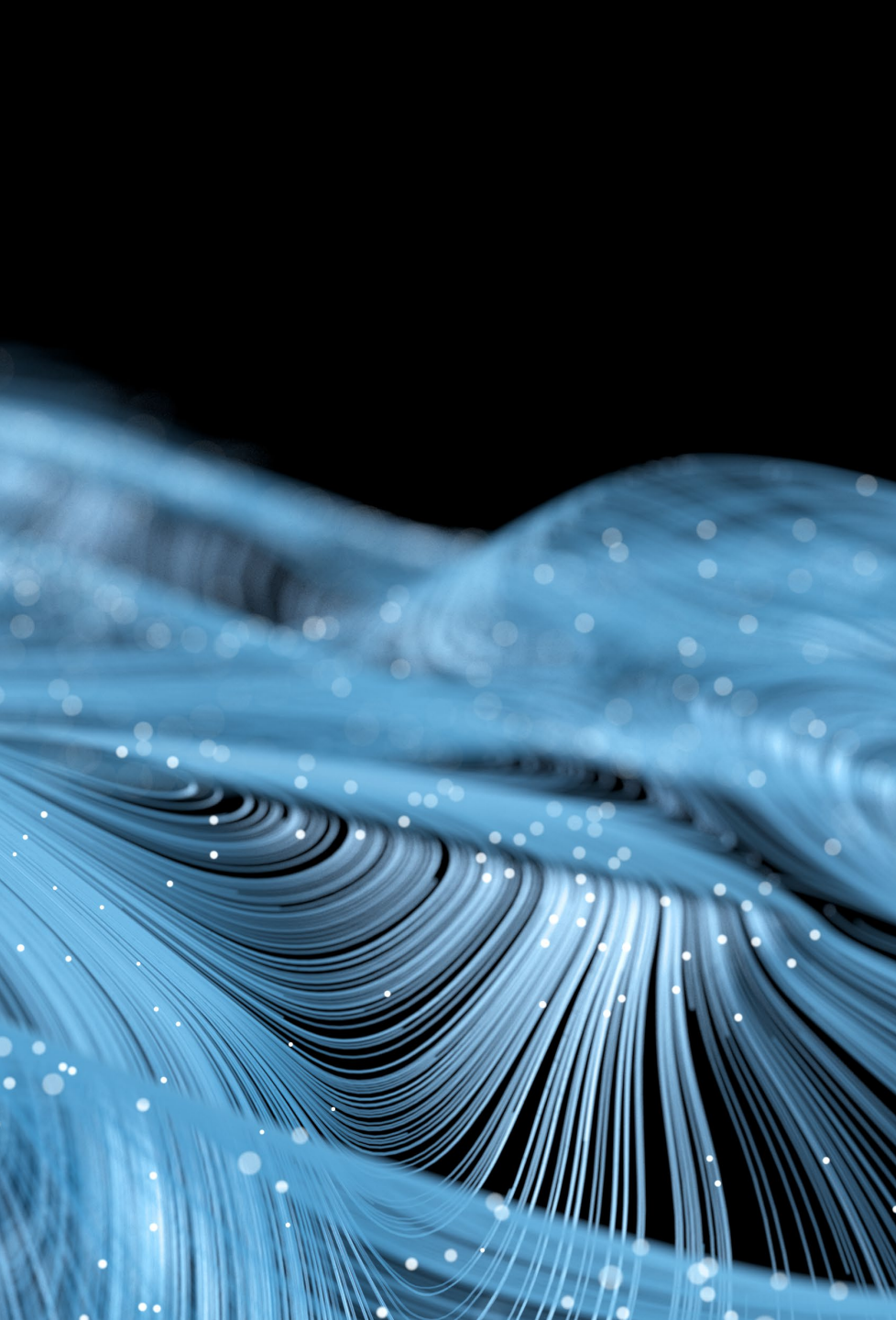
