Vurdering av personvern

i Copilot for Microsoft 365

Vestland
fylkeskommune

Innhald

Introduksjon

Dette dokumenter er ei vurdering av konsekvensar for personvernet ved bruk av Copilot for Microsoft 365. Det er ikkje ei fullverdig DPIA, då det blir opp til kvar enkelt eining å identifisere problemstilling og omfang av sitt bruk.

Ei sjekkliste av kva Vestland fylkeskommune må gjere av overordna vurderingar:

☐Risikoanalyse av Microsoft 365 som leverandør.

☐Det bør vere klart kva Microsoft gjer for å sikre at Copilot overheld krav til dataminimering, formålsavgrensing og tryggleik.

☐Microsoft sin rolle som databehandlar vs. behandlingsansvarleg må bli meir tydeleg.

☐Formål og behandlingsgrunnlag for spesifikke prosessar innan HR, leiing eller undervisning krev svært grundige vurderingar og vil blant anna krevje at vi veit meir enn det Microsoft på noverande tidspunkt har avslørt om kva som skjer med opplysningane våre.
Slike prosessar må dermed haldast utanfor programvara.

Ei sjekkliste av kva kvar eining må gjere av eigne vurderingar:

☐Det kan vere nyttig å ha eit eige avsnitt som tydeleg spesifiserer kva Copilot for M365 skal brukast til i eininga, kva utfordringar det adresserer, og kvifor ein DPIA er naudsynt.

☐Systematisk oversikt over tiltak for å reduserere identifiserte risikoar.

☐Dersom Copilot for M365 innebær høg risiko for personvernet, bør det vurderast om det er nødvendig å kontakte Datatilsynet før implementering.

☐DPIA bør ha ein plan for revisjon og oppfølging av risikovurderingane.

☐Det bør avklarast kor ofte DPIA-en skal oppdaterast, og kven som er ansvarleg for det.

Copilot for Microsoft 365 – ein introduksjon

Copilot for Microsoft 365 (Copilot for M365) eit verktøy som kan bidra til å gjere deg meir effektiv ved til dømes å automatisere repeterande oppgåver, generere innhald, analysere data, eller organisere informasjon. Verktøyet kan integrert i Microsoft 365-applikasjonar som Word, Excel, PowerPoint, Outlook og Teams og kan bidra når du treng det, og kan mellom anna kombinere informasjon på tvers av tenestene du brukar.

Måten du brukar Copilot for M365 på er gjennom ein førespurnad ved å gi kommandoar eller stille spørsmål, også kalla "prompt", og du kan få hjelp til mellom anna å analysere, oppsummere, skape eller forstå informasjon.

Copilot for M365 tilpassar seg tilgangane og behova dine, og vil etter kvart som du brukar tenesta, lære korleis du kommuniserer, korleis du jobbar, kva preferansar du har, og på denne måten vil den fungere betre og betre etter kvart som du brukar tenesta. Personifiseringsmoglegheitene i tenesta gjer at Copilot 365 vil kunne forutse kva du treng, når du treng det og tilpasse forslag til din skrivemåte og arbeidsmønster.

Dette vart skrive med kunnskap frå 2024, og namneendringar og funksjonsendringar kan bety at vi referera til produkt som ikkje lenger eksisterer med eit gitt namn, og at funksjonar kan ha endra seg. Vi veit til dømes at semantisk indeksering no skjer uavhengig av om ein har skrudd på Copilot eller ikkje.

Her er nokre av dei konkrete måtane Copilot kan gjere arbeidsoppgåvene dine enklare og meir produktive, gjennom dei ulike Microsoft 365-programma:

Outlook: Oppsummere e-posttrådar, generere forslag til svar og foreslå kalenderavtalar basert på e-postinnhald.
Word: Lage utkast til dokument, forbetre tekst og stil, og oppsummere rapportar.
Excel: Analysere datasett, identifisere trendar og lage visuelle framstillingar.
PowerPoint: Lage presentasjonar basert på tekst eller idear, og foreslå layout og design.
Teams: Oppsummere diskusjonar, skrive referat og identifisere handlingspunkt.
SharePoint: Finne relevant innhald og lage intanettsider.

Korleis fungerer Copilot for M365?

Den litt meir tekniske forklaringa på kva som skjer når ein bruka Copilot for M365 lisens er at den vil svare på dine prompt ved å kombinere data frå (1) Microsoft Graph og (2) semantisk indeks med (3) store språkmodellar.

Microsoft Graph --> **Oversikt over kva informasjon som er tilgjengeleg**	Microsoft Graph samlar og organiserer informasjon frå Microsoft 365-programma du allereie brukar, som til dømes e-postar, dokument, e-post og møter.	Microsoft Graph (Graph) fungerer som eit slags nav for informasjon og samlar data på tvers av tenester. Graph kan bidra til å automatisere tenester og tilpasse opplevinga for kvar brukar. For eksempel kan du bruke Graph til å finne alle dokument ein person har jobba med i det siste eller sende ei automatisk melding til ein Teams-kanal. Graph er funksjonalitet i M365 og er uavhengig av Copilot. Dette er dermed ikkje ei behandling som tek til ved å skru på Copilot, men eit viktig ledd i korleis Copilot jobbar.
Semantisk index--> **organiserer og kategoriserer informasjon basert på relasjonar** Ordet "semantisk" refererer til betydninga av ord, setningar eller uttrykk i et språk.	En semantisk indeks er en metode for å organisere og søke etter data basert på betydningen av innholdet, ikkje berre nøkkelord. Den analysera tekst for å forstå konteksten og relasjonar, slik at den finn relevant informasjon sjølv om søket ikkje brukar dei eksakte orda. Dette brukast òg i søkemotor som Google. Dette er ei databehandling som blir ny ved å slå på Copilot for M365, og er sjølve kjernen i produktet.	Semantisk indeksering lagrar metadata og skapar samanhengar mellom ord, uttrykk og dokument, slik at når brukaren stiller eit spørsmål eller ein kommando, kan Copilot for M365 finne relevant informasjon i den organiserte informasjonen (den semantiske indeksen). Eit semantisk søk kan forstå intensjonen bak spørsmålet og finne meining og samanheng i informasjon, i kontrast til ordinære søk som berre leitar etter dei eksakte orda du skriv. Eit ordinært søk ville sannsynlegvis gitt deg ei liste med lenker til nettsider som du måtte då klikke og lese gjennom innhaldet i for å finne den informasjonen du leitar etter. Eit semantisk søk kan sette det du skriv i ein kontekst og gi deg eit direkte og samanfatta svar basert på ei tolking av meininga bak spørsmålet ditt sjølv om dei eksakte orda ikkje er brukt i prompt. Til dømes, om du spør om fordelane med å bruke solenergi, kan Copilot svare: 'Fordelane med å bruke solenergi inkluderer å reduserte energikostnader, lågare karbonutslepp, og auka energisikkerheit. Eller om du søkjer etter "møte klokka 15," vil Copilot

