Webinar:

Sikker og compliant brug af AI i din organisation

Præsentationen optages

Webinaret starter om et øjeblik

promte

Agenda

1. Introduktion til Promte
2. Risici ved brug af AI uden styring
3. Skygge-IT
4. Muligheder for at minimere risici
5. Demo af Promte Guardrails
6. Hvad koster det og hvordan kommer man i gang?

Sikkerhed

Compliance

Brugervenlighed

TIETGENSKOLEN

HVIDOVRE KOMMUNE

SBSYS

UEJLE KOMMUNE

Rackbeat

ER

SON OF A TAILOR

Alinea

Praxis

Aalborg Handelsskole

Esbjerg Kommune

ROSKILDE KOMMUNE

learningbank

Gentofte Kommune

KALUNDBORG KOMMUNE

Færdselsstyrelsen

promte

4 risici ved brug af AI uden styring på plads

Overblik

Lovgivning og compliance

Utilsigtet deling af data

Vendor lock-in

Manglende governance

promte

Bryde lovgivning

- AI Act, GDPR og fagspecifik lovgivning

Detaljer

- Medarbejdere bruger AI uden at kende reglerne
- Persondata behandles i ikke godkendte værktøjer
- AI bruges i arbejdsgange, hvor der gælder særlige krav
- Organisationen mangler dokumentation for brugen

Eksempler

- En medarbejder uploader borgersager til ChatGPT
- AI bruges til at formulere svar i en myndighedssag
- HR bruger AI til at vurdere ansøgninger uden klare rammer

Dele data utilsigtet

Fortrolige oplysninger, persondata og forretningshemmeligheder

Detaljer

- Data kopieres ind i åbne AI værktøjer
- Brugere tænker ikke over, at tekst kan indeholde følsomme oplysninger
- Interne dokumenter, kontrakter eller strategier deles utilsigtet
- Data kan ende hos leverandører uden korrekt aftale

Eksempler

- En kontrakt uploades for at få et resumé
- En medarbejder indsætter borgerdata i en prompt
- Intern strategi bruges som input til at skrive en præsentation

promte

Vendor lock-in

Afhængighed af leverandører og amerikansk tech

Detaljer

- Organisationen bygger arbejdsgange op omkring én leverandør, f.eks. ChatGPT
- Data, prompts og processer bliver svære at flytte
- Ændringer i priser, vilkår eller modeller kan ramme driften
- Krav til datasuverænitet kan blive svære at overholde

Eksempler

- En leverandør ændrer vilkår for databehandling
- En model fjernes eller bliver dyrere, og centrale processer påvirkes
- Politisk landskab eller kriser gør det nødvendigt at flytte ud af fx amerikansk tech

Manglende governance

Uklart ansvar, manglende overblik og ingen fælles rammer

Detaljer

- Ingen ved præcist, hvilke AI værktøjer der bruges
- Der mangler ejerskab, godkendelse og risikovurdering
- Brugerne finder egne løsninger gennem skygge-IT
- Der er ingen dokumentation, hvis noget går galt

Eksempler

- Medarbejdere bruger selv ChatGPT
- Der indsamles ikke logs centralt
- Borgeres retssikkerhed krænkes og revisionsspor er umuligt
- Ingen ved, hvem der har ansvar for logs, databehandling og opfølgning

promte

Hvordan sker det?

Skygge-IT

Skygge-IT

Datatilsynet ser en stigning

Medarbejdere bruger persondata fra arbejdet som input i generative AI-værktøjer uden godkendelse.

Kilde: Datatilsynet

78%

af AI-brugere tager deres egne AI-værktøjer med på arbejde.

Kilde: Microsoft

71,6%

af adgang til generative AI-værktøjer sker via private konti.

Kun **11,7%** sker via virksomhedskonto med SSO.

Kilde: LayerX

Når medarbejderne mangler et sikkert alternativ, flytter AI-brugen uden for organisationens kontrol.

Kilder: Datatilsynet, 'Forhold dig til AI-værktøjer' (22.03.2024) • Microsoft Work Trend Index 2024, 'AI at Work Is Here. Now Comes the Hard Part' • LayerX, 'Enterprise Report 2025: GenAI Security'

promte

Sådan kan risikoen reduceres

- **Oplysning og uddannelse af medarbejdere**
- **Godkendt AI platform for alle**
  (god nok til at være reelt alternativ)
- **Guardrails på udvalgte services**
  (mitigerer risiko for specifikt indhold)
- **Blokering af ikke godkendte services**
  (mitigerer risiko for brug af specifikke værktøjer)

promte

Promte Guardrails

Filtrering i tekst og filer inden det sendes til Promte - direkte på brugerens enhed (uden AI og ekstern databehandling)

Guardrails med filtrering af beskeder & blokering på andre værktøjer gennem browserudvidelse (uden AI og ekstern databehandling)

