

KI-forordningen



Litt om meg

- ◆ Siri Tenden, statsviter og jobber i Bergen
- ◆ Jobbet med personvern i forskning i snart 10 år
- ◆ Eksternt personvernombud og personvernrådgiver
- ◆ Sitter i arbeidsgruppe som ser på konsekvenser av KI-forordningen for akademia



Innhold

- ◆ Overordnet om KI-forordningen
- ◆ Oppbygning og sentrale definisjoner
- ◆ Forholdet til GDPR
- ◆ KI med forbud og høy risiko
- ◆ Viktigste roller i KI-forordningen



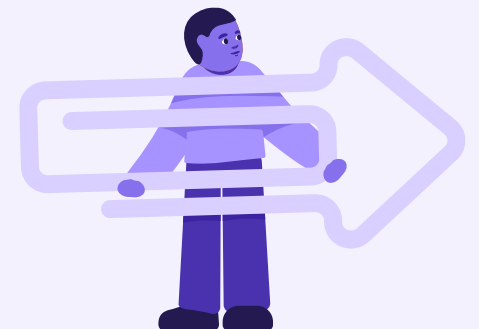


Om KI-forordningen

- ◆ Trådte i kraft i EU i sommer
- ◆ Virksomhetene skal tilpasse seg de nye reglene frem til 2026
- ◆ Ikke vedtatt i Norge enda
- ◆ Når den er innlemmet i norsk rett vil det bli en tilpasningsperiode

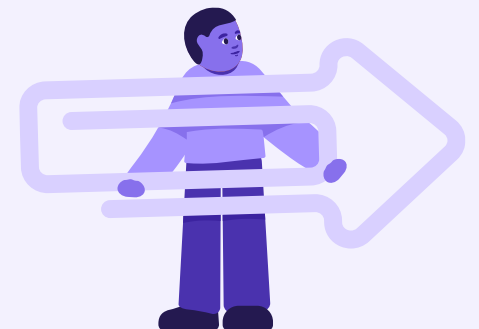
Formålet

- ◆ Et velfungerende indre marked i EU
- ◆ Legge til rette for bruk av KI (“human-centric” og “trustworthy”)
- ◆ Høy grad av beskyttelse med hensyn til helse, sikkerhet og grunnleggende rettigheter
- ◆ Unngå skadevirkninger og støtte innovasjon



Forholdet til GDPR

- ◆ GDPR fortsatt det viktigste regelverket som regulerer personopplysninger og KI
- ◆ inntar en rekke definisjoner og begreper fra GDPR
- ◆ begge har en risikobasert tilnærming
- ◆ rettighetsbasert vs. produktsikkerhetsregelverk



Definisjonen av et KI-system

AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

En viss autonomi/
selvstendighet
(gjøre ting selv)

En viss grad av
tilpasningsdyktighet
(læringsevne)