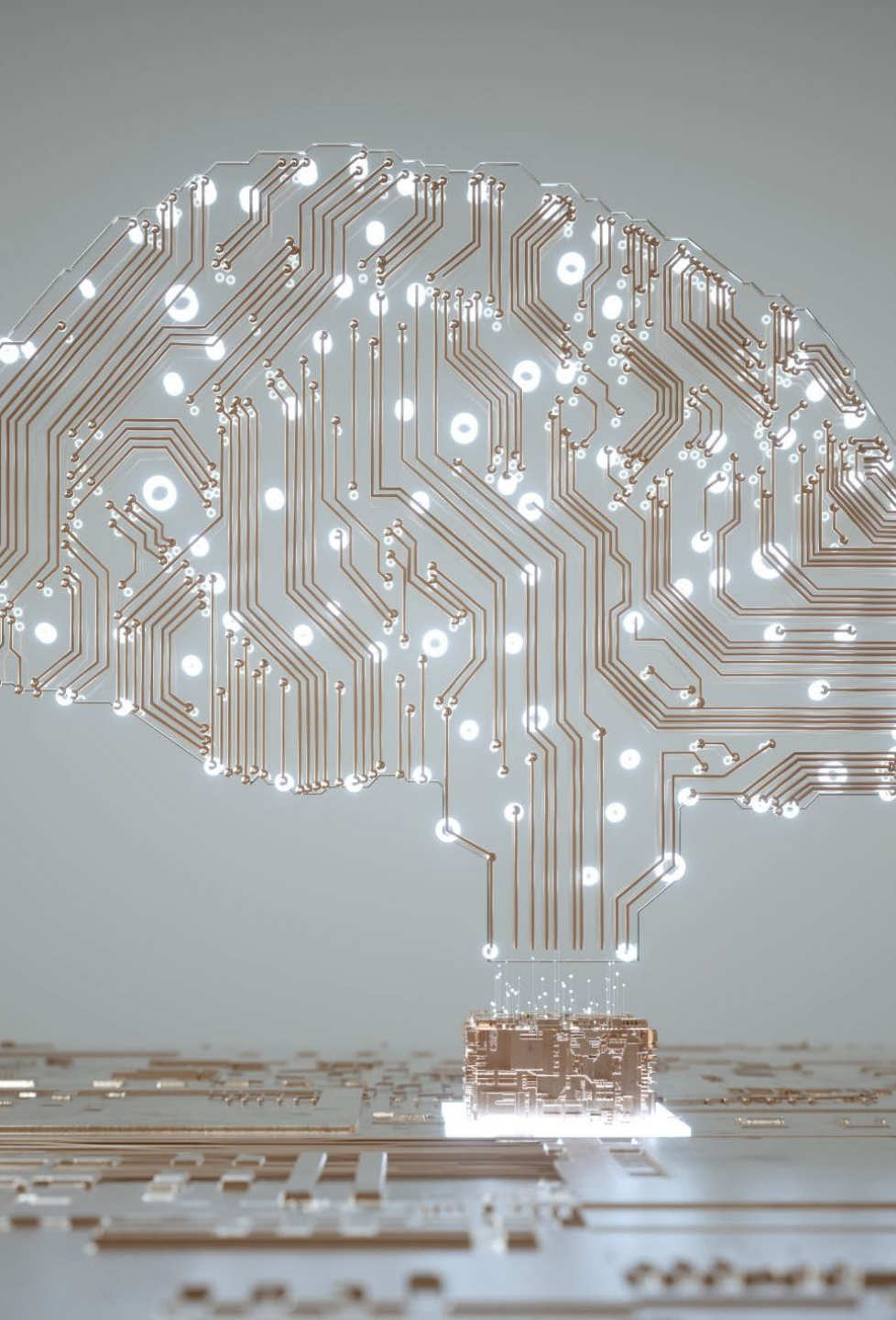


