ITSikkerhedsGruppen´s

Resumé af EU´s forordning om kunstig intelligens (AI Act) - DK

November 2025

1. Formål og baggrund

Forordningen har til formål at skabe et fælles regelsæt for udvikling, markedsføring og anvendelse af kunstig intelligens (AI) i EU. Målet er at fremme innovation, sikre borgernes grundlæggende rettigheder, beskytte sundhed, sikkerhed, demokrati og miljø samt styrke tilliden til AI-systemer. Forordningen skal samtidig forhindre fragmentering af det indre marked og sikre fri bevægelighed for AI-baserede varer og tjenester.

2. Anvendelsesområde

Forordningen gælder for:

- Udbydere, der bringer AI-systemer eller AI-modeller til almen brug i omsætning eller ibrugtagning i EU, uanset etableringsland.
- Idriftsættere, importører og distributører af AI-systemer i EU.
- Brug af AI-systemer, hvis output anvendes i EU, selv hvis systemet er udviklet uden for EU.
- Visse undtagelser gælder for militære formål, national sikkerhed, forskning og udvikling samt privat, ikke-erhvervsmæssig brug.

3. Centrale definitioner

- **AI-system**: Maskinbaseret system, der kan udvise autonomi og tilpasse sig, og som genererer output (forudsigelser, anbefalinger, beslutninger) baseret på input.
- **Udbyder**: Den, der udvikler eller får udviklet et AI-system og bringer det i omsætning eller ibrugtagning.
- **Idriftsætter**: Den, der anvender et AI-system under sin myndighed.
- **AI-model til almen brug**: En AI-model, der kan udføre mange forskellige opgaver og integreres i mange systemer (fx store sprogmodeller).

4. Risikobaseret tilgang og eksempler

4.1 Forbudte AI-praksisser (Uacceptabel risiko)

Visse anvendelser af AI er forbudt, fx:

- Manipulation af adfærd gennem subliminale teknikker.
- Udnyttelse af sårbarheder (alder, handicap, social situation).

- Social scoring af borgere.
- Biometrisk fjernidentifikation i realtid på offentlige steder (med få undtagelser).
- AI til at udlede følelser på arbejdspladsen eller i uddannelsesinstitutioner.
- Oprettelse af ansigtsgenkendelsesdatabaser via masseindsamling.

Eksempler:

- Et AI-system, der bruger skjulte lydsignaler til at påvirke børns beslutninger i legetøjsreklamer.
- Et AI-system, der tildeler borgere point baseret på deres sociale adfærd og bruger dette til at give eller nægte adgang til offentlige ydelser.
- Automatisk ansigtsgenkendelse på offentlige pladser til masseovervågning (fx i en lufthavn uden konkret mistanke).
- Et AI-system, der overvåger medarbejderes ansigtsudtryk for at vurdere deres humør og produktivitet.
- Indsamling af billeder fra sociale medier til at opbygge en ansigtsgenkendelsesdatabase uden samtykke.

4.2 Højrisiko-AI-systemer

Omfatter bl.a. AI-systemer inden for:

- Biometri (fx ansigtsgenkendelse, følelsesgenkendelse).
- Kritisk infrastruktur (energi, transport, vand).
- Uddannelse og beskæftigelse (adgang, evaluering, rekruttering).
- Adgang til væsentlige tjenester (kreditvurdering, forsikring, sundhed).
- Retshåndhævelse, migration, retspleje og demokratiske processer.

Eksempler:

- Ansigtsgenkendelse til adgangskontrol i lufthavne eller på arbejdspladser.
- AI-systemer, der styrer elnettet eller overvåger vandforsyning for at opdage fejl og cyberangreb.
- AI, der automatisk vurderer eksamensbesvarelser eller tildeler elever adgang til bestemte uddannelsesforløb.

- AI-systemer, der screener jobansøgninger, vurderer kandidater eller overvåger medarbejderes præstationer.
- AI, der vurderer kreditværdighed ved lån, eller afgør om en borger er berettiget til sociale ydelser.
- AI, der hjælper politiet med at forudsige kriminalitet (predictive policing) eller identificere mistænkte via videoovervågning.
- AI, der vurderer risikoen ved indrejse eller hjælper med at behandle asylansøgninger.
- AI, der assisterer dommere med at analysere sagsakter eller bruges til at påvirke vælgeradfærd i valgkampagner.

