

## VURDERING AV PERSONVERNKONSEKVENSER (DPIA) FOR TESTPERIODEN

Vurdering av konsekvenser for behandling av personopplysninger (DPIA) er gjennomført som nærmere beskrevet nedenfor. Vurderingen er foretatt med utgangspunkt i personvernforordningen (GDPR) [artikkel 35](#).

|                                                                    |                                                                                          |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Behandlingen gjelder:                                              | Bruk av lisensiert versjon av M365 Copilot i en testperiode på 10 uker                   |
| Behandlingsansvarlig, jf. GDPR art. 4 nr. 7:                       | Klagenemndssekretariatet v/Anneline Vingsgård                                            |
| Ansvarlig/kontaktperson for vurderingen:                           | Olav Ottesen                                                                             |
| Andre involverte i vurderingen (bidragsyttere, interessenter mv.): | Caroline Lønne Michelsen (arkivar/prosjektleder), Marie Tamber Løbach (personvernombud). |

## 1. Om vurdering av personvernkonsekvenser skal gjennomføres

Personvernforordningen artikkel 35 slår fast at en vurdering av personvernkonsekvenser skal gjennomføres når det er sannsynlig at en viss type behandling av personopplysninger medfører høy risiko for at de registrertes rettigheter og friheter etter forordningen ikke ivaretas. I vurderingen skal det legges vekt på behandlingens art, omfang, formål og sammenhengen den utføres i. I tillegg skal det legges vekt på om det tas i bruk ny teknologi eller ny bruk av eksisterende teknologi hvor personvernkonsekvenser ikke har vært vurdert. Risikoen skal vurderes ut fra en objektiv vurdering der det fastslås om behandlingen av personopplysningene innebærer en risiko eller en høy risiko. En vurdering av personvernkonsekvenser krever i tillegg at det iverksettes nødvendige tiltak for å oppfylle de registrertes rettigheter utover minimumskravene, når behandlingen utgjør særskilt risiko for de registrerte (basert på art, omfang, formål og sammenheng). Med nødvendige tiltak menes tiltak som etter en forholdsmessighetsvurdering er nødvendig for å sikre balansen mellom personverninteresser og virksomhetens interesser.

Klagenemndssekretariatet (heretter "KNSE") har besluttet å teste den lisensierte versjonen av Copilot for Microsoft 365 (heretter også «Copilot»). Dette skal skje ved at en testgruppe gis lisenser og i en gitt periode forsøker å bruke systemet i arbeidet i KNSE. Testgruppen skal kun benytte Copilot i arbeidsrelaterte sammenhenger, og skal ikke bruke lisensen i private sammenhenger. Testingen er delt inn i tre faser, hvor fase 1 vil innebære moderat bruk av virksomhetens data, mens dette åpnes for helt i fase 2 og 3. I utgangspunktet er det ikke satt noen begrensninger på hva testgruppen kan gjøre med Copilot, så lenge det er knyttet til arbeidsoppgavene i sekretariatet. Tanken er at dersom testgruppen skal finne ut hvilke oppgaver Copilot kan og ikke kan brukes til, må den stå ganske fritt til å prøve seg frem. Eventuelle endringer i testgruppens mandat og føringer for bruken, vil naturligvis kunne påvirke vurderingene i denne konsekvensutredningen.

Jeg forutsetter at de behandlingsansvarlige og andre som skal ta stilling til bruk av Copilot har satt seg godt inn i systemet. Særlig anbefales NTNUs funnrapport og personvernombud Løbachs risikoanalyse.

Copilot for Microsoft 365 er et system/verktøy som er drevet av kunstig intelligens og som kombinerer store språkmodeller med innhold fra brukernes egne data i Microsoft 365. Det vil innebære at Copilot ikke fungerer som en språkmodell «ved siden av» andre programmer man bruker på pc-en, slik som Copilot Chat og andre åpne språkmodeller fungerer. Med en lisensiert versjon vil Copilot legge seg oppå alle programmene i Office-pakken (f.eks. Word og Excel), Outlook og Teams og få tilgang til alle data i disse programmene, i tillegg til tilgang til alle filer på brukernes OneDrive og SharePoint. Det er mulig å rettighetsstyre tilgangen, for eksempel slik at visse apper eller filer/mapper/områder holdes utenfor Copilots tilganger. I tillegg vil Copilot settes opp slik at den for hver bruker speiler brukerens tilganger. Det vil si at den får tilgang til de samme mappene og filene i OneDrive og SharePoint som brukeren med lisensen har. Copilot vil ikke ha tilgang til Klagenemndssekretariatets arkivsystem Public 360.

Copilot kan brukes fra enhver lokasjon og fra alle typer innretninger som PC, mobiltelefon, nettbrett etc. KNSE vurderer å begrense bruken til kun via PC, hvis mulig.

Dette innebærer for det første at Copilot som system gis tilgang til tilnærmet alle opplysninger som vi i KNSE til sammen har lagret og brukt i OneDrive, SharePoint og i Microsoft 365-universet. Dette vil innbefatte personopplysninger, også innenfor de særlige kategoriene. Jeg legger til grunn at Copilot som en del av Microsoft 365 har samme sikkerhetsnivå som den øvrige Microsoft Office-pakken, og at deling med et nytt verktøy hos Microsoft i seg selv ikke innebærer en større risiko enn tidligere. Bruk av lisensiert versjon av Copilot innebærer at den får tilgang til virksomhetens data i virksomhetens egen tenant, men at den ikke kan bruke dataen til trening av modellen. Det reduserer risikoen for at dataen forlater vår virksomhet.

Imidlertid vil Copilot for det andre, og dette er viktig, gjennom sin ubegrensede tilgang til våre data og sine enorme språkmodeller (som stadig utvikles), kunne benytte personopplysninger i et omfang vi tidligere ikke har vært i nærheten av, på måter vi vanskelig kan kontrollere eller redegjøre for, og på måter vi i dag trolig ennå ikke kjenner til. Det er åpenbart at dette har personvernkonsekvenser, uten at man enkelt kan si i hvilke tilfeller risikoene inntreffer, og om skadeevnen er stor eller liten.

