

# AI-politik på SDU

De overordnede rammer for brug af kunstig intelligens. Gælder alle ansatte (VIP og TAP) og studerende ved al brug af AI i forskning, undervisning, administration og uddannelse.

## Seks principper Forankret i SDU's AI-kodeks og værdigrundlag

|                                                                                                                 |                                                                                                           |                                                                                   |                                                                                                           |                                                                                                                |                                                                                        |
|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|                                |                          |  |                        |                             |     |
| <b>Menneskecentreret anvendelse og ansvar</b>                                                                   | <b>Kvalitet og faglig validitet</b>                                                                       | <b>Transparens</b>                                                                | <b>Etik og ansvarlighed</b>                                                                               | <b>Lovmedholdelighed og databeskyttelse</b>                                                                    | <b>Bæredygtighed</b>                                                                   |
| AI skal støtte, ikke erstatte, menneskelig dømmekraft. Mennesker har altid ansvaret for beslutninger og output. | AI-genereret indhold skal kritisk vurderes, verificeres og kvalitetssikres af den ansvarlige medarbejder. | Brug af AI skal være gennemsigtig og følge gældende retningslinjer.               | AI må ikke bruges i strid med SDU's værdier, fx til manipulation, snyd, diskrimination eller overvågning. | AI skal bruges lovligt (bl.a. ophavsret og GDPR) og efter SDU's politikker for data- og informationssikkerhed. | Valg og brug af AI skal ske med blik for miljømæssige og samfundsmæssige konsekvenser. |

## Risikokategorier Alle AI-systemer vurderes efter risiko, jf. EU's AI Act

|                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br><b>Minimeret og begrænset risiko</b><br><b>Kan anvendes</b><br><br><b>Fx</b> <ul style="list-style-type: none"><li>- Generativ AI til tekst</li><li>- Analyse</li><li>- Administrative opgaver</li></ul><br><b>Forudsætning</b><br>Krav om transparens, databeskyttelse, akademisk integritet og menneskelig ansvarlighed overholdes. | <br><b>Højrisiko-AI</b><br><b>Kun efter særskilt godkendelse</b><br><br><b>Fx systemer til</b> <ul style="list-style-type: none"><li>- Ansættelse og optag</li><li>- Bedømmelse og eksamen</li><li>- Disciplinære forhold</li><li>- Adgang til rettigheder og ydelser</li></ul><br><b>Forudsætning</b><br>Dokumenteret risikostyring, meningsfuld menneskelig involvering, mulighed for kontrol og løbende kvalitetssikring. | <br><b>Forbudte AI-praksisser</b><br><b>Må ikke anvendes på SDU</b><br><br><b>Bl.a.</b> <ul style="list-style-type: none"><li>- Social scoring</li><li>- Manipulativ adfærdsstyring</li><li>- Uretmæssig biometrisk identifikation</li><li>- Anden brug, der krænker grundlæggende rettigheder</li></ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## AI-agenter/AI-assistenter og vibe coding

**Vibe coding:** Du beskriver i naturligt sprog, og en AI-agent eller AI-assistent omsætter det til kode. Mennesket har stadig ansvaret for design, korrekthed, sikkerhed og anvendelse. Vær særligt opmærksom på:

|                                                                                     |                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>Fagligt og juridisk ansvar</b><br>AI-genereret kode skal have en faglig gennemgang. Udvikleren har det fulde ansvar.                                                                                                  |
|  | <b>Informationssikkerhed og datahåndtering</b><br>Ingen fortrolige data, personoplysninger, nøgler eller tokens i AI-tjenester, som SDU RIO og SDU IT ikke har godkendt, medmindre miljøet er lukket for modeludbyderen. |
|  | <b>Supply chain og licens</b><br>Vurdér afhængigheder og licenser på samme måde som ved traditionel udvikling.                                                                                                           |
|  | <b>Sikkerhed og sårbarheder</b><br>Koden skal sikkerhedstestes og gennemgås på linje med al anden software.                                                                                                              |
|  | <b>Overblik og vedligeholdelse</b><br>Software i drift skal være læsbar, versioneret og dokumenteret, så den kan vedligeholdes og overdrages.                                                                            |

## Agentisk AI

Virtuelle assistenter, der ud fra mål og instruktioner kan udføre handlinger og træffe (delvist) autonome valg, fx oprette brugere, sende mails, oprette møder eller købe togbilletter.

### Tre krav ved enhver anvendelse

|                                                                                                                                                                 |                                                                                                                                                                                            |                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>En identificerbar ansvarlig</b><br>En person eller organisatorisk enhed. |  <b>Mulighed for at overvåge og afbryde</b><br>Og til at begrænse eller tilsidesætte dens handlinger. |  <b>Dokumentation</b><br>Af formål, anvendelsesområde og væsentlige AI-understøttede beslutninger. |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Det gælder også

|                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>Ingen root-adgang</b><br>Agentisk AI må ikke selv kunne downloade og installere software fra internettet.                                         |  <b>M365 kræver accept fra SDU IT</b><br>Ingen agentisk AI med rettigheder i M365 uden forudgående kommunikation og accept fra SDU IT.                                                      |
|  <b>Mere frihed i lukkede miljøer</b><br>I lukkede/kontrollerede miljøer som UCloud eller miljøer anvist af SDU IT kan der eksperimenteres mere frit. |  <b>Du har ansvaret</b><br>Brug kun agentisk AI på SDU's udstyr og netværk, hvis du forstår og kontrollerer den. Skadelige handlinger kan få ansættelses- eller studiemæssige konsekvenser. |

|                             |                                                                                                     |                                                                                                                            |                                                                    |                                                                                                 |                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>Ansvar og governance</b> | <b>UID</b><br>Udvalget for informationssikkerhed og databeskyttelse har ansvaret for AI-politikken. | <b>System- og procesejere</b><br>Fastlægger nærmere regler for AI i deres system eller hovedproces, fx HR ved ansættelser. | <b>Ledelsen</b><br>Sørger for, at medarbejderne kender politikken. | <b>Medarbejderne</b><br>Sætter sig ind i og efterlever politikken og tilhørende retningslinjer. | <b>AI-literacy</b><br>SDU sikrer, at medarbejdere har passende AI-kompetence til deres opgaver. |
|-----------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|