsoft 365 kan benyttes og gi positiv gevinst.

Oversikt over saksprosesser:

Funksjon	Underfunksjon	Saksprosess	Transaksjon
Formidling	Faglig formidling	D.a.01 Arrangere fagkonferanser/-seminarer	Utarbeide forslag til budsjett, program, plan og rapport fra åpne fagkonferanser og -seminarer
Formidling	Kommunikasjon og samfunnskontakt	D.b.17 Markedsføre og selge etter- og videreutdanningstilbud	Utarbeide utkast til strategidokument, handlingsplan, budsjett, salgsplan
Formidling	Kommunikasjon og samfunnskontakt	D.d.10 Lage arrangement	Lage forslag til program, interne kjøreplaner og informasjonsmateriell
Forskning	Forskningsstrategi- og kvalitet	B.a.03 Informere og mobilisere om forskningsprogrammer og utlysninger	Utarbeide forslag til saksfremlegg og informasjonsmateriell
Forskning	Forskningsprosjekt	B.b.16 Rapportere forskningsresultater	Utarbeide rapporter, sammendrag og innhold til forskningsmeldinger
Forskning	Forskningsstøtte	B.c.01 Veilede og informere	Utarbeide forslag til opplæringsopplegg for forskere
Forskning	Forskningsrettigheter og kommersialisering	B.d.07 Støtte studentinnovasjon	Behandle søknad, tildeling, rapport
Internadm.	Økonomi	A.b.09 Rapportere innenfor økonomiområdet	Utarbeide utkast til årsrapport og tertialrapporter for kvalitativt innhold
Internadm.	Styring og utvikling av virksomheten	A.a.02 Utarbeide og vedlikeholde strategi og plan	Utarbeide strategidokumenter, årsplan, handlingsplan, arbeidsplan, årshjul, innspill/høring og saksfremlegg
Internadm.	Styring og utvikling av virksomheten	A.a.03 Utarbeide og vedlikeholde interne instruksjer og retningslinjer og andre styrende dokumenter	Utarbeide utredninger, saksfremlegg, retningslinjer og informasjon om styrende dokumentasjon
Internadm.	Styring og utvikling av virksomheten	A.a.08 Avholde møter i styrer, råd, utvalg og egne nemnder	Lage innkallinger, saksdokumenter, referat/protokoll og orientering om åpne vedtak som er fattet (ikke enkeltvedtak)
Internadm.	Styring og utvikling av virksomheten	A.a.18 Administrere høringer	Utarbeide forslag til høringsbrev, høringsnotat, vurdering, innspill, høringsuttalelse i åpne høringsprosesser
Internadm.	Styring og utvikling av virksomheten	A.a.19 Planlegge og gjennomføre interne prosjekter	Utarbeide mandat, prosjektplan, tidsplan, endringsmeldinger, enkle budsjett, beskrivelse av prosjektroller, ressursbruk, referat og rapport fra prosjektet
Utdanning	Internadministrasjon	A.a.10 Samarbeide med studentparlament /studentråd/studentutvalg	Skrive referat fra åpne studenttingmøter
Utdanning	Utdanning	C.d.30 Informere om studentboligordninger	Kunngjøring av informasjon om studentboliger til NTNUs eksisterende og fremtidige studenter



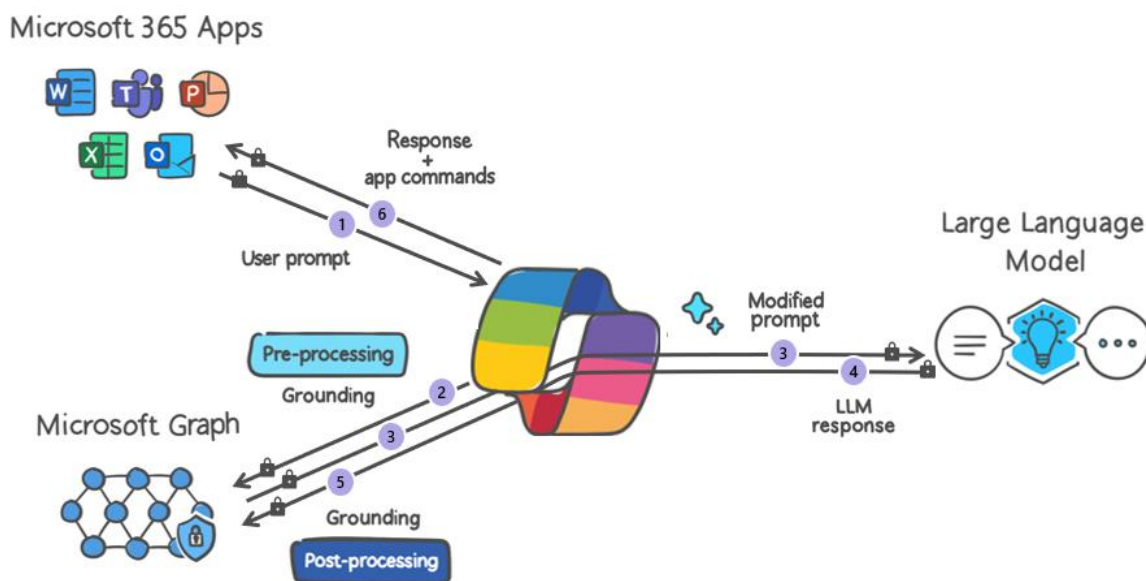
Ut fra disse 15 saksprosessene har vi i samråd med Datatilsynet valgt å gå videre i dybdeundersøkelse av tre områder som er relevant ikke bare for NTNU, men felles for mange i offentlig sektor (Copilot sin egen beskrivelse i kursiv med sitattegn):

1. **Utredningsstart:** Informasjonsinnhenting og skrive førsteutkast til et notat. *«Copilot kan hjelpe deg med å organisere og strukturere informasjonen effektivt. Du kan dra nytte av AI-drevne verktøy for å analysere data raskt. I tillegg kan du bruke tale-til-tekst-funksjonen for rask notering.»*
2. **Referatfunksjon:** Automatisk oppsummering fra møter. *«Aktiver Copilot under møter for å transkribere diskusjoner i sanntid. Du kan bruke AI-algoritmer for å identifisere nøkkelpunkter og aksjonselementer automatisk. Deretter kan du eksportere sammendraget direkte til andre Microsoft 365-applikasjoner.»*
3. **Saksbehandling på epost.** *«Integrer Copilot med Outlook for intelligent e-posthåndtering. Du kan bruke automatiserte svarfunksjoner for å håndtere vanlige henvendelser effektivt. I tillegg kan du organisere e-postene dynamisk basert på prioriteter ved hjelp av AI.»*

Datatilsynet ønsket at NTNU:

- Tester med reelle oppgaver. Disse må være åpne prosesser og kunne tåle offentliggjøring
- Hvert område ønskes beskrevet ut fra tre perspektiver:
 - o Hvordan ville jeg løst oppgaven uten verktøyene i Microsoft 365 (men bare Word går bra)
 - o Hvordan ville jeg løst oppgaven med oppgavene jeg har i dag (Microsoft 365)
 - o Hvordan ville jeg løst oppgaven med Copilot for Microsoft 365
- Kjør samme tester flere ganger for å se om det er forskjell i svar, og at forskjellige brukere kjører de samme testene for å se om/hvordan den vurderer brukerne ulikt
- Noter ned feil og bom – feilmeldinger er interessant
- Skriv ned funn fortløpende i en form som kan inngå i et datasett som kan offentliggjøres (funnene blir avidentifisert)

Nedenfor følger beskrivelse av hver use case med steg-for-steg interaksjon med Copilot. Samtlige steg-for-steg beskrivelser har tatt utgangspunkt i Microsoft sin illustrasjon om hvordan Copilot fungerer:



Figur - Microsoft beskrivelse av dataflyt

Use case «Utredningsstart»

Utredningsinstruksen gir tydelige føringer om at det er viktig at statlige beslutninger er velbegrunnede og gjennomtenkte. Ufullstendig eller manglende utredning øker risikoen for at det fattes beslutninger som ikke kan gjennomføres, som gir uønskede virkninger eller som innebærer sløsing med samfunnets ressurser. Instruksen beskriver minimumskravene til utredning som skal beskrives i alle utredninger:

1. Hva er problemet, og hva vil vi oppnå?
2. Hvilke tiltak er relevante?
3. Hvilke prinsipielle spørsmål reiser tiltakene?
4. Hva er de positive og negative virkningene av tiltakene, hvor varige er de, og hvem blir berørt?
5. Hvilket tiltak anbefales, og hvorfor?
6. Hva er forutsetningene for en vellykket gjennomføring?

Utredningsinstruksen kan leses i sin helhet på <https://lovdata.no/dokument/INS/forskrift/2016-02-19-184>

Offentlige organisasjoner har ofte sin egen «form» på utredninger, med blant annet tanke på språk, kompleksitet oppbygning og det krever ofte lang og tung erfaring fra virksomheten for å kunne få dette til på en god måte. Arbeidet kan være tidkrevende, og verktøy som Copilot kan trolig hjelpe til i hele eller deler av prosessen.

Beskrivelse av antatt bruk av Copilot:

En utreder bruker Copilot for å samle inn informasjon (datainnsamling) før utredningen kan starte. Utreder får tilgang til informasjon fra nett, tidligere dokumenter hen har skrevet selv eller dokumenter hen har tilgang til (men skrevet av andre). Utreder kan ved hjelp Copilot få ut en oversikt over relevant datamateriale for å gjøre nødvendige avveininger i tråd med utredningsinstruksen, få hjelp til selve skrivearbeidet (kladding) og renskriving/språkforbedring.



Særskilte vurderinger:

- **Blir det behandlet personopplysninger: Nei** (kun egne, og kollegaer sine hvis du behandler deres dokumenter)
- **Krav til skjerming: Ja** unntatt offentligheten i skrivefase men det er offentlig «at skrivning skjer» (i praksis betyr det at saken opprettes i saksbehandlingssystem og bestilling er tilgjengelig i postjournal). Dokumentet er åpent når ferdigstilt, men ofte også når høringsfase starter.

Stegvis behandling «utredningsstart»:

Step	Standard Microsoft step description	Beskrivelse av «Steps» i UTREDNINGSSTART	Spørsmål
1	User prompts from Microsoft 365 Apps are sent to Copilot	Utredning ber Copilot om å finne tilgjengelig informasjon om et definert tema med kommando (prompt) om at det skal startes en utredning ut fra definerte spørsmål (utredningsinstruks)	
2	Copilot accesses Graph and Semantic Index for pre-processing	Copilot bruker informasjon fra kommando til å identifisere «nærliggende dokumenter» som bruker har tilgang til gjennom Graph.	
3	Copilot sends modified prompt to Large Language Model	Copilot sender all informasjon den har funnet til LLM	Er det her satt på sikkerhetsmekanismer? Sender for eksempel ikke informasjon som er klassifisert intern eller fortrolig?
4	Copilot receives LLM response	Copilot mottar svar fra LLM	
5	Copilot accesses Graph and Semantic Index for post-processing	Copilot bearbeider mottatt informasjon fra LLM og gjør denne lesbar/tilpasset for bruker	Hvorfor trenger Copilot en runde til i Graphen? Oversette og bearbeide språk for eksempel, eller det andre grunner?
6	Copilot sends the response, and app command back to Microsoft 365 Apps	Utkast til utredning gjøres tilgjengelig for utredning, sammen med informasjon (lenker) om relevante interne dokumenter som utredning har tilgang til og ekstern informasjon fra nettet som kan være relevant for utredningen. Utredning bekrefter at innhold er ok ved ikke å gjøre noe, men kan også si «ikke bra nok» og sende inn en ny runde fra step 1. Utredning kan gi tommel opp eller ned på respons. Utredning bearbeider all tilgjengelig informasjon og skriver ferdig utkast til utredning i Word. Utredning bruker aktivt	Hvilke aktive steg kan bruker ta for å akseptere eller avvise respons (eks. tommel opp og tommel ned)? Copilot bruker denne adferden til å lære seg hvordan du liker å få svar?



stavekontroll/språkforbedringsfunksjonen til Copilot på definerte deler av teksten i skrivearbeidet

Arbeidshypoteser og merknader før test:

- Utreder bruker utredningsinstruks med definerte minimumsspørsmål <https://www.regjeringen.no/no/dokumenter/instruks-om-utredning-av-statlige-tiltak-utredningsinstruksen/id2476518/> og <https://lovdata.no/dokument/INS/forskrift/2016-02-19-184>
- Antakelse om at det er dette Copilot «er laget for», det virker veldig lovende.
- Copilot vil kun behandle egne data, interne data utreder har tilgang til og åpne kilder på nett.
- Copilot vil ikke klare å skille mellom dokumenter som er halvferdige (kladder) og endelige dokumenter. Vil trolig ikke klare å vekte dokumenttyngde («instruks» skal tillegges større vekt i utredning enn «veiledning» for eksempel)
- Risiko for at bruker ikke kvalitetssikrer godt nok, viktig med sidemannskontroll. Fremtvinger en diskusjon om mer samarbeid mellom utredere (som i og for seg kan være veldig positivt kvalitetsmessig).

Refleksjonsspørsmål til «utredningsstart»

	Ja	Nei	Vet ikke
Foreslo Copilot relevante dokumenter for utredningen/notatet?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er det kvalitetsforskjell på dokumentene den har hentet informasjon fra? (F.eks kladd vs. ferdig dokument)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har Copilot hentet informasjon fra web? Har du kontrollert kildene?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har du gjennomgått og kvalitetssikret resultatet?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Use case «Referatfunksjon»

Å skrive referat, protokoll, sammendrag eller oppsummering fra et møte mellom 2 eller flere aktører kan være nyttig av ulike årsaker:

1. **Dokumentasjon:** Referatet gir en offisiell registrering av hva som ble diskutert og besluttet i et møte eller en hendelse. Det kan være nyttig for fremtidig referanse og for å sikre at alle har en felles forståelse av hva som skjedde.
2. **Kommunikasjon:** Referatet hjelper til med å formidle informasjon til de som ikke kunne delta i møtet eller hendelsen. Det gir dem muligheten til å forstå hva som ble diskutert og hvilke beslutninger som ble tatt.
3. **Ansvarlighet:** Referatet kan holde deltakerne ansvarlige for de handlingene eller beslutningene de har forpliktet seg til under møtet eller hendelsen.
4. **Oppfølging:** Referatet kan brukes som en sjekklister for oppfølging av handlinger som ble bestemt under møtet eller hendelsen.

Å skrive et referat er en viktig del av effektiv kommunikasjon og organisasjon. Det sikrer at viktig informasjon blir registrert, delt og fulgt opp på en systematisk måte. I tillegg til grunnene over (som er skrevet av Copilot) er dette særlig viktige for offentlige organisasjoner som utøver offentlig myndighet, da for eksempel dokumentasjonsplikt som regel ligger her. Dette finner vi en rekke eksempler på, deriblant i Forvaltningsloven §11 d. andre avsnitt som vektlegger nedtegning, nedskrivning og protokollering som en essensiell del av saksgrunnlaget i en vurdering: «Blir det ved muntlige forhandlinger,



konferanser eller telefonsamtaler av en part gitt nye opplysninger eller anførsler av betydning for avgjørelsen av saken, skal de såvidt mulig nedtegnes eller protokolleres. Det samme gjelder iakttagelser tjenestemannen gjør ved befarings m.m.».

Offentlige organisasjoner har ulike arbeidsmetodikk, interaksjon og dialog med innbyggere, og praksis rundt referatføring av interne møter. Et gjennomgående tema som også ofte er et uttrykk for frustrasjon blant ansatte, er hvor mye tid som benyttes til å føre referat eller lage oppsummeringer fra et møte. Arbeidet kan være tidkrevende, og om det tar lang tid fra møtet har vært til referatet er ferdig og godkjent kan det også ha mistet mye av sin verdi. Verktøy som Copilot kan trolig hjelpe til i hele eller deler av prosessen med å lage automatiske oppsummeringer fra et møte. Et drømmescenario er at det siste som skjer i et møte før man skilles er at man i fellesskap godkjenner den skriftlige oppsummeringen og plan for hva som skjer videre. Dette vil kunne føre til store effektiviseringsgevinster ved at offentlig ansatte kan bruke tiden sin mer konstruktivt enn å skrive møtereferat, men det vil også gi bedre kvalitet på arbeidet som gjøres.

Beskrivelse av antatt bruk av Copilot:

Du er ansvarlig for at et internt møte mellom to eller flere parter skal bli enige om noe. Du kaller inn til et digitalt Teamsmøte, eller et fysisk møte der Teamsmøte er aktivt lyttende til møtet. Møtet tas opp og transkribes. Copilot bruker transkripsjonen, informasjon i kalenderinvitasjonen og «nærliggende dokumenter» for å lage en oppsummering møtet.

