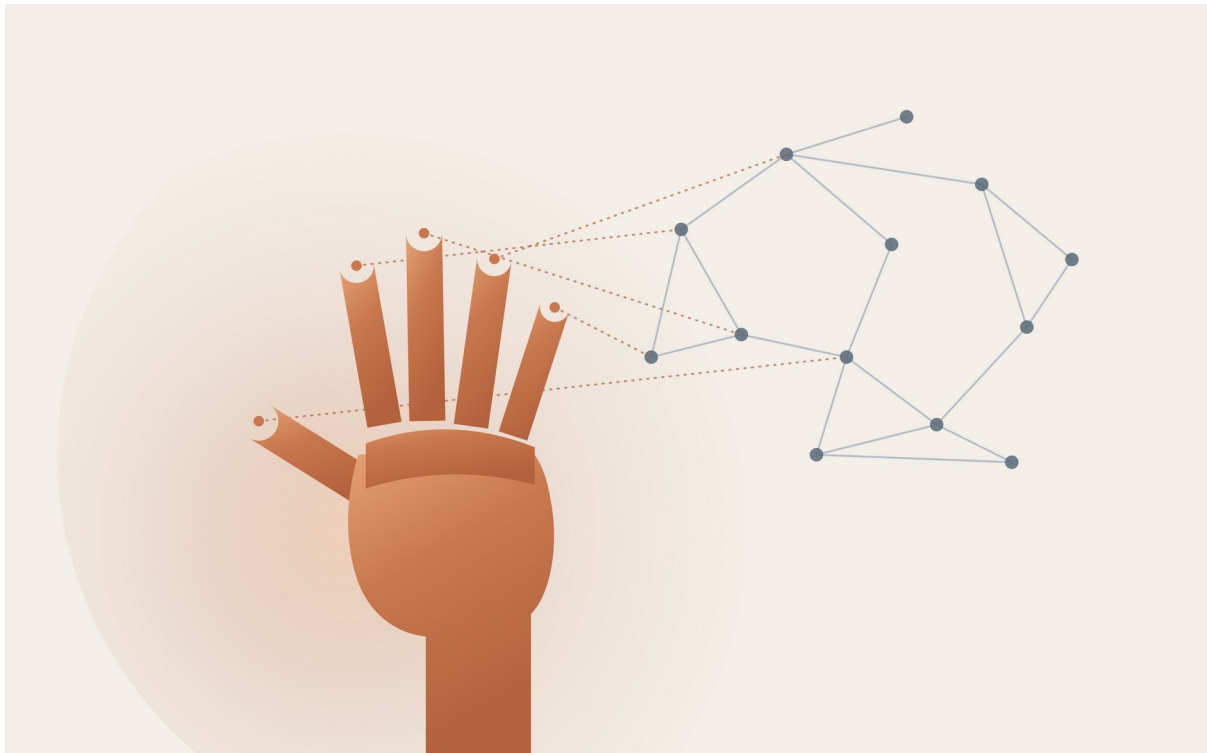


WHITEPAPER

Governance af AI-agenter i danske SMV'er

Hvad danske SMV'er skal vide, før arbejdet
lægges i hænderne på en agent.



Coga Collective

New Nordic AI-rådgivning · AI som konkurrencefordel

SKIFTET

Fra værktøj til medarbejder

AI i danske virksomheder har indtil nu mest handlet om værktøjer, man stiller spørgsmål til. Man skriver en prompt, får et svar og beslutter selv næste skridt. Det er ved at ændre sig.

Den næste generation af AI — agenter — tager et mål, lægger selv en plan, trækker på de systemer og data, de har fået adgang til, og fører arbejdet et stykke videre, før et menneske ser på resultatet. Forskellen er ikke modellen bagved. Forskellen er, hvor meget arbejde man overlader.

En chatbot betjener man ét spørgsmål ad gangen. En agent uddelegerer man en opgave til — og gennemgår resultatet. Det flytter det spørgsmål, en virksomhed skal stille sig selv: ikke længere kun »hvem må bruge AI«, men hvordan det arbejde, agenten udfører, skal afgrænses, overvåges og kontrolleres.

Agenter flytter AI fra at svare på spørgsmål til at føre arbejde videre.

For en dansk SMV er det ikke en akademisk skelnen. Det er forskellen mellem et værktøj, en medarbejder bruger, og en digital kollega, der handler på virksomhedens vegne — med de forpligtelser, det medfører.



AI bevæger sig fra assistent til agent — og styringens tyngdepunkt flytter med.

