



Microsoft 365
Copilot

Datasikkerhet i den kunstig intelligensens tidsalder

En veiledning for IT-sjefer



e-bok

Denne veiledningen er for IT-sjefer som skal begynne å ta i bruk kunstig intelligens og samtidig holde bedriftens data sikre. Den forklarer risikoene som kunstig intelligens kan utgjøre for datasikkerhet og personvern, og gir også innsikten som trengs for å ta i bruk kunstig intelligens på en trygg måte i bedriften.

Innhold

01

De nye reglene for arbeid drevet av kunstig intelligens

02

Hvilken innvirkning har kunstig intelligens på datasikkerheten?

03

Utfordringen med uautorisert kunstig intelligens

04

Medbrakt kunstig intelligens

05

Regelvirvar

06

Sikkerhetsbasert evaluering av kunstig intelligens

07

Microsoft 365 Copilot: Pålitelig kunstig intelligens

08

Sikker bruk av kunstig intelligens

01

De nye reglene for arbeid drevet av kunstig intelligens

Generativ kunstig intelligens åpner nye dører for innovasjon og hjelper ansatte med å arbeide raskere og smartere enn noen gang før. For fremtidsrettede bedrifter er ikke kunstig intelligens bare en teknologitrend – det er avgjørende for hvordan bedriften drives, leverer verdi og beholder konkurransefortrinnet.

Men den raske innføringen av kunstig intelligens gir nye og større utfordringer som IT-sjefer må håndtere proaktivt og få kontroll på. Kunstig intelligens kan aktivt søke etter og kombinere informasjon fra hele dataøkosystemet, noe som øker sikkerhetsrisikoen ved bruk av tradisjonelle verktøy. Til tross for den raske utbredelsen av kunstig intelligens rapporterer bare **1 %** av bedriftene at de har integrert teknologien i arbeidsflyten med adekvate sikkerhetsprotokoller.¹ Ved å implementere robuste sikkerhets- og styringstiltak fra begynnelsen av kan medarbeiderne effektivt beskytte sensitive data, opprettholde etterlevelseskrav og beskytte bedriftens informasjon – samtidig som innovasjonen kan blomstre.

Bruk av kunstig intelligens er allerede omfattende



02

Hvilken innvirkning har kunstig intelligens på datasikkerheten?

Før vi ser på bestemte utfordringer, er det viktig å forstå hvordan kunstig intelligens fundamentalt endrer datasikkerheten. I motsetning til tradisjonell programvare som bare henter data når den blir bedt om det, behandler, analyserer og lager generativ kunstig intelligens innhold aktivt basert på alle dataene den mottar.

Dette er en viktig forskjell av flere grunner:

- Kunstig intelligens kan se sammenhenger mellom data lettere enn mennesker
- Den kan samsvare data fra ulike kilder automatisk
- Den kan generere nytt innhold som inneholder elementer fra sensitive inndata

De tradisjonelle sikkerhetsverktøyene dine er sannsynligvis ikke utviklet med tanke på disse funksjonene. Konvensjonell programvare følger forutsigbare baner når data hentes. Kunstig intelligens kan derimot ta uventede ruter gjennom informasjonssystemet, noe som potensielt eksponerer sensitive data på måter du ikke forventer.

Denne forskjellen krever nye tilnærminger til sikkerhet og dataforvaltning som spesifikt bestemmer hvordan kunstig intelligens skal samhandle med bedriftens informasjonsressurser.

03

Utfordringen med uautorisert kunstig intelligens

Uansett hvor langt du er kommet i bruken av kunstig intelligens, har ansatte sikkert allerede begynt å bruke sine egne løsninger for kunstig intelligens.

Denne uautoriserte bruken skaper betydelige blindsoner i sikkerheten. Når ansatte sender bedriftsdata gjennom sin medbrakte kunstige intelligens, omgås eksisterende sikkerhetskontroller og skaper sårbarheter som de fleste bedrifter ikke er forberedt på å håndtere.