Generative
egenskaper

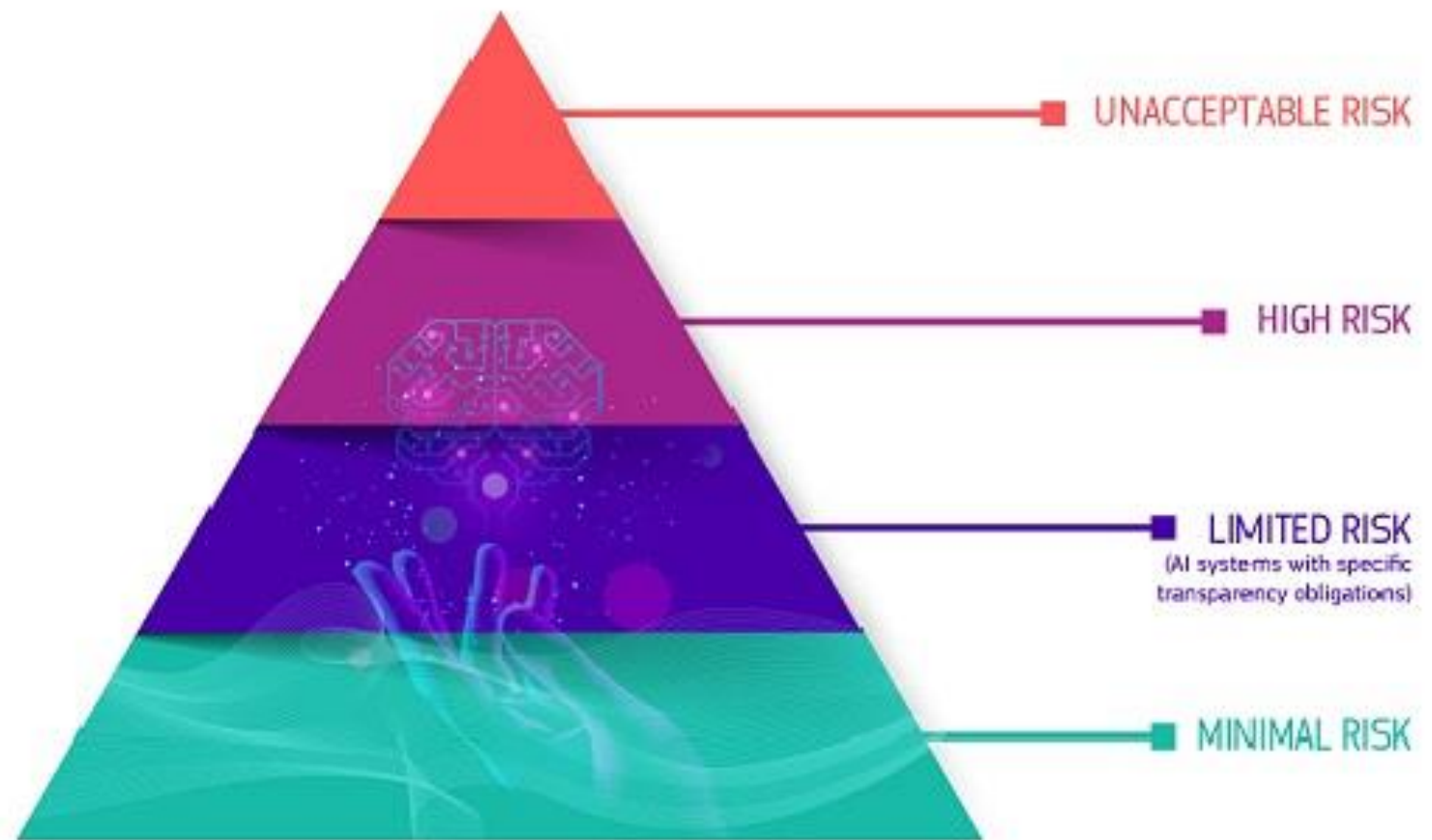
Påvirkningskraft i
samfunnet

Viktige unntak

- ◆ Bruk av KI-systemer av privatpersoner i rent personlige og ikke-profesjonelle sammenhenger
- ◆ Unntak for militære formål, forsvar eller nasjonal sikkerhet
- ◆ KI-systemer og modeller utviklet og brukt utelukkende for **vitenskapelig forskning**
- ◆ **Forskning, testing og utvikling** av KI-modeller eller KI-systemer **før** de settes på markedet (men unntak fra dette unntaket hvis testing on real-life conditions)

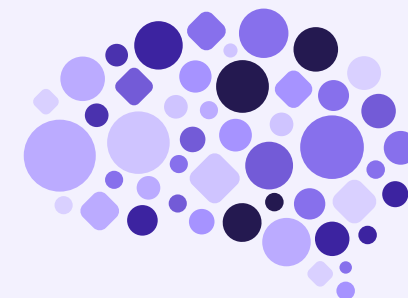


Risiko



Det er **forbud** mot KI systemer som:

- ◆ Manipulerer folks beslutninger eller utnytter deres sårbarheter med hensikt om å forvrengte atferden til enkeltpersoner eller grupper.
- ◆ Kategorisere enkeltpersoner basert på biometriske data for å utlede rase, politiske meninger, fagforeningsmedlemskap, religiøs eller politisk overbevisning eller seksuelle opplysninger.
- ◆ Evaluerer eller klassifiserer mennesker basert på deres sosiale atferd eller personlige egenskaper, som forårsaker skadelig eller ugunstig behandling av personene.
- ◆ Utleder følelser på arbeidsplass eller utdanningsinstitusjoner

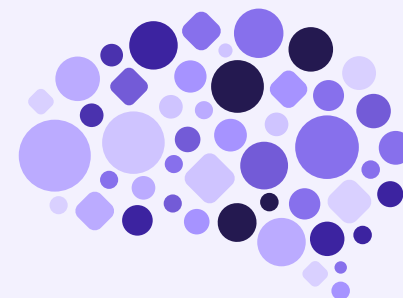


Høy-risiko

(områder som de fleste forpliktelse i forordningen gjelder for)

Systemer som utgjør en betydelig risiko for helse, sikkerhet, eller grunnleggende rettigheter

- Dette gjelder KI-systemer som utgjør sikkerhetskomponenter i f.eks. leker, kjøretøy, medisinsk utstyr og mye mer.
- Og KI-systemer på åtte definerte områder som er forklart i et vedlegg til forordningen. Disse områdene er:
 - (1) Biometri (2) Kritisk infrastruktur **(3) Utdanning og yrkesopplæring (4) Ansettelse, arbeiderledelse og tilgang til selvstendig næringsvirksomhet (5) Tilgang til og nytelse av essensielle private tjenester og essensielle offentlige tjenester og fordeler (inkludert for kredittvurdering og kredittkontroller eller for risikovurdering og prissetting for helse- og livsforsikringer) (6)** Lovhåndhevelse (7) Migrasjon, asyl og grensekontrollhåndtering (8) Administrasjon av rettferdighet og demokratiske prosesser.



Høy risiko (fra vedlegg 3)

Ansettelse, arbeidsledelse

- KI-systemer som brukes til rekruttering eller utvelgelse, målrettede stillingsannonser, analyse og filtrering søknader og evaluering av kandidater.
- Forfremmelse, oppsigelse av kontrakter, tildeling av oppgaver basert på personlighetstrekk eller egenskaper og atferd, overvåkning og evaluering av ytelse.



