Utdrag frå midtvegsrapport Pilot for bruk av M365 Copilot

Innhold

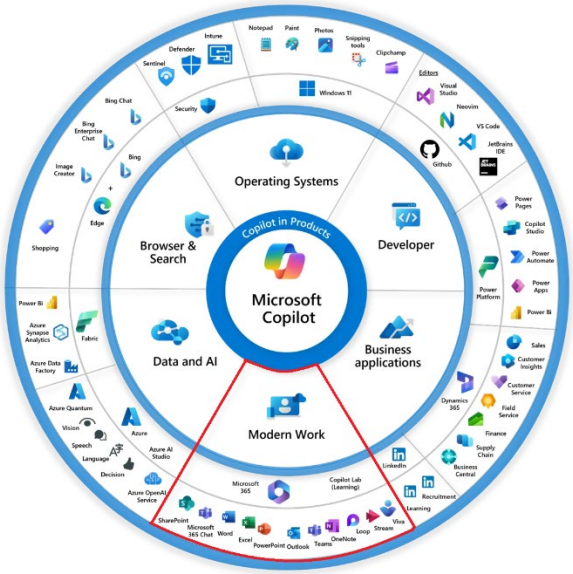
Innleiing

Vedlegget er eit utdrag frå prosjektet sin midtvegsrapport levert 27. mai 2024 og med den kunnskapen prosjektet hadde på det tidspunktet. Den må sjåast i samband med prosjektet sin sluttrapport og DPIA. Mykje av

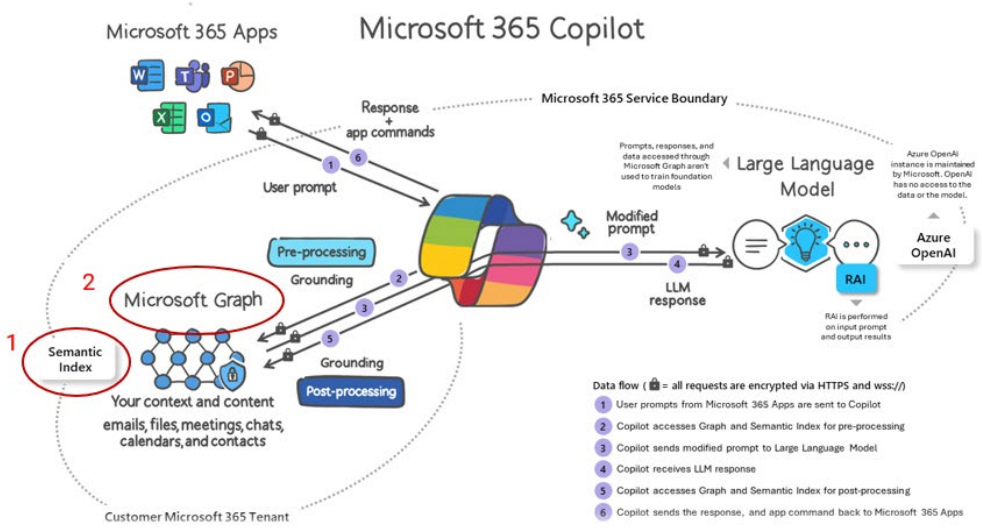
Prosjektet hadde i denne perioden tett kontakt med NTNU og deira sandkasseprosjekt, og vil takke for det gode samarbeidet og informasjonsdeling.

Korleis fungerer M365 Copilot

Copilot er Microsoft sin nye merkevare innan KI, og er å finne i alle produkta deira som symbolet . M365 Copilot er betegnelsen for Copilot integrasjon i Smart Work pakken illustrert under, også kjent som Microsoft Office 365.



Meir spesifikt er M365 Copilot ein KI-assistent som vil vere tett integrert produkt som Word, Outlook, PowerPoint, Teams og Excel. Den vil ha same tilgang til data du som brukar har. Med utgangspunkt i desse tilgangane ser M365 Copilot på kva du etterspør og nyttar informasjon den har tilgjengeleg og kombinerer dei saman med store språkmodellar (LLM, generelt omtalt som KI) til å gi svar. Om du til dømes spør «Ranger personar etter kor mange e-postar eg har sendt dei og lag samandrag av samtalen mellom dei», vil den lese alle e-postane og chattane dine og deretter oppsummere og rangere dei. Den kan også oppsummere innhald i nylege chattar og e-postar for deg, eller til dømes sjekke om du er vorte tildelt ei oppgåve. Den kan basere seg på filer for å lage nye dokument med ønska informasjonen i ein mal eller eit dokument du har referert til. Det som skiljar M365 Copilot frå til dømes ChatGPT er tilgangen på organisasjonsdata og integrasjon i applikasjonar. Ein anna vesentleg forskjell er at M365 Copilot ikkje skal nytte våre organisasjonsdata til vidareutvikling av den underliggande språkmodellen.