Dette utgjør ikke bare et sikkerhetsproblem, det kan være et symptom på udekte produktivetsbehov i bedriften. Når ansatte bruker uautoriserte verktøy, er det et tegn på at bedriftens systemer ikke dekker behovet deres. Problemet krever både sterkere styring og bedre produktivitetsløsninger.



Grunner til at uautorisert kunstig intelligens tas i bruk:

- Ansatte ønsker å øke produktiviteten ved hjelp av de imponerende resultatene kunstig intelligens gir
- Den daglige arbeidsbelastningen tar i økende grad mer tid og energi enn det som står til rådighet
- Ansatte står overfor økende press for å levere mer med samme ressurser
- Medbrakt kunstig intelligens tilbyr umiddelbart en løsning uten å måtte godkjennes først
- Bedriftens IT-innkjøpsprosesser holder ikke tritt med innovasjonstempoet

Risikoen ved bruk av uautorisert kunstig intelligens:

- Ingen oversikt over hvilke bedriftsdata som behandles av medbrakt kunstig intelligens
- Ingen garanti for at konfidensiell informasjon ikke kommer på avveie
- Ingen enhetlige sikkerhetsstandarder på de ulike plattformene
- Ingen mulighet for å kontrollere etterlevelse
- Ingen integrasjon med eksisterende sikkerhetsinfrastruktur



Tenk deg dette scenarioet:

En finansanalytiker som sliter med et komplisert regneark, laster det opp til et medbrakt KI-verktøy for å få hjelp. Dette regnearket inneholder økonomiske kundedata, interne beregninger og prognoser. Selv om analytikeren får den nødvendige hjelpen, befinner bedriftens sensitive finansdata seg nå utenfor sikkerhetssonen og er fullstendig usynlig for overvåkingssystemene.

04

Medbrakt kunstig intelligens

Uten tydelig veiledning fra ledelsen tar ansatte i økende grad (**78 %**) i bruk medbrakt kunstig intelligens i arbeidet.² Denne trenden er enda sterkere i små og mellomstore bedrifter, der **80 %** av ansatte bruker medbrakt kunstig intelligens.²

Denne uautoriserte bruken har betydelige ulemper. Ansatte skjuler ofte at de bruker medbrakt kunstig intelligens. **52 %** vil helst ikke innrømme at de bruker kunstig intelligens til viktige oppgaver, og **53 %** er bekymret for at bruken av kunstig intelligens kan få dem til å bli overflødige.² Dette hemmelighetskremeriet hindrer ikke bare bedriften i å utnytte alle fordelene som strategisk implementering av kunstig intelligens gir, men skaper også alvorlige sikkerhetsproblemer i et miljø der sikkerhet og personvern er bekymring **nummer én**.²

På grunn av den utbredte bruken og den uunngåelige veksten av kunstig intelligens er spørsmålet ikke om du vil tillate teknologien i bedriften. Det handler om hvordan du tilbyr en sikker løsning som dekker de ansattes behov, samtidig som bedriftens data beskyttes.

05

Regelvirvar

Rammeverk og lover rundt personvern og sikkerhet skaper et nytt lag med kompleksitet når du tar i bruk kunstig intelligens. Selv om enkelte rammeverk er spesielt beregnet på styring av kunstig intelligens, har andre bredere anvendelser som fortsatt påvirker hvordan du håndterer informasjon – og straffene for regelbrudd er strenge.

Når de ansatte bruker kunstig intelligens uten ordentlig tilsyn, kan de utilsiktet bryte etterlevelseregler. Kunstig intelligens øker denne risikoen fordi den innhenter, kombinerer og eksponerer kritiske data på måter som tradisjonell teknologi ikke gjør.