		for M365 leite etter møte rundt dette tidspunktet, sjølv om orda ikkje er heilt like i dokumentet eller kalenderen.
Store språksmodellar --> **Analyserer og brukar informasjon og gir presise svar.** Også kalla «LLM» – Large Language Models	Er ein type kunstig intelligens som er trena på enorme mengder tekstdata for å forstå, generere og besvare språk. Modellen lærer mønstre og samaenhengar i tekst, slik at den kan utføre oppgåver som oversetting tekstgenerering og spørsmål-svar. Eksemplpå LLM-er er GPT-3 og GPT-4.	Store språkmodellar (large language models, LLM) er ein type kunstig intelligens (KI) som forstår, analyserer og kan lage tekst på ein måte som liknar på korleis menneske brukar språk. Desse modellane er trent på enorme mengder tekst frå internett, noko som gjer dei i stand til å svare på spørsmål, skrive tekstar og hjelpe med komplekse oppgåver. I 2023 blei LLM og liknande KI-teknologi, som ChatGPT og Copilot, tilgjengelege på marknaden, noko som førte til ein kombinasjon av teknologiske gjennombrot, praktisk bruk og stor merksemd. Dette har gjort LLM til ein viktig del av moderne teknologi og ein stor del av samtalen rundt framtida for arbeid og innovasjon.

Slik jobbar dei saman i Copilot

Når du brukar Copilot for M365, jobbar desse tre komponentane saman for å levere intelligente, relevante svar og tenester, og kan hente fram, analysere og presentere informasjon frå fleire kjelder i Microsoft 365, raskt og nøyaktig – slik at du slepp å lete gjennom data sjølv.

Microsoft Graph samlar informasjon frå tenester som e-post, dokument og møter. Semantisk indeks og semantiske søk organiserer og analyserer desse dataea, forstår spørsmålet ditt og identifiserer informasjonen som er mest relevant. Ved hjelp av LLM kan tenesta generere eit fullstendig og naturleg svar, tilpassa konteksten din.

Kva skil Copilot frå andre KI-verktøy?

Copilot for M365 skil seg frå andre KI-verktøy gjennom den tette integrasjonen med Microsoft 365-plattforma, slik at brukarane kan nytte funksjonane direkte i Word, Excel e-post etc. Copilot har tilgang til alle dokument og all informasjon du har og gjer det mogleg å tilpasse hjelp direkte til konteksten.

Svært mykje av sakshandsaminga vi gjer føregår i Microsoft 365-plattforma i form av Word-filer, Excel-filer, e-postar eller anna. Copilot vil med andre ord få mykje data å trene seg på i å forstå korleis du jobbar. Ikkje berre i form av dokumenta og kva dei inneheld, men også kva dokument du brukar mykje tid på, kva tid du jobbar, kor mykje tid du brukar i møter og andre mønster i åtferda di.

Om pilotprosjektet

Pilotprosjektet for bruk av generativ kunstig intelligens (KI) i Vestland fylkeskommune (VLFK) (heretter referert til som pilotprosjektet) hadde som mål å undersøke om VLFK har føresetningane som skal til for å kunne ta i bruk teknologi basert på KI, slik som til dømes Microsoft sin KI-assistent Copilot (Copilot for M365).

Pilotprosjektet har samarbeida med NTNU og Datatilsynet og deira prosjekt i den regulatoriske sandkassa; «Pilotere Copilot for Microsoft 365» våren 2024. Funnrapporten til NTNU og sluttrapporten til Datatilsynet er viktige kjelder til vårt arbeid, men vi har gjort eigne vurderingar og prioriteringar.

Deltakarar i arbeidsgruppa

Paal Fosdal – Oppdragsgjevar

Ane Storås – Utredningsleiar

Hilde Instefjord – Personvern

Sondre Selle – Microsoft Admin

Sondre S. Mo – Informasjonssikkerheit

Silje Sagen – Juridisk bistand

Mona Mellingen – Juridisk bistand

Vi skal ikkje innføre teknologien, for teknologien si skuld

Dersom teknologien skal innførast i organisasjonen må vi finne ut kva oppgåver denne teknologien kan tilføre verdi, løyse reelle utfordringar elle forbetre eksisterande prosessar.

Frå gevinstarbeidet

Samfunnsmål 1:

Vi tar i bruk ny teknologi og kunstig intelligens der det gir gevinst.

Samfunnsmål 2:

Møte dei forventingane som samfunnet og brukarane har til betre kvalitet, brukaropplevingar og effektivitet.

Potensielle registrerte er tilsette i fylkeskommunen, samarbeidspartnarar, innbyggjarar som kommuniserer med fylkeskommunen inklusive pasientar i tannhelsetenesta, og elevar og føresette i vidaregåande opplæring.

Leiarar, tilsette i HR, tilsette i avdelingar som handsamar mykje sensitive opplysningar og samhandlar med sårbare registrerte, er identifisert som grupper som utgjer ein ekstra personvernsrisiko.

Ny teknologi

Tilsette og innbyggarar i VLFK må, på den eine eller andre måten, forhalda seg til at det stadig dukkar opp nye metodar og system. Tal metodar og system som no kjem med ei form for KI i seg har eksplodert. Derfor er det viktig å undersøke både moglegheitene teknologien medføre og i kva grad VLFK er budd på dei endringane som kjem med denne typen teknologi.

Copilot for M365 har potensial til å gje store gevinstar, men berre dersom den digitale grunnmuren vår er solid. Verktøyet vil ha tilgang til dei same opplysningane som brukaren, noko som betyr at manglar som dårleg tilgangsstyring eller svak kontroll over personopplysningar vil bli meir tilgjengeleg, synlege og forsterka.

Sjølv om enkelte oppgåver utført av Copilot for M365 ikkje nødvendigvis involverer behandling av personopplysningar, er verktøyet komplekst og dynamisk. Måten data vert behandla på kan variere sterkt avhengig av korleis teknologien blir brukt. Den auka tilgjengelegheita som Copilot gir til informasjonen aukar og sansynlegheit for at samanstilling av ulike datasett kan føre til generering av ny, og i ytterste konsekvens sensitiv informasjon. Vi må difor legge til grunn at behandling av personopplysningar alltid vil kunne skje.