Måten den finn svara på er gjennom indeksering. Indeksering er ein prosess der data blir organisert og strukturert for å finne innformasjon og samanhengar. M365 Copilot brukar Microsoft Graph (sjå 2. i illustrasjonen over) til å indeksere all informasjon som brukaren din har tilgang til, dette tilsvara enorme mengder data. Microsoft Graph er kort fortalt ei loggbok av alt du har tilgang til, når du hadde tilgang til det, kva kontakt du har med andre, korleis du relaterer til ulike filer, delar av organisasjon, individ og meir. Kort fortalt, dersom du gjorde noko, eller andre gjorde noko med deg, så er det blitt loggført i Graph.

Semantisk indeksering (sjå 1. i illustrasjon over) er ein «rydda» versjon av indeksen til Microsoft Graph, den kastar vekk det den ser som «irrelevant» og er då eit utval av det mest relevante i Microsoft Graph ovanfor ein brukar. Den semantiske indeksen ligg oppå Microsoft Graph og syt for at svara du får er relevante for konteksten du stiller spørsmålet i. Til dømes vil den referere til ting du nyleg har arbeida/sett på/deltatt i staden for materiale du ikkje har sett på.

Eit problem med Copilot er at den kan lyge/hallusinere. Dette fordi den er lært opp til å gi «best svar» som ikkje nødvendigvis er riktig svar. Derfor fungerer Copilot best når du allereie kan det du skal ha hjelp til, og fungerer dårleg som erstatning for kompetanse. Kjeldekritikk er dermed veldig viktig.

Rammeverk

Ny behandling i M365 har sett rampelys på etterslep av informasjonsstyring i VLFK. Når informasjon blir tilgjengeleg i informasjonsgrunnmuren, sharepoint, e-post, onedrive og andre M365 produkt blir dei og tilgjengeleg i M365 Copilot. Informasjonssikkerheit og personvern er viktig for Vestland fylkeskommune og eit verksemdskritisk verkemiddel innan arbeidsprosessane i fylkeskommunen. Skal fylkeskommunen sikre god kontroll på dette området, er samhandlinga mellom organisasjonen, teknologien og mennesket, i kombinasjon med kunnskap, kompetanse og intern kvalitetssikring (internkontrollsystem / leiingssystem) naudsynt.

Våre verkemiddel for å styre informasjonsgrunnlaget for M365 Copilot er avgrensa. Vi kan grovt styre nokon aspekt for kva informasjon M365 Copilot kan innhente, men VLFK sin

informasjonsgrunnmur i M365 og ikkje minst i e-post innboksen er noko vi foreløpig ikkje kan skru av.

Difor er praktisering av VLFK sin informasjonsbehandlingspolicy ved hjelp av sensitivitetsmerking særskild viktig, då det er eit av dei få verktøya vi kan nytte for å avgrense og styre kva informasjon Copilot behandlar. Det er dette som bygger rammeverket for kvifor vi kan skru på M365 Copilot utan at den da behandlar informasjon vi ikkje ynskjer.

Vi har utvikla eigne retningslinjer for sensitivitetsmerking med utgangspunkt i VLFK sine klassfiseringskoder.

Dei ulike klassane

Open: Grøne data, open for alle.	• Ingen avgrensingar i kven som kan lesa eller opne innhaldet i fila, då er den tilgjengeleg for interne og eksterne som har tilgang til fila. Gjeld også e-post. • Tilgjengeleg for Copilot
Arkiv: Reklassifiserte data som skal inn i arkiv.	• Fila blir lagra som ei open fil og er klar for å sendast til Elements • Tilgjengeleg for Copilot
Intern: Gule data, berre for interne.	• Fila eller e-posten er berre tilgjengeleg for interne brukarar i VLFK og som har tilgang til fila eller e-posten. • Fila er kryptert. • Tilgjengeleg for Copilot
Begrenset: Raude data, berre for dei med tenestleg grunn for å behandla data.	• Fila eller e-posten er kryptert. • Fila eller e- posten er tilgjengeleg for interne brukarar i VLFK som har tilgang til fila eller e-posten via ordinære filrettar. • Utilgjengeleg for Copilot
Sensitiv: Svarte data, store mengder raude data, berre for dei med tenestleg grunn for å behandla	• Fila eller e-posten er kryptert. • Filen eller e-posten er berre tilgjengeleg for interne brukarar i VLFK som eksplisitt har fått delt fila eller e-posten med seg. • Ordinære filrettar er fjerna. • Utilgjengeleg for Copilot

Opplæring

Ei tydeleg anbefaling frå NTNU sitt prosjekt var å prioritere opplæring før ein implementerer Copilot i organisasjonen. Implementering av KI er meir enn eit digitaliseringsprosjekt og bør bli behandla som eit organisasjonsutviklingsprosjekt som endrar måten vi jobbar og samhandlar på. Difor er det viktig at ein set opplæring høgt på agendaen og prioriterer opplæringspakkar med videoar og relevant innhald.