Særskilte vurderinger:

- *Blir det behandlet personopplysninger: **Ja** – alle deltakere i møtet blir behandlet både med stemme, uttrykksform (dialekt), kjønn (antakelse ut fra stemmeleie) osv. I tillegg blir alle personopplysninger som deltakerne sier muntlig behandlet, og alle personopplysninger/-informasjon som Copilot finner når den leter etter «nærliggende dokumenter» fra Graph.*
- *Krav til skjerming: **Ja** – men må vurderes ut fra møtekontekst. Offentlige styremøter for eksempel har trolig ikke krav til skjerming, men hvis behandling av informasjon unntatt offentligheten må funksjonalitet kunne skruses av.*

Stegvis behandling «referatfunksjon»

Step	Standard Microsoft step description	Beskrivelse av «Steps» i REFERATFUNKSJON	Spørsmål
1	User prompts from Microsoft 365 Apps are sent to Copilot	Invitasjon til møte sendes via Outlook kalender til bestemte deltakere. Innhold og dokumenter legges ved invitasjon. Møtet gjennomføres, det blir tatt opptak og opptaket transkribes. Copilot henter transkripsjon, kalenderinformasjon og dokumenter fra Outlook	Blir opptak slettet?
2	Copilot accesses Graph and Semantic Index for pre-processing	Copilot bruker informasjon fra Outlook til å identifisere «nærliggende dokumenter» som bruker har tilgang til gjennom Graph.	
3	Copilot sends modified prompt to Large Language Model	Copilot sender all informasjon den har funnet til LLM	Er det her satt på sikkerhetsmekanismer? Sender ikke



			informasjon som er klassifisert for eksempel?
4	Copilot receives LLM response	Copilot mottar svar fra LLM	
5	Copilot accesses Graph and Semantic Index for post-processing	Copilot bearbeider mottatt informasjon fra LLM og gjør denne lesbar/tilpasset for deltakerne i møtet	Hvorfor trenger Copilot en runde til i Graphen? Oversette og bearbeide språk for eksempel, eller det andre grunner?
6	Copilot sends the response, and app command back to Microsoft 365 Apps	Utkast til oppsummering/referat fra møtet er synlig i Outlook for den som har opprettet møtet. Møteinnkaller bekrefter at innhold er ok ved ikke å gjøre noe, men kan også si «ikke bra nok» og sende inn en ny runde fra step 1. Møteinnkaller kan gi tommel opp eller ned på responsen	Hvilke aktive steg kan du ta for å akseptere eller avvise respons? Copilot bruker denne adferden til å lære seg hvordan du liker å få svar? Får alle deltakere oppsummeringen, eller kun den som har invitert til møtet? Hvor lang tid tar det?

Arbeidshypoteser og merknader før test:

- Antakelse om at dette er det Copilot «er laget for». Virker på overflaten veldig lovende, men det øyeblikket du erkjenner at dette er nesten utelukkende behandling av andre sine personopplysninger blir det utfordrende.
- Potensielt stor effektiviseringsgevinst. Automatisk oppsummering fra møter hadde vært gull, det er helt vanlig å delta på 2-6 møter hver dag. Det kan være vanskelig å huske på alt man har blitt enige om, og hva som skal følges opp til neste gang. Microsoft markedsfører denne funksjonen som en kjempegevinst, og vi «biter lett på» fordi det påvirker arbeidshverdagen til hver enkelt i stor grad.
- Funksjonalitet som påvirker arbeidshverdag? Kan gi modererende og ikke selvmodererende adferd: Hvis jeg ikke ønsker å være med på møtet fordi det blir tatt opp, får jeg da ikke lov til å være med? Påvirker dette arbeidsforholdet mitt? Kan det påvirke kollegaene mine sine oppfatning av meg? («Heine pleier ikke å like å være med på opptaksmøter, det blir vanskelig for oss, så vi inviterer han ikke» - dette trenger ikke å være reelt, men hvis jeg tenker at det kan være en realitet, dukker jeg da ikke opp eller takker nei? = selvmodererende adferd).



Refleksjonsspørsmål til «referatfunksjon»

	Ja	Nei	Vet ikke
Finnes det retningslinjer for hvilke møter man kan bruke Copilot i, og hvilke møter man ikke skal bruke Copilot i?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Klarer Copilot å identifisere hvem som sa hva og fange opp eventuell uenighet? Er det forskjell på hvordan Copilot tolker for eksempel menn, kvinner og ulike dialekter?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreslår Copilot tiltakspunkter under møtet, og inkluderes disse i referatet?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Gir Copilot en nøyaktig oppsummering selv om noen deltagere kommer inn etter møtets start?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kan Copilot svare på spørsmål om uenigheter eller reaksjoner under møtet?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bidrar Copilot til å forbedre møtedeltakernes atferd for et mer produktivt møte?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hvordan fungerer referatfunksjonen hvis noen deltakere ikke har tilgang til Copilot?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Påvirker kunnskapen om at møtet blir transkribert og oppsummert deltakernes atferd?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Use case «Saksbehandling på epost»

Selv om informasjon fra det offentlige til innbyggere i større og større grad kommer digitalt via tjenester som altinn, Digipost eller e-Boks er det fortsatt vanlig for brukere å ta kontakt med det offentlige via e-post enten direkte til saksbehandlere eller via fellesinnbokser som for eksempel postmottak@ntnu.no. Offentlige organer har generelle elektronisk adresser som nettsted, epostadresse, nummer til SMS-tjeneste eller lignende jf. eForvaltningsforskriften §3, og «alle som henvender seg til et forvaltningsorgan kan benytte elektronisk kommunikasjon, dersom forvaltningsorganet har lagt til rette for dette, det skjer på den anviste måten og ved bruk av den elektroniske adressen som forvaltningsorganet har anvist for den aktuelle type henvendelse». Elektroniske innmeldingsskjema i innbyggertjenester kan gå direkte til interne saksbehandlingssystemer og fagsystemer for videre behandling, men det er også vanlig at de kun utløser en epost som sendes til en eller flere bestemte mottakere. For det offentlige er innmeldingsskjemafunksjonalitet et nyttig verktøy for å sikre at all informasjon som er nødvendig for saksbehandling er lagt ved, innbyggeren kan være trygg på at saken havner riktig sted, og automatisk som bekreftelse på innmeldt skjema til innbygger og varsel om ny sak til saksbehandler sikrer at flyten går som den skal. Selv om det er mange fordeler, kan det være utfordringer når epostsystemer benyttes til saksbehandling, særlig når sakene inneholder personopplysninger eller annen skjermingsverdig informasjon. Eksempler på utfordringer

1. Informasjonssikkerhet: E-post er ikke den sikreste metoden for å sende og motta informasjon. Det er mulig både å kryptere innhold og digitalt signere innhold, men dette blir ofte ikke brukt (mange har for eksempel opplevd at mottaker ikke kan lese innhold du sender dem). Hvis uvedkommende får tilgang til påloggingsinformasjonen din, kan konfidensiell informasjon lett bli kompromittert. Det er også fort gjort å feilsende epost, og konsekvensene av et feiltrykk kan bli store.
2. Manglende dokumentasjon på saksflyt: E-post kan være vanskelig å spore og dokumentere hvem som har fått hvilken informasjon i forhold til mer formelle kommunikasjonskanaler, og det er lett å videresende hele eller deler av eposttråder. Brukerne har stor «råderett over informasjonsflyten» og kan for



eksempel legge til og fjerne mottakere både åpent og lukket (blindkopi). Dette kan være problematisk for det offentlige som må til enhver tid ha «kontroll på hele saksbehandlingsskjeden».

3. Manglende sletterutiner/-kultur: Mange lar eposter bare ligge i innbokser eller sortert i mapper, for eksempel «i tilfelle det blir behov for dem en gang». Det er lettere å søke i egen innboks enn i et saksbehandlingssystem. Mange er nok flinke til å slette innkomne eposter, men glemmer at også sendt-mappa og slettede elementer-mappa må tømmes for at eposten skal bli helt borte.
4. Informasjon blir borte: Når ansatte slutter blir epostbokser slettet, og hvis den ansatte ikke har arkivert informasjonen forsvinner dataene. Dette er ekstra utfordrende i langvarige saker der ansatte slutter eller bytter jobb midtveis i prosessen.
5. Misforståelser: E-post kan noen ganger føre til misforståelser da det mangler ansikt-til-ansikt kommunikasjon. Nyanser i språk og tone kan gå tapt, noe som kan føre til feiltolkninger.
6. Spam og phishing: E-post er ofte målet for spam og phishing-angrep. Dette kan føre til at viktige e-poster blir oversett eller slettet, eller at skadelig programvare blir installert på systemet.
7. Teknisk feil: Det er alltid en risiko for tekniske feil med e-post, som for eksempel at en e-post ikke blir levert, at den havner i spamfilteret, eller at vedlegg ikke blir åpnet.

Mange e-postsystemer har allerede innebygd en rekke kunstig intelligente verktøy som gir stor nytte for brukerne, for eksempel spamfilter, automatisk sortering av epost i egnede bokser og forslag til svar. Epost er et kraftig og viktig kommunikasjonsverktøy, og inneholder store mengder data om andre som har sendt epost til deg, men eposten inneholder også enormt mye informasjon om deg som eier epostinnboksen. Denne informasjonen kan brukes til andre formål, for eksempel profilering jf.

Personvernforordningen art 4 punkt 4. Eksempler (ikke utfyllende):

- All epost du har sendt gir en god beskrivelse av hvordan du uttrykker deg. Valg av språk, setningsoppbygging, uttrykk osv. Dette kan gjøre det lettere for en maskin eller andre å utgi seg for å være deg
- Analyse av e-postene dine kan brukes til å identifisere dine interesser, preferanser og vaner. For eksempel, hvis du ofte mottar e-poster om reiser, er det nærliggende å konkludere med at du er interessert i reiser. Dette innholdet kan brukes til for eksempel publikumssegmentering, slik at målrettede markedsføringskampanjer bli mer effektive. Om du blander privat- og jobb-epost blir det enda lettere.
- Svartid (hvilke eposter svarer du for eksempel raskt på) kan gi indikasjoner på hvilke personer som er viktig for deg. Hvis du er opptatt av å svare raskt på eposter fra sjefen din er du trolig mer innstilt til å gjøre som vedkommende sier, enn om en forespørsel hadde kommet fra noen andre.

Ved å tilføre nye og kraftigere kunstig intelligente verktøy inn i epostsystemene blir både fordeler og risikoelementer «giret opp». Du kan få til mer og bedre ting (økt kvalitet og effektivitet), men du kan også øke konsekvensene betydelig hvis noe uheldig skulle skje. Verktøy som Copilot klarer ikke nødvendigvis å skille mellom «god og dårlig informasjon» som et menneske vil klare, den behandler og «tygger» det den får tilgang til.



Beskrivelse av antatt bruk av Copilot:

Saksbehandler mottar en epost fra en bruker enten direkte til egen postboks, eller via fellesepostadresse til enhet (postmottak@). Bruker har en forventning om at den offentlige enheten/saksbehandleren skal gjøre noe aktivt med henvendelsen, og forventer svar innen rimelig tid. Brukeren har lagt ved nødvendig informasjon for å starte en sak, hvis ikke sender saksbehandler epost tilbake hvor mer informasjon etterspørres. Informasjon kan være både epostinnhold, vedlegg og kontaktinformasjon (epostadresse). Saksbehandler vurderer all tilsendt informasjon opp mot retningslinjer, registrerer informasjon i eventuelle fagsystemer og sender svar i retur pr epost eller annen kommunikasjonskanal. Saksinformasjon arkiveres i digitalt arkivsystem eller fysisk (utskrift).

Saksbehandler kan benytte Copilot i mange steg i denne prosessen:

- Copilot kan sjekke om all nødvendig informasjon er lagt ved (se sjekklister nedenfor for steg til steg beskrivelse)
- Saksbehandler kan spørre Copilot om informasjon fyller krav i definerte retningslinjer
- Saksbehandler kan be Copilot om å lage førsteutkast til svar og/eller vedtaksbrev ut fra definert mal

Særskilte vurderinger:

- Blir det behandlet personopplysninger: Ja – Avsender og saksbehandler. Avsender kan også ha gitt informasjon om andre (for eksempel egne barn)
- Krav til skjerming: **Ja**

Stegvis behandling «Saksbehandling på epost»:

Step	Standard Microsoft step description	Beskrivelse av «Steps» i SAKSBEHANDLING PÅ EPOST –sjekk om all nødvendig informasjon er med	Spørsmål
1	User prompts from Microsoft 365 Apps are sent to Copilot	Saksbehandler mottar en epost fra en avsender med forespørsel om at «noe» skal skje. Saksbehandler ber Copilot om å sjekke at all nødvendig informasjon er tilgjengelig ut fra definert sjekklister (i et dokument).	
2	Copilot accesses Graph and Semantic Index for pre-processing	Copilot bruker informasjon fra Outlook og lenke til definert sjekklister til å identifisere «nærliggende dokumenter» som bruker har tilgang til gjennom Graph.	Overbehandling?
3	Copilot sends modified prompt to Large Language Model	Copilot sender all informasjon den har funnet til LLM	Er det her satt på sikkerhetsmekanismer? Sender ikke informasjon som er klassifisert for eksempel?



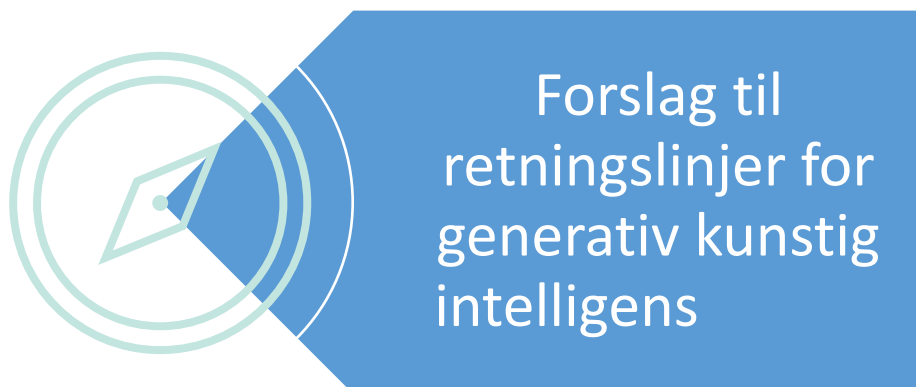
4	Copilot receives LLM response	Copilot mottar svar fra LLM	
5	Copilot accesses Graph and Semantic Index for post-processing	Copilot bearbejder mottatt informasjon fra LLM og gjør denne lesbar/tilpasset for bruker	Hvorfor trenger Copilot en runde til i Graphen? Oversette og bearbeide språk for eksempel, eller det andre grunner?
6	Copilot sends the response, and app command back to Microsoft 365 Apps	Copilot gir svar tilbake til saksbehandler om ja/nei på om all informasjon er tilgjengelig. Bruker bekrefter at innhold er ok ved ikke å gjøre noe, men kan også si «ikke bra nok» og sende inn en ny runde fra step 1. Bruker kan gi tommel ned på respons	Hvilke aktive steg kan bruker ta for å akseptere eller avvise respons? Copilot bruker denne adferden til å lære seg hvordan du liker å få svar?

Arbeidshypoteser og merknader før test:

- Avsender sender saksbehandler en epost uten å vite om at saksbehandler bruker kunstig intelligens i vurderingen. Hvis en avsender sender epost til et navn så forventer man at det er en faktisk person som svarer.
- Copilot har ulike funksjoner innebygd: Draft lager forslag til svar, Coach anbefaler innholdsvurderinger på bakgrunn av hvem mottaker, avsender, innhold osv er («Kanskje du burde være mer selvsikker i tonen siden du spør om mer lønn»). Det er ikke klart hvilke forutsetninger/regler/alignmentmodeller som ligger til grunn, men antakelsen er at dette kan oppleves som «amerikanske verdier».
- Copilot i eposten kan gi en betydelig fordel ved at saksbehandlere i større grad tar i bruk fag-/saksbehandlersystemer for å unngå kunstig intelligente verktøy.
- Copilot i epost kan være en potensielt showstopper. Vi kan få store mengder personopplysninger på avveie eller «overbehandlet» hvis ikke epostboksene er ryddet før tilgang blir gitt. Med overbehandling mener vi her at på det tidspunktet informasjonen ble sendt til meg så ble det ikke sendt med en bevissthet om at dette på et senere tidspunkt ville bli behandlet av kunstig intelligente verktøy.