Copilot M365 er ny teknologi som behandlar enorme mengder personopplysningar, der risiko enda ikkje er kjent. Det er sansynleg at det av ulike grunnar kan bli behandla sensitive opplysningar om mennesker i sårbare situasjonar og den lærer av alt du gjer for å bli mest mulig lik deg. Det er ingen tvil om at denne programvara er utfordrande for personvernet.

Microsoft er utfordrande å forvalte

Vi legg til grunn at «det som kan bli gjort, vil bli gjort», og har med dette utgangspunktet utforska risikoar, svakheiter, moglegheiter og styrker ved teknologien i kontrollerte former og danna grunnlaget for å avgjere korleis-, og i det heile tatt om, vi bør ta i bruk Copilot for M365.

Copilot for M365 er i ein tidleg fase, og i stadig utvikling og endring, i tillegg kan Microsoft sine produkt generelt vere krevjande å forvalte, mellom anna på grunn av at selskapet opererer med ein "opt-out"-policy. Som funnrapporten frå NTNU beskriv:

> *«Microsoft aktiverer nye funksjonar automatisk. Dette krev at administratorar må deaktivere funksjonar dersom dei ikkje skal vere tilgjengelege. Brukarar må akseptere leverandørens vilkår fullt ut, og det er utfordrande å påverke løysingane i tråd med eigne behov eller retningslinjer. Dette kan føre til ein låst situasjon der ein blir avhengig av tenesta utan realistiske alternativ.»*

Namneendringane frå midten av 2024 der mellom anna M365 med Commercial Data Protection vart til M365 med Enterprise Data Protection, kom med endringar i kva opplysningar som blir samla inn til log, og med namneendringane på M365 sin web applikasjon og mobil applikasjon i januar 2025 der M365 vart namngitt M365 Copilot gir usikkerheit i korleis Copilot for M365 kjem til å endre seg, og korleis M365 som ei plattform kjem til å endre seg som følgje av at funksjonar blir lagt til, og namn smeltar saman.

Å skilje informasjon om behandling mellom disse plattformene er vorte ekstremt utfordrande ettersom tenester med same namn, eller veldig liknande namn har ulike omfang ovanfor behandling av informasjon og personopplysningar. Med denne utviklinga er det vanskeleg å ha god tru på at vi har kontroll på opplysningane når nye behandlingar er opt-out og ikkje opt-in.

Måten Copilot for M365 fungera på er i stor grad basert på data frå Microsoft Graph. Ei vurdering av Microsoft 365 plattforma som heilheit og særleg vurdering av Graph er avgjerande for å kunne vurdere den fulle risikoen med bruken av Copilot for M365.

Orden i eige hus

Microsoft sin dokumentasjon og anbefalingar byggjer på føresetnaden om at organisasjonen har full kontroll over forvaltninga av plattforma. Diverre syner funn frå pilotprosjektet at mange eksisterande rutinar og retningsliner ikkje blir etterlevde på ein tilfredsstillande måte.

Informasjon Copilot for M365 hentar frå Graph, er informasjon du allereie i dag har tilgang til å hente gjennom søk i Sharepoint, og kan på kort tid finne samanhengar og setje saman informasjon frå ulike datakjelder inkludert kjelder som du ikkje visste du hadde tilgjengeleg.

Dette krev ikkje berre gode styringssystem og klare prosedyrar, men òg aktiv innsats ute i organisasjonen, for å auke kunnskapen informasjonsforvaltning og informasjonssikkerheit. Vi må gi leiarar den kunnskapen og støtta dei treng for å ta dette ansvaret på alvor, og den enkelte medarbeidar må forstå si rolle og korleis deira daglege handlingar påverkar sikkerheita. Kompetanse er nøkkelen til å lukke gapet mellom intensjon og etterleving, og slik byggjer vi eit solid fundament for digital utvikling i VLFK.

Menneskeleg kontroll er avgjerande, og vi ser at opplæring og kompetanseheving må prioriterast framfor berre å utarbeide nye rutinar og rettleiarar. Kompetanse er nøkkelen til å lukke gapet mellom intensjon og praksis, og å byggje ei felles forståing blant alle i organisasjonen vil vere avgjerande for ein trygg og ansvarleg bruk av verktøy som Copilot for M365.

Kva vurderingar må gjerast dersom vi skal ta verktøy i bruk?

Dersom Copilot for M365 skal implementerast i faktiske arbeidsoppgåver, må ein først og fremst ha gode behandlingsprotokollar, og ein gjennomgang av dei, for å sikre at Copilot-verktøyet passar inn i eksisterande behandling med særleg fokus på formål og behandlingsgrunnlag.

Denne rapporten gir eit utgangspunkt for vidare vurderingar, men vi understrekar at ytterlegare analysar må utførast før ein implementerer Copilot for M365 i konkrete arbeidsprosessar.

Forutsetningar vi har gjort i denne vurderinga er at Copilot for M365 er eit verktøy som blir lagt til i dei definerte, eksisterande behandlingar og får same formål og skal kunne nyttast med same behandlingsgrunnlag som i den oppgåva det skal brukast i. For kvar prosess der ein vurderer å bruke Copilot for M365, må det vurderast om verktøyet er nødvendig, og om det inneber ein balanse mellom nødvendigheit og inngripen.

Denne DPIA kan fungere som eit grunnarbeid, for dei oppgåvespesifikke DPIA som må gjerast før Copilot for M365 kan brukast som verktøy i arbeidet, men det forutset at den held seg relevant. Teknologien er i stadig endring, og vi slit med å levere oppdaterte vurderingar.

Måten Copilot for M365 fungerer på er i stor grad basert på data frå Microsoft Graph. Ei vurdering av Microsoft 365 plattforma som heilheit og særleg vurdering av Graph er avgjerande for å kunne vurdere den fulle risikoen med bruken av Copilot for M365.

Bruken vil også gi oss komplekse utfordringar knytt til mellom anna datatilgang og handsaming av sensitive data og ikkje minst utfordringar knytt til formål, formålsavgrensing og behandlingsgrunnlag som er viktige prinsipp i personvernsarbeidet.

Initialvurdering

Den behandlingsansvarlege er forplikta til å gjennomføre ei personvernkonsekvensvurdering (DPIA) dersom behandlinga medføre høg risiko for personar sine rettigheiter og friheiter, og følgande er vår initialvurdering av risikoane med Copilot for M365.

Omfattar behandlinga særlege kategoriar av personopplysningar eller personopplysningar av svært personleg karakter? - JA

I utgangspunktet ikkje. Copilot for M365 skal berre ha tilgang til opne og interne data.