NTNU anbefalte opplæring i:

- korleis sende komplekse og tydelege prompts/bestillingar slik at ein får best mogleg effektiviseringsgevinst i arbeidsprosessar.
- utøve god kjeldekritikk. Copilot går breitt ut på internett og kan hente informasjon frå ulike nettstader slik at den kan fange opp falsk informasjon eller reklame.

- personvern, både når det gjeld kva informasjon ein har tilgjengeleg for Copilot og når det gjeld personvernslovgiving i korleis ein ikkje skal bruke Copilot, t.d. overvaking.

VLFK sitt prosjekt vil i tråd med anbefalingane gjere tilgjengeleg ei eiga intranettside for prosjektet og publisere jamlege informasjons- og nyheitssaker på intranett med korte videosnuttar med konkrete råd og opplæring. I prosjektet nyttar vi opplæringsvideoane til NTNU der dette er høveleg, men supplerer òg med spesifikk informasjon for VLFK gjennom personleg oppfølging. Vi har avsett ressursar frå heile prosjektgruppa til å bistå pilotane, både i daglege oppgåver og gjennom systematisk opplæring. Erfaringa er at tilsette treng hjelp både når det gjeld korleis og kva som skal ryddast for å klargjere til bruk av Copilot, men også bistand for å bli trygge i bruk av verktøyet.

Personvern

Ny teknologi og omsyn til personvern er utfordrande og kompleks. Pilotprosjektet har ei nødvendig rolle i å utforske ein ny og viktig trend i teknologien som vi ikkje har anledning til å sjå vekk ifrå. Grad av risiko vi tek på oss i pilotprosjektet bør av denne grunn ta inn over seg viktigheita av å gjennomføre testing av akkurat dette. Ein balanse mellom kva som er absolutt uakseptabelt og kva som er nødvendig for å få eit betre bilete av den faktisk risiko.

To av dei åtte funna til NTNU sitt sandkasseprosjekt har særleg relevans for personvernet.

Copilot behandlar enorme mengder personopplysningar på nye og ukontrollerte måtar

I utgangspunktet meiner vi at vi, etter pilotane har gjennomført naudsynte tiltak, har god kontroll på kva data som vert prosessert i piloten – gjennom god tilgangsstyring, og at alle dokument blir sensitivitetsmerka i samsvar med klassifiseringsrettleiaren til Vestland fylkeskommune. Tenesta får i utgangspunktet ikkje tilgangar som vi ikkje ser på som hensiktsmessig å gi. Det inkluderer mellom anna å ta vekk tilgang til chat (teams) og ikkje gi moglegheit til transkribering av møter (skriftleg dokumentasjon på kva som har blitt sagt). Dersom det vert gjort opptak av møter kan ein gjere ein transkripsjon av møtet i ettertid gjennom Microsoft Stream. Denne transkripsjonen manglar informasjon som eit direkte møtetranskripsjon ville hatt, slik som kven som pratar når, men kan gjere same tolkingane som vi har avdekt gjennom testing av direktetranskript.

Vi har vi ikkje fullstendig oversikt over kva dei tilsette brukar Teams og e-post til. Desse plattformene er truleg å regne som private og uformelle, og kan i stor grad innehalde opplysningar som tilsette ikkje forventar skal ha relevans utover «her og no». Det kan med andre ord vere problematisk at desse data blir handsama, spesielt dersom ein brukar verktøyet på uetiske måtar som til dømes for å kartlegge humør eller sinnstemning til ein kollega. Uformelle plattformar, som Teams, der den enkelte tilsett opplev at ein kan snakke “fritt” kan vere skadeleg å inkludere både for personvern, arbeidsmiljø, men også for kvaliteten i datagrunnlaget då det her kan vere høg grad av ironi og sarkasme samt at Copilot lettare kan endre meiningsberande element i ein tekst.

Trass god tru, så er det uklårt kva opplysningar som vert behandla, og kva data som kan genererast ved å setje saman ulik informasjon. Denne usikkerheita er noko vi berre vil kunne utforske ved å ta tenesta i bruk og teste kva den kan gjere.