Det er helt klart at man må gjennomføre en DPIA før Copilot tas i bruk. Jeg mener imidlertid at denne konsekvensutredningen kun kan ta stilling til overordnede forhold og risikoer ved Copilot, slik vi kjenner systemet i dag og med det perspektivet at en testgruppe skal teste og vurdere systemet. Dersom man underveis eller etter testperioden mener at systemet skal tas i bruk, bør det gjennomføres en eller flere nye konsekvensutredninger som ser nærmere på de konkrete bruksområdene testgruppen foreslår, der man også vurderer eventuelle tilgangsbegrensninger for copilot/personer. Dersom man ønsker å gi «full tilgang» til Copilot etter testperioden, bør dette også avstedkomme en ny eller oppdatert DPIA der erfaringene fra testgruppen inngår i vurderingen.

Det er ikke mulig innenfor dette mandatet å ta stilling til alle potensielle risikoer ved bruk av Copilot. Jeg har ikke gått inn i alle risikoer jeg har lest om eller identifisert. Jeg har forsøkt å få frem den sentrale forskjellen på Copilot sammenlignet med andre verktøy vi bruker, der risikoene som tas opp i denne konsekvensutredningen er på overordnet nivå og forhåpentligvis egnet til å beskrive hvilke risikoer bruk av Copilot innebærer. Ha dette i mente i den videre gjennomgangen.

## **2. Beskrivelse av behandlingen**

### **2.1. Behandlingen**

#### *2.1.1. Hvordan behandlingen av personopplysningene skal skje (behandlingsaktiviteter) samt omfanget av og sammenhengen behandlingen skjer i*

Dette punktet er utfordrende, om ikke umulig, å beskrive fullt ut, og dette er også årsaken til at en DPIA av Copilot er såpass krevende å gjøre.

Det er kun ansatte i Klagenemndssekretariatet som skal bruke Copilot i lisensiert versjon, og nemndsmedlemmene vil ikke få en slik lisens.

Copilot er ikke et vanlig program eller system der man kun gjennomfører angitte behandlingsaktiviteter, og hvor det er forholdsvis oversiktlig hvilket omfang bruken vil ha og i hvilken sammenheng behandlingen av personopplysninger vil skje. Copilot vil potensielt snu opp ned på hvordan opplysninger brukes i arbeidsprosessen, og det vil omfatte personopplysninger så lenge brukeren har tilgang til slike. Dette endrer også hvilke personvern vurderinger man må gjøre. Det er for eksempel klart at vi ikke kan slå oss til ro med at Copilot vil benytte personopplysninger som vi uansett har i organisasjonen, og at bruken derfor skal være uproblematisk. Copilot åpner for en bruk vi ikke har sett lignende til tidligere, som både mangedobler risikoer for brukerfeil som tidligere fantes og som kan skape nye risikoer vi ikke tidligere har kjent til, som for eksempel hallusinerer, sammenstilling av nye personopplysninger og bruk av opplysninger mennesker vil skjønne at de ikke skal bruke. Det finnes metoder som kan redusere disse risikoene, for eksempel standardiserte prompts og bruksområder, og dette må vurderes på bakgrunn av erfaringer fra testgruppen og forslag fra dem.

Copilot vil ha tilgang til alle filer i SharePoint og OneDrive som brukeren har tilgang til, samt alle opplysninger i Office-pakken, herunder Outlook og Teams. Copilot vil bruke alle disse opplysningene til å svare på de oppgaver den får, og vil, avhengig av spørsmålene brukeren stiller, generere svar, dokumenter og potensielt også nye personopplysninger til brukeren. Hvilke oppgaver vi kan sette Copilot til, er nesten kun begrenset av våre arbeidsoppgaver og fantasi. Det kan for eksempel være: Skrive avgjørelser, lage presentasjoner, lage møttereferat fra Teams, sladde taushetsbelagte opplysninger, lage svar til e-poster, bistå i arbeid med budsjett og regnskap, vurdere søkerlister og søkere og systematisere info om ansatte og nemndsmedlemmer. Det som blir produkt av testgruppens testing skal ikke brukes i produksjonen.

Siden Copilot bruker all informasjon den har tilgang til, er det kun organisasjonens policy og den enkelte ansattes etterlevelse av denne som setter begrensninger på Copilots tilgang. Videre vil ikke Copilot kunne skille mellom gode og dårlige kilder internt i våre arkiv, slik at den kan ta i bruk opplysninger som vi forstår vi ikke må bruke, slik som utkast med åpenbare feil og opplysninger om personer og ansatte som vi klart skjønner ikke skal benyttes.

Vi har ikke fullstendig informasjon om hvordan behandlinger skjer, annet enn at språkmodellene kort (og altfor enkelt) fortalt vurderer all data den sitter på, og gir det svaret som den mener statistisk sett er korrekt. Det vil ikke være mulig å få en nærmere redegjørelse fra Copilot på hvordan den kom frem til det aktuelle svaret.

### *2.1.2. Ny behandling/ny teknologi for behandlingsansvarlig*

Innføring av Copilot vil innebære en revolusjon i hvordan vi behandler og forholder oss til personopplysninger. Vi vil tillate en teknologi som bruker personopplysninger i et omfang vi ikke har sett før, på en måte vi i begrenset grad kan kontrollere og ha oversikt over, og teknologien kan også lage nye personopplysninger.

Det er åpenbare betenkeligheter ved å innføre systemet, og risikoene må vurderes opp mot de effekter vi tror bruken vil gi oss i arbeidet. Det er en rekke fordeler vi kan oppnå ved bruk av Copilot, både knyttet til effektivitet og kvalitet i arbeidet. Den nærmere vurderingen av dette må gjøres etter testperioden.

### *2.1.3. Tilgang til personopplysningene, herunder deling /overføring*

Det er i utgangspunktet ingen utover databehandlere og ansatte og nemndsmedlemmer med tilgang etter tilgangsstyring som vil ha tilgang til personopplysninger i organisasjonen. Dette utgangspunktet har imidlertid store forbehold, som omtales øvrige steder i konsekvensutredningen. Kort fortalt er ikke problemet at de ansatte har tilgang til personopplysningene i utgangspunktet, problemet er hvilken bruk vi åpner for.

### *2.1.4. Databehandlere (Art 4 nr. 8)*

Følgende leverandører skal benyttes som databehandlere:

Nordlo Bergen AS

Microsoft Norge AS

Det er inngått databehandleravtale med Nordlo Bergen AS, som igjen har databehandleravtale med underleverandør Microsoft Norge AS.