Basert på våre funn så langt, er det likevel svært sannsynleg at avvik vil oppstå, og at tenesta vil få direkte tilgang på sensitiv informasjon. Vi kan ikkje svare nei på denne før vi har lukka gapet mellom intensjon og praksis.
Bruk av labeling og eit aktivt forhold til tilgangsstyring er døme på at intensjon og praksis ikkje stemmer overeins. Det blei mellom anna avdekt at leiar har delt skrivebordet sitt med tilsette som hadde tilgang til alt på skrivebordet utan at vedkommande var klar over det. Eller at arbeidsavtalar vart henta ut frå fagsystem og lagt i Teams utan streng tilgangsstyring.

Samtidig vil Copilot-algoritmen lære av brukaren si åtferd, skrivestil, tankemønster og liknande, noko som samla sett kan bli til opplysningar av svært personleg karakter. Informasjon som Copilot for M365 lære seg om deg er berre tilgjengeleg for deg, og vil krevje jamleg bruk.

Inneber behandlinga predikasjon av åtferd, profilering av, rangering av, evaluering eller poengsetting av individ? - JA

Copilot tilpassar seg til brukaren ved å analysere data frå dokument, e-post og kommunikasjon. Denne prosessen inneber ei form for dynamisk profilering, då verktøyet nyttar data til å etterlikne brukaren sin skrivemåte og åtferd. Vi veit lite om korleis dette føregår, og det er viktig å avklare om Copilot opprettar vedvarande profiler eller berre midlertidige analysar.

Inneber behandlinga automatiserte avgjersler som påverkar den registrerte sine rettar? - NEI

Nei. Copilot gjer ikkje automatiserte avgjersler som har rettslege eller tilsvarande vesentlege konsekvensar for individ.

Inneber behandlinga systematisk overvaking av den registrerte? - NEI

Nei. Copilot for M365 overvakar ikkje kontinuerleg aktivitetar eller handlingar frå brukarar.

Copilot for M365 baserer seg derimot på informasjon frå Graph, som loggar aktivitet uavhengig av Copilot for M365. Denne informasjonen kan fort inngå som systematisk overvaking, og vert underbygd av øvrige påstandar om at det vil være naudsynt med ei vurdering av Graph og Microsoft plattforma som heilheit.

Blir det gjennomført behandling i stor skala? – NEI

Nei. Behandlinga er avgrensa til data som er direkte relevante for den aktuelle brukaren og avgrensa seg til det bruker har direkte tilgang til og brukar.

Matching eller samanstilling av fleire datasett? – Kanskje?

Det er ikkje oppgitt at Copilot samanstiller datasett som inneheld personopplysningar. Likevel baserer Copilot seg på integrasjonar mellom system som Microsoft Graph og Insight. Denne samansettinga kan potensielt skape nye personopplysningar eller føre til utilsikta behandling. Dette bør vurderast nærmare for å sikre samsvar med GDPR.

Omfattar behandlinga personopplysningar om sårbare registrerte? - JA

Maktubalansen mellom tilsett og leiing, og/eller informasjon på avvege som omhandlar tema som set tilsette i ein sårbar situasjon, vil sei at tilsette er sårbare registrerte i dette tilfellet.

Det er og sannsynleg at programvara indirekte eller direkte får tilgang til informasjon om unge under 18 år, til dømes dersom programvara vert brukt i, eller i forbindelse med opplæring i vidaregåande skule. Det skal i utgangspunktet unngåast, men på lik linje med korleis vi ikkje kan utelukka sensitiv informasjon, gjeld det same for sårbare registrerte.

Omfattar behandlinga innovativ bruk av personopplysningar eller teknologiar der risikoen enno ikkje er kjend? - JA

Ja. Copilot for M365 er basert på generativ kunstig intelligens, ein teknologi som framleis er relativt ny og lite dokumentert. Bruken av Copilot må derfor avgrensast til kontrollerte miljø, slik at risikoar kan avdekkast og handterast.

Hindrar behandlinga den registrerte i å utøve ein rett, ein teneste eller ein kontrakt? – NEI

Det er ikkje tydeleg at Copilot sjølv hindrar rettar, tenester eller kontraktar. Likevel kan innsamlinga av data i tilknytte Microsoft-tenester vere problematisk i høve til GDPR. Denne problematikken må vurderast separat, men kan påverke det samla risikobildet for Copilot.

Konklusjon: Det må gjennomførast ein DPIA for M365 Copilot.

Behandlingsansvar

Behandlingsansvarleg: *Vestland fylkeskommune*

Databehandlar: *Microsoft*

Det kan diskuterast i kva grad Vestland fylkeskommune kan regnast som sjølvstendig behandlingsansvarleg, då det er fleire aspekt ved behandlinga vi ikkje er klar over at skjer, eller får anledning til å motsei oss.

Vi er likevel ansvarlege for kva data som blir gjort tilgjengeleg for tenesta og på denne måten vil vi bestemme kva personopplysningar som vert nytta, sjølv om vi har avgrensa tilgang til å sei på kva dei skal brukast til og kvifor.

Microsoft sine standardavtalar har også denne formuleringa. Det er usannsynleg at vi kan gå i forhandlingar med Microsoft på dette. Dei vil ha ei forventning om at vi godkjenner deira standard avtalar.

Microsoft har hovudkontor i USA og er del av the Data Privacy Framework (DPF) Program som betyr at dei har mekanismar som sikrar at personopplysningar får same vern i USA som dei har krav på etter GDPR. Ifølge databehandleravtalen som Microsoft har på sine nettsider, vert data lagra enten i Norge, Sverige, eller Irland.

VLFK må velje kor lenge data skal vere lagra før dei blir sletta.

Behandlingsgrunnlag og føremål

Det som gang på gang stikk kjeppar i hjula i arbeidet med personvern og Copilot for M365 er diskusjonane rundt formål og behandlingsgrunnlag.

Vi har vore innom ulike løysingar i tidlegare versjonar av DPIA blant anna:

- Formål var å teste ut ny teknologi i kontrollerte former – basert på samtykke frå pilotane som var med.
- Formål var tre spesifikke oppgåver basert på legitim interesse og interesseavveginga viste at vi hadde mange gode grunnar for å bruke dette verktøyet, og at dei tre oppgåvene var lavrisiko med tanke på personvern.
- Tredje løysing var å bruke dei same 3 spesifikke oppgåvene, men denne gongen basert på det same behandlingsgrunnlaget som oppgåvene hadde for øvrig.