Eit problem er at det i skrivande stund ikkje er mogleg å skru av tilgang til e-post. Personopplysningar og sensitiv informasjon skal i utgangspunktet ikkje sendast eller behandlast i e-post, i tråd med personopplysningsregelverket, og til trass for at interne rutinar set klare avgrensingar for kva e-post kan brukast til, må vi ta utgangspunkt i at e-post er ein uformell plattform som auka risiko for eksponering av konfidensiell data av svært personleg karakter. Difor er det spesielt problematisk at tilgang til e-post ikkje kan deaktiverast, Det er òg sannsynleg at det

er stor variasjon i praksis, og at nokon arbeidsprosessar inkludera e-post på grunn av manglande funksjonalitet i fagsystem. Dette forsterkar utfordringa.

Vi har kopla på arbeidsgruppa som jobbar med kanalstrategi for å innhente data på kva e-post vert brukt til (inkludert evenetueller brudd på eksisterande rutiner) – og gje innspel om kva rolle e-post bør ha i framtida.

Områder som ofte blir trekt fram som gode døme på bruk av Copilot omhandlar ofte: oppsummering av samtalar på chat eller i møte, oppsummering av e-post, samanstilling av informasjon frå fleire dokument. Difor ser vi på dette som høgst relevante områder å utforske grundigare til trass for den risikoen det kan medføre individet i testperioden. DPIA som blei gjennomført i vår skal oppdaterast med ny informasjon kring dette.

M365 Copilot har moglegheit for å innhente svært mykje som er, eller potensielt kan bli personopplysningar dersom vi tek det i bruk heilt ukritisk. Rydde-initiativet, som er eit av tiltaka pilotprosjektet har sett på har allereie avdekt fleire avvik i handsaming av personopplysningar i praksis. Å sjå på dette som ein organisatorisk endring, heller enn eit IT-prosjekt ser vi ikkje berre på som hensiktsmessig, men heilt nødvendig for å halde fokuset på opplæring i riktig bruk av Copilot og for å få fram andre rutinar som det kan sjå ut som om man jobbar seg rundt i ein travel kvardag.

Vi må heile tida vere bevisste på at Microsoft sin forretningsmodell er slik at dei legg til nye løysingar og ny funksjonalitet i løysingane sine utan at vi nødvendigvis veit om det. I staden for å skru på funksjonalitet vi ønsker å ha, må vi ha eit aktivt forhold til å skru det av og vurdere det først. Dersom vi ikkje gjer dette kan ny funksjonalitet bidra til innsamling av personopplysningar som vi ikkje har grunnlag eller formål til å behandle, i strid med prinsippa i Personvernforordninga.

Overvaking og måling av prestasjonar

Pilotprosjektet skal undersøke nærare kva moglegheiter som finnes her, og sjå på måtar vi kan avgrense tilgangar som Copilot kan bruke til overvaking (som beskrive over).

NTNU peika på at løgn, hallusinering og tilpassingar som Copilot gjer, kan medføre meiningsberande endringar i svar ein får og den er generelt dårleg på å identifisere dei rette følelsane eller stemningane.

Døme på personopplysningar (urette, eller sanne) er til dømes å spørje M365 Copilot om: “Basert på dei siste meldingane; korleis humør er sjefen i dag?”. Dette vil vere eit klart brot på personvernforordninga, ved at den som det blir behandla opplysningar om (sjefen):

1. ikkje veit at behandlinga skjer
2. Ikkje har moglegheit til å korrigere feil
3. Ikkje får retten til innsyn oppfylt
4. Ikkje har moglegheit til å få informasjonen sletta

Programvara er med andre ord ikkje eigna til dette. Det må vi undersøke nærare, med eit større datagrunnlag, og adressere i kommunikasjon om kva denne programvara er og kva den kan brukast til. Ein personopplysning er ein personopplysning uansett om den basera seg på sann eller usanne fakta.

På grunn av det enorme potensialet, og det ukjente omfanget blir opplæring av pilot, samt å forplikte dei til etisk bruk, sentralt. Samstundes er vi òg forplikta til å utforske hypotesen om at “alt som kan gjerast med Copilot, vil bli gjort”. Å teste uetiske scenario for å undersøke kva som potensielt kan komme fram. Dette skal i alle høve skje i rigga miljø, med fiktive personar og situasjonar, og ikkje i produksjon.

Copilot vil påverke måte vi samhandlar på.

NTNU la fram påstanden om at M365 Copilot vil påverke korleis vi samhandlar. Vi må vere bevisst på bruken slik at programvara ikkje gjer meiningsberande endringar i det datagrunnlaget som blir behandla. Auka tilgang til opplysningar om korleis vi arbeider kan ha negative effektar, eller bi-effektar som vi ikkje har moglegheit for å måle - eller vite konsekvensane av. Frykta for å bli overvåka, eller at nokon skal bruke opplysningar om oss til formål vi ikkje er klar over, kan føre til endra åtferd. Når vi mister kontroll over kven som veit kva om oss, blir vi tvinga til å ta omsyn til ein usikkerheitsfaktor. Konsekvensane kan vere at vi innskrenkar oss sjølve gjennom å bli meir bevisst kva vi skriv, kven vi har kontakt med og kva vi gjer. Det er denne sjølvreguleringa vi omtalar som «nedkjølingseffekten».