### *2.1.5. Overføring av personopplysningene ut av EØS (tredjeland) (GDPR kapittel 5)*

Personopplysninger skal som utgangspunktet ikke føres ut av EØS. I NTNUs funnrapport står det:

«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 (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.

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

NTNU skriver videre at «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 an bruk av web plug-in medføre datalekkasje utenfor EU.»

Copilot virker å være underlagt samme regime som resten av Office-pakken og Microsofts løsninger, og risikoen for at data overføres ut av EØS fremstår i utgangspunktet ikke høyere ved bruk av Copilot enn øvrige Microsoft 365-produkter, som Teams. Viser for øvrig til DPIA for bruk av Teams.

#### 2.1.6. Sikkerhet ved behandlingen (informasjonssikkerhet) (Art 32)

Copilot opererer med en sikkerhetsgaranti når man er innlogget med jobbkonto, som heter «Enterprise data protection» (EDP). I høyre hjørne av applikasjonen finnes et skjoldsymbol, som viser at EDP er påskrudd. Når EDP er påskrudd, betyr dette ifølge Microsoft at dataene du skriver inn er beskyttet av sikkerhetspolicyer, at prompts og svar benyttes ikke til å trene de underliggende språkmodellene, og at dataene holdes adskilt fra andre virksomheter. Både ulisensiert versjon og lisensiert versjon på arbeidsplassen har denne beskyttelsen, men en lisensiert versjon vil ha mye bredere tilgang til virksomhetens data.

Personvernrisikoene gjelder i liten grad sikkerheten i selve Copilot-funksjonen, men at man gjennom bruken får tilgang til store mengder personopplysninger bevisst og ubevisst, og at man benytter og viderebringer disse i strid med personvernforordningen. I tillegg er et iboende problem med Copilot at vi risikerer å bruke personopplysninger utover formålsbegrensningene etter personvernforordningen. Dette kan for eksempel være personopplysninger som ligger i faktisk utdrag i en klagesak, og som er sendt inn av den registrerte til behandlingen av en bestemt sak. Vi vil ikke nødvendigvis ha samtykke til å bruke disse opplysningene når vi løser en annen sak, og det var heller ikke formålet med innhenting av opplysningen. Et annet eksempel er personopplysninger fra en ansettelsesprosess som er lagret på OneDrive til en av de ansatte som arbeidet

med ansettelsesprosessen og innstillingen, og så blir opplysningene senere brukt i forslag til e-poster til denne personen eller som omhandler denne. Dette er utenfor de formål opplysningene ble innhentet for.

#### *2.1.7. Involvering*

Nordlo har bistått med en risikoanalyse, og personvernombudet har skrevet en risikovurdering.

Direktør Anneline Vingsgård er tett involvert i prosessen og holder ledergruppen informert. Testgruppen vil få en sentral rolle i det videre arbeidet. Testgruppen består av Andrea Olstad Solberg, Caroline Lønne Michelsen, Hallstein Vinje, Julie Vabø, Marie Tamber Løbach og Mathilde Thorbjørnsen.

Man bør på et tidspunkt vurdere å hente inn erfaringer og bistand utenfra, for eksempel organer som allerede har forsøkt å benytte Copilot og/eller Datatilsynet. Det er etablert kontakt med Diskrimineringsnemnda.

## **2.2. De registrerte**

### *2.2.1. Registrerte*

Med «Registrerte» menes de fysiske personer som personopplysningene som omfattes av behandlingen, kan knytte seg til direkte eller indirekte, jf. GDPR art. 4 nr. 1.

De registrerte vil være kunder (klagere og deres evt. representanter samt ansatte ved andre offentlige instanser), alle ansatte i KNSE, Teams-medlemmer og alle andre som er eller har vært i kontakt med KNSE per e-post, Teams og brev (selv om brev går direkte til p360, vil for eksempel brev som senere (mellom)lagres lokalt eller inngår i faktiske utdrag bli tilgjengelig for Copilot).

Siden vi stort sett jobber med norske aktører, vil de registrerte i hovedsak være lokalisert i Norge. Gitt hvilke type saker vi jobber med, vil behandlingen av personopplysninger til sårbare grupper være begrenset for de fleste nemnder.

Her er likevel noen eksempler på registrerte som kan trekkes frem.

- Energiklagenemnda har saker der man behandler helseopplysninger om enkeltpersoner, som det vil være særlig kritisk om blir brukt utover det formål de ble innhentet for.

- Stiftelsesklagenemnda, frivillighetsregisternemnda og Finanstilsynsklagenemnda behandler saker der det gis mange opplysninger om ledelsen i selskapene. Disse opplysningene kan være av særlig kategori, eller kan ved en sammenstilling skape nye personopplysninger om de registrerte.
- Søkere til stillinger hos oss. Det er svært viktig med disiplin i lagring og tilgangsstyring i disse sakene, slik at informasjonen ikke går til Copilot. Ved bruk av Jobbnorge vil pdf-er man åpner alltid lagres i nedlastinger (i hvert fall på min bruker), slik at jeg må inn i nedlastinger og slette etter hver gang jeg har jobbet i Jobbnorge. Denne innstillingen må endres, evt. Nekte Copilot tilgang til nedlastingsmappen til den enkelte bruker.
- KUY – kan potensielt ha personopplysninger knyttet til enkeltpersoner fra andre land, også okkupert området og innen særlige kategorier.

### 2.2.2. Behandlingens åpenhet/transparens (art. 5 nr. 1 bokstav a)

KNSE lagrer og behandler opplysninger i klagesaker vi blir tilsendt. I utgangspunktet behandler KNSE kun personopplysninger som vi har fått tilsendt fra brukere av sekretariatet (typisk klagere og underliggende tilsyn), ansatte og andre som vi er i kontakt med gjennom vårt arbeid. Deltakere på kurs og konferanser, for eksempel KOFA-konferansen, og jobbsøkere vil også inngå så lenge vi er i kontakt med dem via e-post eller andre Office 365-systemer (for eksempel intervjuer på Teams), eller lagrer dokumentasjon i Onedrive eller Sharepoint. Det er i utgangspunktet åpenhet om at vi mottar og behandler personopplysninger vi sitter på.