Problemet vi ikkje klarte å løyse i desse scenarioa, er at Copilot M365 er eit massivt verktøy som prosesserer enorme mengder data. Mykje av behandlinga skjer uavhengig av kva vi vel å definere som hensiktsmessige formål. Den integrerte oppbygginga av produktet er designa for å kunne brukast i mange ulike kontekstar og til forskjellige oppgåver. Det er urealistisk å tru at ein brukar med tilgang vil avgrense bruken til dei definerte formåla, og på same måte urealistisk å tru at data som blir brukt i behandlingane er avgrensa til formålet med å ta tenesta i bruk.

I denne utgåva av DPIA fokusera vi primært på personvernkonsekvensar av teknologien og ikkje på spesifikke prosessar og vil undersøke personvernsrisikoar rundt følgande to spørsmål:

Kva data får Copilot for M365 tilgang til?

Dette handlar om å forstå korleis data blir prosessert og lagra, og korleis dette kan føre til utilsikta bruk eller eksponering av sensitive opplysningar.

Kva data Copilot for M365 kan generere?

Her må vi undersøke korleis algoritmen etterliknar brukaren ved å analysere åtferd, skrivestil og tankemønster.

Behandling

Dei risikoane som vi ser på i denne DPIA er dei vi har identifisert som oppstår ved bruk av Copilot for M365, uavhengig av kva overordna oppgåve som skal løysast.

Avgrensingar

DPIA er avgrensa til dei operasjonane som vert utløyste ved aktivering av Copilot, og omfattar ikkje bruksområda som tenesta kan nyttast til. Det vil seie at dei operasjonane vi beskriv her, vil være nødvendige for å mogleggjere funksjonaliteten til Microsoft 365 Copilot og er uavhengig av kva formål og behandlingsgrunnlag du har.

Vidare er denne DPIA avgrensa til Copilot for M365 og inkluderer ikkje testing eller vurdering av andre Copilot-produkt. Det er viktig å merke seg at Microsoft brukar «Copilot» som eit generisk merkevareomgrep for fleire ulike produkt, og denne rapporten omfattar ikkje andre tenester med same namn.

Operasjonar utløyst ved aktivering av Copilot for M365

Følgande er ei liste over operasjonar som sannsynlegvis vil bli utløyste ved bruk av Copilot for M365 basert på det vi veit om tenesta.

- **Behandling av data frå Graph som er innsamla frå ulike M365-applikasjonar**:
    - Henting av data frå e-post i Outlook (inkludert innhald, metadata, og vedlegg).
    - Tilgang til filer i OneDrive og SharePoint for å analysere innhald.
    - Innsamling av chatteloggar og samtalar i Microsoft Teams.
    - Analyse av kalenderinformasjon for møtedetaljar, deltakarar og tidsplanlegging.

- **Analysere**, **organisere og kategorisere informasjon basert på relasjonar**
    - Semantisk analyse av dokument og e-post for å identifisere relevante punkt.
    - Oppbygging av relasjonar mellom ulike datakjelder for å gi kontekstuelle forslag.
    - Prosessering og lagring av data i Microsoft sine serverar, også andre servera enn de er lagra – men alltid innanfor EU.
- **Analyse og bruk av informasjon for å generere**
    - Oppretting av samandrag av e-post, dokument eller samtalar.
    - Generering av forslag til møtenotatar, oppgåver eller dokumentutkast.
- **Loggføring og overvaking**:
    - Lagring av brukarinteraksjonar og spørjingar sendt til Copilot, og lagra i samsvar med avtale.
    - Bruk av loggfiler for feilsøking og forbetring av yting.
- **Tilgangsstyring og brukaridentifikasjon**:
    - Autentisering og autorisering av brukarar via Microsoft Azure Active Directory.
    - Tilgangskontroll for å sikre at berre godkjente brukarar kan aktivere og bruke Copilot.
- **Kontinuerleg læring og tilpassing**:
    - Tilpassing basert på brukaren sine arbeidsmønster og preferansar.

Personopplysningar

Omfang

Vi har hatt mindre enn 40 pilotar. Så lenge Microsoft ikkje tillèt å skru av funksjonalitet som gjer at Copilot har tilgang til e-post, vil alle som sender e-post til ein av pilotane potensielt bli behandla. Vi har 7000 tilsette. Dei av dei tilsette som pilotane er i kontakt med kan potensielt bli behandla. Piloten har berre vore tilgjengeleg for utvalde tilsette på avdelinga næring, plan og innovasjon, ei avdeling som normalt har relativt lite personopplysningar i saksbehandlinga si.

Personopplysningane som blei nytta vart henta frå M365 profilen, som betyr at informasjonen om pilotane vart henta inn frå andre kjelder enn brukaren sjølv.

Behandlinga skjer kontinuerleg.

Sikring av personopplysningar

Personopplysningar er sikra ved at dei berre blir lagra og behandla på Vestland fylkeskommune sin Microsoft 356 tenant. Ved å skru av «Web search for Microsoft 365 Copilot and Microsoft Copilot» sikrar vi oss mot at informasjon frå brukaren sine prompts blir sendt ut mot internett via Bing-søk.

Det er i utgangspunktet ingen "overføring" mellom Microsoft Graph og Semantic Indeks ettersom det er innanfor tenant til Vestland fylkeskommune. Informasjon som blir overført mellom brukars einheit og tenant er sikra med HTTPS. Dette vil da vere interaksjonar som brukaren gjer.

Personopplysningane er behandla/brukt innanfor tenant til Vestland fylkeskommune.

Personopplysningane blir kryptert ved lagring og er berre tilgjengelege for den enkelte brukar og administrator. Disse personopplysningane er da lagra innanfor tenant til Vestland fylkeskommune.

Informasjon i prompt som legg inn i Copilot for M365 kan bli sletta på to ulike måtar. Anten blir det sletta via at enkeltbrukar gjer det sjølv ved sletting av interaksjonslogg, eller via å legge inn førespurnad til systemforvaltar for sletting i Microsoft Graph. Personopplysningar blir også sletta via ivaretaking av informasjon i tenant til Vestland fylkeskommune.