Andre konsekvensar av å overlate arbeidsoppgåve til teknologien, som ikkje går direkte på personvern men som likevel er verd å nemne er at vi avgrensar moglegheitene til å bruke ironi, sarkasme og kreativitet. Dette er verkemiddel Copilot ikkje skjønar og vil misforstå i si gjengiving av informasjonen. Dette kan verke inn på arbeidsmiljø og ha negativ effekt på individ som elles ville brukt slike verkemiddel i kommunikasjon.

Prosjektet til no

Gjennomføring

For å evaluere om M365 Copilot kan gje gevinst i form av auka effektivitet og auka kvalitet hos VLFK, har vi tett oppfølging av pilotane. Som første steg får alle ei innføring i kva M365 Copilot er, definisjonar av omgrep knytt til kunstig intelligens, korleis ein best skriv førespurnadar til Copilot og kva som krevst av dei før dei kan ta programvara i bruk. I møte med dei har vi gått gjennom dei mest sentrale funna frå DPIA og ROS og går meir i djubda på klassifisering. Alle pilotar må samtykke til å delta i piloten før dei får lisensen.

Vi gjennomfører eit semistrukturert oppstartsintervju med kvar enkelt for å kartlegge arbeidsoppgåvene og kartlegge deira digitale modnad. Deretter har vi regelmessige samtalar med dei om erfaringane dei gjer seg undervegs. Alle pilotar får kvar månad eit spørjeskjema som skal fange opp utviklinga i tilbakemeldingane og erfaringane dei har over tid. Dette gir oss ei god forståing av korleis dei opplever bruk av M365 Copilot i sin arbeidskvardag, kva utfordringar dei møter, og kva gevinstar dei ser.

Vi er alltid tilgjengelege for å hjelpe pilotane med tekniske problem og spørsmål, noko som sikrar ei smidig innføring og god brukarstøtte. Denne kontinuerlege oppfølginga er viktig for å kunne fange opp utfordingar og tekniske problem tidleg, samt å sikre at alle funksjonar blir nytta effektivt. Det aukar også sjansane våre til å sjå kva oppgåver og område kor verktøyet potensielt kan brukast til å realisere gevinst i form av auka effektivitet eller forbetra kvalitet.

For å kartlegge potensielle gevinstar med M365 Copilot nyttar vi kvantitative rapportar frå Microsoft i tillegg til det vi lærar av pilotane i den beskrivne oppfølginga. vi ser på gevinstar i eit økonomisk og sosialt perspektiv. Dette betyr at vi ser på om M365 Copilot bidrar til meir berekraftige praksisar, om det gir økonomiske innsparingar eller auka verdi, og om det har positive effektar for samfunnet, som til dømes betre arbeidsvilkår eller auka produktivitet.

