# Om AI-förordningen

Håkan Burden & Susanne Stenberg

# AI Act
# AI-förordningen

AI som teknologi medför både möjligheter och risker

EU-kommissionen vill därför reglera användandet av AI som teknologi för att värna om medborgarnas hälsa, grundläggande rättigheter och säkerhet

Syftet är att skapa tillit till AI som teknologi, som en del av det digitala årtiondet

Det görs genom en förordning som gäller som lag i Sverige när EU antagit den (jmfr GDPR)

# Tidslinje

2021: Första förslaget

2022: Ministerrådet förhandlar

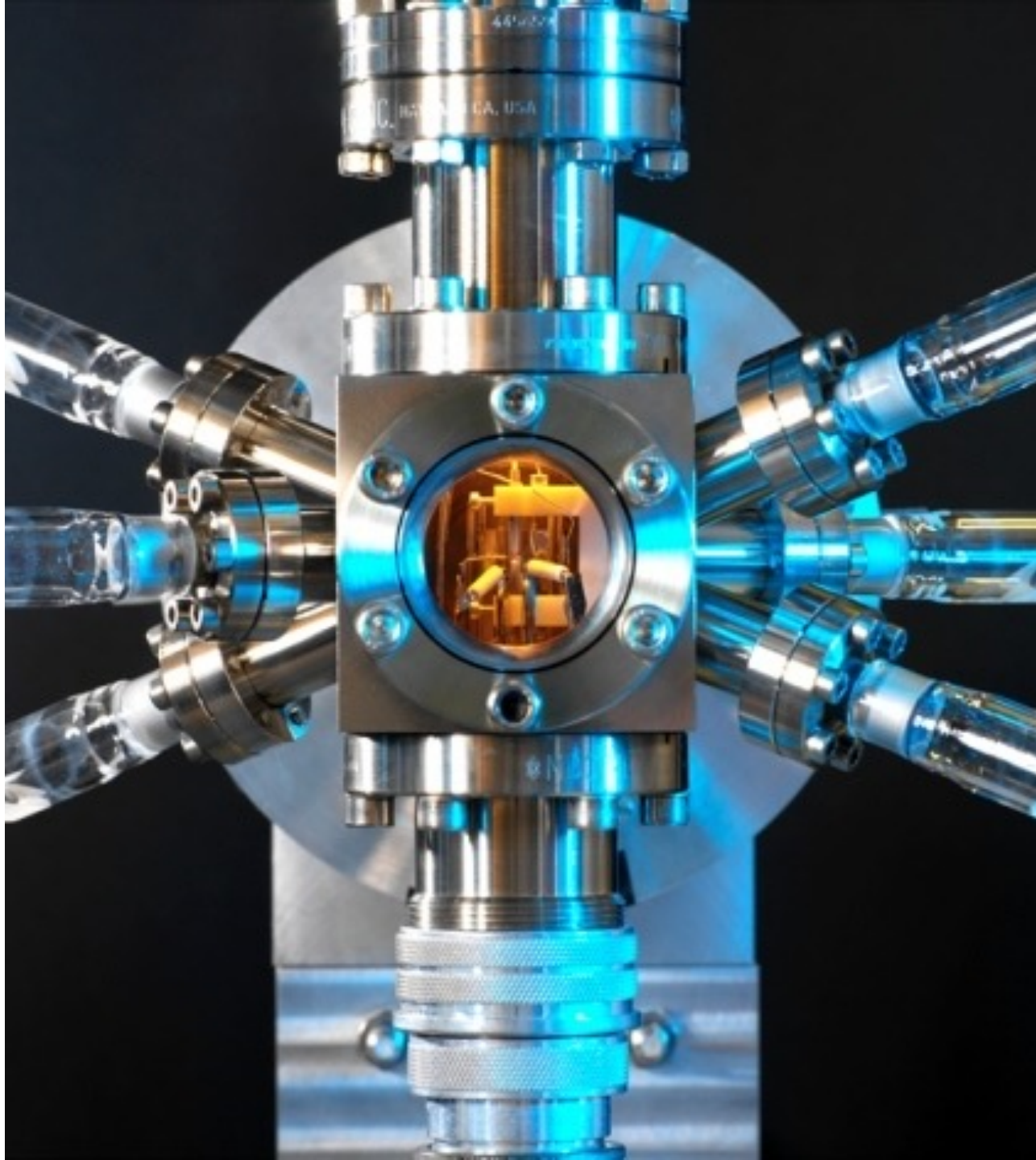
2023: Parlamentet förhandlar

Trilog och beslut i höst?