4.3 AI-systemer med begrænset risiko (Gennemsigtighedskrav)

Skal opfylde visse gennemsigtighedskrav, fx oplysning om, at man interagerer med et AI-system eller at indhold er AI-genereret (deepfakes).

Eksempler:

- En kundeservice-chatbot, der besvarer spørgsmål på en hjemmeside.
- Virtuelle assistenter, der hjælper brugere med at booke møder eller finde information.
- AI, der genererer realistiske billeder eller videoer af personer, som ikke eksisterer, eller manipulerer eksisterende indhold (deepfakes).
- Værktøjer, der automatisk skriver artikler eller produktbeskrivelser.

4.4 Minimal risiko (Ingen særlige krav)

De fleste AI-systemer, fx spamfiltre, er ikke underlagt særlige krav.

Eksempler:

- AI, der sorterer uønskede e-mails fra i din indbakke (spamfilter).
- AI, der foreslår film på Netflix eller produkter på en webshop (anbefalingssystemer).
- AI, der automatisk retter stavefejl i tekstbehandlingsprogrammer (stavekontrol).
- AI, der automatisk organiserer billeder i albums på din telefon (billedsortering).

5. Krav til højrisiko-AI-systemer

- Risikostyringssystem og løbende overvågning.
- Kvalitetskrav til data (repræsentativitet, bias-minimering).
- Teknisk dokumentation og logning.
- Gennemsigtighed og brugsanvisning til idriftsættere.
- Menneskeligt tilsyn og mulighed for at tilsidesætte AI-beslutninger.
- Nøjagtighed, robusthed og cybersikkerhed.
- CE-mærkning og overensstemmelsesvurdering før markedsføring.
- Registrering i EU-database.

6. Forpligtelser for operatører

- Udbydere: Skal sikre overholdelse af krav, opbevare dokumentation, foretage overensstemmelsesvurdering, anbringe CE-mærkning, registrere systemet mv.
- Importører og distributører: Skal kontrollere, at systemet opfylder kravene.
- Idriftsættere: Skal sikre korrekt brug, informere berørte personer, opbevare logfiler, overvåge systemet og foretage konsekvensanalyser for grundlæggende rettigheder, hvis relevant.

7. AI-modeller til almen brug

- Særlige krav til dokumentation, gennemsigtighed og risikostyring for AI-modeller, der kan anvendes bredt og udgør systemiske risici.
- Open source-modeller er undtaget fra visse krav, medmindre de udgør systemiske risici.
- Krav om offentliggørelse af træningsdata-sammenfatning og politik for ophavsret.

8. Gennemsigtighed og mærkning

- Brugere skal informeres, når de interagerer med AI, eller når indhold er genereret/manipuleret af AI (deepfakes).
- Særlige regler for mærkning og sporbarhed.
- Krav om, at AI-genereret indhold kan identificeres maskinelt (fx vandmærkning).

9. Innovation og støtte til SMV'er

- Reguleringsmæssige sandkasser for at fremme innovation og støtte SMV'er.
- Forenklede krav for mikrovirksomheder.
- Prioriteret adgang til sandkasser og vejledning for SMV'er.

10. Markedsovervågning, håndhævelse og sanktioner

- Nationale myndigheder fører tilsyn og kan pålægge sanktioner, herunder bøder på op til 35 mio. EUR eller 7% af global omsætning for alvorlige overtrædelser.
- Klageadgang og ret til forklaring for personer, der påvirkes af AI-beslutninger.
- Mulighed for at indgive klage til markedsovervågningsmyndigheden.
- Whistleblower-beskyttelse.

11. Bilag og overgangsregler

- Bilagene indeholder detaljerede lister over højrisiko-AI-systemer, teknisk dokumentation, krav til overensstemmelsesvurdering, oplysninger til registrering mv.
- Overgangsregler sikrer, at eksisterende systemer får tid til at tilpasse sig de nye krav.
- Forordningen træder i kraft 20 dage efter offentliggørelse og anvendes generelt efter 24 måneder, med visse undtagelser for forbudte praksisser og administrative bestemmelser.