CLP

AI Act kort forklart - implikasjoner for kraftbransjen

The Norwegian Smartgrid Centre
24.4.2024



Oversikt

- Behovet for regulering
- Dagens regulatoriske landskap for AI
- AI Act kort oppsummert
- Relevans for kraftbransjen
- De viktigste kravene
- Noen praktiske råd – hva bør man tenke på nå?
- Data Act - teaser

Behovet for regulering

Google hit with lawsuit saying it scraped data without consent

Deepfake of British politician abusing staff goes viral

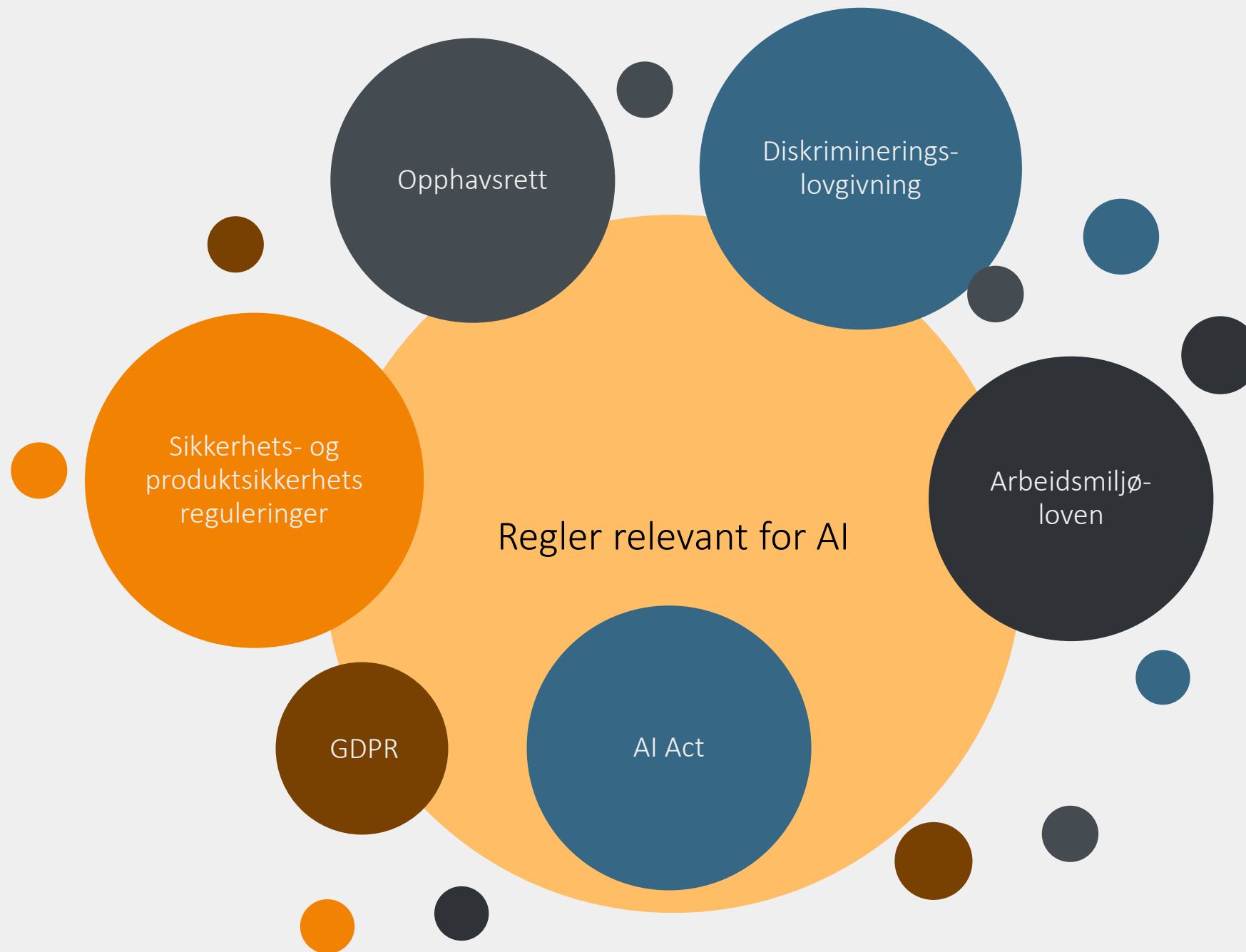
Amazon AI-enabled recruitment tool only recommended men

False facial recognition match leads to Black man's arrest

15 Potential AI Risks

- 1 Automation-spurred job loss
- 2 Deepfakes
- 3 Privacy Violations
- 4 Algorithmic bias caused by bad data
- 5 Socioeconomic inequality
- 6 Danger to humans
- 7 Unclear legal regulation
- 8 Social manipulation
- 9 Invasion of privacy and social grading
- 10 Misalignment between our goals and AI's goals
- 11 A lack of transparency
- 12 Loss of control
- 13 Introducing program bias into decision-making
- 14 Data sourcing and violation of personal privacy
- 15 Techno-solutionism





AI-forordningen kort oppsummert



Hvem?