2024: Klargöranden och

2025: Standarder

2026: Gäller som lag i Sverige
Givet att antas i år

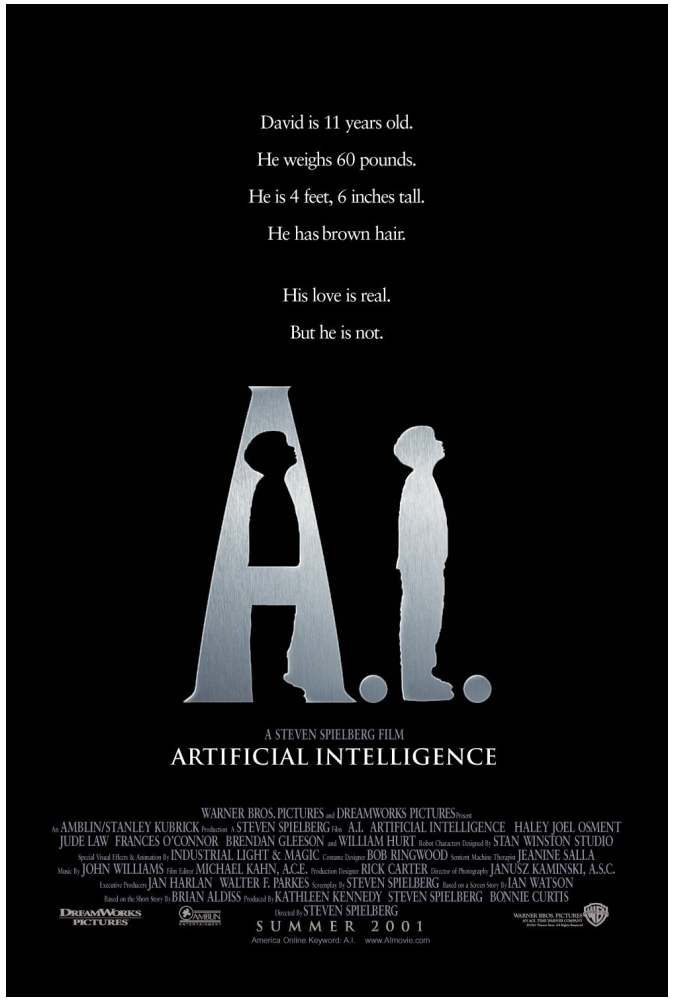



# EU avgör vad som är ett AI-system

Både som tillhandahållare och som användare av mjukvara behöver du kunna förstå om din verksamhet fr.o.m. 2026 omfattar

- ett AI-system, och i så fall om det
- ska CE-märkas

RI.SE




# Definitionen av AI

## Artikel 3.1

Ett AI-system är designat för att med viss autonomi, härleda ett resultat utifrån indata

Härledandet görs genom maskininlärning eller logik- och kunskapsbaserade teknologier

Resultatet kan vara en rekommendation, en förutsägelse, innehåll såsom text eller bild, eller nåt annat som påverkar dess omgivning


# AI och CE

Vissa AI-system ska CE-märkas:

- a) Säkerhetskomponenter i produkter som regleras av EUs produktregleringar (såsom maskiner, hissar och medicinsk utrustning, men inte fordon eller fartyg, artikel 6 & annex II)
- b) System som automatiserar beslutsfattande inom vissa verksamheter (t.ex. underhåll av vägtrafik, sociala förmåner, försäkringspremier, utbildning och arbetsförmedling, artikel 6 & annex III)
- c) *General Purpose AI* som används för textgenerering, översättning, mönsterigenkänning etc. (artikel 4b)

Grupp a & b kallas tillsammans för hög-risk system

CE-märkning innebär bl.a. att uppfylla kraven i artiklarna 9-15

RI.
SE

# CE-märkning av högrisk AI

Artikel 9: Riskhanteringssystem där bland annat testprocedurerna är beskrivna

Artikel 10: Data som används för träning, validering och testning ska vara relevant, representativ och i möjligaste mån felfri och komplett