Det er imidlertid krevende å vite alle måter vi kommer til å bruke personopplysninger på, og å ha løpende oversikt over hvilke opplysninger vi bruker. Ved enhver bruk av Copilot risikerer vi at personopplysninger brukes, avhengig av hva den enkelte ansatte ber Copilot gjøre og hvilke tilganger den ansatte sitter på. Copilot kan også generere personopplysninger gjennom sine svar/oppgaveløsning, uten at de registrerte kjenner til dette. Dette gjelder særlig den enkelte ansatte som bruker Copilot i arbeidshverdagen.

Ledelsen må derfor nøye vurdere hvordan man skal opplyse brukere av våre tjenester og registrerte om bruken. Personvernerklæringen må i alle tilfelle oppdateres, og man må vurdere om ytterligere opplysninger skal gis. Dette kan for eksempel være i bekreftelsesbrev, en linje i e-poster eller i Teams-invitasjoner, en nyhetssak på nettsiden m.m.

Angående hva som skal stå i personvernerklæringen på våre nettsider, er det viktig at vi er åpne om hva Copilot-teknologien innebærer og hva vi vil bruke den til. Dersom vi etter testperioden begrenser hvilke områder Copilot skal brukes til og hvilke data den har tilgang til, vil dette kunne spesifiseres i erklæringen.

### 2.2.3. Registrertes rettigheter og risikoen for de registrertes personvern

De registrertes rettigheter (retten til å kreve innsyn ([artikkel 15](#)), retting ([artikkel 16](#)), sletting ([artikkel 17](#)), begrensning i behandlingen ([artikkel 18](#)), dataportabilitet ([artikkel 20](#)) mv.) opplyses om i personvernserklæringen.

En av risikoene for de registrerte er spredning/deling av personopplysninger. Årsaken kan være datatyveri, men sannsynligvis vil det skyldes brukerfeil/ubevisst deling av data samlet sammen eller generert av Copilot. Siden dokumentene saksbehandlerne i hovedsak gir ut er avgjørelser og e-poster til partene, vil vi imidlertid normalt ha god kontroll på hvilke opplysninger som forlater organisasjonen. Det innebærer at risikoen for at personopplysninger forlater organisasjonen gjennom ubevisst deling er relativt lav.

Hva gjelder de registrertes rettigheter etter personvernforordningen artikkel 15 til 20, vil disse være krevende å etterleve for KNSE. Det ligger i Copilots system at behandlingen av personopplysninger (og alle data den har tilgang til), vil skje løpende og uten at vi kontrollerer bruken. Dette gjør det vanskelig å redegjøre for hvordan personopplysningene blir brukt og å oppgi hvilke begrensninger som ligger i bruken. Vi kan gi innsyn i de dataene vi vet foreligger og søke etter øvrige opplysninger, og vi kan slette opplysninger vi finner. Vi kan imidlertid ikke være sikker på at vi har fanget opp alle opplysninger som finnes, da de kan være generert av Copilot i etterkant og ikke bli fanget opp ved søk. Det er også usikkert i hvilken grad man vil klare å endre uriktige opplysninger.

I motsetning til tidligere vurderinger av arkivsystem og Teams, kan vi ikke legge til grunn at de registrerte forventer at vi bruker personopplysninger på denne måten. Tvert imot vil nok mange kunne reagere på den potensielt ubegrensede tilgangen Copilot vil ha til opplysningene. Dette vil særlig gjelde personopplysninger vi sitter på fra tidligere av, før Copilot og tilsvarende teknologi eksisterte. Samtidig vil det være en viss forventning fra brukerne om at KNSE vil ta i bruk KI på bakgrunn av dagens samfunn og regjeringens KI strategi. Virksomheten kan imidlertid ikke gå ut fra at denne oppfatningen gjelder alle. Dette må tas med i vurderingen både når man vurderer bruken, hvordan ivareta brukernes rettigheter og hvordan man opplyser brukerne om deres rettigheter.

Vi må legge til rette for full åpenhet på våre nettsider/personvernserklæring om hvordan Copilot fungerer og hvilken bruk vi legger til rette for. Dette bør også inkludere informasjon om brukernes rettigheter og eventuelle utfordringer med å etterleve disse. Brukerne bør informeres om testperioden og eventuelle resultater av denne.

## 2.3. Personopplysningene som behandles

### 2.3.1. Personopplysninger/kategorier opplysninger som skal behandles

Med personopplysninger menes alle opplysninger som kan knyttes direkte eller indirekte til en identifisert eller identifiserbar fysisk person.

Generelle personopplysninger (art. 6):

- **Informasjon om parter** som navn, tittel, adresse, e-postadresse og telefonnummer
- **Leverandørinformasjon** som navn tittel, adresse, e-postadresse og telefonnummer
- **Ansatte og arbeidsforhold**, for eksempel navn, adresse, e-postadresse, telefonnummer, alder, kjønn, fødselsdato, personnummer, CV, rekrutterings- og oppsigelsesdetaljer, vurderinger og opplærings- og sikkerhetsjournaler
- **Økonomiske opplysninger**

Særlige kategorier av personopplysninger (art. 9):

- Rasemessig eller etnisk opprinnelse
- Fagforeningsmedlemskap
- Helseopplysninger

Personopplysninger skal bare samles inn og lagres i den grad det er nødvendig for arbeidet i KNSE, typisk til opplysning og behandling av den enkelte sak. Når det gjelder særlige kategorier av personopplysninger vil behandling og tilgang til disse opplysningene være svært begrenset, og kontrollert via tilgangsstyring. Det er i hovedsak KNSE sine egne ansatte som vil være registrert med slike opplysninger.

Bruk av Copilot vil kunne samle inn og generere personopplysninger vi ikke tidligere har behandlet. Det kan være opplysninger gjennom Teams og personopplysninger Copilot selv genererer, for eksempel gjennom sammenstilling av opplysninger i ulike dokumenter eller gjennom andre sammendrag brukeren ber Copilot generere (for eksempel oppsummering av møter og personenes opptreden i møtene, eller sammenstilling av arbeidsinnsats mm.)