Leverandører, importører, distributører og brukere av AI-systemer



Hva?

En produktsikkerhetslov for AI



Hvorfor?

Sikre trygg, sikker og rettferdig utvikling og bruk av AI

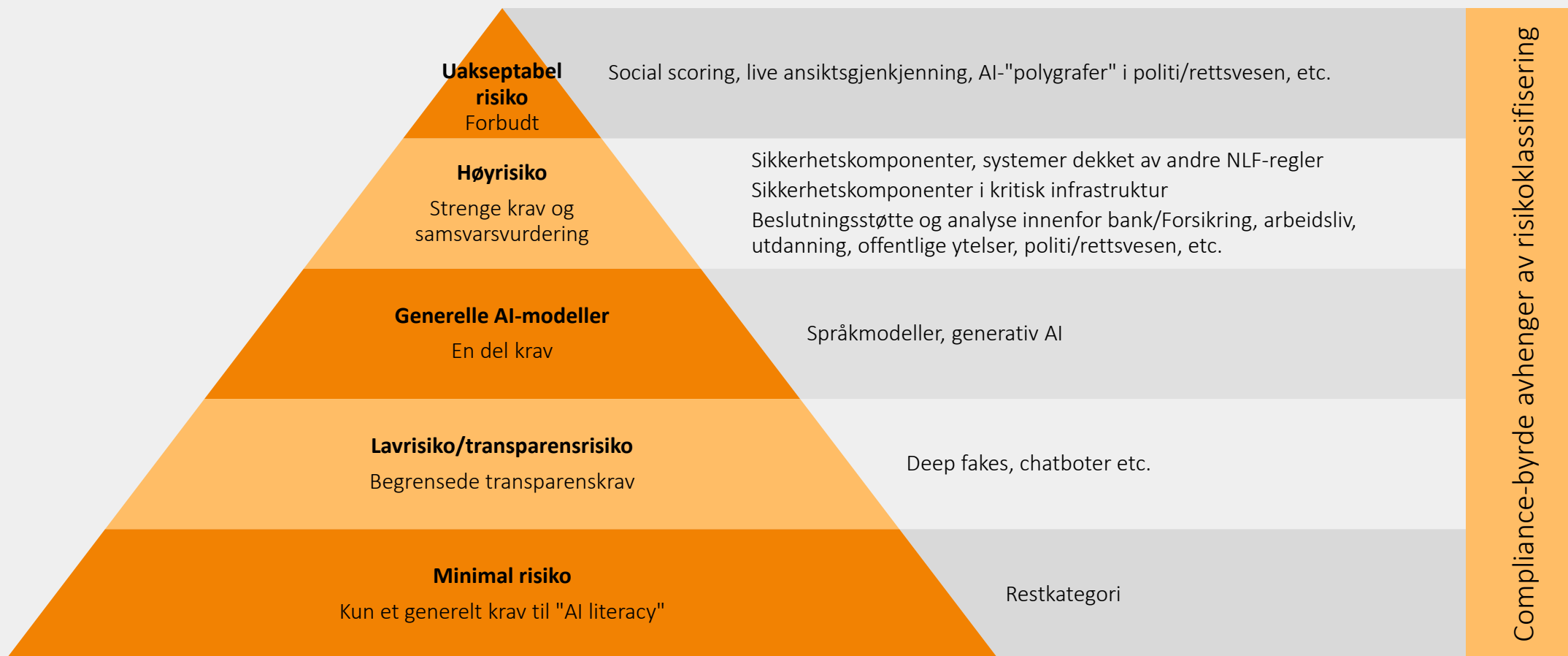


Når?