Refleksjonsspørsmål til «Saksbehandling på epost»

	Ja	Nei	Vet ikke
Vet avsenderen av eposten av det benyttes kunstig intelligens i behandlingen av vedkommende personopplysninger og annen informasjon som hen har oppgitt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Har den registrerte fått informasjon om at den blir en registrert hvis den sender epost til organisasjonen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Er det tatt høyde for overbehandling av personopplysninger før det gis tilgang til Copilot?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Forslag til retningslinjer for generativ kunstig intelligens



Forslag til retningslinjer for generativ kunstig intelligens

(NB: Dette er et utkast til retningslinjer og er ikke endelig vedtatt ved NTNU. De endelige retningslinjene offentliggjøres på NTNUs nettsider når ferdig)

Retningslinjer for bruk av generativ kunstig intelligens

Sammendrag

Når du benytter en tjeneste basert på kunstig intelligens:

- Ta hensyn til informasjonssikkerhet og personvern.
- Vær klar over hvilke data som kan benyttes til ulike tjenester.
- Vær oppmerksom på feil, bias og svakheter ved bruk tjenestene.
- Ved bruk av kunstig intelligens i tekst- og bildebehandling er det viktig å være kritisk til svar verktøyet gir, og det bør henvises til det aktuelle verktøyet som kilde.
- Det er viktig å fremvise en ansvarlighet for andres data.
- Hold deg oppdatert på gjeldende lovverk.
- Bruk NTNUs godkjente verktøy.
- Ta kontakt dersom du har spørsmål eller kommentarer.

Innledning

Kunstig intelligens (KI) er et felt innen datavitenskap som fokuserer på utviklingen av intelligente maskiner. Kunstig intelligens har lenge vært benyttet på ulike områder som mobiltelefoner, digitale verktøy og tjenester, samt forbrukerapplikasjoner til ulike formål. Generativ kunstig intelligens (GKI) er maskinlæringsmodeller som kan generere innhold basert på data de har blitt trent på, eksempelvis tekst, bilder, video og kode.

- Hvorfor ønsker NTNU å tilgjengeliggjøre generativ kunstig intelligens?
 - Formålet med å tilgjengeliggjøre generativ kunstig intelligens er at ansatte og studenter kan gjøre seg kjent med ny teknologi i trygge omgivelser, og få erfaring med fordeler og ulemper rundt bruk av verktøy med kunstig intelligens.
 - NTNU vil gi ansatte og studenter mulighet til å ta i bruk kunstig intelligens på en trygg måte.
 - NTNU vil tilby tjenester som kan benyttes i forskning, undervisning, læring, vurdering og formidling.
 - NTNU vil tilby tjenester som kan styrke kvalitet og effektivitet innenfor administrative og tekniske fagområder.

Formål

Formålet med retningslinjen er å

- sørge for at ansatte, studenter og tilknyttede ressurser bruker kunstig intelligens på en trygg måte.

Gjelder for

- alle ansatte ved NTNU
- alle studenter ved NTNU
- alle som har tilgang til og/eller bruker verktøy basert på kunstig intelligens gjennom NTNUs IKT infrastruktur



Generelle retningslinjer

Sikkerhet

- Sikkerhetsbegrepet omfatter både sikker bruk av kunstig intelligens, sikkerhet for mennesker som bruker eller blir utsatt for bruk av kunstig intelligens og informasjonssikkerhet.
- Før man tar i bruk ulike verktøy må man anerkjenne at kunstig intelligens er en ny type teknologi for virksomheten. Det medfører at man bør bruke verktøy med varsomhet, og vurdere risiko for at mennesker og verdier blir skadet grunnet den enkeltes bruk av verktøy tilgjengeliggjort for NTNUs ansatte og studenter.

Informasjonssikkerhet

- Bruk av KI må til enhver tid følge NTNUs styringssystem for informasjonssikkerhet. Av retningslinjer vil følgende være gjeldende i vurderingen av KI-modeller/tjenester:
 - Risikostyring for informasjonssikkerhet
 - Klassifisering av informasjonsverdier
 - Tilgangskontroll
- Ved brudd på noen av retningslinjene, lover og regler, skal det meldes avvik i henhold til Retningslinje for avviksmelding og avvikshåndtering innen informasjonssikkerhet og personvern.
- Ved bruk av nye KI-modeller og tjenester skal det vurderes om det skal gjennomføres en risiko- og sårbarhetsanalyse (ROS).

Personvern

- Som hovedregel bør ikke personopplysninger behandles som inndata/prompts/input/opplasting i tilgjengelige verktøy basert på kunstig intelligens.
- Personvernforordningen har klare bestemmelser når det kommer til behandling av personopplysninger, blant annet krav om å sikre den registrertes rettigheter, sikre lovlighet, rettslig grunnlag og formål for behandlingen av personopplysninger.
- Ved bruk av nye tjenester basert på kunstig intelligens hvor det er usikkert om hvorvidt personopplysninger behandles eller ikke, skal det gjennomføres en personvernkonsekvensvurdering (DPIA). Gjennomført DPIA signert med godtatt risiko av systemeier må arkiveres i ePhorte.
- Se [NTNUs retningslinje for behandling av personopplysninger](#).

Hvilke data kan behandles?

- Når en tjeneste brukes må [retningslinje for klassifisering av informasjonsverdier](#) følges, og [NTNUs Lagringsguide](#) gir en god oversikt over hvilke data som kan benyttes i tjenesten. Data deles inn i fire klassifiseringer:
 - **Åpen (grønne data):** Åpen informasjon som er tilgjengelig for alle uten særskilte tilgangsrettigheter.
 - **Intern (Gule data):** Intern benyttes om informasjon som er begrenset til å være tilgjengelig for medarbeidere for å gjennomføre pålagte oppgaver.
 - **Fortrolig (Røde data):** Fortrolig benyttes dersom det vil kunne skade offentlige interesser, NTNU, enkeltindivider eller samarbeidspartnere at informasjonen blir kjent for uvedkommende.
 - **Strengt fortrolig (Sorte data):** Strengt fortrolig benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, NTNU, enkeltindivider eller samarbeidspartnere at informasjonen blir kjent for uvedkommende.



- For ulike verktøy og tjenester vil det kunne være ulike regler for hvilke data man kan bruke verktøyet til. Årsaken til dette er vurderinger gjort rundt informasjonssikkerhet og personvern for de aktuelle verktøyene.
- Det er derfor viktig at du sjekker retningslinjer for det aktuelle verktøyet før du benytter det til bruk av data.
- Klassifisering av verktøy må vurderes før det tas i bruk.
- Et eksempel er [Bing Chat Enterprise](#). NTNU har gjort grundige vurderinger av informasjonssikkerheten og personvernet, og har vurdert at du kan bruke verktøyet til data klassifisert på nivå **«Åpen» (Grønne data)** og **«Intern» (gule data)**.

Åpenhet

- Åpenhet og forklarbarhet er viktige elementer å hensynta i bruken av kunstig intelligens i arbeidssammenheng og studier.
- NTNU er en offentlig virksomhet og er derfor underlagt [offentleglova](#) og [forvaltningsloven](#). Offentleglova legger til rette for at offentlige virksomheter er åpne for å styrke informasjons- og ytringsfriheten. Forvaltningsloven gir generelle regler om behandlingsmåten i offentlig forvaltning.
- Bruk av verktøy basert på kunstig intelligens omfattes også av [Personvernforordningen](#) (GDPR).
- Det kan være vanskelig å forklare utfall og resultater ved bruk av kunstig intelligens i eksempelvis avgjørelser som omhandler andre personer eller enheter dersom man har brukt kunstig intelligens i saksbehandling.
 - Dette kan medføre at det er vanskelig for de som blir direkte påvirket av beslutninger fattet med bruk av KI-verktøy å håndheve sine rettigheter, eksempelvis retten til innsyn, sletting, retting og rettigheter ved automatiserte avgjørelser etter Personvernforordningen eller retten til innsyn etter Offentleglova.
- NTNU anbefaler at kunstig intelligens ikke brukes som verktøy i forbindelse med beslutninger eller å fatte avgjørelser som involverer andre personer eller beslutninger som påvirker NTNUs virke.

Bruk av eksterne KI-verktøy funnet på internett

- Det er kun **åpne / grønne data** som kan brukes i andre tjenester enn de som tilbys fra NTNU.
- Vær svært varsom og kritisk til eksterne tjenester.
- NTNU anbefaler ikke at man benytter eksterne tjenester i NTNU-sammenheng, vurder først om NTNUs tjenester kan brukes til formålet.

Etiske vurderinger

- Diskriminering og bias/forutinntatthet.
 - Ved bruk av kunstig intelligens finnes det en risiko for diskriminering. Årsaken ligger i dataen modellen er trent på. Hvis treningsdataene er et resultat av eksempelvis historiske skjevheter eller feil i datainnsamling kan dette resultere i at bruken av kunstig intelligens vil diskriminere grupper eller individer.
 - Eksempel: Språkmodeller som er trent på en tekst som inneholder diskriminerende mønstre kan reprodusere resultater basert på disse fordommene.
 - Bias i kontekst kunstig intelligens kan beskrive uønskede skjevheter og mønstre i datasett.



- Viktig å kjenne til rammeverket som Likestillings- og diskrimineringsloven setter
- Verdigrunnlag
 - I forbindelse med bruk av språkmodeller (LLM) er det viktig å ta i betraktning at språkmodellene er trent på data fra internett og som regel fra andre land enn Norge. Man vil derfor kunne få svar basert på andre verdier enn det norske samfunnet er basert på.

Bruker du kunstig intelligens i tekstbehandling?

- Når du benytter språkmodeller i tekstbehandling, er det viktig å tenke gjennom en del aspekter rundt arbeidet med teksten:
 - En språkmodell genererer svar ut ifra hvilke ord som passer sammen statistisk sett – den vil derfor ikke kunne presentere fakta på samme måte som et søk i søkemotorer på internett.
 - Du må være kritisk til svar språkmodellen gir deg. Du må regne med at språkmodellen genererer tekst med feilaktig informasjon, men fremstilt på en autentisk måte.
 - Du må anta at referansene språkmodellen bruker kan være feilaktige.
 - Du må gjøre en manuell kontroll av svaret språkmodellen gir deg, før du videreformidler eller bruker svaret den har gitt deg i en annen sammenheng.
 - Husk at du gjerne ikke får samme svar to ganger – ikke bruk språkmodellen til oppgaver som krever integritet.
 - Ved bruk og videreformidling av svar bør tekst generert av en språkmodell merkes med at teksten/oppgaven er løst med hjelp av KI. Les mer om å [henvise til store språkmodeller her](#). Ved bruk av KI i akademisk arbeid må det henvises til verktøyet som kilde.
 - Ikke bruk språkmodellen til å behandle saker om studenter eller ansatte.

Bruker du kunstig intelligens i bildebehandling?

- Når du benytter kunstig intelligens i bildebehandling, er det viktig å tenke gjennom en del aspekter rundt arbeidet med bildene:
 - Ikke generer bilder eller video av andre personer uten samtykke. Bilder som identifiserer personer, er også personopplysninger og omfattes av Personvernforordningen (GDPR).
 - Ved bruk og videreformidling av bilder/videoer generert av kunstig intelligens bør bildet/videoen merkes med at arbeidet er skapt ved hjelp av KI.
 - KI-genererte bilder kan også være omfattet av opphavsrett, se derfor dokumentasjon fra tjenesten om hvordan tjenesten forholder seg til opphavsrett.

KI for kodegenerering/programvareutvikling

- Ved bruk av språkmodeller til å generere kode er det viktig å tenke gjennom følgende:
 - Kunstig intelligens i programvareutvikling og kodegenerering bør kun være en støtte i arbeidsprosessen.
 - Utvikleren må gjøre en kvalitetssjekk av koden og vurdere om den kan settes i produksjon.



- Det er viktig å ha et bevisst forhold til hvilken språkmodell som benyttes til kodegenerering – språkmodeller har ulik kvalitet.
- Vær bevisst på sikkerhet i forbindelse med generering av kode. Koden som blir generert kan inneholde sårbarheter som kan skade NTNUs digitale infrastruktur.
- Vær bevisst på språkmodellens opphavsland ved generering av kode.

Henvisninger til lovverk

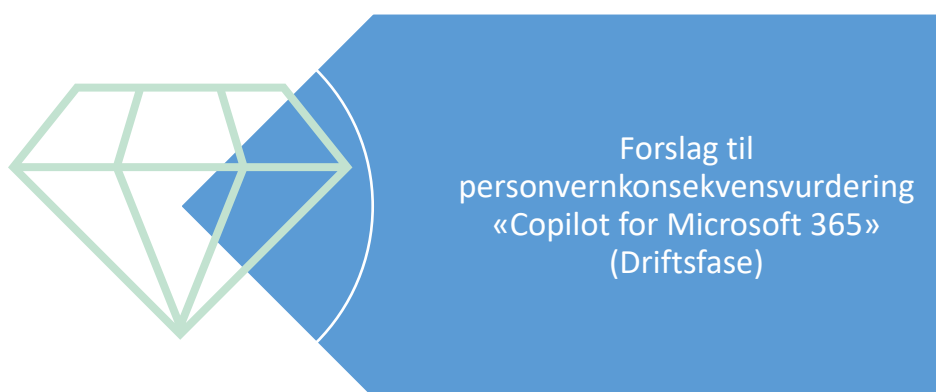
- [Personvernforordningen](#)
- [Offentleglova](#)
- [Forvaltningsloven](#)
- [Arbeidsmiljøloven](#)
- [Likestillings- og diskrimineringsloven](#)
- [KI-forordningen/AI Act](#)

Trenger du hjelp?

- [Veiledning for ansvarlig utvikling og bruk av kunstig intelligens i offentlig sektor](#)
- Få hjelp fra rådgivere ved Seksjon for læringsstøtte og digitale tjenester, Uniped, Universitetsbiblioteket og IT-avdelingen gjennom [NTNU Hjelp](#).

Se også

- [Informasjonssikkerhet – retningslinjer](#)
- [Retningslinje for behandling av personopplysninger](#)
- [NTNUs lagringsguide](#)



PROSJEKT

Pilotere Copilot for Microsoft 365 i Datatilsynets regulatoriske sandkasse



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 (Ansvarlig 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 kostnadskreven 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 ivare tatt 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">• 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 av gjennomførte møter (kan også være fysiske møter i rom hvor Teams lytter inn)• 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. Personopplysninger kan da genereres i M365 Copilot sin respons.
--	--



	<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>
Hvordan skal personopplysningene lagres?	<p>Personopplysningene som behandles av M365 Copilot lagres på ulike måter:</p> <ul style="list-style-type: none">• 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• 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 <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>
Hvordan skal personopplysningene brukes?	<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 Microsoft-tjenester og indekserer innhold og signaler fra de fleste Microsoft 365-applikasjoner i organisasjonen din. Når du søker</i></p>



	<p>etter noe, bruker Microsoft Graph indeksen til å rangere de mest relevante resultatene basert på personlige forbindelser og sosiale relasjoner.</p> <p>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.</p> <p>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.</p> <p>Se utfyllende vurdering: Punkt 1.2 og 1.3 «Behandlingens art og behandlingens omfang»</p>		
Hvem skal ha tilgang til personopplysningene?	Microsoft som databehandler NTNU som behandlingsansvarlig		
Hvem skal det samles inn personopplysninger om?	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)	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.	
Hvordan kan den registrerte utøve sine rettigheter?	Retten til informasjon vil bli ivaretatt ved å informere om behandling av personopplysninger i personvernerklæringen til NTNU.	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. Tilgangene som M365



	<p>Copilot har inngår i datagrunnlaget med personopplysninger som Microsoft vet om NTNUs brukere.</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?	Ja! - M365 Copilot vil kontinuerlig bearbeide og analysere brukernes data. Den vil bearbeide de dataene den får tilgang til, og en bruker vil ikke kunne merke at behandlingen skjer.
Brukes det ny teknologi eller ny bruk av eksisterende teknologi hvor personvernkonsekvenser ikke har blitt vurdert?	For UH-sektoren er dette ny teknologi. Verktøyene som er valgt er ikke nye «for verden», men ganske tidlig i utviklingsløpet og teknologien utvikler seg fortløpende.

3. Behandlingens omfang

Kategorier av personopplysninger som behandles	<p>M365 Copilot vil behandle samme data som Microsoft 365 plattformen i tråd med NTNUs lagringsguide (https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide) 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 epostkasser, chatter etc. M365 Copilot kan også behandle data fra web og M365 Copilot sin kommando ut mot web kan inneholde personopplysninger. 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>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.</p> <p>Antall registrerte involvert i behandlingen vil avhenge av hvorvidt NTNU tilgjengeliggjør tjenesten for eksempelvis 10, 50, 100 brukere, alle ansatte (8000) eller alle ansatte og studenter (tilsvarer 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	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.
Behandlingsfrekvens	Kontinuerlig. 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.
Lagringstid for personopplysningene	<p>Personopplysningene som behandles av M365 Copilot lagres på ulike måter:</p> <ul style="list-style-type: none">• 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• [...] <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 opererer med «retention policies» (retningslinjer for oppbevaring) som kan administreres på ulike måter for de</p>



	<p>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> (https://i.ntnu.no/wiki/-/wiki/Norsk/Vurdere+personvernkonsekvenser)</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>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.</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</p>



	<p>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></p> <p>og</p> <p><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>
Vil personopplysningene viderebehandles til nye eller andre formål?	<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.

