

# Det du behöver veta om den nya AI-förordningen

Johan Thörn, Johan Sundberg & Fredrik Eråker, den 29 januari 2024



# Kort om oss



**Johan Thörn**

Advokat / Partner

E: [johan.thorn@edplaw.com](mailto:johan.thorn@edplaw.com)

T: 073-582 04 51



**Johan Sundberg**

Advokat / Partner

E: [johan.sundberg@edplaw.com](mailto:johan.sundberg@edplaw.com)

T: 070-302 75 62



**Fredrik Eråker**

Advokat / Senior Associate

E: [fredrik.eraker@edplaw.com](mailto:fredrik.eraker@edplaw.com)

T: 072-537 02 56

# Agenda

AI-förordningen – vad är status?

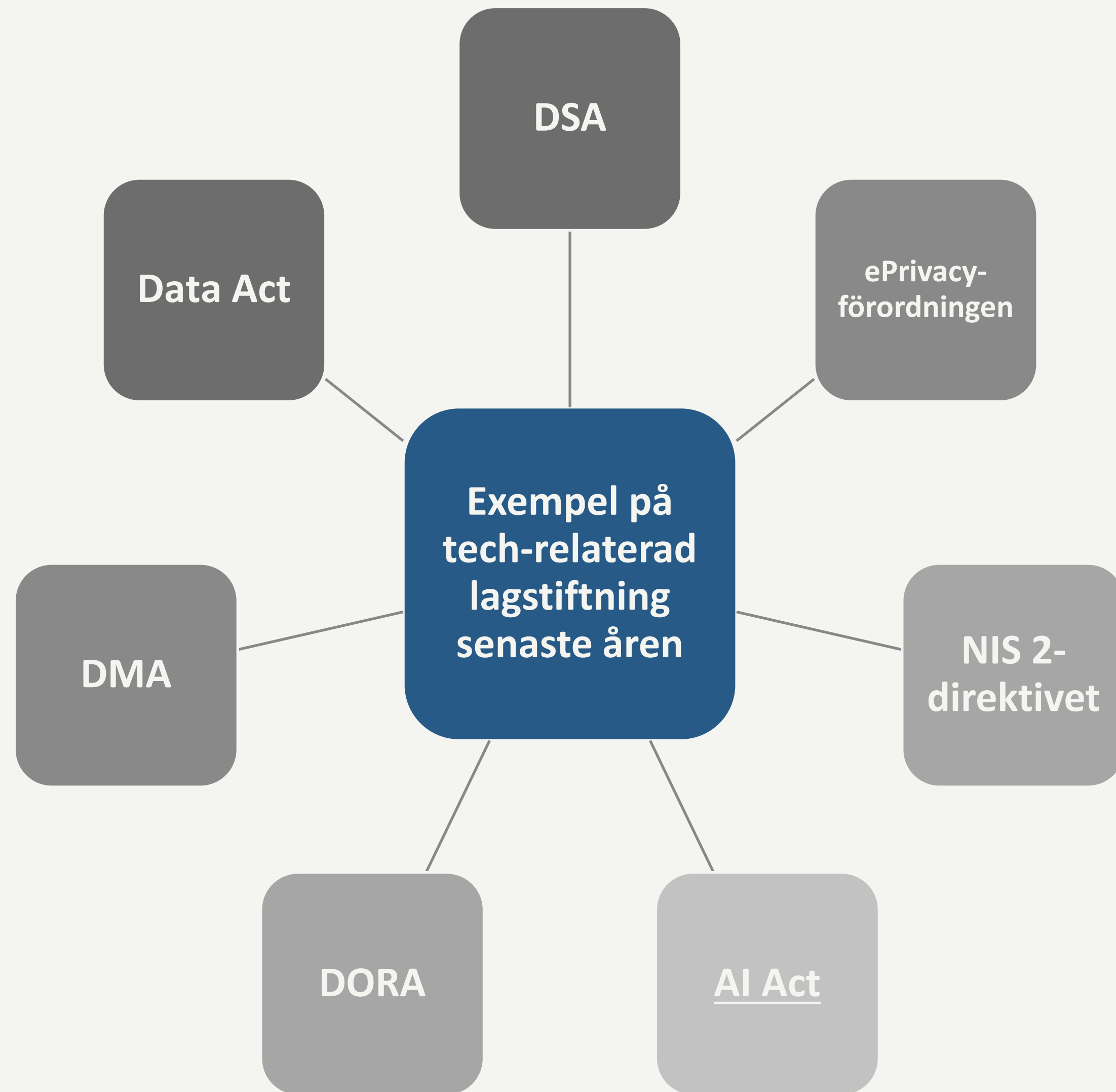
Varför en AI-förordning och vem omfattas?