Table 1 Personopplysningar som sannsynlegvis blir, eller kan bli behandla i samband med bruk av Microsoft 365 Copilot

Kategori	Type data	Beskrivelse
Identifikasjonsinformasjon	Namn	Brukarens namn for å identifisere brukaren.
Identifikasjonsinformasjon	E-postadresse	Tilknytt brukarens Microsoft 365-konto.
Identifikasjonsinformasjon	Brukarnamn	Unikt namn eller ID brukt i Microsoft-systemet.
Identifikasjonsinformasjon	Organisasjonstilknyting	Informasjon om organisasjonen brukaren er tilknytt.
Identifikasjonsinformasjon	IP-adresse	Brukaren sin nettverksadresse for å sikre at datahandsaming skjer innanfor avtalt område og sikkerheitskrav.
Identifikasjonsinformasjon	Einingsinformasjon	Informasjon om brukte einingar, som operativsystem og nettlesartype.
Kommunikasjonsdata	E-postmeldingar	Innhald og metadata frå e-postar i brukaren sin konto.
Kommunikasjonsdata	Chatteloggar	Innhald og metadata frå Teams eller andre Microsoft 365-chatfunksjonar.
Kommunikasjonsdata	Kalenderdata	Informasjon om møter, arrangement og tilknytte deltakarar.
Dokument og filer	Innhald i dokument	Tekst, tabellar, bilete og annan informasjon frå dokument lagra i OneDrive, SharePoint eller Teams.

Dokument og filer	Filnamn og filmetadata	Informasjon som namn, opprettingsdato og eigarskap.
Brukardata og tilgangsinformasjon	Brukaraktivitet	Loggar over bruk av Copilot-funksjonar (når og korleis tenesta blir brukt).
Brukardata og tilgangsinformasjon	Tilgangsrettar	Rettar og tilgangsnivå som definerer kva data brukaren har lov å sjå.
Kontekstuelt genererte data	Forslag generert av Copilot	Automatiske forslag, oppsummeringar og innsikt skapt ved bruk av data frå brukaren.
Kontekstuelt genererte data	KI-modellerte innsikter	Mønster eller samanhengar identifiserte av KI-verktøyet for å tilby meirverdi (t.d. prediksjonar eller anbefalingar).
Deling og samhandling	Deltakarar i kommunikasjon	Namn og kontaktinformasjon for andre involverte i e-postar, chattar og møte.
Deling og samhandling	Delte dokument	Dokument som er delt med andre, inkludert tilgangsnivå og brukshistorikk.
Andre metadata	Tidsstempel	Informasjon om når data vart oppretta, brukt eller endra.

Risikoanalyse

Rett til innsyn

Vi har ikkje full oversikt over informasjonen som blir forvalta i denne tenesta, og det er utfordrande å etterleve dette kravet. Det er og viktig å ha eit bevisst forhold til problematikken rundt at M365 er eit stort univers med lagring i OneNote, SharePoint, teams, Outlook og e-post.

Informasjon som kjem på overflata som følge av bruk av Copilot, stammar sannsynlegvis frå eit avvik i ein anna prosess.

Vi har ikkje oversikt over eventuelt skjult informasjon og loggar av bruk som Microsoft forbeheld seg retten til å lagre, for å kunne oppdage ulovleg bruk.

På grunn av den såkalla «black box»-naturen og tilpassingsdyktigheita høyrer denne typen algoritmar til klassen av forsterkingslæringsalgoritmar. For at algoritmen skal fungere og skape verdi for VLFK, er han avhengig av både informasjon og åtferda til dei menneska som brukar han. Algoritmen lærer på liknande vis som anbefalingsalgoritmar for plattformer som TikTok, YouTube og Netflix.

Rett til informasjon

Den informasjonen som er tilgjengeleg frå Microsoft, tar ikkje høgde for offentlege aktørar. Microsoft hevdar dei etterlev krav, og delar informasjon som skal understøtte dette, men vil ikkje svare på direkte spørsmål. Pilotprosjektet skal ideelt sett gi oss eit fullstendig og klart bilete av behandlinga. Eksterne aktørar som er i kontakt med oss veit ikkje om at vi brukar Copilot for M365.

Lovleg behandling

Problem med samtykke Først vurderte vi pilotprosjektet som ei eiga behandling – og at formålet var å utforske teknologien og programvara. Og til dette ville vi samle inn samtykke frå dei som fekk programvara aktivert på sin brukar. Behandlinga av personopplysningar i dette prosjektet var derimot ikkje avgrensa til å gjelde berre dei med lisens på Copilot. Også alle tilsette som samhandlar med pilotørane, til dømes via e-post, ville blitt omfatta. Dette ville i praksis innebere at alle tilsette, og eit ukjent tal eksterne aktørar vil kunne komme i ein situasjon kor ein samhandlar med ein pilotør og dernest dele personopplysingar anten om seg sjølv eller andre.

Problem med formålsavgrensing Det blei samtidig vanskeleg å få eit reelt bilde av personvernskonsekvensane når «testing av verktøy» var formålet. Det som programvara kan brukast til, vil den og bli brukt til og det var vanskeleg å sjå føre seg spekteret av scenario, og ikkje minst tenkje seg til verst tenkelege scenario – noko man gjerne ønsker å sjå føre seg i ei slik vurdering. Ei anna utfordring var å handtere at vi enda stort sett opp med den same konklusjonen uansett kva vurderingar vi gjorde: problema handla om bruk av M365-plattformen som heilskap – og ikkje at det ville lagt til noko ekstra risiko å bruke Copilot i oppgåva. Det manglar og ei oppdatert risikovurdering av M365-plattformen som heilskap. Som gjorde det vanskeleg å konkludere.

Dette betyr i sum at Copilot ville komme til å behandle «enorme mengder personopplysningar» på «ukontrollerte måtar», noko som harmonerer dårleg med personvern, som berre skal behandle personopplysningar for spesifikke formål.

Når vi gjekk over til å vurdere enkelte formål (spesifikke oppgåver på NPI) blei det klart at dette verktøyet blei altfor kraftig og inngripande sett i lys av den oppgåva som skal gjerast.

Problem med legitim/rettkomen berettiga interesse: For å bruke dette behandlingsgrunnlaget må behandlinga vere «nødvendig» og den må vere knytt til dei formåla dei rettkomne interessene er meint å ha for den behandlingsansvarlege. Dette inneber at det må ligge føre ei interesseavveging som synleggjer kva for interesser som er vektlagde og korleis desse er vurderte. Både i denne interesseavveginga og midtvegsrapporten går det fram at ein er usikker på kor mykje data M365 eigentleg samlar inn. Sidan Copilot for M365 skal kunne samle/hente nok data til å gje svar på spørsmål, må ein legge til grunn at det vert samla, eller henta, inn både relevante og irrelevante data om personar. Ambisjon om eit velluka resultat er ikkje tungtvegande nok når ein potensielt samlar inn data om tilsette i eit prøveprosjekt.