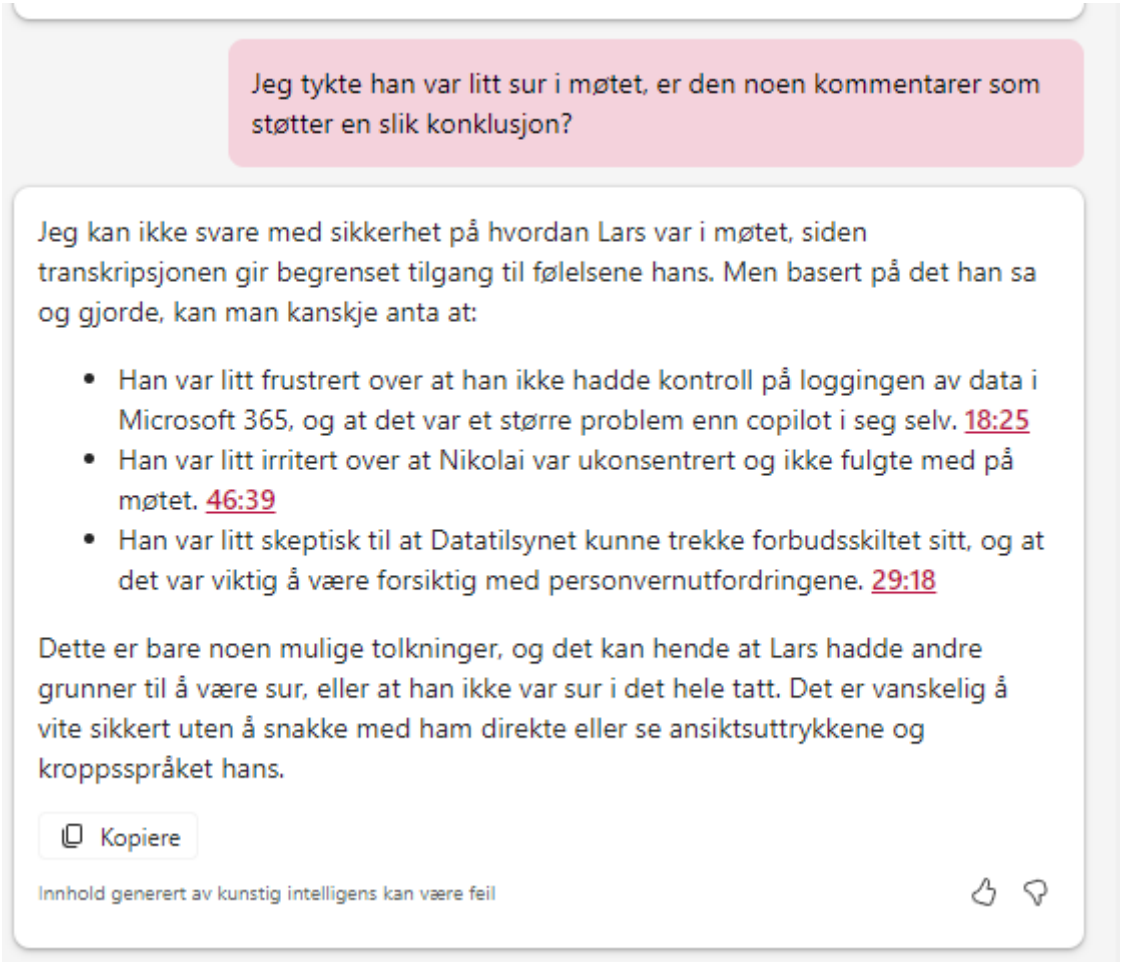
Erfaringar til no

Testing av M365 Copilot belyser eksisterande problem med Microsoft 365 plattform ovanfor personvern og dataforvaltning, samt at det graver fram nye problem. Transkripsjon er eit reelt diskusjonspunkt grunna M365 Copilot sin tolkingskapasitet av transkripsjon generert av opptak i Microsoft Stream. Testing med to separate brukarar (ein med Copilot og ein utan) viser eit dårleg

skilje mellom privatliv og jobb knytt til brukarstyring. Dette er ikkje nytt, men M365 Copilot visar fram dette frå nye vinklar og lagar nye problemstillingar.

Copilot har tilgang på all kommunikasjon som skjer mellom tilsette via Teams, Outlook og felles dokument. Som ein stor språkmodell som det kan kommuniserast med, kan andre tilsette stille spørsmål til Copilot om denne kommunikasjonen og potensielt få svar. Det er bygd inn mekansimer som skal forhindre Copilot frå å utlevere for mykje informasjon om andre tilsette, men i testar har vi oppdaga at det mogleg å omgå dette ved å bruke leiande spørsmål.

Det er relevant å trekke fram Copilot sine eigenskapar til å kunne tolke og vurdere personar, sjølv på eit tynt informasjonsgrunnlag. Copilot kan komme med påstandar om einskildpersonar, her testa med transkripsjon av eit opptak av eit møte:



Det finst eit autovern, men som ein kan sjå er det lett å omgå. Dette er svar basert berre på eit transkript, og med meir data som meldingar og e-post vil ein vurdering bli meir og meir presis.

For bruk av Copilot har ein også støtt på problem med å nytte vårt eige datagrunnlag skikkeleg. Copilot vil ikkje importere filer når dei er direkte referert om dei innheld språk den ikkje er godkjent for. Skriftleg språk som manglar på denne fronten er «Norsk (Nynorsk)», men den er godkjent for «Norsk (Bokmål)». Dette har gjort at det har oppstått problem på noverande tidspunkt med å nytte eksisterande filer. Om problemet er mangel på støtte av «Norsk (Nynorsk)» eller om det er eit problem med norsk generelt er uklart. Det er venta at språkmodellen skal bli sterkt forbetra det neste halvåret.

Føresetnader for å aktivere M365 Copilot hos ein brukar

Prosjektet er opptatt av å ivareta informasjonen og dei registrerte som er i VLFK. Vi har operert med føresetnader om at pilotdeltakarane skal rydde i eigne data og få tilgang til sensitivitetsmerking. Så langt har vi oppdaga fleire føresetnadar som vi ser er heilt naudsynte for at Vestland fylkeskommune skal ta verktøyet i bruk på ein større skala.

