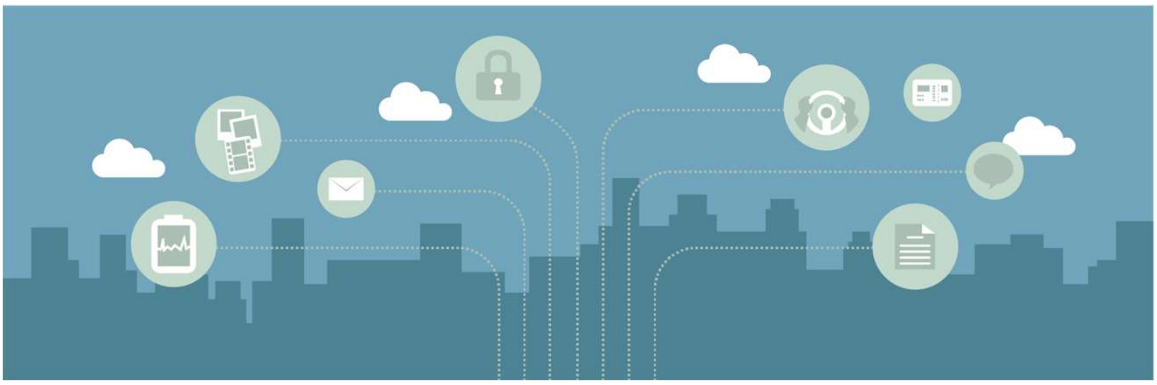


Personvernperspektivet på M365 Copilot

Sebastian Forbes og Eirik Gulbrandsen

31.05.2024

Datatilsynet

1

Om oss

Sebastian Forbes

Prosjektleder og jurist i Datatilsynets internasjonal seksjon

Eirik Gulbrandsen

Senioringeniør i Datatilsynets teknologi seksjon og prosjektleder i Datatilsynets sandkasse

2

Hva er M365 Copilot, med personvernbriller på?

3

Hva er M365 Copilot?

- Pust med magen
- Bryte Copilot opp i mindre og mer forståelige biter
- Kort fortalt: kraftig søkeverktøy + språkmodell som genererer svar
- Et (nytt) verktøy (med nye risikoer)

4

4

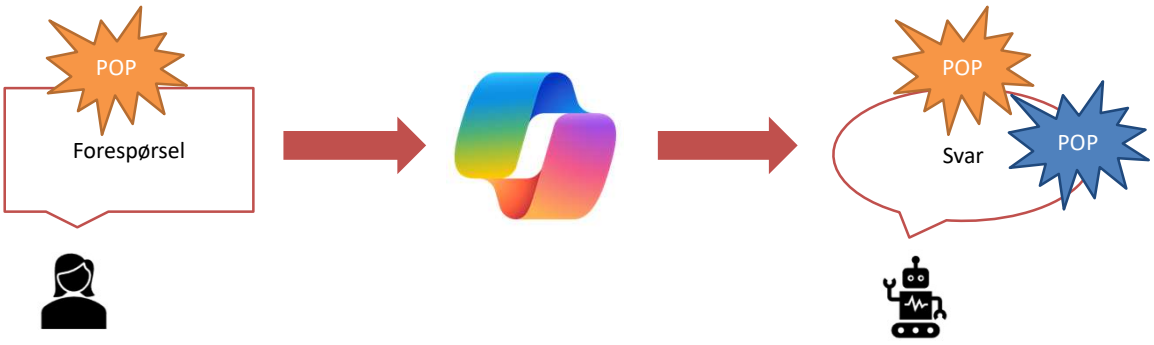
Hva er en «behandling» etter personvernforordningen?

- **Formålet** med å behandle **personopplysninger**
  - Hvorfor skal behandlingen skje?
  - Hva skal personopplysningene brukes til?
- **Midler**
  - Hvem sine personopplysninger? (essensielle)
  - Hvilke personopplysninger? (essensielle)
  - Hvor lenge skal de behandles? (essensielle)
  - Hvem skal ha tilgang til dem? (essensielle)
- **Behandlingsprotokoll!**