Viktige forskrifter som påvirker bruken av kunstig intelligens:



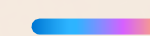
EUs personvernforordning

EUs personvernforordning gir brukere kontroll over personopplysningene sine og krever klart samtykke for behandling av dataene



EUs forordning om kunstig intelligens

EUs omfattende rammeverk regulerer systemer for kunstig intelligens basert på risikonivået



HIPAA

Denne amerikanske føderale loven for helsetjenester setter strenge standarder for håndtering av beskyttede helseopplysninger



NIST-rammeverket for risikohåndtering av kunstig intelligens

Denne frivillige amerikanske veiledningen hjelper bedrifter med å håndtere risikoer innen utforming, utvikling og utrulling av kunstig intelligens

Etterlevelsesrisikoen med kunstig intelligens:

- Kundedata behandles på servere utenfor godkjente regioner
- Personopplysninger brukes uten samtykke
- Sensitive data blir liggende igjen i systemer uten nødvendige lagringskontroller
- Ingen revisjonsspor for hvordan beskyttet informasjon innhentes og brukes
- Innhold generert av kunstig intelligens bryter med etterlevelseskrav

Disse bruddene kan ha alvorlige konsekvenser:

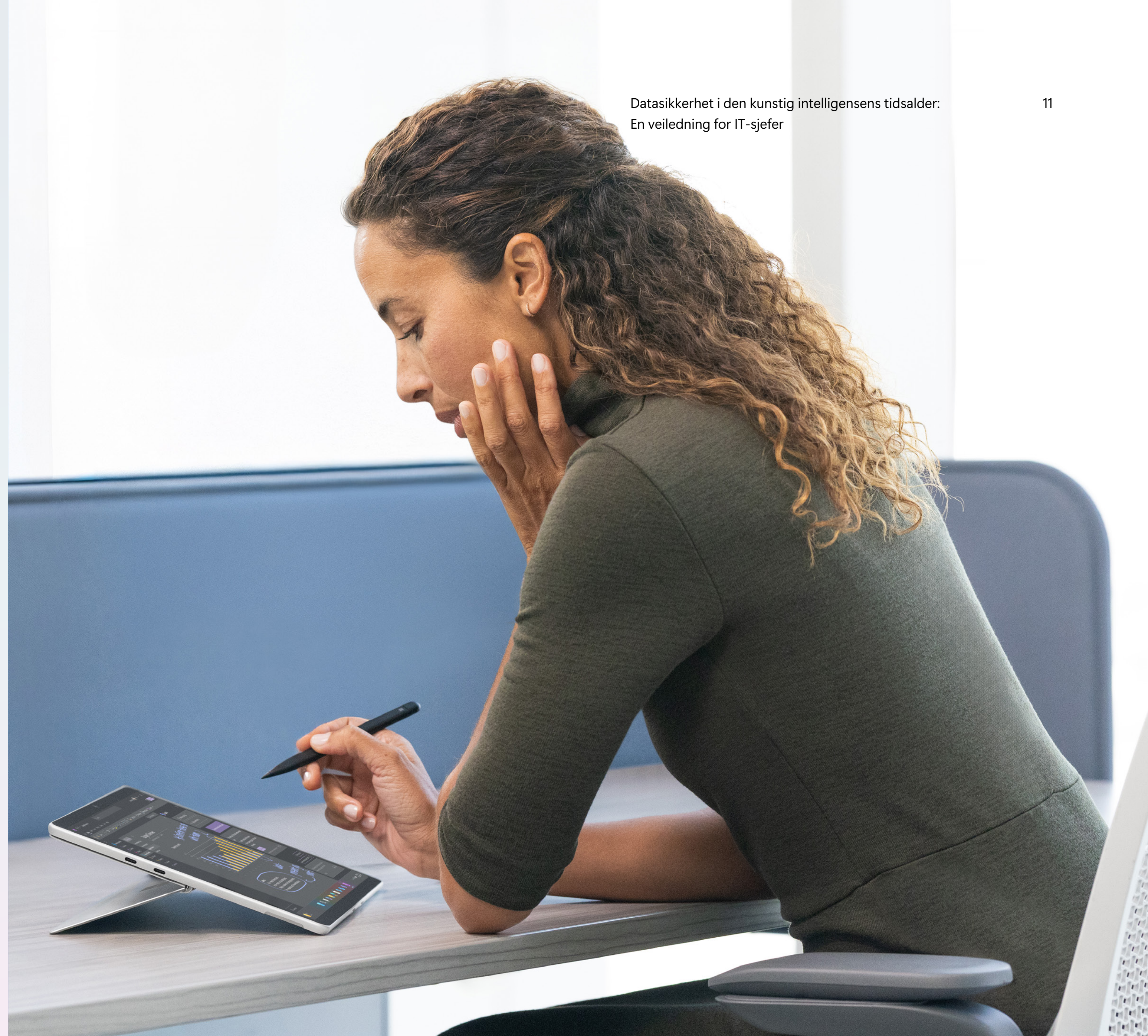
- Store økonomiske bøter (GDPR-bøter kan være på opptil **4 %** av de globale inntektene)⁴
- Krav om å varsle berørte parter om databrudd
- Berørte kan ta rettslige grep
- Skade på bedriftens omdømme og kundetillit