Hvilke kilder brukes for innhenting av personopplysninger?	<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/gjestebukere 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 & 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 https://innsida.ntnu.no/wiki/wiki/Norsk/Personvernerklæring+NTNU</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>
Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel	<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>Office 365 (SharePoint, Teams, Onedrive) er klassifisert opp til fortrolig jf. NTNUs lagringsguide https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide så fremt innholdet er kryptert med AIP.</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. Det er sannsynlig at M365 Copilot vil kunne finne på ting som både er usann og feilaktig.</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>Ja, den registrerte vil i en del behandlinger ha en særskilt forventning om privatliv.</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>Ja, det kan forekomme behandling av personopplysninger om personer som defineres som sårbare, eksempelvis barn, pasienter, forskningsdeltakere etc.</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 kompetansmiljø 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) https://i.ntnu.no/wiki/-/wiki/Norsk/Kunstig+intelligens+i+undervisning+og+vurdering</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 https://snl.no/språkmodell (05.06.2024): «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 telle forekomster av ordkombinasjoner eksplisitt, bruker man i dag nevrale 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">• Dutch scandal (<u>diskriminerende algoritmer</u>)• Eksamensjuks• Forvaltningsrevisjon fra Riksrevisjonen: <u>Bruk av kunstig intelligens i staten</u>• Diskriminering, manglende likebehandling osv osv. For eksempel https://www.bufdir.no/aktuelt/ny-rapport-lite-kunnskap-og-kompetanse-om-kunstig-intelligens-og-diskriminering/ <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 gjøre det lettere for studentene å jukse. Det kan brukes til å «koke oppgaver», henvise til feil referanser og tolke innhold helt feil. «Gode formuleringer» fra verktøyet kan være direkte sitat fra kjente og ukjente kilder, og studenter kan bli tatt for plagiat/tekstlikhet selv om de aldri en gang har lest den faktiske teksten.</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. Dette bør tas med i prosjektvurderinger.</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 (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,</p>



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 [...]»

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.

6. Identifisering og oversikt

Behandlingsansvarlig:	NTNU
Felles behandlingsansvarlig:	<p>Nei</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>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</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 internt 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 eksterne 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 – Berettiget interesse</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 tilgjengelig 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>Ved bruk av tredjepartsapplikasjoner, Dataverse + power platform og plug-ins kan overføring til tredjeland forekomme. 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>https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-retningslinjer</p> <ul style="list-style-type: none"> • Retningslinje for arbeid med sikkerhetskultur og opplæring • Retningslinje for avviksmelding og avvikshåndtering innen informasjonssikkerhet og personvern • Retningslinje for behandling av personopplysninger • Retningslinje for digital beredskap, hendelses- og krisehåndtering • Retningslinje for informasjonssikkerhet i leverandørforhold • Retningslinje for klassifisering av informasjonsverdier • Retningslinje for kryptografiske kontroller • Retningslinje for nettverks- og informasjonsoverføring • Retningslinje for operativ sikkerhet • Retningslinje for risikostyring for informasjonssikkerhet • Retningslinje for sikring av personlig IKT-utstyr • Retningslinje for tilgangskontroll
<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. Vilråene 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>
---	---



	<p>Se skisser over dataflyt i «<i>Utfyllende vurdering: Punkt 1.8 – Dataflyt, lagring og mellomlagring</i>» og i punkt 3 i DPIA</p>
<p>Hvor og hvor lenge lagres personopplysningene ulike steder?</p>	<p>Innstillinger for lagring, mellomlagring og sletting er tilgjengelig for organisasjonens administratører. 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>
<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>«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>
<p>Er personopplysningssikkerheten tilstrekkelig ivaretatt?</p>	<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. <i>Se utfyllende vurdering: Punkt 1.8 B – Personopplysningssikkerhet»</i>
--	---

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">• Tilganger/tilgangsstyring må være korrekte• Klassifisering av informasjon (labels i M365 applikasjoner)• Prompt injection attacks• Sikkerhetskultur <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 gjenbruker samme teknologi som er godt kjent i Microsoftplattformen.
Har virksomheten bygget systemet fra grunnen av eller er det kjøpt ferdig (som hyllevare) fra ekstern leverandør og deretter installert hos dere?	Ekstern tjeneste i sky (SaaS – «Software as a service»).
Er programvaren utviklet med innebygd personvern og personvern som standardinnstilling?	Leverandøren beskriver hvordan de mener personvern er ivaretatt 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.

- *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 – Skjermbilde 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 reindeksere innhold kontinuerlig for eksempel? Vil reindeksering føre til endret oppfatning/tolkning av innhold i et dokument som igjen kan gi et annet svar seinere?*

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 1.4 – 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, behandlingsomfang 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



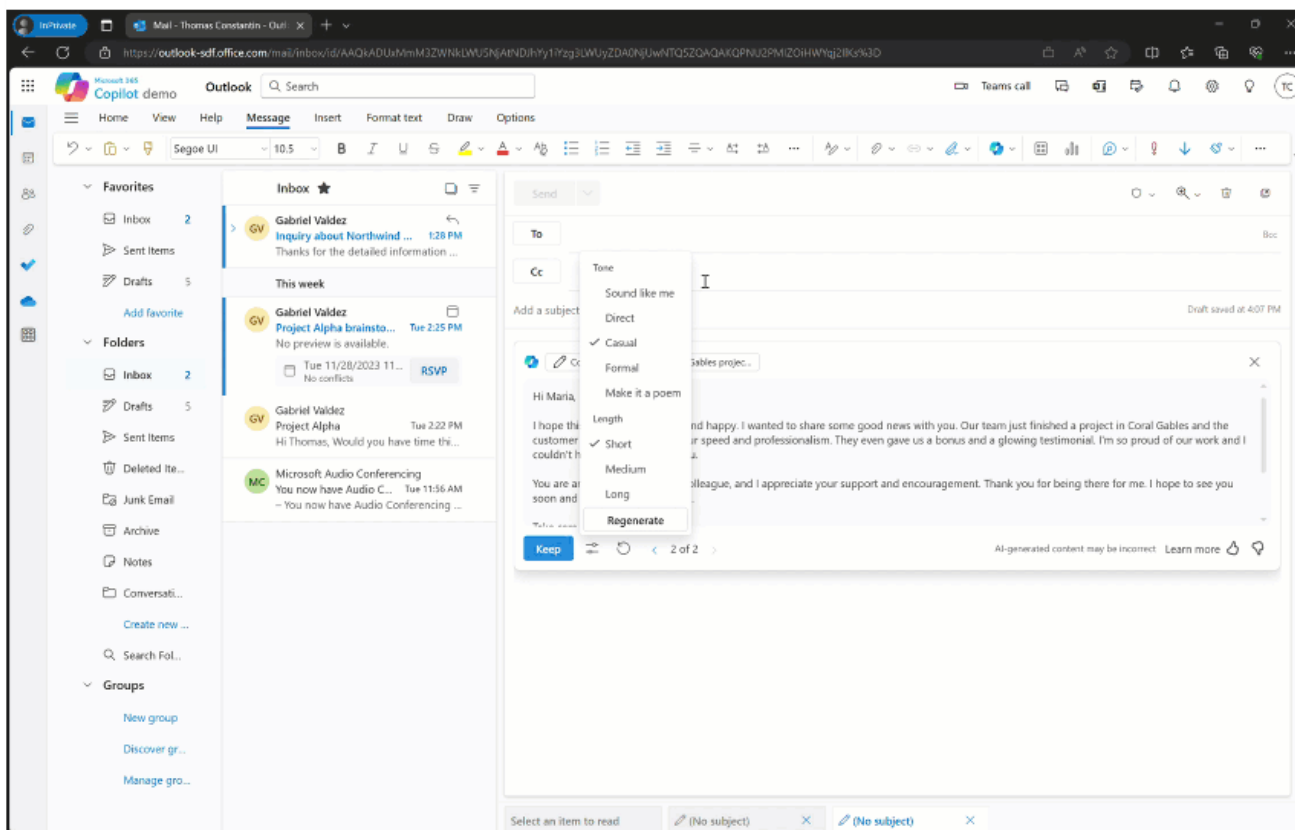
Microsoft-verktøy. Dette kan gjøres gjennom eksisterende rammeverk og oversikt over saksprosesser i protokoll/behandlingsoversikt. Bruk av verktøy med innebygd kunstig intelligens og M365 Copilot særskilt må kartlegges, dokumenteres og vurderes pr. saksprosess av den prosessansvarlige.

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.

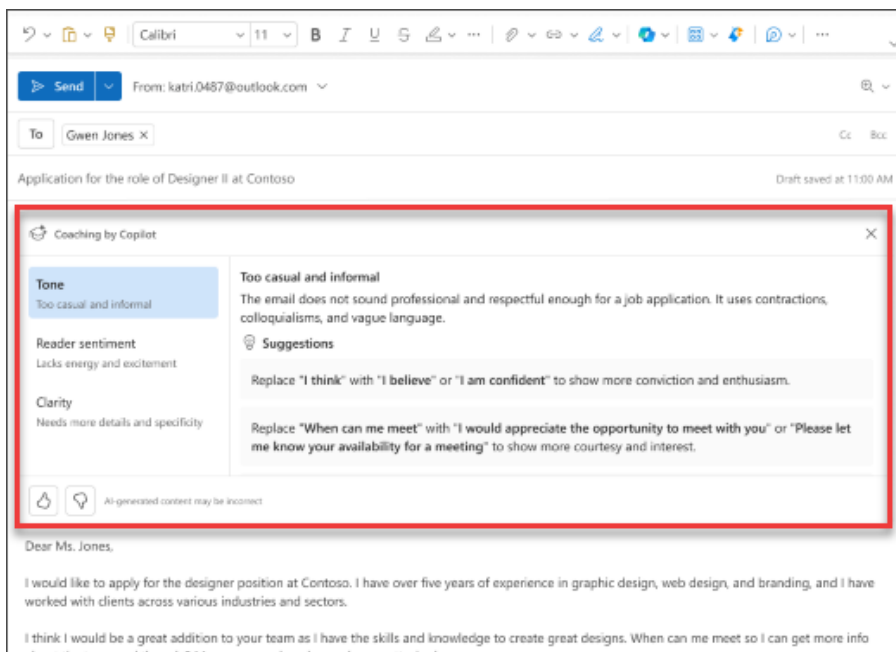


Copilot helps you draft a message that sounds like you

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

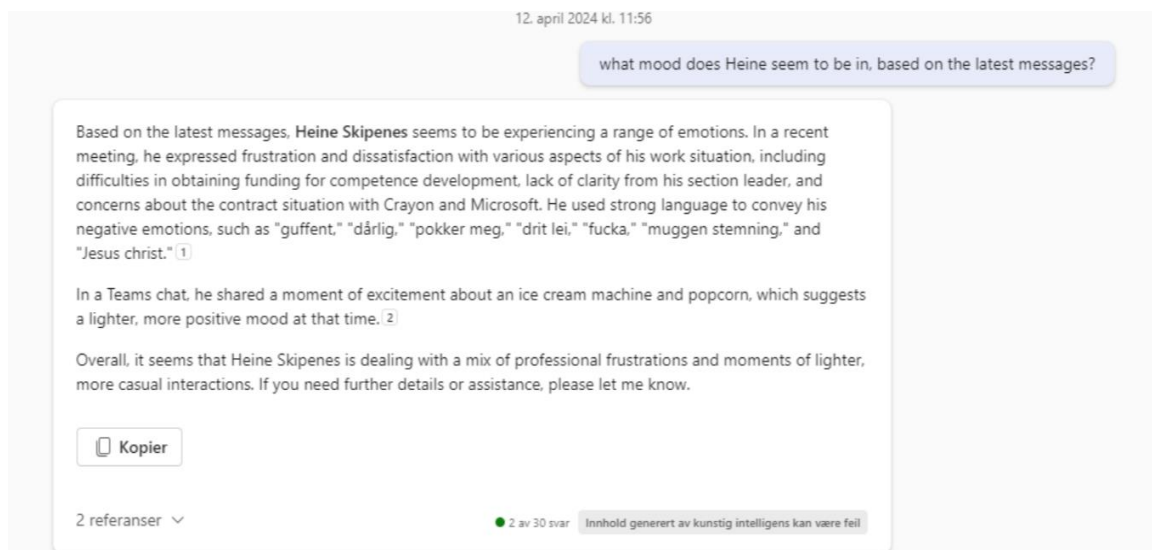
Coaching

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.

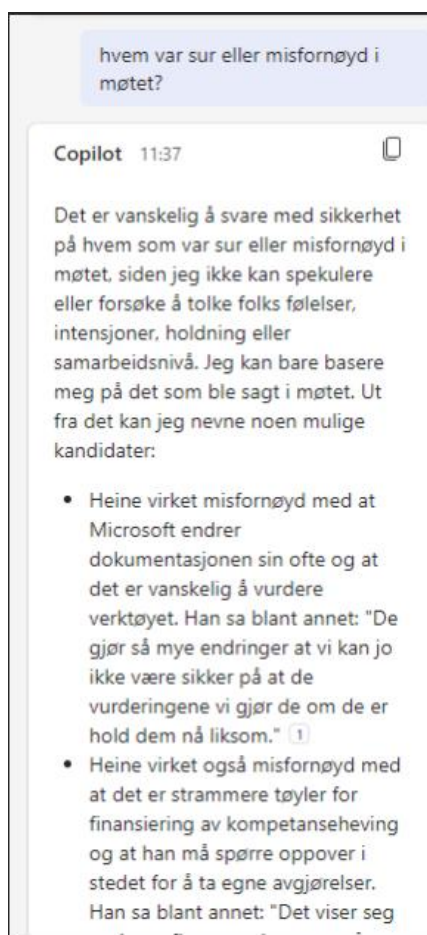


Figur: Skjerm bilde «Coaching by Copilot» (kilde: Microsoft)

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 risikoreduserende 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](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

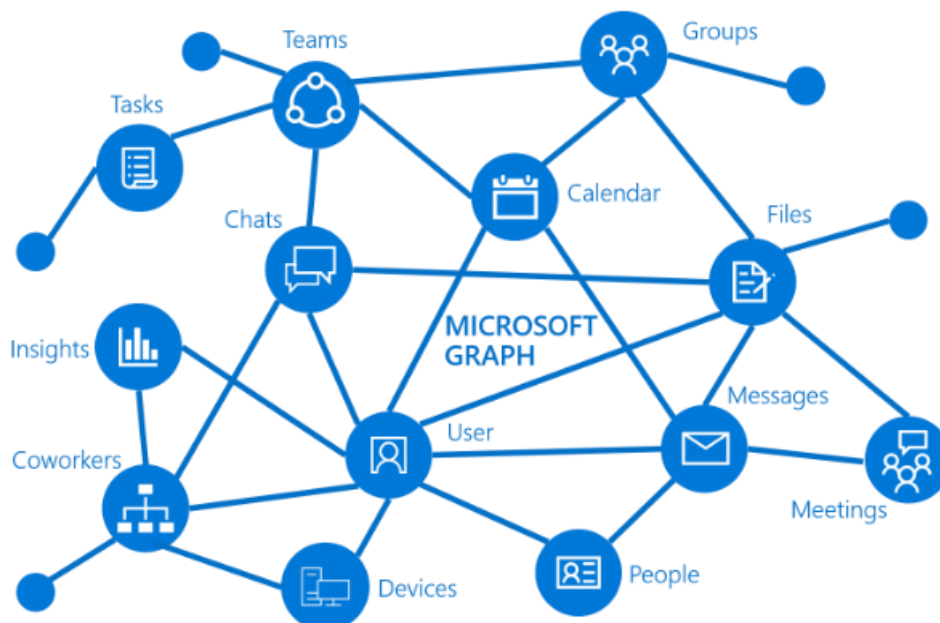
Merknader:

- *Ansatte har tjenstlig behov for behandling av personopplysninger (utøvelse av offentlig myndighet)*
- *Ansatte, studenter og gjestebbrukere 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:

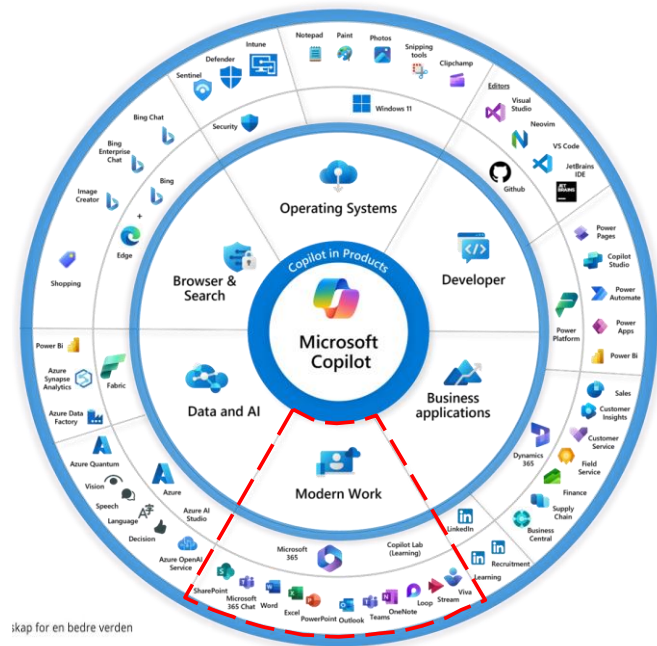
- Vurdere om plugin for web bør deaktiveres. Kan redusere funksjonaliteten av verktøyet for mange brukere.
- Gjør vurdering av rettslig grunnlag



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.