5

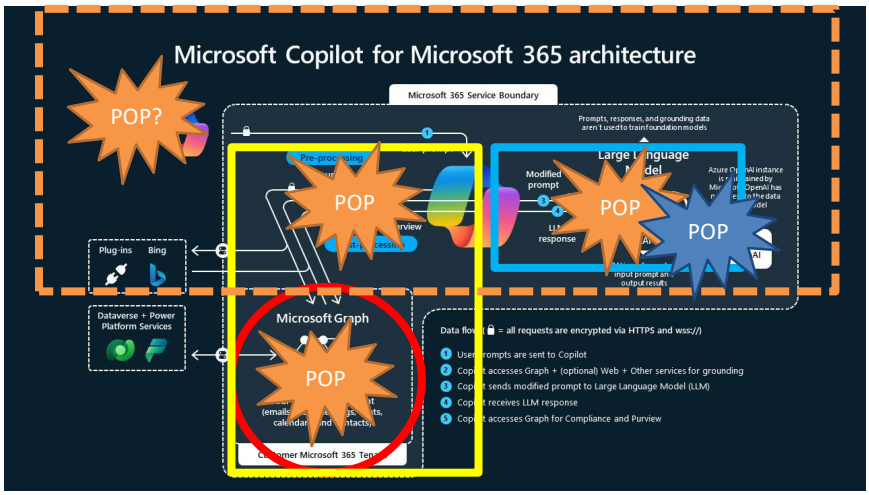
5

M365 Copilot – brukerens perspektiv



6

M365 Copilot – bak kulissene

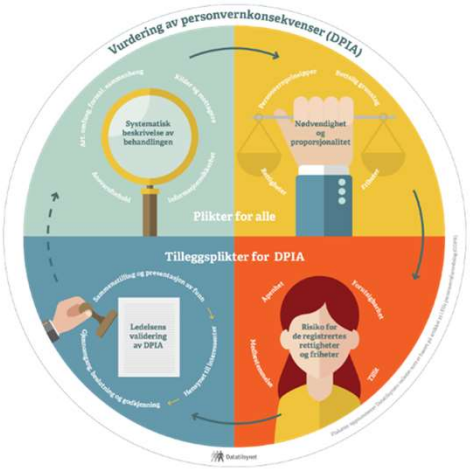


Personvernprinsippene

- Lovlighet, rettferdighet og åpenhet
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet
- Ansvar

Gjør en personvernkonsekvensvurdering

- Viktig å gjøre fordi generativ KI er nytt!
- Får en oversikt
- Vurder nødvendighet og proporsjonalitet
- Ser ting fra den registrertes perspektiv
  - rettigheter og friheter
- Oppdag risikoer og vurder tiltak
- Forankre hos ledelsen



9

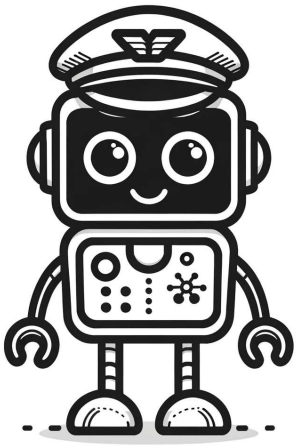
9

Datatilsynets foreløpige praktiske observasjoner

10

Samarbeidet med NTNU

- Prosjektet har bidratt til:
  - Bedre forståelse av hva Copilot er, og ikke er
  - Bedre forståelse av hva Copilot kan brukes til, og ikke brukes til
  - Bedre forståelse av forutsetninger og risiki
- Kort sagt - nyttig



11

11

Tidlig fase og krever mye manuell kontroll

- Copilot er et produkt i en tidlig utviklingsfase («versjon 0.001»)
- Vil sette store krav til «tidlige brukere»

12

12

Dataflyten

- Vanskelig og krevende å få oversikt over hvilke data som behandles på hvilken måte
  - Datakilder av/på?
  - (Query Manager)
  - Microsoft Graph
  - Bing Search
  - Plug-ins

13

13

Tilgangsstyring og dataforvaltning

- Urealistiske krav
- Forutsetninger
  - Høy opplæring
  - Høy disiplin
  - …
- Mye ansvar påligges anskaffende virksomhet

14

14

Overvåkingsverktøy?

- Ekstremt kraftig søkeverktøy
- Avanserte sammenstillinger av eksisterende informasjon
- «Enkle» forespørsler kan resultere komplekse analyser

Som er akkurat det Copilot skal gjøre…

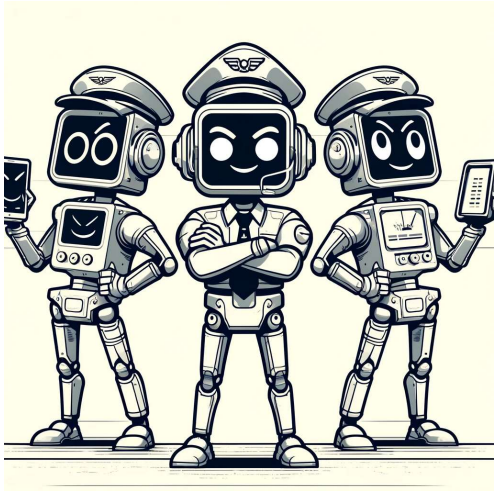
- Men dermed også et verktøy for (KI-assistert) overvåking og analyse av ansatte
  - Selv med «åpne» data

15

15

Finnes det alternativer?

- Hvilke oppgaver tenker man på?
- Bare et produkt
- Kan andre løsninger være mer aktuelt?



16

16

Sluttrapport

- Hvor begynner man med å vurdere bruk av teknologi som Copilot i lys av personvernregelverket?
- Grunnleggende forståelse av konsepter og begreper
- Hvilke forutsetninger foreligger det før man kan vurdere å ta det i bruk?
- Hva bør man tenke på i personvernkonsekvensvurderinger?

17

17

Hva ønsker dere?

- Det er kjempenyttig for oss å vite hva dere lurer på.
- Tips oss om hva dere ønsker!
- Sluttrapport, eller på annen måte (veiledning, artikler osv.)

Sebastian Forbes

Prosjektleder og jurist i Datatilsynets internasjonal seksjon

sebastian.forbes@datatilsynet.no

18

18

Takk for oss!

Datatilsynet

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no

19