Når kunstig intelligens tas mer og mer i bruk i hele bedriften, trenger du styring som hjelper ansatte med å jobbe effektivt samtidig som bedriften etterlever forskriftene for bedriften og kundene.

Sikkerhetsbasert evaluering av kunstig intelligens

Medbrakt kunstig intelligens kan bryte med forskriftene og skape betydelige risiko. Derfor trenger du en strukturert evaluering av KI-løsninger som sikrer at de kan hjelpe bedriften med å drive innovasjon – samtidig som du beskytter sensitive data og sikrer etterlevelse av forskrifter som stadig endres.

Her følger seks enkle spørsmål for å vurdere om en KI-plattform leverer på begge fronter.



Spørsmål 1

Tilbyr løsningen avansert sikkerhet fra grunnen av?

Med riktig løsning blir det slutt på å reagere på problemer etter at de har skjedd. I stedet oppsøkes sårbarheter proaktivt i bedriftens data før de blir et større problem.

Se etter løsninger med følgende egenskaper:

- Gir sanntidsinnsyn i hele dataøkosystemet
- Oppdager potensielle datafarer automatisk før de blir til et problem
- Beskytter sensitiv informasjon på alle nivåer

Spørsmål 2

Kan løsningen enkelt tas i bruk og forbedre eksisterende sikkerhetskontroller?

Bedriftens sikkerhetsregler bør fungere problemfritt med kunstig intelligens. Løsningsleverandøren bør kunne integreres i de eksisterende sikkerhetsrammeverkene dine – ikke kreve at du oppretter helt nye.

Se etter løsninger med følgende egenskaper:

- Tar problemfritt i bruk eksisterende regler, sensitivitetsmerkelapper og innstillinger for informasjonsbeskyttelse
- Gir detaljert tilgangskontroll på individuelt nivå, slik at ingen brukere får tilgang til data de ikke skal ha tilgang til.
- Varsler aktivt om forsøk på å omgå tilgangskontroller

Spørsmål 3

Har løsningen innebygd styring og personvernkontroller?

Siden KI-verktøy fungerer mer proaktivt, må sikkerhetstiltakene også være proaktive. Implementering av sterk datastyring skaper klare grenser der de ansatte kan innovere trygt uten å sette sensitiv informasjon i fare.

Se etter løsninger med følgende egenskaper:

- Sentraliserer KI-styring med automatisert regelhåndhevelse for alle aktiviteter
- Har tidlig oppdagelse av potensiell overdrevet deling av data
- Følger rammeverk for å sikre etterlevelse av forskriftene for bruk av kunstig intelligens

Spørsmål 4

Kan løsningen rulles ut i hele bedriften?

De ansatte har sine egne arbeidsstiler, sine egne tidsplaner og kan befinne seg over hele verden. Kunstig intelligens bør være til nytte for alle.

Se etter løsninger med følgende egenskaper:

- Kan enkelt konfigureres og tas i bruk i den daglige arbeidsflyten
- Gir fleksibel tilgang, fra gratis KI-nettprat til skalerbare agentløsninger
- Hjelper ansatte med å integrere kunstig intelligens på en smidig måte i arbeidet

Spørsmål 5

Kan løsningen integreres problemfritt med de eksisterende rammeverkene?