Skyldigheter och krav

Förhållandet till GDPR



# EU:s digitala strategi



## Ytterligare exempel

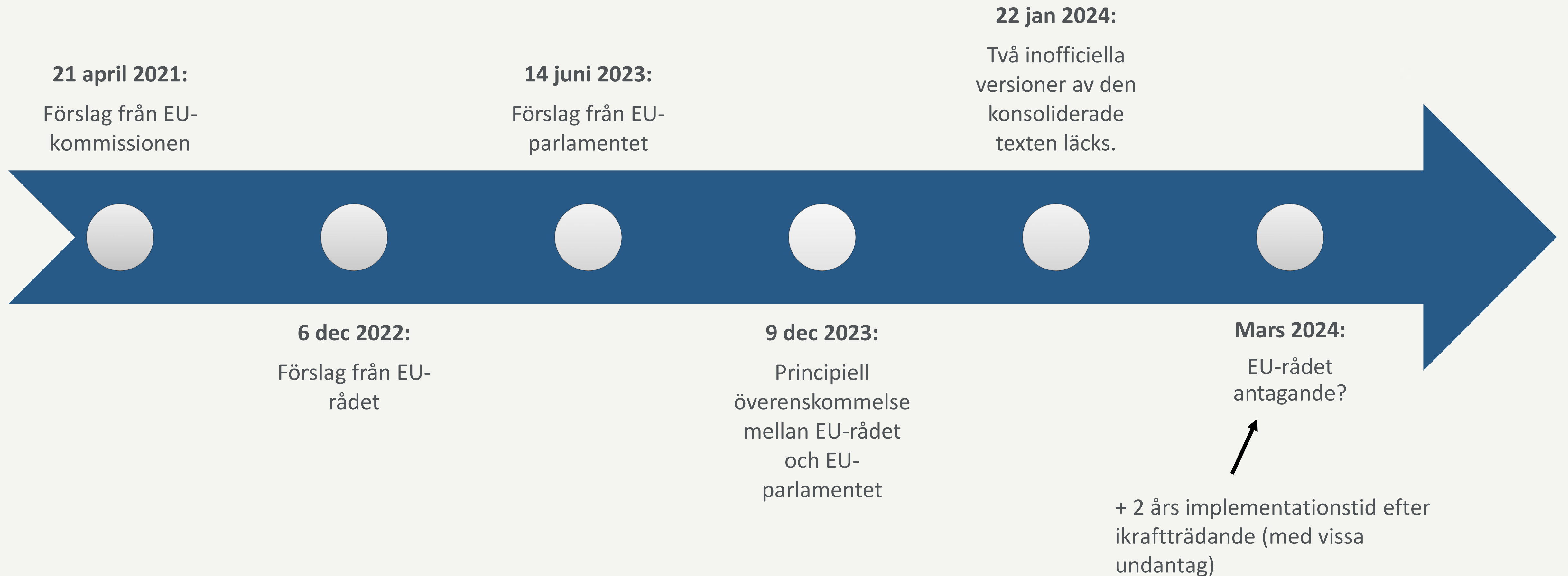
Översyn av eIDAS-förordningen

DGA

Platform Work Directive

Cyber Resilience Act

# AI-förordningen – vad som hänt i stora drag



# Syftet med AI-förordningen

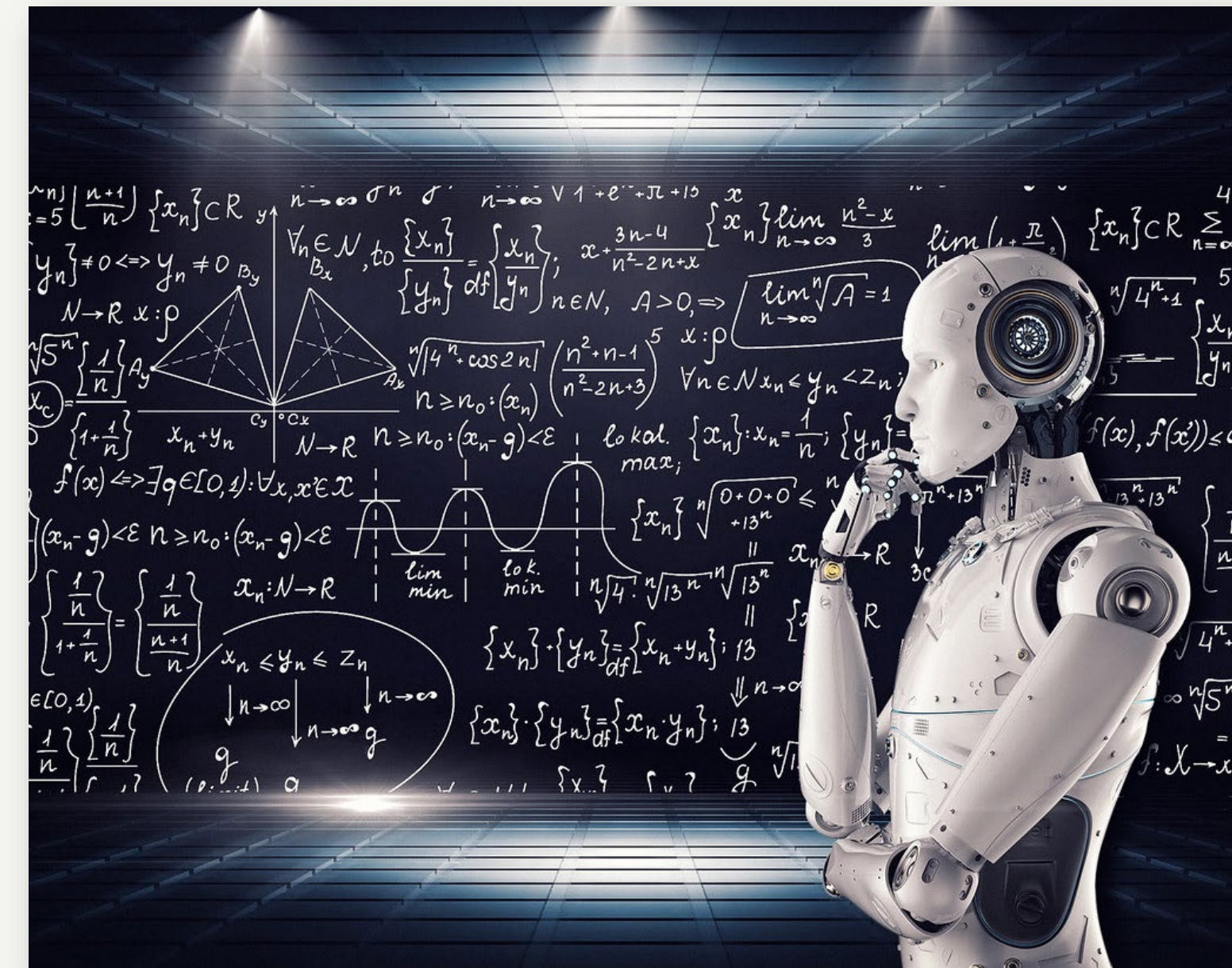
Syftet med AI-förordningen är att **enhetligt reglera användningen av AI-system** och särskilt begränsa användningen av AI-system för vissa syften som innebär risker.

AI-förordningen erkänner såväl **möjligheterna** som **riskerna** med användningen av AI-system.