Artikel 11: Teknisk dokumentation

Artikel 12: Loggar

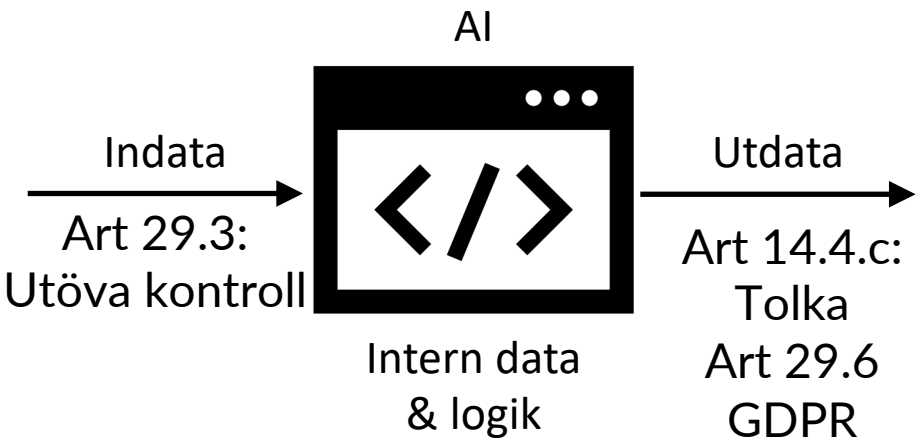
Artikel 13: Transparens och information till användare

Artikel 14: Människans möjligheter att övervaka och ingripa

Artikel 15: Robusthet, precision och cyber-säkerhet

→ Upphandling: När distribueras  på marknaden under kommersiella former
→ Egen regi: När används av användaren eller utifrån tänkt användande

# Användarens ansvar




Art 13:
Transparens
Art 29.5:
Loggar (art 12)

Är man som användare nöjd med hur…
… Strategier (Art 14.3) och
… Dokumentation (Annex IV) relaterar till
… Den egna förståelsen av systemet och hur det är tänkt att användas?

Hur mycket av affärslogiken måste användaren se för att fullgöra sina åtaganden?

# Lagen kopplar etiken till standarder

| Aktör | *Bias* | *Human-in-the-loop* |
|---|---|---|
| EUs High-level expert group | Systemen ska vara opartiska | Människan ska kunna intervenera |
| AI-förordningen<br>General approach från november 2022 | Data ska vara representativ, relevant och i möjligaste mån felfri och komplett (artikel 10) | Mänsklig översyn ska motverka risker i relation till de grundläggande rättigheterna (artikel 14) |
| CEN / CENELEC<br>Utkast till begäran från kommissionen | Förvaltning och kvalitet för data inom AI | Mänsklig översyn av AI-system |
| ISO / IEC<br>Pågående internationellt arbete | Standard: Data Governance<br>Rapport: Bias in AI | Rapport: Trustworthy AI<br>Rapport: Human-system interaction |

RI.
SE

# Databas över hög-risk AI-system

Kommissionen ska upprätta en databas. I den ska ...

... tillhandahållare registrera sina hög-risk AI-system (artikel 51)

... offentliga aktörer registrera att de använder hög-risk AI-system (artikel 29.5a)

Om AI-systemet är listat i annex III (undantag för brottsbekämpande aktörer och system)