### 2.3.2. Omfanget personopplysninger ved behandlingen

Som det er forsøkt redegjort for over, ligger det i Copilots system at omfanget av bruken er vanskelig å kvantifisere. Vi må legge til grunn at alle personopplysninger brukeren av Copilot har tilgang til, vil inngå i behandlingen som Copilot gjør, uten at de av den grunn ender opp i dokument Copilot genererer. Jeg viser til vurderingene ellers i konsekvensutredningen, men vil likevel bemerke at tilgangsstyringen blant saksbehandlere i hovedsak er knyttet til hvilken avdeling man jobber på. I Sharepoint innebærer det blant annet at alle de ansatte på hver avdeling har tilgang til alle faktiske utdrag som lagres der. I tillegg har man tilgang til de fleste saker som nemndene man arbeider for behandler i Teams. Mange av de ansatte jobber på mange forskjellige nemnder, og har tilganger på tvers av mange nemnder og også på tvers av avdelinger. De ansatte i administrasjonen har flere tilganger enn de ansatte. Arkivarer har tilgang til alt i nemndens SharePoint/Teams. HR/Økonomi har noe mer begrenset tilgang ved at de ikke har tilgang i teams, men tilganger i SharePoint). HR/Økonomi har likevel tilgang til store mengder personopplysninger og saksdokumenter. Derfor bør det legges til grunn at dette vil gjelde for dem også.

Det innebærer at selv om Copilot speiler tilgangene til den enkelte saksbehandler, vil Copilot normalt ha tilgang til store datamengder internt. Dette er viktig å huske på i risikovurderingene man gjør. Streng tilgangsstyring og strenge krav til rydding og sletting må gjennomføres og følges opp løpende. Det anbefales at dette implementeres i årshjul og i internkontroll med solid lederforankring.

### *2.3.3. Innhenting av opplysningene*

Det er i hovedsak partene som opplyser sakene vi har til behandling, enten gjennom overføring av dokumenter til klageinstans, frivillig opplysning av saken eller ved at KNSE etterspør dokumentasjon. Vi må imidlertid være oppmerksom på at Copilot selv kan generere opplysninger, for eksempel gjennom sammenstilling av opplysninger fra forskjellige dokumenter eller gjennom møtereferat.

### *2.3.4. Sikring av personopplysningenes riktighet*

Det er i hovedsak partene som opplyser sakene selv og også de ansatte som oppgir personopplysninger som arkiveres. Ansatte i KNSE vil ha ansvar for å sikre opplysningers riktighet i alle dokumenter de produserer ved hjelp av Copilot. God opplæring av de ansatte er her en sentral forutsetning.

Copilot kan hallusinere, altså skape personopplysninger som ikke er korrekte. Dette må brukerne være seg meget bevisst. I tillegg er ikke Copilot i dag i stand til å etterprøve riktigheten av opplysningene i dokumentene den gjennomgår. Altså vil feile opplysninger kunne bli gjenbrukt uten at det fanges opp av

Copilot. Denne risikoen vil ligge her også uten Copilot, men alle disse risikoene økes substansielt ved (ukritisk) bruk av Copilot.

Klagenemndssekretariatet må utarbeide rutiner for sletting eller endring av ukorrekte personopplysninger, samt hvordan man best kan ha oversikt over personopplysningene vi behandler.

### *2.3.5. Perioden behandlingen skal skje/sletting av personopplysningene*

Siden Copilot får tilgang til alle opplysninger vi sitter på, vil bruk av Copilot øke risikoen for at opplysninger vi sitter med utover perioden vi har lov til, også vil bli brukt av Copilot. Dette er en forhøyet risiko fra tidligere. I tillegg risikerer vi at man gjennom Copilot genererer nye dokumenter som inneholder personopplysninger, og at disse lagres utover perioden vi har behov for dem og lov til å lagre dem. Dette bør også undersøkes opp mot arkivloven, for å finne ut hva som er akseptabelt for virksomheten.

Ved bruk av Copilot må organet intensivere arbeidet med å slette personopplysninger etter hvert som vi ikke lenger har rett til å sitte på dem. Det må innebære forbedret opplæring og bevisstgjøring av de ansatte, samt kontroll av at de ansatte følger det opp. Dette må også inkludere nemndsmedlemmer, som gis tilgang til faktisk utdrag og avgjørelser, og kan laste disse ned på sine områder. Nemndsmedlemmer bør instrueres i å slette dokumenter tilknyttet en enkelt sak så snart denne er avgjort.

Det må etableres gode rutiner i organet for sletting av personopplysninger. Dette gjelder særlig opplysninger om tidligere ansatte, da disse opplysningene ikke er knyttet til virksomhetens oppgaver, saksbehandling eller arkivformål. Det er etablert automatiske rutiner for sletting av chat i teams, men virksomheten bør se på rutiner knyttet til sletting av epost o.l.

## **3. Formål og grunnlag for behandlingen – GDPR art. 5**

### **3.1. Behandlingens formål og sikring**

Dette og de neste punktene er etter mitt syn de mest krevende i denne konsekvensutredningen.

Bruk av Copilot har potensiale for å effektivisere flere av arbeidsoppgavene våre, og også øke kvaliteten på mange deler av arbeidet vi leverer. Dette er viktige hensyn. Som forvaltningsorgan er vi også pålagt å forsøke å øke bruken av KI i arbeidet.

Personopplysninger skal imidlertid samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene, jf. forordningen art. 5 bokstav b. Det er, slik jeg forstår Copilot, vanskelig å forene Copilots ubegrensede tilgang og bruk av alle opplysninger vi sitter på med dette prinsippet. Bruk av Copilot vil åpne for at innsamlede personopplysninger kan brukes i enhver sammenheng der Copilot brukes, avhengig av brukernes spørsmål og tilganger. Vi åpner i realiteten døren for enhver bruk av personopplysningene, og må stole på at egne tilgangsstyringer og de ansattes egne begrensninger er et tilstrekkelig vern mot uvettig bruk. Jeg kan ikke se at rapporter, risikoanalyser og -vurderinger fullt ut svarer på denne problemstillingen. Med mindre man har en meget streng tilgangsstyring/begrenser Copilots tilganger og virkeområde til et nivå hvor mye av dens intenderte funksjonalitet forsvinner, vil ikke dette problemet løses. Dette er en risiko den behandlingsansvarlige må være klar over og vurdere opp mot de fordelene bruk av Copilot potensielt vil ha.

### 3.2. Nødvendigheten av behandlingsaktivitetene – behandlingsaktiviteter vurdert mot formål

Behandlingsaktivitetene til KNSE er lovpålagte etter bestemmelser for den enkelte klagenemnd i lov og forskrift i tråd med GDPR art. 6 nr. 1 bokstav c og e og GDPR art. 9 nr. 2 bokstav g. Innhenting og lagring, samt bruk begrenset til å løse den saken eller den konkrete oppgaven opplysningene er hentet inn for, er aktiviteter som er nødvendige for saksbehandlingen og står i rimelig forhold til formålene. Dette er uproblematisk.