Rettferdig behandling

Tilsette kan i utgangspunktet ikkje reservere seg mot å få sine opplysningar behandla i Copilot for M365 dersom VLFK bestemmer seg for å aktivere lisens på ei gruppe, eller alle tilsette. Tilsette er avhengig av at leiar, og andre som behandlar personopplysningar om dei, ikkje lagra opplysningane på feil område og at dei er gode på merking av (labeling) eventuelle filer på rett måte. Det er ein stor risiko med ein så stor grad av menneskeleg avhengigheit. Dette er ikkje ein innarbeida praksis i VLFK og vi må jobbe med den digitale grunnmuren. Avgrensa og sensitiv informasjon blir indeksert i Microsoft Graph – men skal ikkje være tilgjengeleg for denne behandlinga.

Openheit

Vi formidlar alt vi veit om tenesta. Leverandør ikkje har full openheit rundt kva opplysningar som blir behandla. Vi veit mykje om datastraum og kva som går inn og ut av vår tenant, men ikkje heit kva opplysningar det er snakk om.

Det er likevel personopplysningar iform av koplingar mellom filer, e-post og andre informasjonskjelder og den registrerte som ikkje er synlege. Eksempel på dette kan være at Graph/Insight registrera at ein

person har vore inne i eit dokument i eit gitt tidsrom. Det kan tenkast at Copilot blir brukt i oppgåver utover det dei registrerte er kjend med, men pilotprosjektet har klare definerte formål.

Formålsavgrensing

Copilot for M365 gjer det vanskeleg å definere formål, og å sikre lovleg heimel. Formålsavgrensing er på noverande tidspunkt berre mogleg med mindre inngripande verktøy som er meir spissa mot ei spesifikk oppgåve, og med klare definerte formål.

Dataminimering

Informasjonsklassifisering (følsomheitsetikettar) syt for at sensitiv og avgrensa informasjon blir unnateke, og ryddejobben på førehand skal syte for at det berre er nødvendig data som blir del av behandlinga. Vi avgrensar kva tenesta har tilgang til gjennom sensitivitetsmerking og sletting av dokument. Datagrunnlaget er i stor grad brukarstyrt. Vi kan ikkje forvente at det ikkje blir avdekt avvik.

Den såkalla «black box»-naturen som er avhengig av både informasjon og åtferda til dei menneska som brukar den og mangelfull dokumentasjon frå leverandør er det sannsynleg at dataminimering ikkje er eit konsept som Copilot for M365 er i stand til å etterleve. Heile poenget med å teste mindre kraftige verktøy, for å rette seg mot den aktuelle behandlinga, underbygger dette.

Rett behandling

Sensitivitetsmerking av datakjelda er ein sentral del av tiltak som må gjennomførast. Dette krev stor grad av manuell kontroll. Vi er i tidleg stadiet i sesitivitetsmerking i Vestland Fylkeskommune, og ein kjent utfordring er å oppretthalde kvaliteten i datagrunnlaget. Vi forventar at avvik vil oppstå.

Usannheit og hallusinering i svara frå programvara er eit anna spekter av dette. Data som tenesta kjem med som svar på prompt kan i stor grad være personopplysningar som ikkje treng å stemme. Usannheit og hallusinering er eit vanleg problem med dagens KI-modellar.

Lagringsavgrensing

Her må vi referere til at vi treng ei vurdering av bruk av M365-plattformen som heilskap – og ikkje sjå på dette som risiko som kjem ved å bruke Copilot i oppgåva.

Integritet og konfidensialitet

Ut frå omtale av løysning frå Microsoft, skal den vere tilstrekkeleg sikra mot uautorisert eller ulovleg behandling. Rollebasert tilgangskontroll, at behandling av personopplysningar går føre innanfor tenant til Vestland Fylkeskommune, samt kryptering av personopplysningar er det ansett at det er eit tilstrekkeleg behandlingsnivå ved behandlingsaktiveteten.

Vi har derimot betydelege hol i den digitale grunnmuren vår og i den digitale kompetansen som gjer at vi ikkje er ein plass der vi kan ta dette i bruk, utan at det vil kunne ha stor risiko for integritet og konfidensialitet.

Konklusjon

Copilot M365 er ei ny teknologi som behandlar enorme mengder personopplysningar, der risikoen enno ikkje er fullstendig kartlagt. Det er sannsynleg at det, av ulike grunnar, kan bli behandla sensitive opplysningar om menneske i sårbare situasjonar. Teknologien lærer kontinuerleg av brukarane for å tilpasse seg deira arbeidsmønster. Dette gjer at personvern er ein av dei mest utfordrande aspekta ved bruken av Copilot M365, noko som krev grundige og hyppige vurderingar.

Personvernrisikovurderingar

For å adressere desse utfordringane er det lagt ned betydeleg arbeid i å overvake dei personvernsmessige aspekta ved teknologien. I prosjektperioden er det gjennomført tre hovudversjonar av personvernrisikovurderingar (DPIA), kvar med fleire revisjonar. DPIA er påkravd når det er identifisert risiko som krev tiltak for å identifisere og redusere personvernrisikoar.

Dette arbeidet handlar om å finne ein balanse mellom behovet for behandling av data og sikre lovleg og ansvarleg handsaming av personopplysningar.

Bruken av Copilot M365 i offentleg sektor

Overskrifter som «Toget går no!» og «80 % av offentleg sektor skal bruke KI» utfordra oss på balansen mellom personvernet til involverte personar, og nytten for VLFK.

Sjølv om dette kan ha ført til at vi på tidleg stadium av prosjektet tillét høg risiko ved å skru det på, blei risiko og personvern alltid nøye vurdert.

Grunnen til at vi slo av Copilot for M365 i vår organisasjon er samansett, blant anna at vi var usikre på om vi hadde basert det på eit faktisk lovleg grunnlag etter personvernforordninga.

Teknologiske utfordringar og risiko

Den integrerte oppbygginga av produktet er designa for å kunne brukast i mange ulike kontekstar og til forskjellige oppgåver.

Særleg viktig er det at teknologiens kompleksitet og dynamikk gjer det vanskeleg å føresjå korleis data vert behandla. Den auka tilgjengelegheita til informasjon aukar sannsynet for samanstilling av ulike datasett, noko som kan generere ny, og i verste fall sensitiv, informasjon.

Difor må vi alltid legge til grunn at behandling av personopplysningar kan skje, uavhengig av brukarens intensjon.

Alternativ til Copilot M365

Gjennom utprøving av andre KI-løysingar er det ikkje identifisert unike eigenskapar ved Copilot M365 som ikkje kan løysast like godt eller betre med mindre inngripande verktøy. Dette utfordrar prinsippet om dataminimering.