Vedtas april 2024, i kraft fra 2025

(gradvis innføring / overgangsregler frem til 2030)

Oversikt over AI-forordningen - risikoklassifisering



Sanksjoner: Tilbakekalling av produkter, forbud mot salg og store bøter

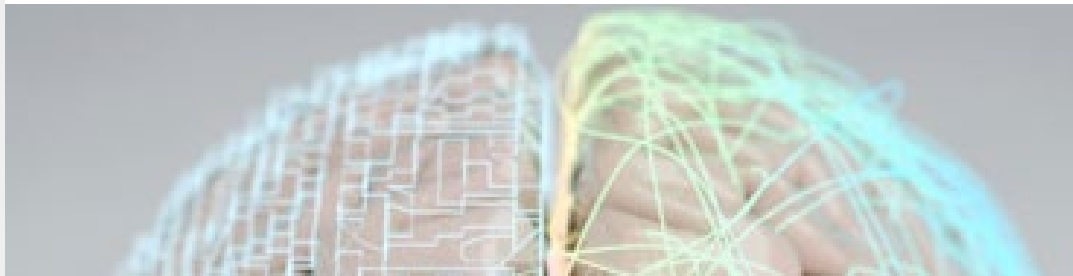
Høyrisikosystemer - eksempler

Annex III

High-Risk AI Systems Referred to in Article 6(2)

Updated on Feb 6th 2024 based on the version endorsed by the Coreper I on Feb 2nd

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:



Sikkerhetskomponent i ulike produkter

Medisinsk tech

Sikkerhetskomponenter for kritisk infrastruktur

Kredittvurdering

Rekrutteringsalgoritmer

Avgjøre opptak til utdanning

Saksbehandling i NAV

Vurdering av bevis i straffesak

MERK - DYNAMISK KLASSIFISERING

Betydning for kraftbransjen – det vi vet så langt



Potensielle høyrisiko-systemer?

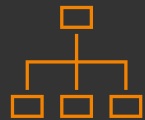
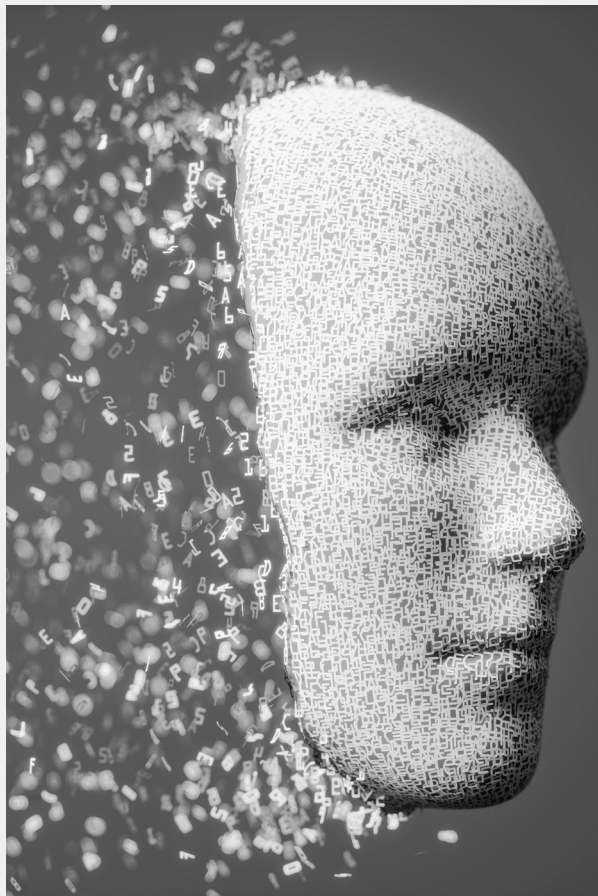
- ▶ AI-systemer brukt som "safety components" i
 - ▶ "Critical **digital** infrastructure"
 - ▶ "supply of water, gas, heating or electricity"
- ▶ Unntak
 - ▶ Cybersikkerhetsmoduler
 - ▶ Ikke foreligger risiko for skade på helse, sikkerhet eller fundamentale rettigheter