Bruk av Copilot åpner for at opplysningene brukes langt utover det nødvendige. Nødvendigheten av bruken er dels kommentert over i formålsvurderingen, og vurderingene henger sammen.

Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for de formålene de behandles for, jf. forordningen art. 5 første ledd bokstav c. Utfordringen er, som allerede nevnt over, at Copilot vil gjøre bruk av alle opplysninger den har tilgang til ved enhver oppgave den utfører. Slik som for formålsbegrensningen over, er det vanskelig å argumentere for at vi vil vite at personopplysningene begrenses til det som er nødvendig for de formålene de behandles for. vi vil simpelthen ikke kunne kontrollere omfanget og bruken av opplysningene på måten vi tradisjonelt har kunnet.

Også dette må den behandlingsansvarlig ta med i vurderingen av om vi skal benytte verktøyet.

### 3.3. Lovgrunnlag for behandlingen – GDPR art. 6

Behandling av personopplysninger er etter personvernforordningen artikkel 6 første ledd kun lovlig dersom minst ett av følgende vilkår er oppfylt:

- «a. den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål,
- 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,
- c. behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,
- d. behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser,
- e. behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,
- f. behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.

Nr. 1 bokstav f) får ikke anvendelse på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver»

Fra tidligere vil personopplysninger vi sitter med være innhentet enten ved samtykke eller etter hjemmel i lov. Så lenge bruken knyttes til oppgavene vi er pålagt og som opplysningene er hentet inn for, vil bruken være lovlig. I tidligere konsekvensutredninger har hjemlene vi har for å behandle personopplysningene vært opplistet, men det er ikke gjort her. Det skyldes at utfordringen ved bruk av Copilot gjelder noe annet enn hvilken hjemmel vi opprinnelig har for bruken.

Ved innføring av Copilot vil vi ikke i forkant være helt sikre på hvilke oppgaver Copilot vil bruke personopplysningene til. Vi vet derfor ikke om vi har samtykke til behandlingen, og vi vet ikke om behandlingen strengt tatt er nødvendig for å utøve den offentlige myndighet vi er pålagt. Vi vil også sitte med opplysninger som vi lovlig kan behandle etter bokstav b og c, men det samme problemene knyttet til formålsbegrensninger gjelder for disse.

Denne usikkerheten må den behandlingsansvarlige ta stilling til.

### 3.4. Lovligheten av behandlingen og behandlingsansvarliges ansvar

Hva gjelder overholdelse av prinsippene for behandling av personopplysninger ellers i GDPR [artikkel 5](#), er mitt syn dekket i vurderingen ellers.

## 4. Oppsummering. Samlet vurdering

Konsekvensutredningen har forsøkt å belyse hvilket potensielt omfang bruk av Copilot vil ha for behandlingen av personopplysninger, og den usikkerhet som ligger i bruk av Copilot. Ved bruk av Copilot må organisasjonen tenke helt nytt om hvordan vi forholder oss til lagring og bruk av personopplysninger,

tilgangsstyring, slettepolitikk og bruk av lagring og mellomlagring på egne områder. Det er sentralt at organisasjonen tar innover seg disse konsekvensene.

Bruk av Copilot kan bli et formidabelt verktøy i arbeidet vårt og kan gi oss mange fordeler sammenlignet med tidligere. God tilgangsstyring og fornuftig bruk fra de ansatte kan gjøre at mulige risikoer minimeres og ikke materialiserer seg.

De ovennevnte risikoer og fordeler må holdes opp mot hverandre, der særlig sikringen av at opplysninger ikke brukes utover sitt formål og at opplysninger er korrekte må ivaretas. I tillegg må risikoer holdes opp mot den overordnede føringen om at 80 % av offentlige virksomheter skal ha implementert og tatt i bruk KI innen 2030.

En overordnet vurdering vil ikke gi et godt svar på nøyaktig hva konsekvensene ved bruk av Copilot vil bli. Dens viktigste oppgave er å påpeke de overordnede risikoer og hvilke vurderinger den behandlingsansvarlige må gjøre ved den videre bruken og utrulling. En oversikt over mulige risikoer og tiltak kan finnes i vedlegget under. Merk at denne tabellen ikke er utfyllende, og kan være gjenstand for endring. Etter mitt syn er etablering av en testgruppe en fornuftig fremgangsmåte for å prøve ut verktøyet. En viktig forutsetning er imidlertid at man underveis i testperioden gjør løpende vurderinger av testbrukernes tilganger og hvilke dokumenter de har på egen Onedrive. Videre må testperioden etterfølges av en nøye gjennomgang av bruken og hvilke konsekvenser det har for bruken av personopplysninger.

Basert på dette, mener jeg det er akseptabelt å gjennomføre en testperiode av Copilot for en begrenset gruppe brukere. Dette fordrer imidlertid at testbrukerne følges opp nøye i testperioden og at man før verktøyet rulles ut til flere i organisasjonen, gjennomfører en ny DPIA hvor man ser på erfaringer fra testgruppen, presiserer hvilke oppgaver man vil benytte Copilot til og vurderer disse konkret.

## 5. Råd fra personvernombud

Personvernombud Marie Tamber Løbach er konferert 21.09.2026 og har følgende råd/kommentarer til behandlingen og vurderingen:

DPIA vurderingen må oppdateres etter endt testperiode for å fange opp eventuelle ytterligere svakheter. Det må informeres på nettsiden at vi setter i gang en testperiode med lisensiert versjon av Copilot, med denne DPIAen vedlagt.

Risikovurderingen og tiltak er i denne omgang rettet mot testperioden og må også oppdateres etter endt testperiode.

Frist for ny DPIA etter endt testperiode anbefales å være 14 dager før eventuell utrulling til øvrige ansatte. Dette er for å sikre tilstrekkelig tid til gjennomgang av ledelsen og personvernombud, samt opplæring av ansatte.

## **6. Godkjenning**

### **6.1. Revisjon videre kontroll**

Vurderingen skal kontrolleres og eventuelt oppdateres/endres hver 6. måned.

### **6.2. Forhåndsdrøftelse med Datatilsynet**

På nåværende tidspunkt, der kun testgruppen gis tilgang, mener jeg det ikke er nødvendig, men det bør vurderes sterkt før ytterligere utrulling av Copilot.