Hvorfor det rammer de fleste SMV'er

Store advokatfirmaer og banker har talt om agent-governance i et stykke tid. Men det er ikke kun deres problem. Agenter giver størst værdi på arbejde, der er veldefineret, gentaget og dokumenttungt — og det beskriver en stor del af hverdagen i næsten enhver dansk SMV.

Tænk på de opgaver, der fylder:

- Gennemgang af tilbud, kontrakter og aftaler for vilkår, frister og forbehold.
- Sammenligning af leverandører og indhentning af tilbud.
- Kvalitetssikring mod tjeklister, normer og standarder.
- Opfølgning på ændringer i regler, priser og krav.
- Håndtering af strømmen af dokumenter, mails og sager, en virksomhed genererer.

Det er præcis den slags struktureret, tilbagevendende arbejde, en agent kan bære. Men det er også arbejde med konsekvenser. En agent, der læser forkert i en kontrakt, misforstår et vilkår eller sender noget afsted uden kontrol, kan koste mere, end den sparer.

Værdien og risikoen bor samme sted. Derfor er styring ikke en bremse på AI — det er forudsætningen for, at den kan bruges på noget, der faktisk betyder noget.

PRINCIPPET

Man styrer arbejdet — ikke kun brugeren

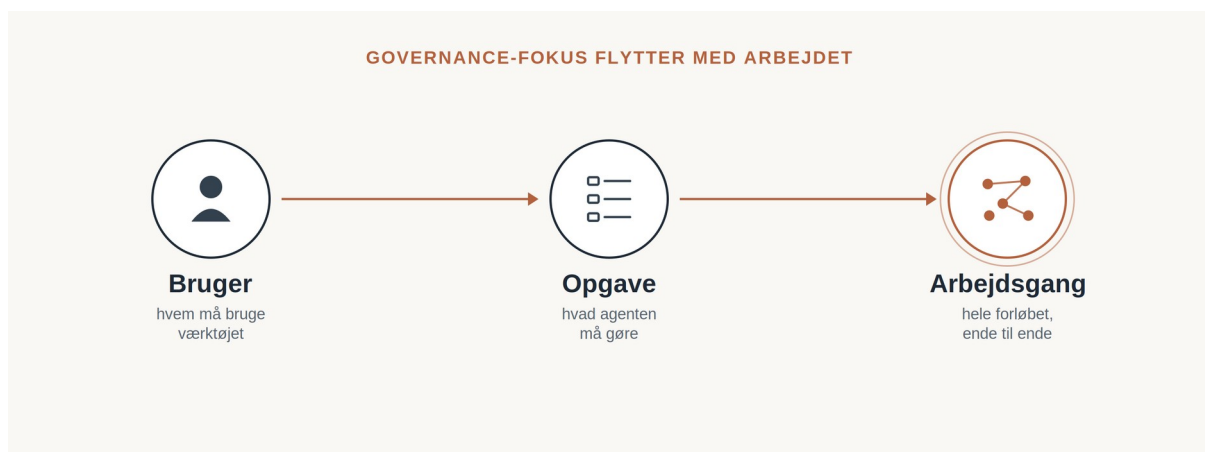
Den måde, de fleste virksomheder styrer AI på i dag, handler om personen: hvem har adgang, hvem må bruge hvilket værktøj. Det holder, så længe AI'en svarer på ét spørgsmål ad gangen.

Når en agent kører en proces på tværs af flere trin og systemer, flytter tyngdepunktet sig. Mennesket gennemgår stadig resultatet og griber ind undervejs, hvor det er nødvendigt — men mere af styringen ligger nu i selve arbejdet, agenten udfører, end i den enkelte prompt.

Styringens fokus flytter med arbejdet: fra bruger, til opgave, til arbejdsgang.

De klassiske risikotyper ændrer sig ikke: fortrolighed og data, korrekthed i output, adgang og autorisation, regelefterlevelse. Det, der ændrer sig, er hvornår man håndterer dem. Meget af arbejdet flytter fremad — til de rammer, man sætter for agenten, før den kører, frem for til indgreb undervejs.

I praksis betyder det, at man på forhånd tager stilling til fire ting: hvad må agenten læse, hvad må den gøre, hvem må køre den, og hvordan holder et menneske øje.



Fokus flytter fra personen, til den enkelte opgave, til hele arbejdsgangen.