Hypotese: Mye blir minimal risiko

- ▶ Det meste av specific purpose-AI som ikke er høyrisiko
 - ▶ Etterspørselsprognoser
 - ▶ Optimalisering av strømnett
 - ▶ Integrasjonsverktøy
 - ▶ Kundebehandling (kan utgjøre **lavrisiko**)

Høyriskosystemer - krav



Leverandør

- ▶ Krav til:
 - ▶ Datakvalitet
 - ▶ Forklarbarhet
 - ▶ Treffsikkerhet
 - ▶ Risikohåndtering
 - ▶ Kvalitetsstyring
 - ▶ Dokumentasjon
 - ▶ Cybersikkerhet
- ▶ Gjennomføre samsvarsvurderinger, CE-merking
- ▶ Post-market monitorering



Brukere

- ▶ Bruke relevante input-data
- ▶ Følge bruksanvisning/instrukser
- ▶ Overvåke og føre menneskelig tilsyn
- ▶ Ivareta transparens overfor sluttbruker
- ▶ Varsle ved mistanke om risiko for skade/alvorlige hendelser

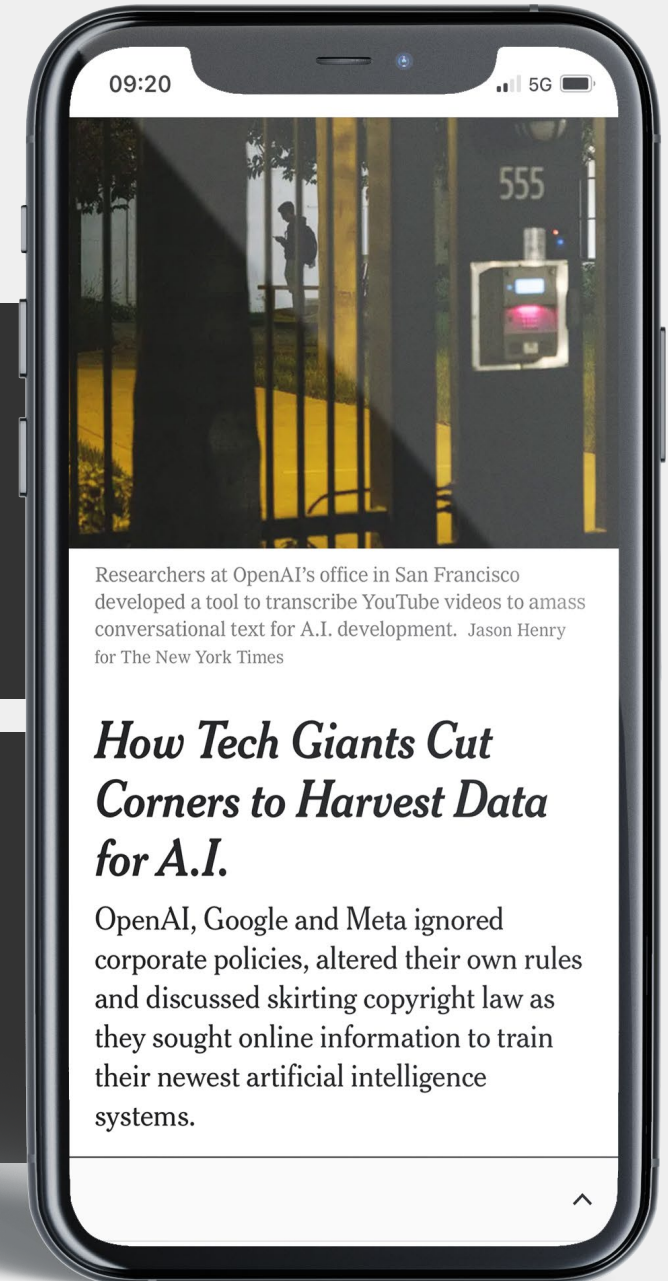
Generelle AI-modeller (general purpose AI)

Generelt

- ▶ Transparenskrav
- ▶ Teknisk dokumentasjon
- ▶ Overholdelse av immaterialrettslige regler under trening og bruk
- ▶ Dele detaljerte sammendrag om treningsdata som er brukt

For de største modellene som kan utgjøre "systemisk risiko"