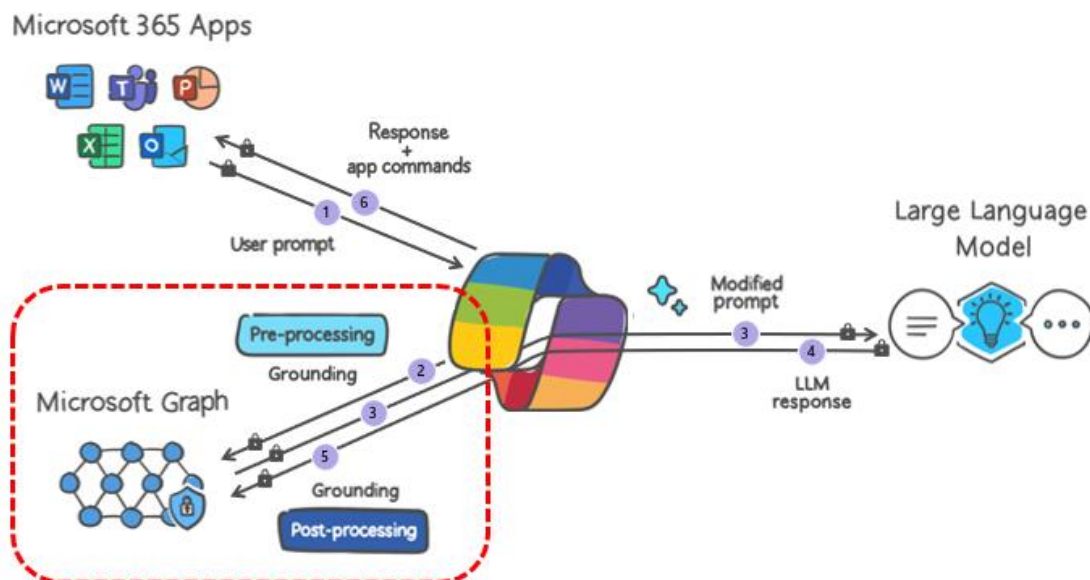
Denne vurderingen tar utgangspunkt i applikasjoner som faller innunder Microsofts beskrivelse av egne tjenester som «Modern work-plattformen» (se figur 1).



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 gjennomganger, og kommandogenerering.

Svaret returneres til appen for brukerens vurdering. Brukerens ledetekst og Copilots svar beskrives som "innholdet i samhandlinger", 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, samhandlinger 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.

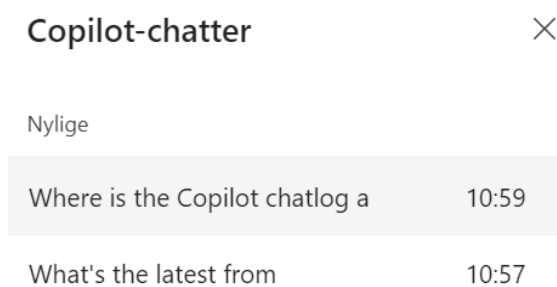
Microsoft har utarbeidet fem prinsipper for bevaring og sletting av data. Prinsipp nr. 1 tilsier at bevaring av data alltid overgår policier for sletting. Det vil si, hvis eksempelvis en epost har flere «conflicting retention policies», vil alltid bevaringspolicyen overgå slettepolicyen.

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 aksesseres 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 aksesseres 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 – Skjermbilde av brukers chatlog



Figur – Skjermbilde 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.

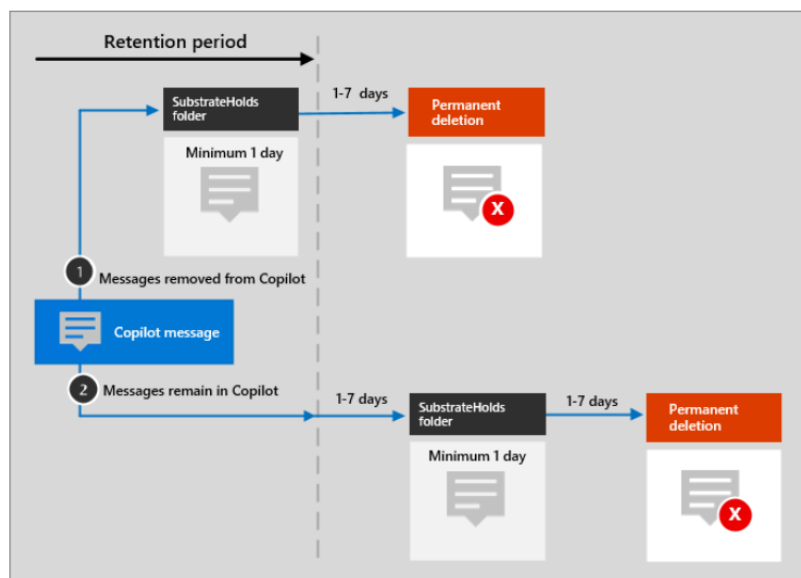
Forklaring av de to veiene i diagrammet:

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 risikoreduserende 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. Utilsiktet 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?	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. <i>Se utfyllende vurdering: Punkt 2.1.2 – Formålsbegrensning</i>
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 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.
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.



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 brukers 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">- Administratorene i M365 teamet holder en korrekt og oppdatert oversikt over alle brukere i brukerdatatabasen i form av tilgangsstyring via Entra ID.- 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. <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>
Vurder innhenting av samtykke, jf. art 7 og 8	<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>
Vurder hvordan den registrertes rett til innsyn og til dataportabilitet ivaretas, jf. art. 15 og 20	<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.</p> <p>Utfyllende informasjon på https://innsida.ntnu.no/wiki/-/wiki/Norsk/Personvernerklæring+NTNU</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>
Vurder hvordan den registrertes rett til korrigerings og sletting ivaretas, jf. 16 og 17	<p>De registrerte har rett til å få uriktige personopplysninger rettet eller slettet og ufullstendige personopplysninger komplett. 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>
Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas, jf. art. 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.
Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering, håndheves, jf. art. 22	<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 profilering 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



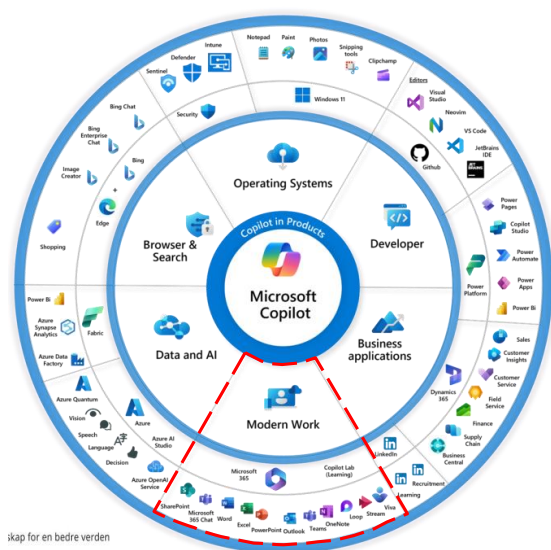
personopplysninger og bruken av verktøy med innebygd kunstig intelligens. M365 Copilot må vurderes for hver enkelt saksprosess av prosessansvarlige.

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.

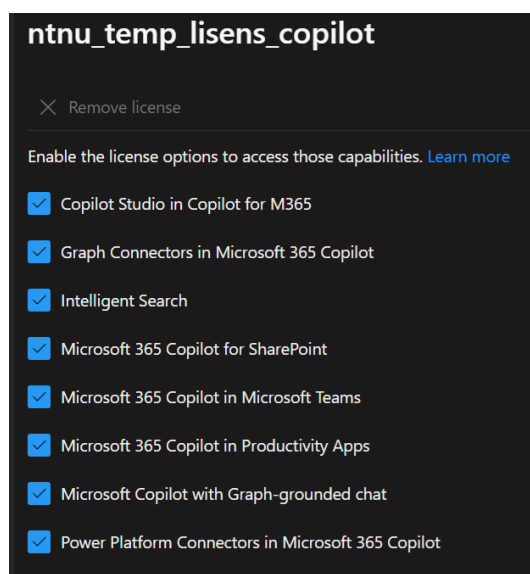
Vurder om formålet kan oppnås med en mindre inngripende behandling

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 teamsmeldingen 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

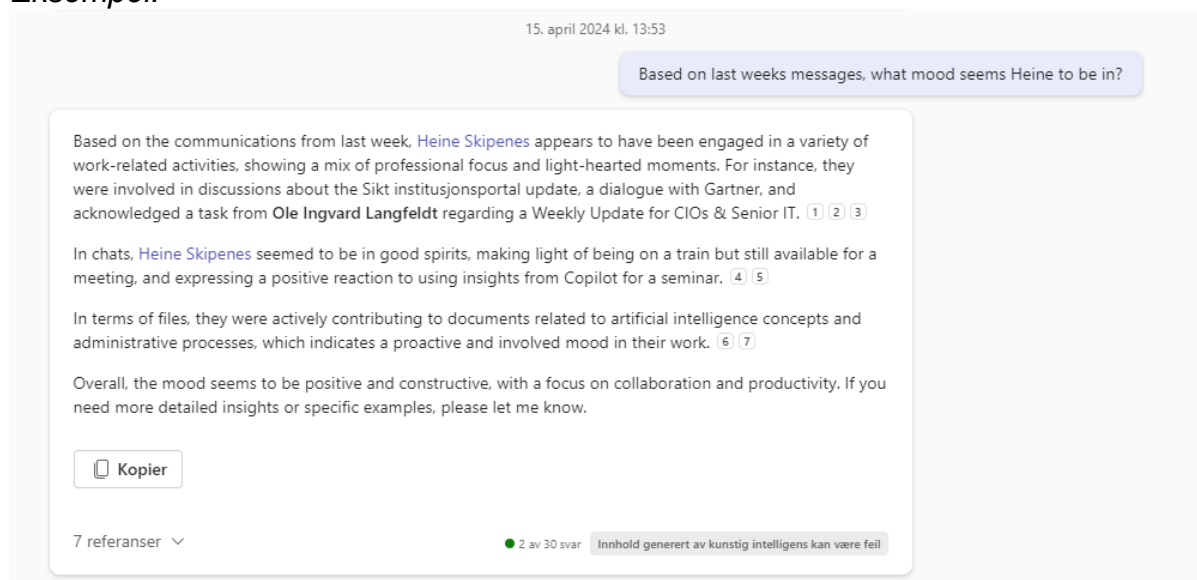
En språkmodell (large language model – LLM) vil beregne sannsynligheten for hva det neste ordet i en sammenheng er, og dermed skape en tekst som kan bestå av personopplysninger som oppfattes som ukorrekt eller udaterte. Tolkning av personopplysninger i en slik tekst er det umulig å forutse resultatet 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 risikoreduserende 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 backupløsninger 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 risikoreduserende 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 personvernkonsekvensvurderingen (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 (overvåkingmekanismer).

Innspill til risikoreduserende 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 saksbehandlingsskjede 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. **Informér 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.*



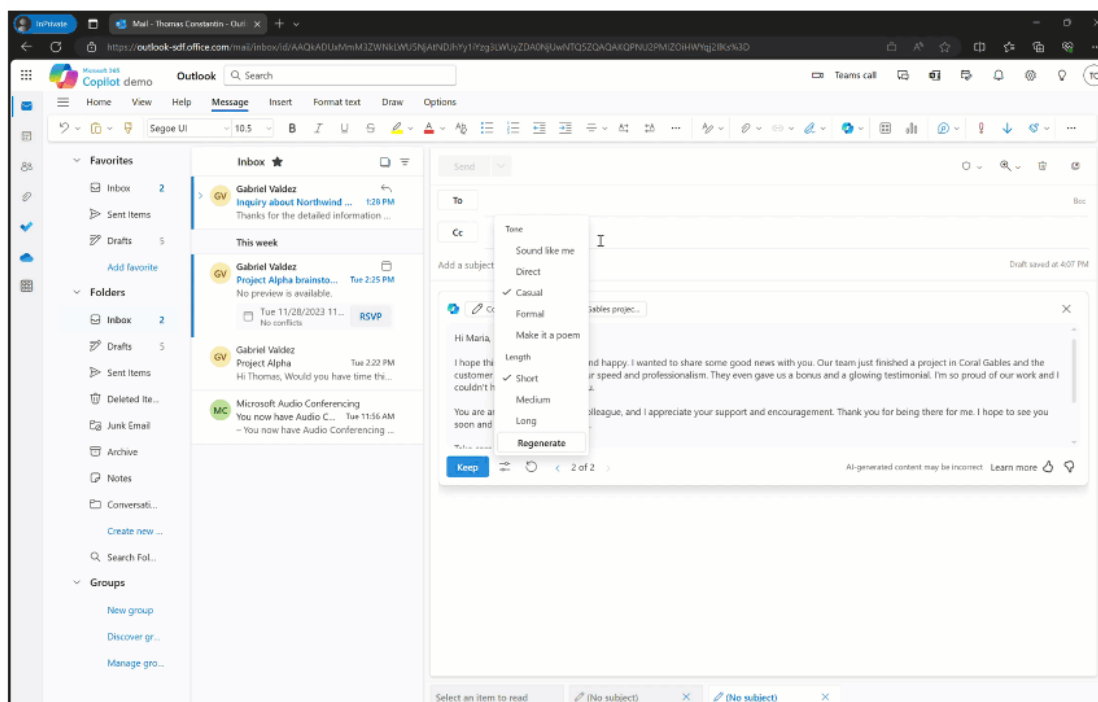
5. **Datasikkerhet:** Implementer passende tekniske og organisatoriske tiltak for å sikre datasikkerheten og beskytte den registrertes personopplysninger mot uautorisert tilgang, endring, sletting eller overføring.
6. **Regelmessig gjennomgang:** Gjennomgå regelmessig de automatiserte beslutningsprosessene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



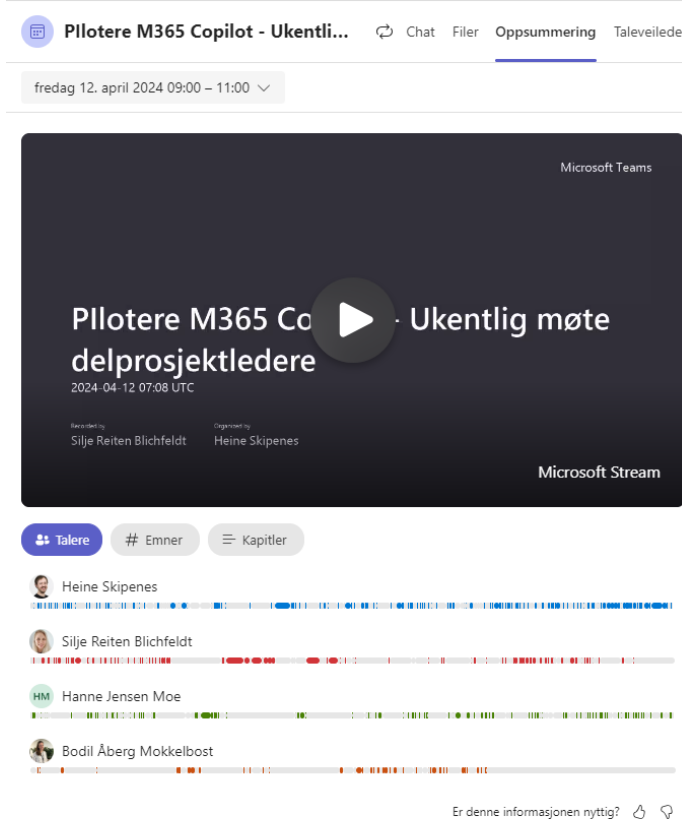
Copilot helps you draft a message that sounds like you

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.