Fem dimensioner, du skal have styr på

Det meste af det, en virksomhed allerede gør for at styre IT-adgang, gælder også for agenter. Men agenter rækker længere ind i systemerne, og det rejser fem spørgsmål, som er værd at tage stilling til, før en agent sættes i drift.

Dimension	Kernespørgsmål
1 · Adgangsomfang	Hvilke kilder og systemer må agenten trække på — og hvad må den gøre med adgangen?
2 · Autoriserede handlinger	Hvilke handlinger må agenten udføre selv, og hvilke kræver et menneskes godkendelse — især dem, der forlader virksomheden?
3 · Gennemgang og tilsyn	Hvordan følger og godkender et menneske arbejdet undervejs, og kan man efterprøve, hvad agenten byggede på?
4 · Udrulning og konfiguration	Hvem må køre en agent — og hvem må konfigurere eller udgive én til andre?
5 · Regelefterlevelse & EU AI Act	Er I deployer eller provider, er anvendelsen risikoklassificeret, og kan I dokumentere det?

Man behøver ikke svare perfekt på alle fem fra dag ét. Men man skal vide, hvor man står — og det er netop det, en modenhedsanalyse afdækker.

REGLERNE

EU AI Act: hvor står I?

Den femte dimension fortjener sin egen plads, fordi den er ny for de fleste danske SMV'er. EU AI Act er trådt i kraft og rulles ud i faser, og den skelner skarpt mellem to roller.

En provider udvikler eller markedsfører et AI-system. En deployer bruger det i egen drift. De fleste SMV'er vil være deployere — men i det øjeblik man begynder at bygge eller væsentligt tilpasse egne agenter, kan man glide over i provider-rollen, med langt tungere krav til følge. At vide, hvilken rolle man har for hver enkelt anvendelse, er ikke en formalitet. Det afgør, hvilke pligter man har.

Dertil kommer risikoklassificeringen. De fleste agent-opgaver i en typisk SMV vil ikke være høj-risiko i lovens forstand — men nogle kan være det, og grænsen er ikke altid indlysende. En forkert antagelse her kan blive dyr.

Kontrol er ikke en bremse på AI. Det er det, der gør AI til et forspring.

Pointen er ikke at skræmme. Det er, at styr på reglerne er præcis det, der gør det muligt at sætte AI i arbejde dér, hvor den skaber værdi. Den virksomhed, der har sin AI under kontrol, kan rykke hurtigere og med større tillid fra kunder, samarbejdspartnere og udbud — mens konkurrenten stadig tøver. Dér bliver AI et reelt konkurrenceforspring.

FØRSTE SKRIDT

Sådan kommer I i gang

Fire spørgsmål er et godt sted at begynde.

1. Hvilket arbejde vil en agent først kunne aflaste hos jer?

De oplagte kandidater er veldefineret, gentaget og dokumenttungt arbejde: kontrakt- og tilbudsgennemgang, leverandørsammenligning, kvalitetssikring mod tjeklister og regelovervågning.

2. Hvordan passer jeres nuværende IT-styring på det arbejde?

Overvej, hvilke politikker der allerede ville gælde for en agent, der løser opgaven i dag — og hvor der opstår nye spørgsmål på agent-niveau.

3. Hvad er jeres holdning til menneske-i-loopet?

Beslut, hvor i forløbet et menneske skal ind — og hold fast i, at det færdige resultat altid skal gennemgås og godkendes af en ansvarlig.

4. Hvordan udvides jeres log og overblik til agenter?

Agenter genererer mere data om, hvad der er sket. Overvej, hvordan det passer ind i jeres eksisterende måde at kunne revidere og forklare beslutninger på.

TIL SIDST

Et personligt ord

AI-agenter er ikke science fiction længere — de er ved at rykke ind i den danske hverdag, også i de små og mellemstore virksomheder. Min erfaring er, at de virksomheder, der kommer bedst fra start, ikke er dem med de fleste værktøjer, men dem med den klareste styring. Kontrol er ikke det modsatte af fart. Det er det, der gør farten forsvarlig.

Vil I vide, hvor I selv står på de fem dimensioner, tager jeg gerne en uforpligtende snak. Det er som regel en kort samtale, der sparer en lang omvej.

Med venlig hilsen og på genhør,



Jeppe Lindberg

Chefrådgiver · Coga Collective

Coga Collective

AI Modenhedsanalyse & Roadmap — kortlægger hvor I står på de fem dimensioner og lægger en konkret plan for de næste skridt. Med EU AI Act som fundament og risikominimering som udgangspunkt.

coga.dk · Køge, Danmark · *AI som konkurrencefordel*