### **6.3. Beslutning**

Ledelsen ved Anneline Vingsgård har godkjent vurderingen og den risiko som foreligger ved behandlingen. Risikoen er nærmere beskrevet i punkt 0. Ledelsen har lagt til grunn personvernombudets vurdering.

### **6.4 Signatur**

Dokumentet signeres elektronisk av Direktør.

### Vedlegg: Identifikasjon og vurdering av risiko, risikoreduserende tiltak

Risikovurderingen er tatt med utgangspunkt med en person som har rolle som eier i Teams, og dermed vil være den med tilgang til flest personopplysninger.

#### Risikovurdering og tiltak i testperioden

| Verdi sannsynlighet / konsekvens | 1: Meget liten sannsynlighet / Ubetydelig konsekvens                                                                                                           | 2: Liten sannsynlighet / lav konsekvens                                                                                                       | 3: Moderat sannsynlighet / moderat konsekvens                                                                                                                       | 4: Stor sannsynlighet / alvorlig konsekvens                                                                                                                                           | 5: Svært stor sannsynlighet / svært alvorlig konsekvens                                                                                                                                                        |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Eksempler sannsynlighet:         | Hendelsen vil kunne skje én gang hvert 10 år eller sjeldnere.                                                                                                  | Hendelsen vil kunne skje én gang mellom hvert 5 og 10 år.                                                                                     | Hendelsen vil kunne skje én gang mellom hvert 3 til 5 år.                                                                                                           | Hendelsen ville kunne skje én gang mellom hvert 1 til 2 år.                                                                                                                           | Hendelse vil kunne skje flere ganger hvert år.                                                                                                                                                                 |
| Eksempler konsekvens:            | 1. Lite opplysninger om 1-10 personer eller<br><br>2. Noe mer opplysninger om 1-5 personer. Ingen omfattende eller følsomme/særskilte kategorier opplysninger. | 1. Mindre opplysninger om 10-50 personer eller<br><br>2. Mer opplysninger om 1-10 personer. Ingen følsomme/særskilte kategorier opplysninger. | 1. Mindre opplysninger om 50-100 personer eller<br><br>2. Mer opplysninger om 10-50 personer eller<br><br>3. Følsomme/særskilte kategorier opplysninger om 1 person | 1. Mindre omfattende opplysninger om 100-500 personer eller<br><br>2. Mer opplysninger om 50-100 personer eller<br><br>3. Følsomme/særskilte kategorier opplysninger om 2-10 personer | 1. Mindre omfattende personopplysninger om mer enn 500 personer eller<br><br>2. Mer opplysninger om mer enn 100 personer eller<br><br>3. Følsomme/særskilte kategorier opplysninger om 10 eller flere personer |

| ID                         | Beskrivelse                                                                      | 1                                                                                                                                                                    | 2                                                                                                                                                                        | 3                                                                                                                                                                         | 4                                                                                                                                                                             | 5                                                                                                                                                                                                                                                       |
|----------------------------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hendelse eller situasjon   | Hva er den uønskede hendelse eller situasjon (personvernbruddet) som kan oppstå? | Personopplysninger kommer på avveie utenfor organisasjonen                                                                                                           | Personopplysning er kommer på avveie internt i organisasjonen                                                                                                            | Generering av nye og uriktige personopplysninger og bruk av disse                                                                                                         | Bruk av personopplysninger i strid med formålsbegrensningene i personvernforordningen                                                                                         | Generering av nye personopplysninger og profilering av den enkelte ansatte                                                                                                                                                                              |
| Sårbarhet/årsak            | Hvilke sårbarheter/forhold kan være årsak til at hendelsen oppstår?              | Copilot bruker (eller genererer nye) personopplysninger i sine svar, og brukeren deler disse videre utenfor organisasjonen, for eksempel i epost eller presentasjon. | Feil tilgangsstyring eller feil lagring av personopplysning er gjør at en bruker av Copilot får opp og bruker personopplysning er som personen ikke skal ha tilgang til. | Copilot hallusinerer og skaper uriktige personopplysninger. Copilot «misforstår» informasjon, og sammenstiller i utgangspunktet riktige personopplysning er på feil måte. | Vi vet ikke hvordan Copilot faktisk bruker opplysninger i sin behandling ("black box"), og vi har derfor ikke kontroll på alt som blir gjort.                                 | Profilering av den enkelte ansatte basert på dokumenter som ligger på den enkeltes område. Copilot kan lage en profil av den enkelte ansatte basert på spørsmål og chatter med copilot fordi copilot trenes på data og ved hjelp av input fra brukeren. |
| Sannsynlighet for hendelse | Hvor sannsynlig er det at hendelsen skjer? Hvorfor?                              | Hendelsen vil kunne skje, men det er ikke særlig sannsynlig da presentasjoner ikke gjøres ofte. I epost har ansatte allerede et særlig ansvar på grunn av            | Stor sannsynlighet dersom vi ikke har orden i eget system. Ved innføring av Copilot og i testperioden er sannsynligheten                                                 | Sannsynlig fordi copilot er en språkmodell, og den enkelte ansatt har i testperioden ikke fått opplæring i prompting eller måter å stille                                 | Usikker sannsynlighet. Bruk av Copilot i saksbehandlingen kan være i tråd med formålet, da det blir brukt som et verktøy i saksbehandlingen (dette er formålet med å behandle | Middels sannsynlighet, da alle har en bestemt måte å formulere spørsmål på og kan finne på å benytte Copilot til andre formål enn                                                                                                                       |