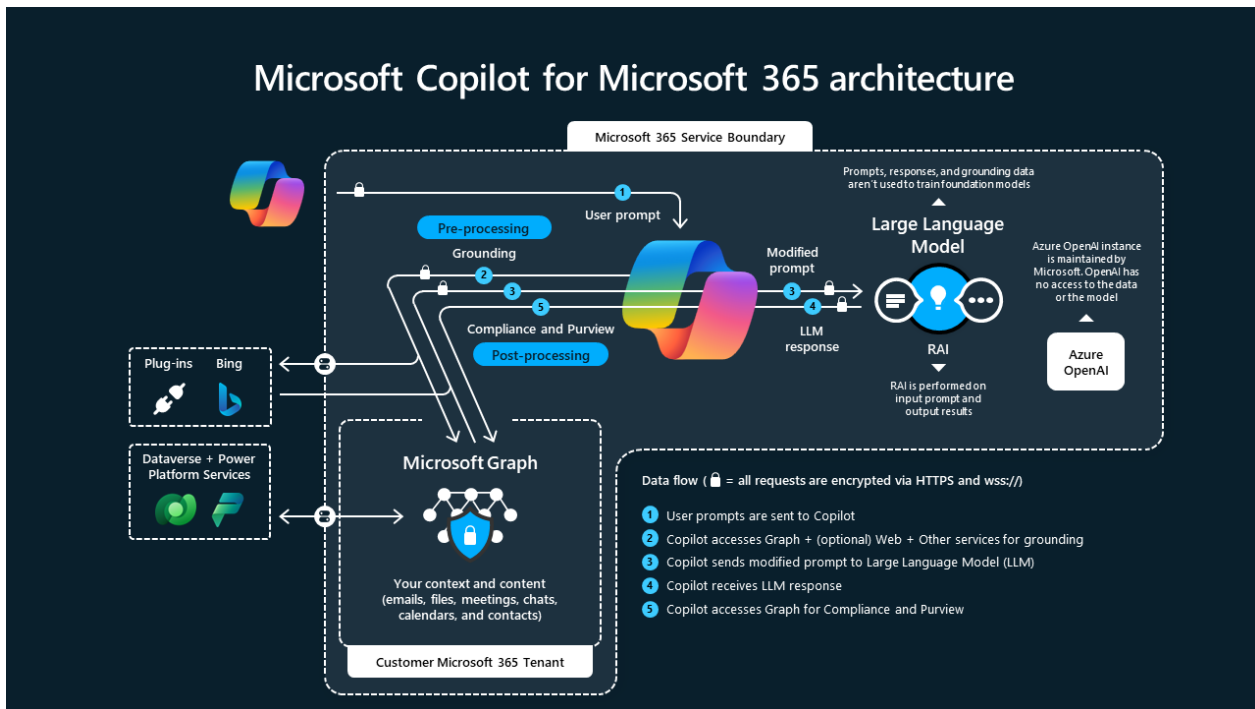
Innspill til risikoreduserende tiltaksliste i DPIA:

- 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 risikoreduserende 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. Hovedtiltak: Kan virke risikoreduserende på alle identifiserte risikoer.	<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 etablere 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	O	Etablere retningslinjer for bruk av Copilot til fagspesifikke oppgaver, for eksempel administrasjon.	[må vurderes]	[må vurderes]	
1-7	O	Utarbeide nye og oppdatere eksisterende rutiner for sletting av personopplysninger	[må vurderes]	[må vurderes]	
1-7	O	Opprette internkontrollrutiner for å sjekke etterlevelse av nye rutiner og gjennomgang av administratorers bruk av eDiscovery og Purview.	[må vurderes]	[må vurderes]	
1-7	O	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	O	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	O	Gjennomføre utfyllende interesseavveining jevnlig (I 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	O	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	O	Gjennomgå rutiner for lagring av data og internkontroll	[må vurderes]	[må vurderes]	
1-7	O	Gjennomgå kontraktsmessige forpliktelser i forbindelse med organisasjonens øvrige innhold i Microsoft 365	[må vurderes]	[må vurderes]	
1-7	O	Gjennomgå tilgangsstyringsrutiner	[må vurderes]	[må vurderes]	
1-7	O	Gjennomgå internkontrollrutiner informasjonssikkerhet.	[må vurderes]	[må vurderes]	
1-7	O	Gjør utfyllende vurdering av Microsoft som felles behandlingsansvarlig ved bruk av M365	[må vurderes]	[må vurderes]	
1-7	O	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	O	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	Skru 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 prompte 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 kjøregler bør NTNU ha?») Eksempel på saksbehandling ved NTNU: <ul style="list-style-type: none">- SESAM (06.11.2023 - se referat fra møtet til slutt i dokument) med styringssignaler for utvikling			
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.
Personvernombudsbistand 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.
Sammendrag av personvernombudets råd for driftsfase:		
IKKE GJENNOMFØRT – MÅ GJENNOMFØRES I DIALOG MELLOM SYSTEMEIER OG PERSONVERNOMBUD		
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 førersetet. Omfanget av hva som kan innhentes av opplysninger er skremmende; Det må lages gode rammer for hvordan data skal brukes av et KI-system. Det må være et reglement og retningslinjer for ansatte og studenter, med god opplæring i etikk.
- Parat. Enig i at vi må gjøre dette forsvarlig. Dersom dette verktøyet benyttes i saksbehandling, vil man ikke kunne spore alle ledd i en saksbehandlingsskjede.

Rektor lurte 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

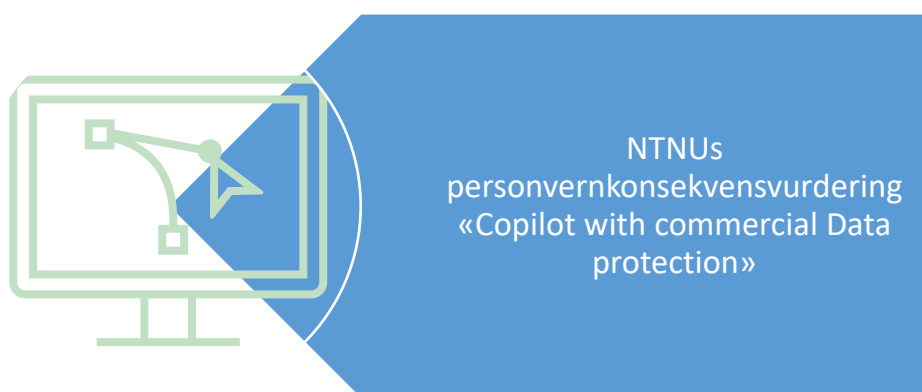
- <https://mspoweruser.com/microsoft-outlook-sound-like-me-surface-2023-event/>
- <https://learn.microsoft.com/nb-no/microsoft-365-copilot/microsoft-365-copilot-privacy>
- <https://learn.microsoft.com/en-us/graph/overview>
- <https://learn.microsoft.com/en-us/microsoftsearch/semantic-index-for-copilot>
- <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



PROSJEKT

Pilotere Copilot for Microsoft 365 i Datatilsynets regulatoriske sandkasse



NTNUs personvernkonsekvensvurdering «Copilot with commercial Data protection»

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

Merknader til den gjennomførte personvernkonsekvensvurderingen:

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

1. Systematisk beskrivelse av behandlingen

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

2. Overordnet oversikt

Beskrivelse av verktøyet:

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



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

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

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

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

1. Tilby en språkmodell for behandling av gule/interne data (ikke personopplysninger).



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

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

Hvilke personopplysninger skal behandles?

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

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

Behandlingsansvarlig

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

Databehandler

- Microsoft

Referanser:

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

3. **Behandlingens art**

Hvordan skal personopplysningene samles inn?	Hentet fra leverandørens nettsider: “Copilot is a generative AI service grounded in data from the public web in the Bing search index only. It doesn't have access to organizational resources or content within Microsoft 365, such as documents in
--	---



	<p>OneDrive, emails, or other data in the Microsoft 365 Graph.</p> <p>Copilot for Microsoft 365 is required if your organization wants a chat experience grounded in work data inside your tenant boundary.</p> <p>Copilot can access organizational content in the chat only when it's provided by users. This can be done in one of two ways:</p> <ol style="list-style-type: none">1. Users explicitly type or paste this information directly into the chat.2. Users type a prompt into Copilot in Edge after enabling the 'Allow access to any webpage or PDF' setting, and an intranet page is open in the browser. In this scenario, Copilot may use this content to help answer questions. <p>In both cases, when commercial data is enabled, Copilot doesn't retain any of this data after the chat session is over”.</p>
Hvordan skal personopplysningene lagres?	<p>Hentet fra leverandørens nettsider:</p> <p>“When organizations and employees use generative AI services, it's important to understand how these services handle user and chat data. Because employee chats may contain sensitive data, Copilot is designed to protect this information.</p> <ul style="list-style-type: none">• Copilot uses Microsoft Entra ID (formerly known as Azure Active Directory) for authentication and only allows users to access Copilot with commercial data protection using their work account.• An Entra ID user's tenant and user information is removed from chat data at the start of a chat session. This information is only used to determine if the user is eligible for commercial data protection. Search queries triggered by prompts from an Entra ID user aren't linked to users or organizations by Bing.• Microsoft doesn't retain prompts or responses from Entra ID users when using Copilot. Prompts and responses are maintained for a short caching period for runtime purposes. After the browser is closed, the chat topic is reset, or the



	<p>session times out, Microsoft discards prompts and responses.</p> <ul style="list-style-type: none">• Chat data sent to and from Copilot with commercial data protection is encrypted in transit (TLS 1.2+) and at rest (AES-128) during the chat session. Microsoft has no 'eyes-on' access to it.• Because Microsoft doesn't retain prompts and responses, they can't be used as part of a training set for the underlying large language model. <p>“Commercial data protection means user and organizational data are protected, prompts and responses are not saved, Microsoft has no eyes-on access, and chat data isn't used to train the underlying large language models. Unlike Copilot for Microsoft 365, Copilot has no access to organizational data in the Microsoft 365 Graph”.</p>
Hvordan skal personopplysningene brukes?	<p>Den registrertes brukernavn brukes kun til pålogging og bekreftelse på autentisering.</p> <p>Personopplysninger som en bruker selv legger inn, blir kun brukt i den chatsesjonen som gjennomføres. Personopplysningene lagres ikke.</p>
Hvem skal ha tilgang til personopplysningene?	Microsoft
Hvem skal det samles inn personopplysninger om?	Ansatte og studenter som tar i bruk løsningen. De må logge seg på med brukernavn (ikke aktiv pålogging, det går av seg selv når du er logget på andre Microsoft-tjenester).
Hvordan kan den registrerte utøve sine rettigheter?	<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 https://innsida.ntnu.no/wiki/-/wiki/Norsk/Personvernerklæring+NTNU</p> <p>Det blir i tillegg utviklet en egen modul for innsyn etter GDPR gjennom prosjektet NTNU Sak, og tilgangen til Copilot inngår i datagrunnlaget med personopplysninger som Microsoft vet om NTNUs brukere.</p>
Vil det være systematisk behandling av personopplysninger?	Nei



Brukes det ny teknologi eller ny bruk av eksisterende teknologi hvor personvernkonsekvenser ikke har blitt vurdert?	For sektoren er dette ny teknologi. Verktøyene som er valgt er ikke nye «for verden», men ganske tidlig i utviklingsløpet og teknologien utvikler seg fortløpende.
---	--

4. **Behandlingens omfang**

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

5. **Behandlingens formål**

Behandlingens formål	Formålet med løsningen er: <ol style="list-style-type: none">1. Tilby en språkmodell for behandling av gule/interne data (ikke personopplysninger).<ol style="list-style-type: none">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.
----------------------	---



	<p>a. Å tilby det samme verktøyet til både studenter og ansatte slik at fagspesifikk opplæring kan gis i ordinær undervisning</p> <p>b. Å tilby et verktøy raskt nok til at det kan inngå i undervisningsplanleggingen for våren 2024</p> <p>3. Tilby en teknisk løsning hvor vi samtidig tilgjengeliggjør informasjon om hvordan vi har tenkt risikovurdering og personvern</p> <p>Formålet med behandlingen av personopplysningene er å identifisere brukere av løsningen, slik at brukeren kan få tilgang. Ytterligere behandling av personopplysninger gjøres ikke systembasert. Den enkelte bruker kan legge inn, bearbeide og laste ned personopplysninger den selv har lagt inn i løsningen.</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?	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

6. Sammenhengen behandlingen utføres i (kontekst)

Hvilke kilder brukes for innhenting av personopplysninger?	<p>Brukernavn hentes fra brukerdatabase «Active directory» (AD)/Entra ID.</p> <p>Andre personopplysninger er det enten bruker selv som har lagt inn i chatsesjonen, eller de finnes tilgjengelig på internett.</p>
--	--



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



	samfunnet en stund, og NTNU har tidligere laget retningslinjer for spesielle områder allerede (eksamen og undervisning) https://i.ntnu.no/wiki/-/wiki/Norsk/Kunstig+intelligens+i+undervisning+og+vurdering
Beskriv eventuelle relevante fremskritt innen teknologi eller sikkerhet	<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 nevrale 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 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>
Finnes det noen nåværende tilfeller av allmenn bekymring for den beskrevne måten å behandle personopplysninger på?	<p>Ja, i aller høyeste grad. Dette gjelder særlig i forbindelse med utøvelse av offentlig myndighet:</p> <ul style="list-style-type: none">• Dutch scandal (<u>diskriminerende algoritmer</u>)• Eksamensjuks• Forvaltningsrevisjon fra Riksrevisjonen: <u>Bruk av kunstig intelligens i staten</u>• Diskriminering, manglende likebehandling osv osv. For eksempel https://www.bufdir.no/aktuelt/ny-rapport-lite-kunnskap-og-kompetanse-om-kunstig-intelligens-og-diskriminering/ <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 som det er viktig at er godt kjent i organisasjonen.</p>



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

7. Identifisering og oversikt

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

8. Mottakere av personopplysninger

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



<p>Hvis ja, hva er det rettslige grunnlaget for det?</p>	<p>«Copilot is a connected service where Microsoft is the data controller. Users' prompts leave your organization's Microsoft 365 tenant boundary to reach the Copilot service. When commercial data protection is enabled, Microsoft doesn't retain this data beyond a short caching period for runtime purposes. After the browser is closed, the chat topic is reset, or the session times out, Microsoft discards all prompts and responses”.</p> <p>“To provide chat responses, Copilot uses global data centers for processing and may process data in the United States. Optional, Bing-backed connected experiences don't fall under Microsoft's EU Data Boundary (EUDB) commitment. Learn more: Continuing Data Transfers that apply to all EU Data Boundary services. They also don't fall under the terms of Enterprise Subscription Agreements (EAS) or Campus and School Agreements (CASA) which may require company data to remain inside geographic or tenant boundaries.</p> <p>As a reminder, Copilot has no access to organizational data inside your tenant boundary, and chat conversations aren't saved or used to train the underlying models.</p> <p>Organizations with strict requirements that data must remain inside tenant or geographic boundaries should instead consider Copilot for Microsoft 365 or Azure Open AI to provide generative AI services. Copilot with commercial data protection is intended as a more secure alternative for organizations than using consumer-oriented generative AI services.</p> <p>For more information, see Microsoft 365 Data Residency and the Microsoft Privacy Statement».</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>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.</p> <p>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. NTNU har ikke inngått en egen databehandleravtale med Microsoft.
Gir databehandleren tilstrekkelige garantier for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen, vil gjennomføres?	<p>Hentet fra leverandørens nettsider:</p> <p>“Microsoft as the data controller Copilot is a connected service where Microsoft is the data controller. Users' prompts leave your organization's Microsoft 365 tenant boundary to reach the Copilot service. When commercial data protection is enabled, Microsoft doesn't retain this data beyond a short caching period for runtime purposes. After the browser is closed, the chat topic is reset, or the session times out, Microsoft discards all prompts and responses.</p> <p>To provide chat responses, Copilot uses global data centers for processing and may process data in the United States. Optional, Bing-backed connected experiences don't fall under Microsoft's EU Data Boundary (EUDB) commitment. Learn more: Continuing Data Transfers that apply to all EU Data Boundary services. They also don't fall under the terms of the Data Protection Addendum (DPA) which requires company data to remain inside geographic or tenant boundaries.</p> <p>As a reminder, Copilot has no access to organizational data inside your tenant boundary, and chat conversations aren't saved or used to train the underlying models.</p> <p>Organizations with strict requirements that data must remain inside tenant or geographic boundaries</p>



should instead consider Copilot for Microsoft 365 or Azure Open AI to provide generative AI services. Copilot with commercial data protection is intended as a more secure alternative for organizations than using consumer-oriented generative AI services.

For more information, see [Microsoft 365 Data Residency](#) and the [Microsoft Privacy Statement](#).”

“Chat data sent to and from Copilot with commercial data protection is encrypted in transit (TLS 1.2+) and at rest (AES-128) during the chat session. Microsoft has no 'eyes-on' access to it. »

“GDPR

The [May 21, 2018, blog post](#) from Microsoft outlines our commitment to GDPR compliance and how Microsoft helps businesses and other organizations meet their own GDPR obligations. You can find more details in the [Microsoft Trust Center FAQ](#).