# Regulatoriska sandlådor enligt AI Act

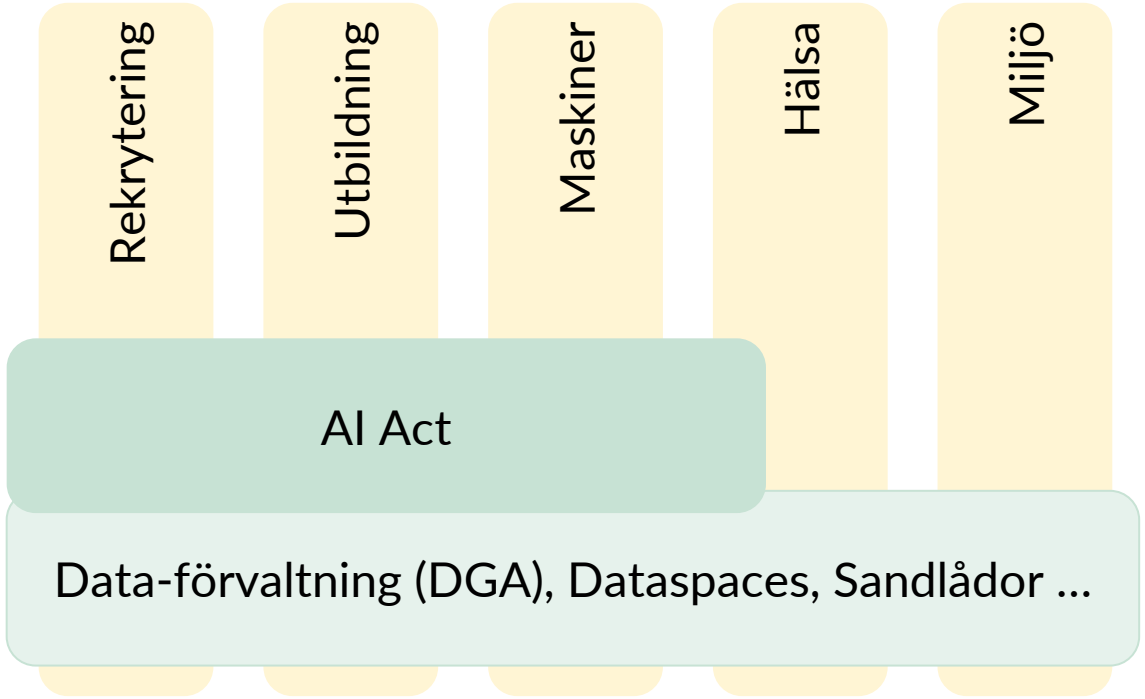
**Artikel 53**: Villkor för sandlådor
Främja innovation, regelefterlevnad, ekosystem av aktörer, ...

*”Written proof of successful work”* utfärdat av myndigheten som ansvarar för den regulatoriska sandlådan

**Artikel 54**: Undantag från GDPR, personuppgifter får användas för andra ändamål än den som angavs vid insamlandet om det sker i en regulatorisk sandlåda

Villkor:
- Inom transport och mobilitet, offentlig sektors effektivisering, bekämpa pandemier och klimatkatastrofen, mfl
- Datan behövs för att efterleva de tekniska kraven i artikel 9-15, däribland datakvalitet
- Konsekvensbedömning enligt artikel 35 i GDPR

→ Att hänvisa till de tekniska kraven i artiklarna 9 – 15 ger intryck av att sandlådorna är till för AI som ska CE-märkas men områdena som villkorar undantaget är mer generösa än så




# Svensk offentlig förvaltning i det digitala årtiondet

En tillsynsmyndighet för AI (precis som för personuppgifter a’ la GDPR)

Återkommande att myndighet ska både utöva tillsyn och främja innovation (IMY är ett intressant exempel på utvecklingen av myndighetsuppdragen)

Myndigheten som innovationspartner och datamäklare

Flera av initiativen inom det digitala årtiondet berör områden som är medlemsstaternas angelägenhet (jfr subsidaritetsprincipen)

# Välj en. Eller två.

Det här behöver jag veta mer om gällande AI-förordningen

De viktigaste aspekterna att få med i nästa nationella AI-strategi

Världens bästa regeringsuppdrag i relation till AI

”Three options and a choice”, deepai.org

# Mer för den som vill

**Bilaga i rapport från regeringsuppdrag**:
https://www.digg.se/analys-och-uppfoljning/publikationer/publikationer/2023-01-23-slutrapport-uppdrag-att-framja-offentlig-forvaltnings-formaga-att-anvanda-artificiell-intelligens

**Pod om AI Act**:
Får man verkligen göra så?
Finns på Acast and Spotify

**Rapport**:
Regulating Trust – An Ongoing Analysis of the AI Act:
Finns på DiVA

**Remisser**:
AI, skadestånd samt standarder
ri.se/sv/nyheter/remissyttranden

# Tack

hakan.burden@ri.se
susanne.stenberg@ri.se