- ▶ Krav til risikohåndtering
- ▶ Modellevaluering og testing
- ▶ Cybersikkerhet
- ▶ Monitorering og rapportering om alvorlige hendelser



Lavrisikosystemer - krav



Unknown creator – licensed under CC BY-NC-ND

Systemer som interagerer med mennesker

- ▶ Chatboter etc
- ▶ **Leverandør** må sørge for å informere mennesker om at de interagerer med et AI-system

Generering og manipulering av bilder, lyd, video og tekst

- ▶ **Leverandør** må sørge for at output merkes som AI-generert eller –manipulert
- ▶ **Brukere** må merke deep fakes, og informereinformere dersom publisert tekst med formål om å opplyse allmennheten om saker av allmenn interesse er AI-generert eller –manipulert

Følelsesgjenkjenning/biometrisk kategorisering

- ▶ **Brukere** må informere personer som underlegges systemet om bruken

Hvordan bør kraftbransjen forberede seg?



Identifiser og kartlegg

- ▶ Dagens og fremtidens AI-systemer
- ▶ AI-strategi



Bli kjent med regelverket

- ▶ Hvilken rolle har vår virksomhet?
- ▶ Risikoklassifisering



Etabler internkontroll

- ▶ Rutiner for onboarding av nye AI-systemer



Ha en tydelig datastrategi

- ▶ Hva slags data trenger vi?
- ▶ Sikre god datakvalitet

Og så kommer Data Act i tillegg...

Teaser



Hva

- ▶ Regulere rettigheter og tilgang til data generert av IoT-produkter
- ▶ Forbud mot urimelige avtalevilkår i datadelingskontrakter
- ▶ Tiltak for å hindre vendor lock-in hos cloud-leverandører



Hvem?

- ▶ Produsenter, distributører og selgere av IoT-produkter
- ▶ Leverandører av IoT-relaterte tjenester
- ▶ Enkelte leverandører av cloud og edge-tjenester



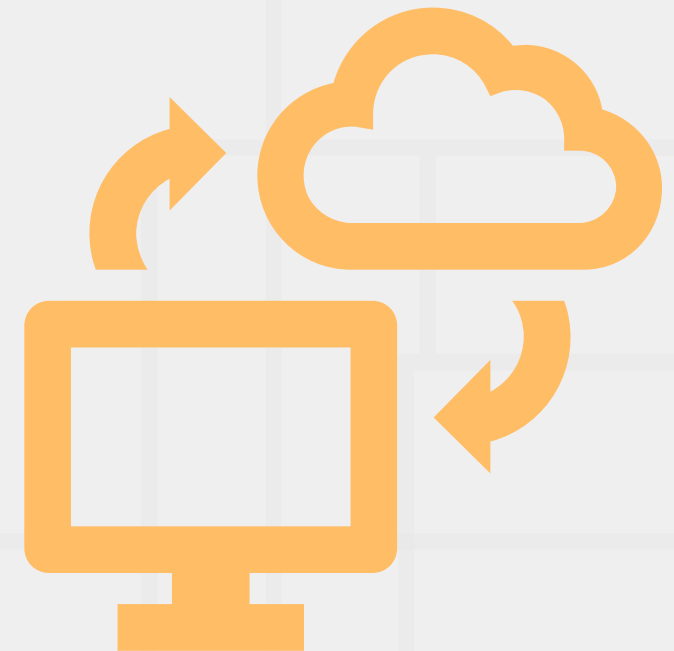
Hvorfor?

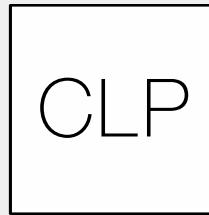
- ▶ Sikre økt utnyttelse av data i samfunnet
- ▶ Gi brukeren kontroll over egne data – unngå leverandør lock-in



Når?

- ▶ I kraft fra september 2025 (gradvis innføring / overgangsregler)





Hanne Heltne

Partner

E-post: hhe@clp.no

Tlf.nr: +47 92 46 36 20



Erik Sletner

Senior Associate

E-post: esl@clp.no

Tlf.nr: +47 412 66 115