Høy risiko (fra vedlegg 3)

Utdanning og yrkesopplæring

- KI-systemer som bestemmer tilgang, opptak eller tildeling til utdanning eller yrkesopplæring på alle nivå.
- Evaluering av læringsutbytte, inkludert bruk til å styre studentens læringsprosess.
- Vurdering av riktig utdanningsnivå
- Overvåke og oppdage forbudt atferd hos elever under prøver.



Høy risiko

(fra vedlegg 3)

Tilgang til og nytelse av viktige offentlige og private tjenester

- KI-system som brukes av myndighetene til å vurdere kvalifisering til fordeler og tjenester
- Evaluering av kredittverdighet
- Evaluering og klassifisering av nødannrop
- Risikovurdering og prising i helse og livsforsikring



Unntak

KI-systemer skal **ikke** anses som høyrisiko når det ikke utgjør en betydelig risiko for skade på helsen, sikkerheten eller grunnleggende rettigheter for naturlige personer, inkludert ved ikke vesentlig å påvirke utfallet av beslutningstaking.



Noen vilkår må være oppfylt:

- a KI-systemet er ment å utføre en smal prosedyreoppgave;
- b KI-systemet er ment å forbedre resultatet av en tidligere utført menneskelig aktivitet;
- c KI-systemet er ment å oppdage beslutningsmønstre eller avvik fra tidligere beslutningsmønstre og er ikke ment å erstatte eller påvirke den tidligere fullførte menneskelige vurderingen, uten riktig menneskelig gjennomgang; eller
- d KI-systemet er ment å utføre en forberedende oppgave til en vurdering relevant for formålene med bruksområdene oppført i vedlegg III.



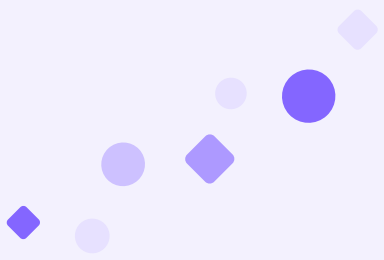
DEBATT • ØYSTEIN FLØ BASTE

Når KI bestemmer eksamens- karakteren

Premature forsøk på å sensurere eksamensoppgaver ved hjelp av kunstig intelligens undergraver tilliten til en allerede presset sensurordning. Dette må hver enkelt sensor og utdanningsinstitusjonene ta på alvor.



Språkmodellene er ikke nøytrale verktøy i en sensurprosess, skriver forfatteren. – Dette stiller ikke bare krav til myndighetene og institusjonene, men også den enkelte sensor. Foto: UiO



De to viktigste rollene

◆ **Provider (leverandør)**

- Leverandører som setter i bruk KI-systemer eller setter KI-system eller KI-modeller på markedet.

◆ **Deployer (bruker)**

- gjelder for fysiske og juridiske personer (virksomheter, offentlige myndigheter, osv.)
- bruker KI til andre enn rent personlige/ikke-profesjonelle formål.

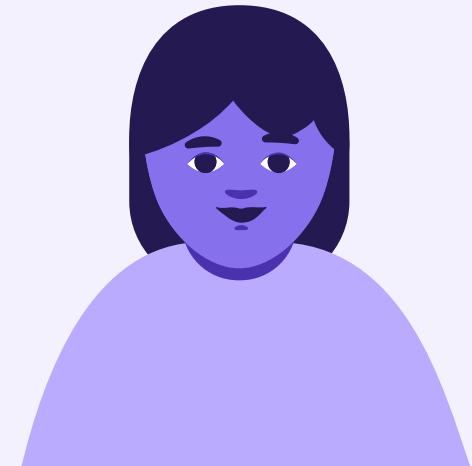


Forpliktelser **leverandør**

- ◆ Registreringsplikt i EU-database
- ◆ Kvalitetsstyringssystem og risikostyringssystem
- ◆ Rapportering av alvorlige hendelser og loggføring
- ◆ Datastyring og kvalitet (krav til kvalitet på testdatasett)
- ◆ Teknisk dokumentasjon
- ◆ Åpenhet og menneskelig tilsyn
- ◆ Cybersikkerhet

Forpliktelser **bruker**

- ◆ Iverksette passende tekniske og organisatoriske tiltak for å sikre at bruk av høyrisiko KI-system skjer i samsvar med instruksjoner for bruk
- ◆ Varslingsplikt dersom avdekker risiko i system
- ◆ Involvere fagforeninger hvis bruk på arbeidsplass
- ◆ Fundamental Rights Impact Assessment (FRIA)



Oppsummering

- For å finne ut hvilke forpliktelser som gjelder, må du avgjøre om du er en leverandør eller bruker og om bruken faller innenfor bruksområdene som har høy risiko
- Husk at GDPR fortsatt er viktigste regelverk for KI og personopplysninger

Tusen takk for meg!

siri.tenden@sikt.no