Bedriften har for tiden sin egen digitale infrastruktur med programmer, apper og så videre.

Se etter løsninger med følgende egenskaper:

- Kan integreres problemfritt og avbruddsfritt med verktøy og programmer
- Tilbyr enhetlig KI-funksjonalitet i alle apper, slik at arbeidet kan flyte uhindret mellom verktøyene
- Automatiserer og optimerer oppgaver i eksisterende arbeidsflyt

Spørsmål 6

Har brukerne mulighet til å innovere?

Kunstig intelligens skal som hovedsak gjøre arbeidet mer effektivt. Det dreier seg ikke bare om automatisering, men om å forbedre produktiviteten og drive innovasjon.

Se etter løsninger med følgende egenskaper:

- Reduserer sløsing av tid og muliggjør effektive prosesser
- Automatiserer gjentakende oppgaver
- Gir de ansatte tilbake tid til å fokusere på prioriterte oppgaver

07

Microsoft 365 Copilot: Pålitelig kunstig intelligens

Microsoft 365 Copilot er en løsning med generativ kunstig intelligens, utviklet for å levere robuste sikkerhets-, styrings- og tilgangskontroller – noe som gir sikker utrulling og varig innovasjon. Løsningen forbedrer produktiviteten med intuitive verktøy som Copilot Chat, som fungerer der du jobber, og Copilot Studio, der medarbeidere uten kodingserfaring kan opprette sine egne KI-agenter.

Copilot integreres problemfritt i Microsoft 365-miljøet ditt, arver brukertillatelser, sensitivetsmerkelapper, regler for hindring av datatap og geografiske krav til datalagring – uten ekstra konfigurasjon. Ved å integrere kunstig intelligens i verktøyene de ansatte allerede bruker, reduserer Copilot sikkerhetsrisikoen samtidig som dataene blir værende i et pålitelig Microsoft 365-miljø.

Microsofts forpliktelser sikrer at bedriften fortsatt har kontroll:

- Dataene dine er sikre under lagring og under overføring
- Dataene brukes ikke til å lære opp språkmodeller.
- Du velger hvilken informasjon som havner i skyen
- Du beskyttes mot sikkerhets- og opphavsrettsrisiko under bruk av kunstig intelligens

Spesialbygde styringsverktøy som Copilot Control System og SharePoint Advanced Management gir IT-ansatte innsynet, kontrollene og revisjonsloggene som trengs for etterlevelse.

Med Microsoft 365 Copilot trenger du ikke å velge mellom innovasjon og sikkerhet – du kan få begge deler.

Sikker bruk av kunstig intelligens

KI-revolusjonen gir en unik mulighet for IT-sjefer til å levere strategisk verdi ved å balansere innovasjon og sikkerhet.

Når du implementerer sikre KI-verktøy som Microsoft 365 Copilot, gir du de ansatte verktøy for økt produktivitet, samtidig som du fjerner risikoen ved uautorisert bruk av kunstig intelligens. Veien fremover handler om å muliggjøre innovasjon på en sikker måte. Ditt lederskap innen sikker bruk av kunstig intelligens vil hjelpe bedriften din med å trives i denne nye tidsalderen samtidig som dataene sikres og etterlever forskriftene.



Kom i gang med Microsoft 365 Copilot

Kilder:

¹ «Superagency in the workplace: Empowering people to unlock AI's full potential», McKinsey & Company, 28. januar 2025. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work>.

² «Kunstig intelligens i arbeidslivet. Nå kommer den vanskelige biten», Microsofts arbeidstrendindeks, 8. mai 2024. <https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>.

³ «Er kunstig intelligens arbeidslivets redning?», Microsofts arbeidstrendindeks, 9. mai 2023. <https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>.

⁴ «EU-forordning 2016/679 av Europaparlamentet og Rådet 27. april 2016 om beskyttelse av fysiske personer med hensyn til behandling av personopplysninger og om fri bevegelse av slike data, og opphevelse av direktiv 95/46/EF (GDPR), Europaparlamentet og Rådet for Den europeiske union, 27. april 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.