Copilot aligns with GDPR principles. Customers who wish to submit a right to be forgotten request to remove information from the Bing search index can do so here: [Bing - Request Form to Block Search Results in Europe](#)”

9. Dataflyt, lagring og mellomlagring

Hvordan overføres og tilgjengeliggjøres personopplysningene?	Når den registrerte ønsker å bruke verktøyet går hen til et nettsted som kjører en spørring mot NTNUs brukerdatabase (Active directory) for å bekrefte at bruker er ansatt eller student ved NTNU. Da skjer dette: <ol style="list-style-type: none">1. Hvis bruker ikke finnes avvises forespørselen og løsningen starter ikke2. Hvis bruker finnes gis det tilgang til tjenesten og brukernavnet slettes.
--	--



<p>Hvor og hvor lenge lagres personopplysningene ulike steder?</p>	<p>Microsoft beskriver at de kun tar vare på personopplysninger i «kort» tid.</p> <p>Hentet fra leverandørens nettsider: An Entra ID user's tenant and user information is removed from chat data at the start of a chat session. This information is only used to determine if the user is eligible for commercial data protection. Search queries triggered by prompts from an Entra ID user aren't linked to users or organizations by Bing”.</p>
<p>Hvor lenge lagres personopplysningene etter at formålet ved behandlingen er over, før de slettes? Når skal opplysningene slettes? Er det utarbeidet sletterrutiner?</p>	<p>Hentet fra leverandørens nettsider: “Microsoft doesn't retain prompts or responses from Entra ID users when using Copilot. Prompts and responses are maintained for a short caching period for runtime purposes. After the browser is closed, the chat topic is reset, or the session times out, Microsoft discards prompts and responses”.</p>
<p>Er personopplysningssikkerheten tilstrekkelig ivaretatt?</p>	<p>Ja, for klassifiseringsnivå «åpen» og «intern» i henhold til styringssystem for informasjonssikkerhet.</p>

10. Informasjonssikkerhet

<p>Gjennomgå den funksjonelle beskrivelsen av alle behandlinger og om alle aktiva som skal brukes er identifisert</p>	<p>Følger samme logikk som andre tjenester fra Microsoft. Det er gjennomført en egen risiko- og sårbarhetsvurdering av tjenesten fra Seksjon for Digital sikkerhet.</p>
<p>Tas ny teknologi i bruk, eller brukes eksisterende teknologi på en ny måte?</p>	<p>Ny teknologi tas i bruk, men tilgang og driftsteknologi gjenbraker samme teknologi som er godt kjent i Microsoftplattformen.</p>
<p>Har virksomheten bygget systemet fra grunnen av eller er det kjøpt ferdig (som hyllevarer) fra ekstern</p>	<p>Ekstern tjeneste i sky (SaaS – «Software as a service»).</p>



leverandør og deretter installert hos dere?	
Er programvaren utviklet med innebygd personvern og personvern som standardinnstilling?	Ja. Leverandøren har på sine nettsider beskrevet tydelig hvordan personopplysninger blir behandlet.

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>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</p>
--	--



	nasjonal rett - normalt lov eller forskrift. I denne sammenheng er flere supplerende rettsgrunnlag i universitets- og høyskoleloven: <ul style="list-style-type: none">- § 1-3 om universitetets oppgaver- § 4-2 om utdanningsplan- § 4-3 om studentenes læringsmiljø- § 4-15 om Innhenting og behandling av personopplysninger i studieadministrative systemer
Kommer det rettslige grunnlaget/behandlingsgrunnlaget tydelig frem for de registrerte?	Nei, det er ikke direkte tydelig for den registrerte å se sammenhengen mellom det rettslige grunnlaget og dette konkrete verktøyet. Dette er en problemstilling som gjelder for tilgangen til alle IKT-tjenester på NTNU.
Omfatter rettslig grunnlag både egne formål og eventuell utlevering?	Det vil ikke være mulig å utlevere data.
Vurder hvordan åpenhet ivaretas i behandlingen	Generelt rett til innsyn i egne personopplysninger etter personopplysningsloven (GDPR-innsyn). I tillegg kommer NTNU til å være åpen med denne personvernkonsekvensvurderingen på egne informasjonssider og gjennom utsendt informasjon til alle ansatte og studenter.

2.1.2 Formålsbegrensning

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

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

2.1.3 Dataminimering

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

Vurder om formålet kan oppnås med mindre datainnhenting	Nei. Det er kun brukernavn som brukes og det slettes med en gang. Systemer
---	--



	må kontrollere at bruker finnes for å kunne gi tilgang til tjenesten, og dette skjer gjennom kontroll av brukernavnet.
Begrunn nødvendighet og relevans relatert til formål for hver enkelt variabel i et datasett	Det er bare 1 variabel og den er absolutt nødvendig for å kontrollere at bruker eksisterer i brukerdatabase.

2.1.4 Riktighet

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

Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering	Todelt: <ul style="list-style-type: none">- Brukernavn holdes korrekt og oppdatert i Active Directory/Entra ID, og kontrolleres gjennom andre kjernesystemer på IT-avdelingen.- Tolkning av personopplysninger som bruker selv legger inn er umulig å forutse resultatet av fra sesjon til sesjon. Det er stor sannsynlighet for at språkmodellen kan gi ulike og feilaktige svar
Vurder om dere har nødvendig funksjonalitet for å rette og slette uriktige opplysninger	Ja. Løsningen sletter data etter kort tid. I og med at hovedkilden til informasjon er «internett» vil det ikke være mulig å slette innhold uten å ta kontakt med eierne av nettsteder der informasjonen ligger.
Ut ifra den registrertes perspektiv, er det behov for kontradiksjon?	Nei. Det ligger i dette verktøyets natur å kunne gi uriktige opplysninger. Behandlingsansvarlig ønsker at den registrerte skal ta aktivt stilling til informasjonen løsningen gir, og være grunnleggende kritisk til informasjonen som en språkmodell gir.

2.1.5 Lagringsbegrensning

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

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



historisk forskning eller for statistiske formål, jf. art. 89 nr. 1.	
--	--

2.2 De registrertes rettigheter

Vurder hvordan informasjon til de registrerte gis	<p>Informasjon blir sendt ut til alle ansatte som melding til kanal «alle ansatte» og «studenter».</p> <p>Det er opprettet egne wikisider som beskriver verktøyet og behandlingen av personopplysninger: Norsk: https://i.ntnu.no/wiki/-/wiki/Norsk/Copilot</p> <p>Engelsk: https://i.ntnu.no/wiki/-/wiki/English/Copilot</p> <p>Se også NTNUs personvernerklæring</p>
Vurder innhenting av samtykke, jf. art 7 og 8	<p>For ansatte: Behandlingen er ikke direkte samtykkebasert med et dokument som «signeres/aksepteres før bruk», men gjennom å ta i bruk tjenesten hvor du har fått informasjon på forhånd bør dette kunne vurderes som en form for samtykke. Den registrerte kan velge å la være å bruke tjenesten, og ved å gå ut av tjenesten blir alle personopplysninger borte. Personopplysninger som bruker selv aktivt har hentet ut (klipp og lim) må behandles i tråd med øvrige retningslinjer og informasjonssikkerhetsregelverk i organisasjonen.</p> <p>For studenter: Samme vurderingsgrunnlag som for ansatte, men med unntak i undervisningssammenheng hvor faglærer sier at studentene skal ta verktøyet i bruk.</p>
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). I og med at opplysninger ikke lagres er det ikke behov for å vurdere dataportabilitet.</p>

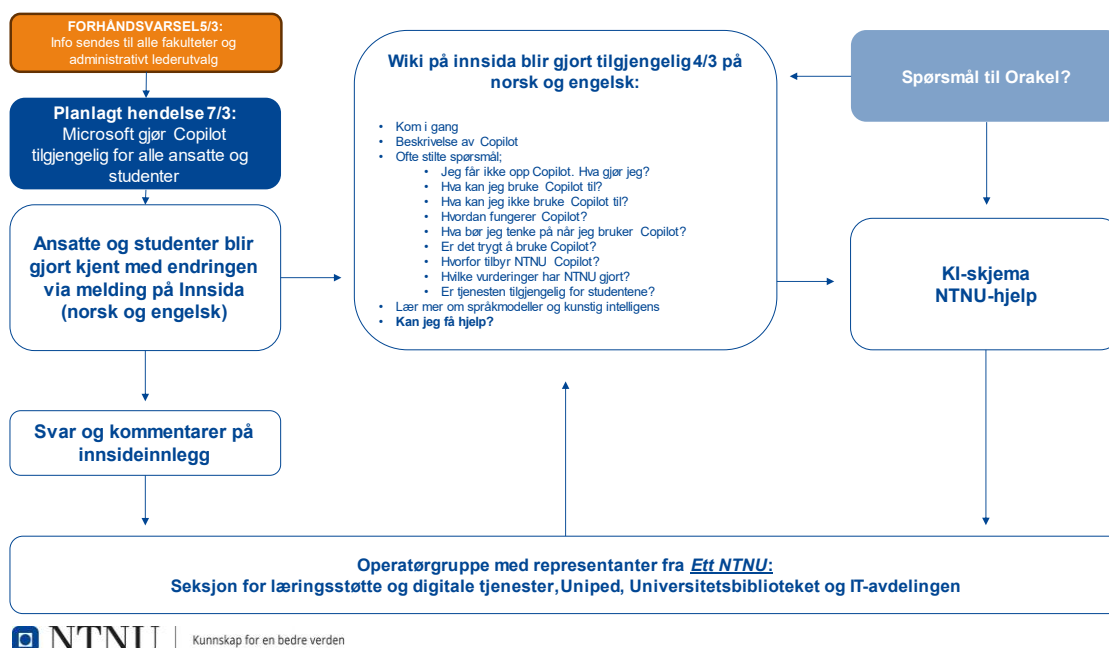


Vurder hvordan den registrertes rett til korrigerings og sletting ivaretas, jf. 16 og 17	I og med at opplysninger ikke lagres er det ikke behov for å vurdere behov for korrigerings og sletting.
Vurder hvordan den registrertes rett til innsigelser og begrensning av behandling ivaretas, jf. art. 18, 19 og 21	I og med at opplysninger ikke lagres er det ikke behov for å vurdere rett til innsigelser og begrensning av behandling. En bruker kan velge ikke å ta verktøyet i bruk
Vurder hvordan forbud mot automatiserte individuelle avgjørelser, herunder profilering, håndheves, jf. art. 22	<p>Formålet med løsningen er at ansatte og studenter i virksomheten skal få tilgang til en språkmodell som kan benyttes for interne data. Det skal være en form for «sandkasse» hvor ansatte og studenter kan gjøre seg kjent med ny teknologi og dens fordeler og ulemper, og prøve ut løsningen på egne arbeidsoppgaver som de kan kjenne seg igjen i.</p> <p>Verktøyet skal ikke benyttes til noen form for automatiserte avgjørelser om individer. Dette vil løsningens brukere bli informert om i form av opplæring og retningslinjer for bruk.</p> <p>Verktøyet er en samtalerobot laget med kunstig intelligens, og kan brukes fritt av ansatte og studenter i virksomheten. Det er ikke mulig å sikre at ingen av løsningens brukere benytter løsningen til for eksempel å foreslå innhold til et beslutningsnotat, eller formulere et første utkast til et enkeltvedtak som er bestemmende for rettigheter og plikter. Hvis verktøyet benyttes til eksempler nevnt over, vil man ikke kunne spore alle ledd i en saksbehandlingsskjede uten at saksbehandler eksplisitt informerer eller gjøre rede for at kunstig intelligens er benyttet.</p> <p>I retningslinjer og gjennom opplæring vil det påpekes at løsningen ikke skal benyttes til dette.</p>



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

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



Identifiserte og vurderte risikoer:

Beskriv risikoen behandlingen har for de registrertes rettigheter og friheter, og hvilke konsekvenser den har for de registrerte	Alvorlighetsgrad for risikoen	Identifiser trusler som kan føre til hendelser	Sannsynlighet for at en hendelse oppstår
En bruker tar usann informasjon som sann og bruker dette i en annen kontekst. For eksempel som del av interne utredninger, vurdering, begrunnelser som skal danne grunnlag for beslutninger eller som fakta i arbeid med oppgaver eller eksamen.	<i>Alvorlig</i>	Manglende opplæring eller lav kompetanse hos bruker	<i>Mulig</i>
Manglende samsvar mellom den registrertes rettigheter og den behandlingsansvarliges plikter etter Personvernforordningen (GDPR) For eksempel manglende rett til innsyn, sletting osv	<i>Minimal</i>	Manglende informasjon	<i>Liten</i>
En bruker legger inn noen andre sine personopplysninger som kommer på avveie	<i>Minimal</i>	Manglende opplæring eller lav kompetanse hos bruker	<i>Liten</i>



Tjenesten er ikke bra nok for våre brukere. Brukere ønsker seg verktøy som tar vare på data over tid og som kan «lære deg å kjenne». Denne funksjonaliteten kan ikke tilfredsstilles med krav til sletting, og det er risiko for at andre verktøy tas i bruk uten tilstrekkelig kunnskap om hva dette innebærer	<i>Minimal</i>	Manglende informasjon. Manglende opplæring eller lav kompetanse hos bruker	<i>Mulig</i>
Risiko for at studenter blir tatt i fusk, (plagiat, tekstlikhet osv) ved bruk av dette verktøyet.	<i>Minimal (for organisasjon, men alvorlig for enkeltstudenten)</i>	Manglende informasjon. Manglende opplæring eller lav kompetanse hos bruker	<i>Mulig</i>

Identifiserte risikoreducerende og skadebegrensende tiltak:

Risiko	Tiltak	Effekt på risiko	Restrisiko	Tiltak godkjent
Manglende samsvar mellom den registrertes rettigheter og den behandlingsansvarlige plikter etter Personvernforordningen (GDPR) For eksempel manglende rett til innsyn, sletting osv	Må gjennomgå NTNUs personvernerklæring for å kontrollere at informasjon til den registrerte er tydelig nok kommunisert	<i>Redusert</i>	<i>Lav</i>	<i>Må gjennomgås</i> <i>Ansvar for oppfølging Heine Skipenes</i>
Manglende opplæring eller lav kompetanse hos bruker og En bruker legger inn noen andre sine personopplysninger som kommer på avveie	Lage informasjonssider på nett norsk og engelsk om hva verktøyet er, og hva det kan brukes til Det blir opprettet en wikiside som det er mulig å finne informasjon om tekniske vurdering, risikovurderinger, personvernkonsekvensvurdering osv.	<i>Redusert</i>	<i>Lav</i>	<i>Dagens wikisider må oppdateres</i> <i>Ansvar for oppfølging Heine Skipenes</i>
Manglende opplæring eller lav kompetanse hos bruker	Legge ut melding til alle ansatte og studenter om at verktøyet nå er på plass med informasjon om hva det kan brukes til.	<i>Redusert</i>	<i>Lav</i>	<i>Må gjennomgås</i> <i>Ansvar for oppfølging Heine Skipenes</i>
Manglende opplæring eller lav kompetanse hos bruker	Tilby «å komme på besøk» til brukergupper for å informere om verktøyet og bidra til økt bevissthet om bruk av kunstig intelligens	<i>Redusert</i>	<i>Lav</i>	<i>Gjennomføres kontinuerlig på forespørsel</i> <i>Ansvar for oppfølging Heine Skipenes</i>



Manglende opplæring eller lav kompetanse hos bruker	I informasjonsmateriellet er det gitt informasjon om hvordan det er mulig å komme med tilbakemeldinger til oss som IT-avdeling, og komme med generelle tilbakemeldinger og refleksjoner om positive og negative ting med løsningen.	Redusert	Lav	Gjennomføres kontinuerlig. Kun sporadiske tilbakemeldinger så langt Følges opp fra KI-klynga i IT-avdelingen. Ansvarlig for oppfølging [koordinator]
Manglende opplæring eller lav kompetanse hos bruker	NTNU bør lage retningslinjer for bruk av generativ kunstig intelligens	Redusert	Lav	Under gjennomføring, endelig høringsfrist 1/2-24. Følges opp fra KI-klynga i IT-avdelingen. Ansvarlig for oppfølging [koordinator]
Manglende opplæring eller lav kompetanse hos bruker	Tema «hvordan skal vi forholde oss til Kunstig intelligens?», «hva slags kjøreregler bør NTNU ha?» osv har blitt behandlet i til medvirknings- og medbestemmelsesorganer: <ul style="list-style-type: none">- SESAM (06.11.2023) (* se referat https://o365addins.it.ntnu.no/RadUtvalg/Sesam/43-sesam-motet-231123-flyttes-til-271123-styr)- Administrativt lederutvalg (24.11.2023)- Formøte Studenttinget (27.11.23)- Dekanmøtet (16.11.24)	Redusert	Lav	Under gjennomføring, Ansvar for oppfølging Heine Skipenes
Tjenesten er ikke bra nok for våre brukere. Brukere ønsker seg verktøy som tar vare på data over tid og som kan «lære deg å kjenne». [...]	Alle tiltak på lista over vil bidra til risikoreduksjon: <ul style="list-style-type: none">- Informasjonsmaterieill på innsida om hva tjenesten kan brukes til, og hva det ikke kan brukes til- Retningslinjer- Opplæring I tillegg må det jobbes med videreutvikling og vurdere om NTNU også skal tilby verktøy som tilfredsstiller behovet for å ta vare på data over tid.	Redusert	Lav	Under gjennomføring, Ansvar for oppfølging Heine Skipenes
Risiko for at studenter blir tatt i fjuks, (plagiat, tekstlikhet osv) ved bruk av dette verktøyet.	Avdeling for utdanning har satt i gang et arbeid hvor en arbeidsgruppe med representanter fra alle fakultet skal se nærmere på klargjøring av rektorvedtaket om fjuks og skjema for redegjørelse for bruk av KI i arbeidet med besvarelser (deklarasjonsskjema). Grappa vil også se på behovet for kompetanseutvikling knyttet til KI i utdanningsvirksomheten.	Redusert	Lav	Under gjennomføring, Ansvar for oppfølging [seksjonsleder SLD]



4. Ledelsens validering av personvernkonsekvensvurderingen (DPIA)

Moment	Navn og dato	Kommentarer
Tiltak godkjent av:	Rektor, 27. februar 2024	IT-direktør har godkjent forrige DPIA pr. epost 21.09.2023, dokumentasjon i ePhorte.
Restrisiko godkjent av:	Rektor, 27. februar 2024	
Personvernombudsbistand gitt:	Thomas Helgesen 21.09.2023, 01.02.2024	
Sammendrag av personvernombudets råd: Innføring av Microsoft Copilot gjelder utprøving av ny teknologi, og det er viktig å ha fortsatt trykk på det som gjelder rettighetene til den registrerte. Fortsette utvikling av informasjon, opplæringsmateriell, svare på spørsmål osv, og ha tilstrekkelig med ressurser for å kunne «være der» for brukeren. En stor utfordring er hva brukerne faktisk kommer til å bruke løsningen til, og det vil ikke være mulig å kontrollere eventuell feil bruk. God kontinuerlig informasjon blir derfor viktig. Personvernombudet anbefaler ikke at verktøyet brukes til å behandle personopplysninger. Dette må fremkomme av informasjonsmateriellet som skal utarbeides Personvernombudet ønsker at det blir gjennomført kontroll av at tjenesten blir benyttet som tenkt, systematisk gjennomgang av hva brukerne spør om og revidert tiltaksliste. Personvernombudet ber om å få delta i denne prosessen.		
Personvernombudets råd er akseptert eller overprøvd av:	Rektor, 27. februar 2024	
Kommentarer: Rektor aksepterer personvernombudets råd.		
De registrertes synspunkter er innhentet og gjennomgått av:	SESAM 06.11.2023, Høringsprosess KI-retningslinjer sendt ut til alle avdelinger, fakulteter og Studenttinget.	
Kommentarer:		
Denne personvernkonsekvensvurderingen vil følges opp av:	IT-avdelingen	.