# Definitionen av AI

*“An AI system is a machine-based system 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.”*

Speglar OECD-definitionen



# Vilka omfattas av AI-förordningen?

**Leverantörer** som släpper ut AI-system på marknaden eller tar AI-system i bruk i unionen eller släpper ut AI-system för allmänna ändamål i unionen, oavsett om leverantören är etablerad i eller befinner sig i eller utanför unionen.

**Användare** (utställare) av AI-system som är etablerade eller befinner sig i unionen.

**Leverantörer och användare** som är etablerade eller befinner sig utanför unionen där utdata som produceras av AI-systemet används i unionen.

**Importörer och distributörer** av AI-system.

**Produkttilverkare** som släpper ut AI-system på marknaden eller tar AI-system i bruk tillsammans med sin produkt och under deras egna namn eller varumärke.



# AI-förordningen intar ett riskbaserat angreppssätt

AI-förordningen intar ett riskbaserat angreppssätt baserat på tre risknivåer:

- AI-system som inbegriper **oacceptabla risker** och därmed är förbjudna.
- AI-system som inbegriper **hög risk** och som därmed är föremål för särskilda regler.
- AI-system som inte inbegriper en hög risk (**begränsad risk**).

Även särskilda regler för **grundmodeller**, benämnt *general-purpose AI systems* (GPAI) i förordningen.



# Förbjuden användning av AI-system

Bl.a. följande AI-system föreslås att vara förbjudna:

- Användning av s.k. **sublima tekniker** för att väsentligt snedvrída en persons beteende.
- **Utnyttjande av sårbarhet** hos individer som härrör från ålder, funktionsnedsättning eller särskild social eller ekonomisk situation.
- **Utvärdering och klassificering** av fysiska personens pålitlighet baserat på t.ex. socialt beteende med **social poängsättning** som leder till vissa följder.
- **Biometrisk fjärridentifiering** i realtid på allmänt tillgängliga platser för brottsbekämpning (med vissa undantag).



# AI-system som inbegriper ”hög risk”

I **bilaga 3** till AI-förordningen anges AI-system som inbegriper en hög risk och som måste uppfylla vissa krav.

**Exempel** på AI-system som inbegriper en hög risk är:

- AI-system som är avsedda att användas för biometrisk fjärridentifiering av fysiska personer i ”realtid” och i ”efterhand”.
- AI-system som är avsedda att användas för rekrytering eller urval av fysiska personer.
- AI-system som är avsedda att användas för att utvärdera fysiska personers kreditvärdighet eller fastställa deras kreditbetyg.

AI-system ska dock inte inbegripa en hög risk om dessa inte innebär en risk för skada på individers hälsa, säkerhet eller grundläggande rättigheter.

# Krav på AI-system som inbegriper ”hög risk”

Riskhanteringsystem som löper under hela livscykeln för AI-systemet och som bl.a. avser identifiering, utvärdering och antagande av lämpliga riskhanteringsåtgärder för att reducera risken till acceptabel

Testning och implementering av testförfaranden

Användning av dataset som uppfyller vissa kvalitetskriterier

Teknisk dokumentation

Automatisk loggning av händelser för att möjliggöra övervakning av driften av AI-systemet

Transparenskrav och information till användare

Utformas på sådant sätt för att möjliggöra mänsklig tillsyn

Utvecklas och utformas på sådant sätt att systemet uppfyller en lämplig nivå avseende noggrannhet, robusthet och cybersäkerhet

# Skyldigheter för leverantörer av AI-system med ”hög risk”

Utöver att **leverantören** ska säkerställa att AI-systemet uppfyller de legala kraven enligt AI-förordningen ska leverantören bl.a.:

- Säkerställa att AI-systemet genomgår ett förfarande för bedömning av överensstämmelse innan systemet tas i bruk eller släpps ut på marknaden.
- Fullgöra registreringskyldigheter.
- CE-märkning om överensstämmelse.
- Upprätta kvalitetsstyrningssystem.
- Spara automatiskt genererade loggar.
- Utse ett ombud (om leverantören är etablerad utanför unionen).