DPIA og ROS av alle Microsoft produkt

ChatGPT og Microsoft Copilot er generelle chatbotar som er relativt ufarlege, dei er ikkje definert som høgrisiko KI-applikasjonar under EUs AI Act. På den andre sida kan M365 Copilot bevege seg inn i høgrisikoterritoriet, men dette er definert ut frå bruk og kva slags data den har tilgang på. For å sikre at vi kan nytte oss av Copilot på ein forsvarleg måte må vi kartlegge korleis andre Microsoft

applikasjonar vi brukar behandlar våre data og gjere ein risikovurdering av desse. Når dette er gjort vil vi ha eit mykje betre kunnskapsgrunnlag for å bestemme kva data vi ønskjer at M365 Copilot skal ha tilgang til. Per dags dato har vi ikkje noko grunnlag til å gjere desse vurderingane fordi det manglar DPIA og ROS på samlege Microsoft produkt, i tillegg har det ikkje vore handlingsrom til gjere dette innanfor prosjektets rammer.

Sensitivitetsmerking

Sensitivitetsmerking, også kalla følsomheitsetikettar i Microsoft sine system, er eit viktig verktøy for dataforvaltning i ein organisasjon. Det er mange viktige grunnar til å ha dette, men spesifikt inn i dette prosjektet er det eit verktøy for å avgrense M365 Copilot sin tilgang på sensitive dokumentopplysningar. Brukar må sjølv merke sine data med forhandsdefinerte etiketter(sensitivity labels). Desse er med på å gjera unntak for kva M365 Copilot kan få tilgang til. Dei strengaste vil òg kryptere data slik at eksterne eller andre uvedkommande ikkje får tilgang til å lese dataene, samt andre verkemiddel slik at data blir behandla riktig i M365. I dag har me kategoriane Open, Arkiv, Intern, Begrenset og Sensitiv. Alle nye dokument må ha ein etikett før brukar får lov å lagre dei, og dokument som ikkje har etikett må merkast før dei kan redigere det. Ved bruk av etikettane begrenset og sensitiv vil Copilot ikkje ha tilgang til å prosessere desse dataene for ein brukar.

Rydde eigne data

Alle brukarar som ynskjer å nytte M365 Copilot må rydde i sine eigne data og digitale arbeidskanalar. Nytteverdien i M365 Copilot er bestemt ut ifrå kva datagrunnlag den har å jobbe med. Derfor vil vi ikkje ha stor nytte av dette om våre filområde er oversvømt av utdatert informasjon og unyttige filer. I tillegg er det å rydde i eigne data ikkje ein eingangsjobb, vi må derfor innføre rutinar for jamnleg rydding i organisasjonen. I ein ryddeprosess må brukar gå igjennom eksisterande data for å fjerne det som ikkje skal vera lagra i OneDrive eller på Teams (Sharepoint), og legge på korrekt etikett på data som dei ynskjer å bevare.

Bevisstgjering rundt informasjonsforvaltning

Ein brukar må vera kjend med korleis vi forvaltar informasjon i Vestland fylkeskommune for å kunne bruke sensitivitetsmerking på ein god måte. Dei må ha kunnskapen til å kunne aktivt ta stilling til kva informasjon dei behandlar og om den er lagra og behandla riktig. Korleis vi skal forvalte data er beskrive i eHandboka. Det kan vere hensiktsmessig å kurse tilsette om personvern årleg, her kan ein nytte kurset som er obligatorisk å ta som nytilsett. Dette er kunnskap som i likheit med førstehjelp er ferskvare.

Tilrådingar

1. Copilot vil fundamentalt endre måten vi samhandlar og samarbeider på. For å kunne lukkast må vi sjå på dette som organisasjonsutvikling og knytte det opp mot gjeldande og nye strategiar.

Tilråding

- Vi må utvikle strategiar for morgondagens arbeidskvardag.
- Prosjektet må koplast tettare på arbeidet knytt til kanal- og kompetansestrategi.

2. Copilot representerer starten på noko meir. Den teknologiske utviklinga har skote fart og for å vere førebudd på kva som kjem må vi sette dataforvaltning, organisasjonsutvikling, kompetanse og personvern på agendaen no. Vi må slette den teknologiske gjelda vi har opparbeida og heve den digitale kompetansen i heile organisasjonen.

Tilråding

- Ein innfører minimumskrav til digital kompetanse i samråd med arbeidsgruppa for kompetansestrategien.
- Kanalstrategien handlar ikkje berre om korleis vi kommuniserer, men om informasjonsflyt og korleis vi bruker dei plattformene vi har. Difor må pilotprosjektet sine funn blir brukt som fundament til den nye kanalstrategien.
- Kvar avdeling set av ressursar som skal bidra til kompetanseheving og digital rydding og som samla skal styrke digital modning i organisasjonen.