|                                      |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                             |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                      |                                                                                                                                                                                                                   | sakstypene vi behandler.                                                                                                                                                                                                                                      | større da vi ikke nødvendigvis vet hvor eventuelle hull eller mangler i tilgangsstyring ligger.                                                                                                                                                                                                                                                                             | spørsmål på for å redusere risiko for hallusinerer                                                                                                                                                                                                            | opplysningene til andre i utgangspunktet).                                                                                                                                                                                                                                                                         | arbeid. Private dokumenter som ligge på pcen kan påvirke copilot sine svar og oppfatning av brukeren.                                                                                                       |
| Kvantifisering av sannsynlighet (S1) | Kvantifisering basert på tabellen over (1-5)                                                                                                                                                                      | 1                                                                                                                                                                                                                                                             | 4                                                                                                                                                                                                                                                                                                                                                                           | 3                                                                                                                                                                                                                                                             | 3                                                                                                                                                                                                                                                                                                                  | 3                                                                                                                                                                                                           |
| Antatte konsekvenser av hendelse     | Konsekvenser ved hendelsen - virkningen for de registrerte. Omfang (antall registrerte/personopplysninger, mv.) Type personvernbrudd (konfidensialitet, integritet, tilgjengelighet, de registrertes rettigheter) | Vil trolig ikke være særlig alvorlige opplysninger som gis ut på denne måten, da man selv uten tiltak må kunne forvente at ansatte kontrollerer opplysninger de sender ut av organet. Det kan likevel oppleves vanskelig for den personopplysningene gjelder. | Dersom det knytter seg til saker vi arbeider med, er konsekvensen ikke så stor, da de ansatte uansett er underlagt taushetsplikt og opplysningene normalt ikke vil være særlig alvorlige å få kjennskap til. Dersom opplysningene gjelder medansatte eller søkere til stillinger hos oss, vil bruddet være mer alvorlig. Det kan gjelde en særlig kategori opplysninger, og | Dette er en iboende risiko, og man må kunne forvente at de ansatte i mange tilfeller vil fange opp feilen og ikke deler den videre. Dersom man ikke fanger opp feilen, vil konsekvensen avhenge av hva opplysningen gjelder. Omdømmetapet kan være betydelig. | Denne bruken av personopplysningene vil ikke nødvendigvis ende opp med at opplysningene deles med uvedkommende. Dette er dekket av punkt 1 til 3. Konsekvensen, bruk av personopplysninger i strid med formålet for innhenting, er imidlertid alvorlig i seg selv, også der personene det gjelder ikke vet om det. | Dette kan påvirke svarene copilot gir den enkelte ansatte, og gjøre at ulike ansatte får ulike svar. I tillegg kan det være uheldig fordi virkningen ender opp med et program som har profilert de ansatte. |

|                                           |                                                                                                                              |                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           |                                                                                                                              |                                                                                                                                                                                                                                                               | det vil uansett kunne oppleves invaderende at en (fremtidig) kollega får opplysninger om deg som den ikke har krav på.                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                     |
| kvantifisering av konsekvens (K1)         | Kvantifisering basert på tabellen over (1-5)                                                                                 | 3                                                                                                                                                                                                                                                             | 4                                                                                                                                                                                                                                                                                                                   | 4                                                                                                                                                                                                                                                                                                      | 3                                                                                                                                                                                                                                                                                                  | 3                                                                                                                                                                                                                                                                                                                                   |
| Risiko (sannsynlighet x konsekvens) S1xK1 | Total risiko (1-25)                                                                                                          | 3                                                                                                                                                                                                                                                             | 16                                                                                                                                                                                                                                                                                                                  | 12                                                                                                                                                                                                                                                                                                     | 9                                                                                                                                                                                                                                                                                                  | 9                                                                                                                                                                                                                                                                                                                                   |
| Risikoreduserende tiltak                  | Hvilke tiltak har vi satt i verks for å redusere risiko i testperioden? Hvilke tiltak ser vi for oss etter endt testperiode? | <p>Testgruppen skal ikke utforme dokumenter, eposter eller andre ting som skal ut av huset i testperioden. Dette vil si at Copilot ikke skal brukes på aktive saker.</p> <p>Testgruppen er informert av prosjektansvarlig om dette og har et eget ansvar.</p> | <p>Gjennomgang av tilganger før testperioden starter, for å luke ut eventuelle feil. Etter endt testperiode skal vi ha en oppdatering av tilganger før Copilot eventuelt settes i bruk.</p> <p>Virksomheten må ha jevnlig gjennomgang av tilgangsstyring i P360, sharepoint og annet.</p> <p>Det skal være lett</p> | <p>Opplæring om hallusinerer og bevisstgjøring av testteamet.</p> <p>Testteamet er instruert i å være ekstra oppmerksom og skal oppdage hvor ofte hallusinerer skjer.</p> <p>Testteamet skal etter testperioden jobbe med utforming av standardprompter og undersøke innstillinger i copilot for å</p> | <p>Testgruppen skal ikke bruke Copilot til private formål, eller formål som ikke er knyttet til virksomhetens oppgaver/saksbehandling.</p> <p>Dette vil mest sannsynlig videreføres etter endt testperiode.</p> <p>En del av denne risikoen kan ikke fjernes på grunn av hvordan LLMer virker.</p> | <p>Den ansatte har selv ansvar for å rydde på eget område, slik at dokumenter som inneholder egne personopplysninger den ansatte ikke vil gi Copilot tilgang til slettes.</p> <p>Copilot skal ikke benyttes til private formål. Testgruppen er informert.</p> <p>Etter fullført testperiode skal vi ha opplæring av den enkelte</p> |

|                                         |                                               |   |                                                                                 |                                                                                                                                                                                                                                                             |   |                                                                                                                                |
|-----------------------------------------|-----------------------------------------------|---|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------|
|                                         |                                               |   | for den enkelte ansatte å melde feil i tilgangsstyring. Rutiner for håndtering. | <p>redusere sannsynligheten for hallusisering og feil bruk av personopplysninger.</p> <p>Den ansatte har selv ansvar for å rydde på eget område, slik at dokumenter som inneholder personopplysninger som ikke skal deles med copilot er utilgjengelig.</p> |   | <p>ansatte om prompting, og etter hvert utvikling av standardprompter.</p> <p>Bevisstgjøring av muligheten for ulike svar.</p> |
| Ny kvantifisering av sannsynlighet (S2) | Hva er nå sannsynligheten?                    | 1 | 2                                                                               | 2                                                                                                                                                                                                                                                           | 2 | 2                                                                                                                              |
| Ny kvantifisering av konsekvens (K2)    | Hva er nå konsekvensen?                       | 3 | 4                                                                               | 4                                                                                                                                                                                                                                                           | 3 | 2                                                                                                                              |
| Ny risiko (S2+K2)                       | Hva er nå risikoen?                           | 3 | 8                                                                               | 8                                                                                                                                                                                                                                                           | 6 | 4                                                                                                                              |
| Kommentarer til ny risiko               | Eventuelle vurderinger knyttet til ny risiko. |   |                                                                                 |                                                                                                                                                                                                                                                             |   | Om copilot brukes til private formål er risikoen større.                                                                       |