**Importörer, distributörer och användare** av AI-system med hög risk har även **vissa skyldigheter** beroende på deras roll i leveranskedjan. Användare ska t.ex. endast använda systemet i enlighet med bruksanvisningar.

Vissa användare ska t.ex. genomföra en konsekvensbedömning avseende grundläggande rättigheter.

# Transparenskrav för vissa AI-system

Vissa AI-system omfattas, som huvudregel, av **utökade transparenskrav**:

- System som är avsedda att interagera med fysiska personer utformas och utvecklas på ett sådant sätt att fysiska personer informeras om att de interagerar med ett AI-system.
- System för känsligenkänning eller system för biometrisk kategorisering.
- AI-system som genererar eller manipulerar bilder eller ljud eller videoinnehåll (*deepfake*).

Reglerna omfattar AI-system med hög risk och utan hög risk.

Även rätt till att få en förklaring vid individuellt beslutsfattande i förhållande till högrisk-system under vissa förutsättningar.



# Sanktioner och tillsyn

En **europaisk nämnd** för artificiell intelligens föreslås att inrättas, vars syfte ska vara utbyte av sakkunskap, bidra till enhetlig administrativ praxis, utfärda yttranden och rekommendationer etc.

Även **AI Office** ska inrättas, som bl.a. ska övervaka GPAI-system och -modeller samt vara stödfunktion för uppförandekoder, regulatoriska sandlådor och konsultationer med berörda parter.

**Scientific panel and advisory forum** som stödfunktioner.

En **EU-databas för AI-system** med hög risk vars information ska vara tillgänglig för allmänheten.

**Administrativa sanktionsavgifter om upp till 35 miljoner euro** eller **7 %** av den totala globala årsomsättningen.

Mer proportionerliga sanktionsavgifter för mindre företag och start-ups.

Särskilda sanktionsbestämmelser för GPAI-modeller.

# GDPR och användning av AI-system

När ett AI-system hanterar personuppgifter blir GDPR, som utgångspunkt, tillämpligt.

Med **personuppgift** avses alla upplysningar som avser en identifierad eller identifierbar individ och inkluderar både direkt identifierande uppgifter och indirekt identifierande uppgifter.

I vissa fall är det klart att användningen av ett AI-system inbegriper behandling av personuppgifter (t.ex. virtuella assistenter eller ansiktsanalys i bilder), men inte alltid, t.ex. i samband med analys av olika "anonymiserade" datamängder.



# GDPR och användning av AI-system

GDPR reglerar inte användningen av AI-system i sig, utan är ”**teknikneutral**” i den meningen att reglerna är tillämpliga oavsett vilken teknik som används om det rör sig om behandling av personuppgifter

Vissa bestämmelser i GDPR har dock **särskild relevans** vid användning av AI-system:

- Definitionen av ”profilering”
- Principerna för behandling av personuppgifter, särskilt ändamålsbegränsning och uppgiftsminimering
- Kravet på rättslig grund
- Automatiserat beslutsfattande
- Registrerade individers rättigheter, särskilt informationskravet
- Konsekvensbedömning



# Checklista

Omfattas den aktuella tekniken av AI-förordningen?

Klassificera användningen av AI, vilken risknivå?

Få på plats nödvändiga AI-dokument, -bedömningar och – rutiner – ta fram ett internt förvaltningsramverk för AI.

Ta ställning till om personuppgifter kommer att hanteras i AI-systemet och vem som ansvarar för hanteringen.

Gör en noggrann laglighetsanalys enligt GDPR och i förekommande fall en konsekvensbedömning (DPIA).

## Vill du fördjupa dig?

Till dig som deltog på dagens webinarium erbjuder vi nu  
**20 % rabatt** på uppföljningskursen den 8 april:

### AI och skyddet för personlig integritet

Boka din plats senast den 5 februari för att ta del av erbjudandet.

Använd rabattkod: AI20

# Vad tyckte du om dagens webinarium?

Ta gärna 30 sekunder och svara på frågorna under fliken  
“Omröstningar” bredvid chattfliken.

**Tack för dina synpunkter!**

Frågor?