Formålsavgrensing og brukaråtferd

Den integrerte oppbygginga av produktet er designa for å kunne brukast i mange ulike kontekstar og til forskjellige oppgåver.

Eit viktig personvernprinsipp er formålsavgrensing, men det er urealistisk å tru at brukarar avgrensar seg til definerte formål. Mye av behandlinga skjer utanfor dei formåla vi har definert, og dette utgjer ein personvernrisiko.

Transparens og kontroll

Copilot for M365 er ein svart boks der du legg inn eit prompt og Copilot for M365 gjer resten. Brukar har få verkemiddel til å påverke kvar Copilot for M365 skal hente informasjonen sin frå når den får eit prompt. Den går til Microsoft Graph og hentar den informasjon den trur det er relevant og det einaste teiknet på at slik behandling har skjedd, er svaret den returnera. Dersom brukaren kunne avgrensa behandlinga til å peike på relevante samtalar med andre personar, e-postar eller dokument som faktisk er relevante, kunne det vore med å redusere unødvendig behandling av personopplysningar.

Overvaking av tilsette

Eit anna viktig spørsmål er i kva grad tenesta kan overvake tilsette.

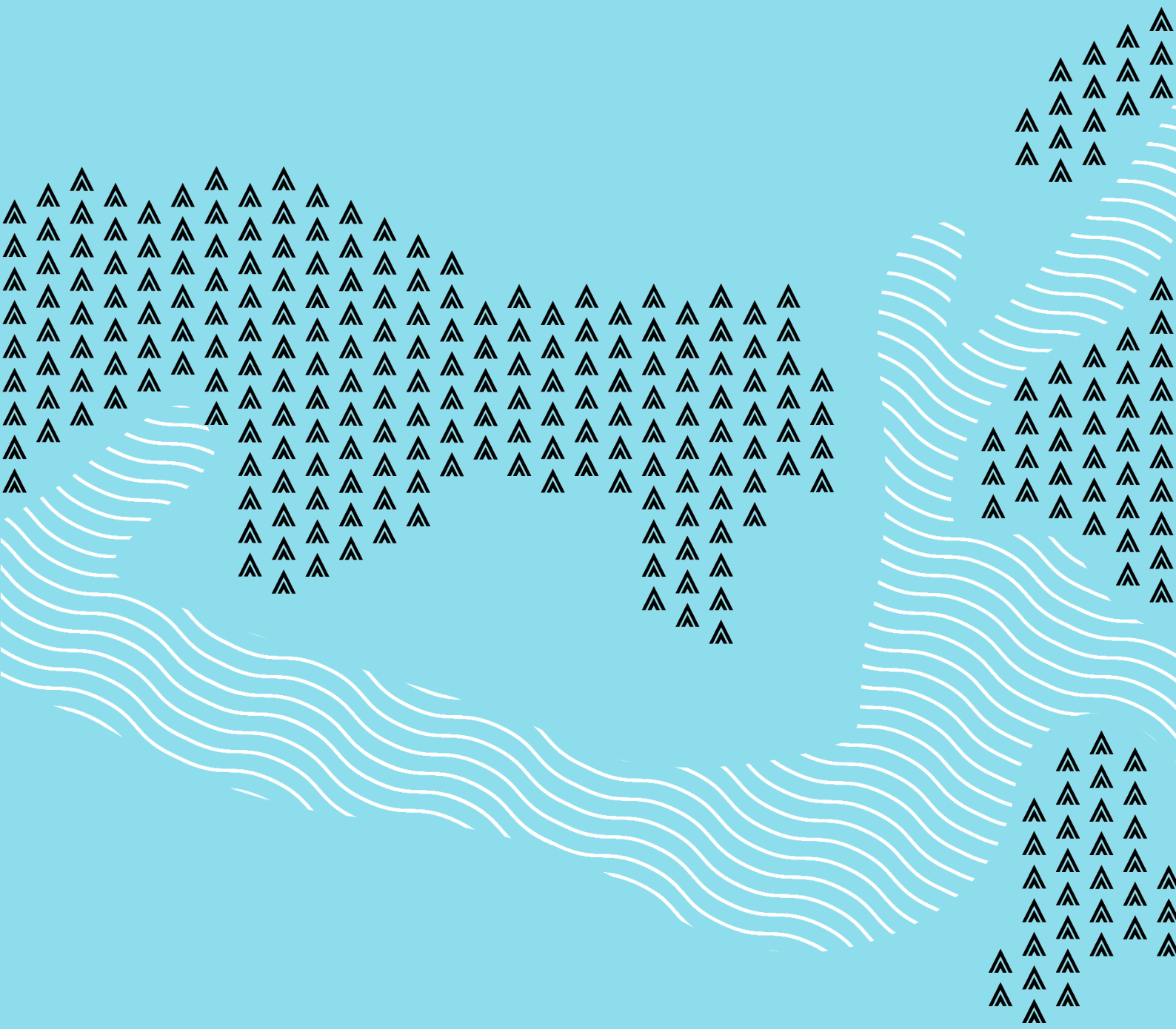
NTNU har, i sitt regulatorisk sandkasseprosjekt med Datatilsynet, identifisert at arbeidsgjevar kan overvake tilsette sin bruk av e-post og andre verktøy gjennom samhandlingsloggar, noko som kan vere i strid med e-postforskrifta. Per dags dato er den ikkje mogleg å skru på Copilot for M365 utan at den får tilgang til epost. I tillegg har Microsoft ein Microsoft "opt-out"-policy som inneber at funksjonalitet kan bli aktivert utan at organisasjonen er klar over det, noko som forsterkar risikoen.

Behov for kompetanseutvikling

For å kunne bruke Copilot for M365 på ein trygg og ansvarleg måte, må leiarar og tilsette få opplæring i teknologiens funksjonalitet og personvernimplikasjonar. Kompetanseutvikling er avgjerande for trygg bruk, og ei felles forståing av verktøya vil sikre ansvarleg bruk. Menneskeleg kontroll er viktig, og organisasjonen må prioritere kompetanseheving framfor berre å utarbeide rutinar og rettleiarar.

For å møte utfordringane med Copilot M365, krevst det gode styringssystem, klare prosedyrar og aktiv innsats i organisasjonen. Leiarar må få kunnskap og støtte for å ta ansvar, medan medarbeidarar må forstå deira rolle og handlingar.

Verktøyet har tilgang til all informasjon brukaren har, og kan forsterke svakheiter i tilgangsstyringa. Dette understrekar behovet for ein heilskapleg vurdering av Microsoft 365-plattforma, med særleg fokus på Microsoft Graph, for å sikre trygg bruk av Copilot for M365.



vestlandfylke.no