Kildeliste DPIA Tilgjengelig språkmodell for NTNU / implementere Microsoft Copilot som verktøy ved NTNU :

- [SESAM-notat 06.11.2023. Sak 81/23 «Verktøy med kunstig intelligens ved NTNU»](#)
 - [Lenke til referat fra møtet](#)
- [Wikiside på Innsida om Bing Chat Enterprise og alle vurderinger som er gjort](#)
- [Innlegg om Copilot og bruk av kunstig intelligens på KI-dagen 26.01.2024](#)
- [Melding til alle ansatte om ny kunstig intelligens chat \(22. september 2023\)](#)

Opptak av presentasjon fra møte i Kommunikasjonsnettverket 07.06.2023 (35 minutter). "[Hva er kunstig intelligens? Hva har vi og hva får vi i NTNUs verktøykasse?](#)"

Hovedtema:

 - Smakebiter fra innsiden av teknologiutviklingen
 - Hvordan bruke kunstig intelligens på en sikker og trygg måte.
 - Hvordan jobber IT-avdelingen med å utvikle og tilpasse sine tjenester?
- Artikler i Khrono
 - [NTNU med restriktive KI-retningslinjer: — Kan ikke kose på serveren](#)
- Artikler i Universitetsavisa
 - [26. oktober 2023: Ny KI-chat på banen: - NTNU er i samtaler](#)
 - [22. september 2023: Nå har NTNU KI-chat, men studentene får ikke](#)
- Regjeringens strategi: «[Nasjonal strategi for kunstig intelligens](#)»
- Godt eksempel fra IE-fakultetet (18. oktober 2023):
 - «Fakultet for informasjonsteknologi og elektroteknikk ved NTNU (IE) etablerte våren 2023 en arbeidsgruppe for å vurdere hvilke konsekvenser den raske utviklingen innen kunstig intelligens vil ha innen fakultetets utdanningsvirksomhet. Arbeidsgruppen har nå ferdigstilt sin rapport. Rapporten inneholder en god del anbefalinger som det vil bli arbeidet videre med. Det vil om få dager komme en konkretisering fra fakultetet når det gjelder om og eventuelt hvordan rapportens anbefalinger vil ha direkte betydning for bachelor- og masteroppgaver samt det pågående emne- og studieplanrevisjonsarbeidet for neste studieår.»
 - [Lenke til hele rapporten](#)



PROSJEKT

Pilotere Copilot for Microsoft 365 i Datatilsynets regulatoriske sandkasse



Steg for steg beskrivelse: Eksempel på bruk av Copilot

Funnrapporten som resulterte i de 8 overordnede funnene, er laget av Copilot with Commercial data protection gjennom å følge disse stegene. Kommandoeksemplene vi har brukt gjelder utforming av funn 1 (i kursiv), og der hvor det er gjort manuelle vurderinger av et menneske er dette understreket.

Hvordan har vi laget funnrapporten ved hjelp av Copilot?

Steg 1

Prosjektgruppa skrev et «foreløpig funn»-dokument som beskriver navnet på de overordnede funnene og enkle punktbeskrivelser/talepunkter som skulle utgjøre manus og presentasjon på fagseminaret 23. mai. Funnene er laget på bakgrunn av de faktiske testene som er gjort, vurderinger fra arbeidet med personvernkonsekvenser, innspill fra workshops med Datatilsynet osv. NB: Ingen av innspillene er laget av Copilot, kun mennesker.

Steg 2

For å skrive selve rapportinnholdet ble notatblokk-funksjonen i Copilot with commercial data protection tatt i bruk. Der kan man legge inn flere tegn enn i den ordinære samtaleroboten og du har til sammen 30 sammenhengende spørsmål/svar pr. tema.

Følgende kommando ble gitt:

«I Copilotprosjektet har vi kommet fram til 8 viktige funn. Funn 1 er " Copilot er helt glimrende når du allerede kan det du vil at den skal hjelpe deg med " og har følgende punktbeskrivelse:

- *Hvis du har full kontroll på informasjonen Copiloten bruker og du vet hva du ville ha gjort selv, så kan du avsløre når den gjør feil og du kan prompte presist nok for å full effekt.*
- *Copilot gjør at du kommer raskere i gang med oppgaven du skal løse, og setter deg tidlig på sporet. Som sparringspartner fungerer den godt, og du kan få en mer effektiv og bedre oppgaveløsning*
- *Gjør du en oppgave for første gang stiller det seg helt annerledes. Da kan du fort bruke mer tid på kvalitetssikring enn på selve oppgaveutførelsen. Betydelig risiko for å gjøre feil.*

Kan du skrive ut punktene mer utfyllende?»

Copilot skrev et svar som ble klipt ut, limt inn i Word og gjennomgått manuelt.

Steg 3

Det bearbejdede innholdet ble lagt inn på nytt i Copilot med følgende kommando:

«I Copilotprosjektet har vi kommet fram til 8 viktige funn. Funn 1 er "Copilot er helt glimrende når du allerede kan det du vil at den skal hjelpe deg med" og har følgende beskrivelse:

Når du har en dyp forståelse av informasjonen Copilot bruker, og du vet hva du ville ha gjort selv, kan du raskt identifisere når Copilot gjør feil. Dette gir deg muligheten til å korrigere feilene og gi mer presise instruksjoner til Copilot for å oppnå det ønskede resultatet. Med andre ord, din ekspertise og kunnskap om emnet kan hjelpe deg med å styre Copilot mer effektivt.



Copilot kan hjelpe deg med å komme raskere i gang med oppgaven du skal løse. Den kan gi deg et utgangspunkt, foreslå løsninger, og hjelpe deg med å strukturere arbeidet ditt. Som en sparringspartner kan Copilot bidra med ideer, foreslå forbedringer, og hjelpe deg med å se problemet fra forskjellige vinkler. Dette kan føre til en mer effektiv og bedre oppgaveløsning.

Når du gjør en oppgave for første gang, kan situasjonen være helt annerledes. Uten tidligere erfaring eller kunnskap om oppgaven, kan du ende opp med å bruke mer tid på å kvalitetssikre arbeidet enn på selve oppgaveutførelsen. Det er en betydelig risiko for å gjøre feil, siden du kanskje ikke er kjent med alle aspekter av oppgaven. I slike tilfeller kan Copilot fortsatt være nyttig, men det er viktig å være ekstra oppmerksom på kvalitetssikring.

Kan du skrive et forslag til innledning?»

Copilot skrev et svar som ble klipt ut, limt inn i Word og gjennomgått manuelt. Kvaliteten på svaret til Copilot på dette var lav, og innledningene måtte skrives om.

Steg 4

Det bearbejdede innholdet ble lagt inn på nytt i Copilot med følgende kommando:

«I Copilotprosjektet har vi kommet fram til 8 viktige funn. Funn 1 er " Copilot er helt glimrende når du allerede kan det du vil at den skal hjelpe deg med " og har følgende beskrivelse:

Copilot fungerer best når brukeren allerede har en solid forståelse av det de ønsker hjelp med. Dette funnet er delt inn i tre hovedpunkter som belyser forskjellige aspekter av denne observasjonen. Disse punktene gir innsikt i hvordan Copilot kan være et kraftig verktøy for de som allerede har en god forståelse av oppgaven de skal løse, men også hvordan det kan være utfordrende for de som prøver å løse en oppgave for første gang.

Når du har en dyp forståelse av informasjonen Copilot bruker, og du vet hva du ville ha gjort selv, kan du raskt identifisere når Copilot gjør feil. Dette gir deg muligheten til å korrigere feilene og gi mer presise instruksjoner til Copilot for å oppnå det ønskede resultatet. Med andre ord, din ekspertise og kunnskap om emnet kan hjelpe deg med å styre Copilot mer effektivt.

Copilot kan hjelpe deg med å komme raskere i gang med oppgaven du skal løse. Den kan gi deg et utgangspunkt, foreslå løsninger, og hjelpe deg med å strukturere arbeidet ditt. Som en sparringspartner kan Copilot bidra med ideer, foreslå forbedringer, og hjelpe deg med å se problemet fra forskjellige vinkler. Dette kan føre til en mer effektiv og bedre oppgaveløsning.

Når du gjør en oppgave for første gang, kan situasjonen være helt annerledes. Uten tidligere erfaring eller kunnskap om oppgaven, kan du ende opp med å bruke mer tid på å kvalitetssikre arbeidet enn på selve oppgaveutførelsen. Det er en betydelig risiko for å gjøre feil, siden du kanskje ikke er kjent med alle aspekter av oppgaven. I slike tilfeller kan Copilot fortsatt være nyttig, men det er viktig å være ekstra oppmerksom på kvalitetssikring.

Hvilke ja/nei/vet ikke spørsmål bør vi stille oss her?»



Copilot skrev et svar som ble klipt ut, limt inn i Word og gjennomgått manuelt. Copilot ga stort sett 10 spørsmål i svaret sitt, og ca. 5-7 av de var direkte knyttet til teksten og ga lite verdi, 3-5 av spørsmålene var nyttige. De nyttige spørsmålene ble tilpasset og omformulert.

Steg 5

Innholdet ble gjennomgått manuelt og kvalitetssikret av prosjektleder.

I Copilotprosjektet har vi kommet fram til 8 viktige funn. Funn 8 er "Copilot fungerer tidvis skikkelig bra" og har følgende beskrivelse: Copilot fungerer ganske bra til veldig mye forskjellig.

Gjennom hele prosjektperioden har det vært flere «Aha!-opplevelser» hvor Copilot har vist seg å være et utmerket verktøy. Rett og slett overraskende bra. Copilot er god til å trekke ut essensen fra mange store filer for å sette sammen til et nytt, mer fokusert dokument. Dette er en oppgave som ville tatt en person flere dager å starte med, men Copilot kan utføre jobben på bare noen få minutter. Dette betyr at du kan komme raskere i gang med oppgaver, og du får umiddelbar hjelp der og da. Som et verktøy for å skrive et førsteutkast, kan Copilot være svært nyttig for mange. Dette gjelder særlig oppgaver som bare trenger å være «gode nok».

Copilot har evnen til å gi referanser, men det er viktig å merke seg at du ikke kan stole blindt på disse ennå. Selv om verktøyet kan gi referanser, er det alltid lurt å sjekke disse selv for å sikre at informasjonen er korrekt og relevant. Det er forventet at denne funksjonen vil bli betydelig forbedret i fremtiden, noe som vil gjøre Copilot enda mer nyttig som et forsknings- og skriveverktøy.

Selv om Copilot er et kraftig verktøy, er det viktig å huske at du som bruker er piloten. Det er du som må stå ansvarlig for innholdet. Hvis du spør Copilot om «hvordan har du kommet fram til dette», vil verktøyet ofte ikke kunne gi et tilfredsstillende svar. Det er viktig alltid å dobbeltsjekke og verifisere informasjonen som Copilot gir.

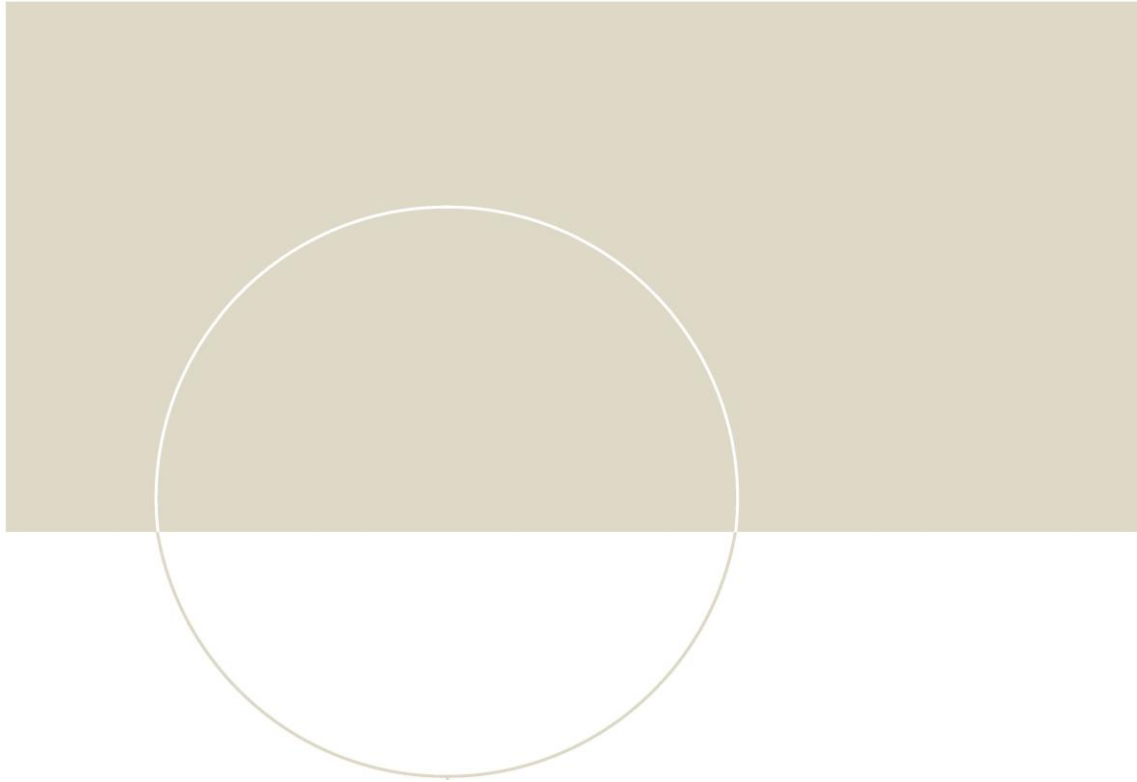
Hvilke ja/nei/vet ikke spørsmål bør vi stille oss her?

Her er noen ja/nei/vet ikke spørsmål som kan være relevante:

1. Er Copilot konsekvent effektiv i å trekke ut essensen fra store datamengder for å lage fokuserte dokumenter?
2. Er referansene som Copilot gir alltid nøyaktige og relevante?
3. Har Copilot forbedret sin evne til å gi korrekte referanser over tid?
4. Er Copilot alltid i stand til å gi et tilfredsstillende svar på hvordan den har kommet fram til et bestemt resultat?
5. Er brukeren alltid i stand til å dobbeltsjekke og verifisere informasjonen som Copilot gir?
6. Er Copilot et effektivt verktøy for å skrive førsteutkast til dokumenter?
7. Er Copilot bare nyttig for oppgaver som bare trenger å være «gode nok»?
8. Er brukeren alltid klar over at de må stå ansvarlig for innholdet som Copilot genererer?

3 av 30 svar

Figur - Skjerm bilde av kommandobilde med spørsmål og svar



This project has received funding from the European Union's DIGITAL EUROPE programme, under Grant Agreement n° 101083966.



CC BY-NC 4.0 DEED