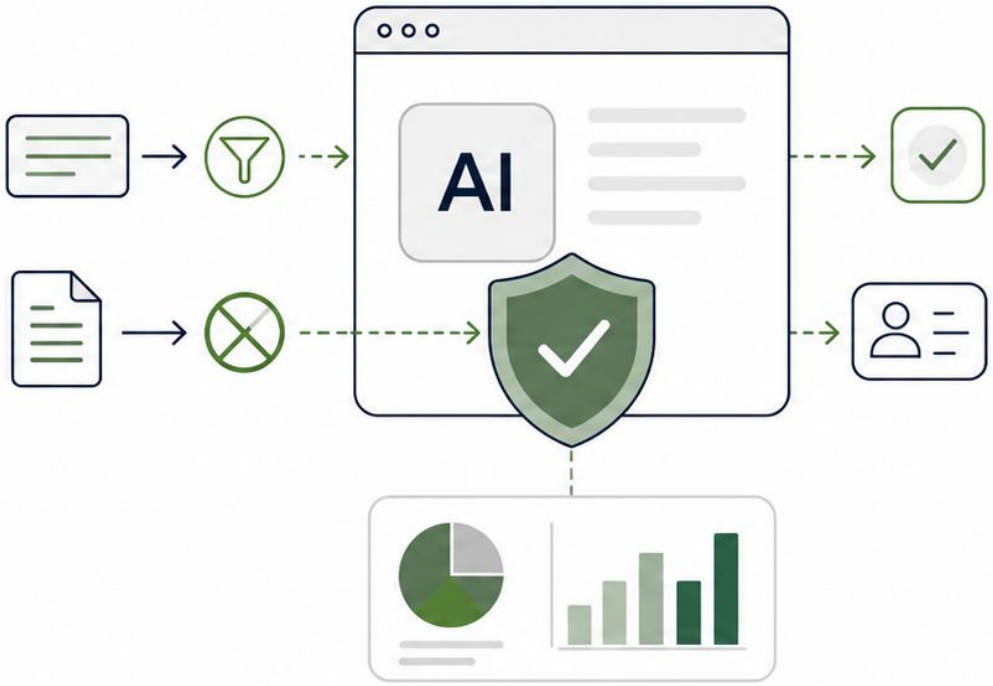
Overblik med aggregeret data for AI-forbrug hele organisationen

promte

Demonstration

Kontrol uden at stoppe AI-brug

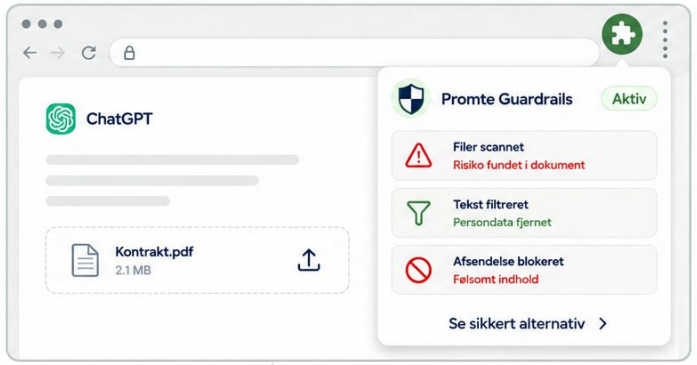
- Blokér ikke-godkendte AI services
- Filtrér tekst og filer før de sendes
- Giv brugerne tydelig vejledning
- Få overblik på aggregeret niveau



promte

Guardrails i brugerens browser

- Browserudvidelse til Chrome/Edge installeres centralt i organisationen
- Genkender udvalgte AI services
- Kan blokere adgang helt
- Kan filtrere tekst og filer før afsendelse
- Viser brugeren tydelige advarsler



Eksempler

- En medarbejder forsøger at uploade en kontrakt
- En prompt indeholder persondata
- En ikke godkendt AI service åbnes
- Brugeren får besked om, hvilket sikkert alternativ der bør bruges

promte

Overblik uden individuel overvågning

- Viser samlet AI brug i organisationen (både forbrug og antal gange det bliver filtreret)
- Data vises på aggregeret niveau
- Ingen rapportering eller dataindsamling på specifikke brugere
- Tydeligt banner forklarer, hvad der indsamles
- Kan slås fra, hvis organisationen ikke ønsker dataindsamling

promte

Et filter reducerer risikoen, men løser ikke hele problemet

Er problemet så løst?

- Guardrails mitigerer risikoen
- Ingen filterløsning er 100% sikker
- Brugerne finder ofte en vej udenom
- Platformene ændrer sig løbende, og et filter som dette kan derfor være bagud
- Derfor kræver det et godt og sikkert alternativ ala Promte AI-platform, så brugerne bruger det i stedet

Hvad koster det?

- I kan få lov at bruge Promtes Guardrails gratis
- Vedligeholdes alligevel som del af Promte-platformen
- Begrænsninger løser kun halvdelen af problemet; En god platform som fx Promte er den anden halvdel

Kontakt for opfølgende spørgsmål:

Promte.com

Victor Skytte, medstifter

Victor@promte.com

28 76 22 98

Note: Hele præsentationen er lavet med Promte Chat

Hvad sker der herefter

- Optagelse af webinar sendes ud til deltagere
- Vores præsentation fra i dag sendes som en PDF
- Guardrails fra Promte er gratis så book et møde hvis vi skal koordinere, hvordan vi sætter det op i din organisation

promte