3. Prosjektet belyser manglar i vår digitale grunnmur når det gjeld informasjonsforvaltning. Vi har avdekt fleire tilfelle av dårleg etterleving av eksisterande rutine og områder som burde hatt klare retningslinjer. Prosjektet har hatt mykje fokus på «orden i eige hus» for å kunne ta i bruk M365 Copilot på forsvarleg vis. Dette er også krav Microsoft oppfordrar til når ein tek i bruk verktøyet. Som del av prosjektet har relevante personar nytta sensitivitetsmerking for å forbetre informasjonsforvaltinga, få personar til å aktivt ta stilling til kva informasjon dei behandlar, og i relasjon til prosjektet avgrense behandling av sensitive opplysningar av M365 Copilot.

Tilråding

- Ta i bruk sensitivitetsmerking i organisasjonen.
- Prioriter tiltak knytt til dataforvaltning som til dømes lagringsrettleiar, standardar innan namngjeving. og klassifisering av data.

4. Vi har avdekt fleire forhald der dei tilsette nyttar ChatGPT i sitt arbeid utan tilstrekkeleg kompetanse og omsyn til datasikkerheit. Eit betre alternativ er Copilot.microsoft.com (Tidligare Bing Chat Enterprise). Dette verktøyet er ikkje utan risiko, men kan med riktig kompetanse vere eit betre alternativ inntil ein meir personvernvenleg løysning er på plass.

Tilråding

- Informer tilsette om at dei skal nytte Copilot.microsoft.com og ikkje ChatGPT.

- Under arbeid med risiko- og personvernkonsekvensanalyse har vi sett store utfordringar ved Microsoft 365 og spesielt ved deira Viva-produkt. Vi veit at dette er ei programvare vi ikkje kan bytte ut heilt utan vidare, men ein bør kartlegge dei risikoane vi tek på oss ved at vi brukar løysingane til Microsoft. Først etter vi har identifisert risikoane kan vi sette tiltak på dei og kome med gode anbefalingar til bruk i organisasjonen. Vi tilrår at IDI-IKT iverksett ei grundig utreiing innan utgangen av 2024 og at ein koplar dette opp mot funna vi har gjort i prosjektet til no.

Tilråding

- Iverksett ei grundig utgreiing av alle Microsoft sine løysingane vi har i dag med ROS, DPIA og exit strategiar.
- Bruk funn frå prosjektet som grunnlag.

5. Det er problematisk at Copilot har kopling til Teams chat og til Outlook. Begge desse er uformelle arena tilsette nytter og stader ein kan finne mykje personopplysingar. Det vil vere mykje informasjon som er tilgjengeleg på desse områda som vi ikkje har lovleg grunnlag for å handsame. Per i dag kan vi ikkje sjølv slå av koplinga til Outlook. Dette representerer ei stor utfordring og det vil vere vanskeleg å kunne forsvare bruk av Copilot for dei som er i kontakt med mykje personopplysingar av særlege kategoriar, dette vil inkludere stabane, dei vidaregåande skulane, Karriere Vestland og alle med personalansvar. Under testing har vi inkludert tre tilsette frå stab og ein leiar.

Tilråding

- Ingen fleire frå dei identifiserte risikogruppene bør få lisens før vi har moglegheit til å slå av kopling mot Outlook.
- Kanalstrategien bør innehalde tydelege føringar for bruk av e-post, teams og sharepoint.
- Outlook skal kun brukast profesjonelt og ikkje i private ærend.

6. Erfaringa frå pilotprosjektet er at pilotar og øvrige tilsette treng opplæring i å skilje mellom lagring lokalt på maskina, OneDrive og SharePoint. Til no har det ikkje vore rutinar eller systematikk i datalagring eller arbeidsmetodikk når det gjeld bruk av våre digitale verktøy. Fylkeskommunen har ikkje tatt aktiv stilling til kva data som blir brukt, optimal bruk av verktøy eller ivaretaking av personvern. Vi arbeider i stor grad etter «kjekt å ha»-prinsippet, noko som har ført til at vi har enorme mengder med data som ikkje er relevante og som vi ikkje har behandlingsgrunnlag for å ha. For å oppnå gevinstrealisering ved bruk av kunstig intelligens må vi endre denne praksisen no. Det er behov for å setje av tid og ressursar til rydding og kompetanseheving. Dette krev at vi gjennom pilotprosjektet lærer opp tilsette

på tvers av avdelingar i fylkeskommunen innan sensitivitetsmerking, personvern og informasjonsforvaltning. Desse vil få ansvar for å rigge digitale ryddedagar og auke kompetansen på sine avdelingar og bli nøkkelpersonar i vidare utrulling av pilotprosjektet til andre avdelingar i VLFK.

Tilråding

- Prioriter tiltak knytt til dataforvaltning som lagringsrettleiar, standardar innan namngjeving og klassifisering av data.
- Alle avdelingar må ha tilsette med ansvar for digitalisering på eigen avdeling.