Integritetsskydds myndigheten

3 juni 2025

Värt att veta om AI-förordningen

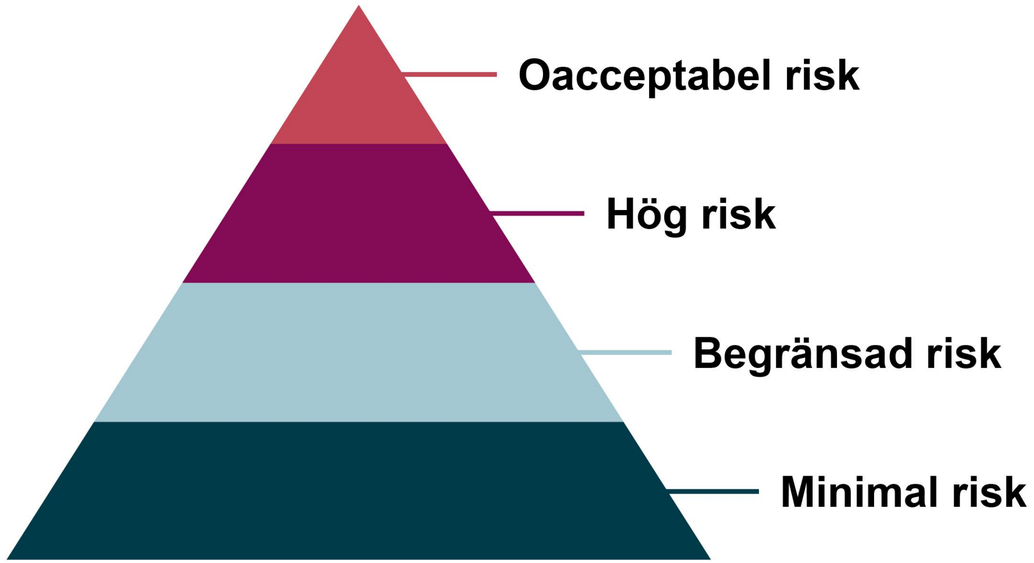
Agenda

- Introduktion till AI-förordningen
- AI-system med oacceptabel risk
- AI-system med hög risk m.m.
- Sanktioner, AI-kunnighet m.m.
- Frågor
- Avslutande ord

Introduktion till AI-förordningen

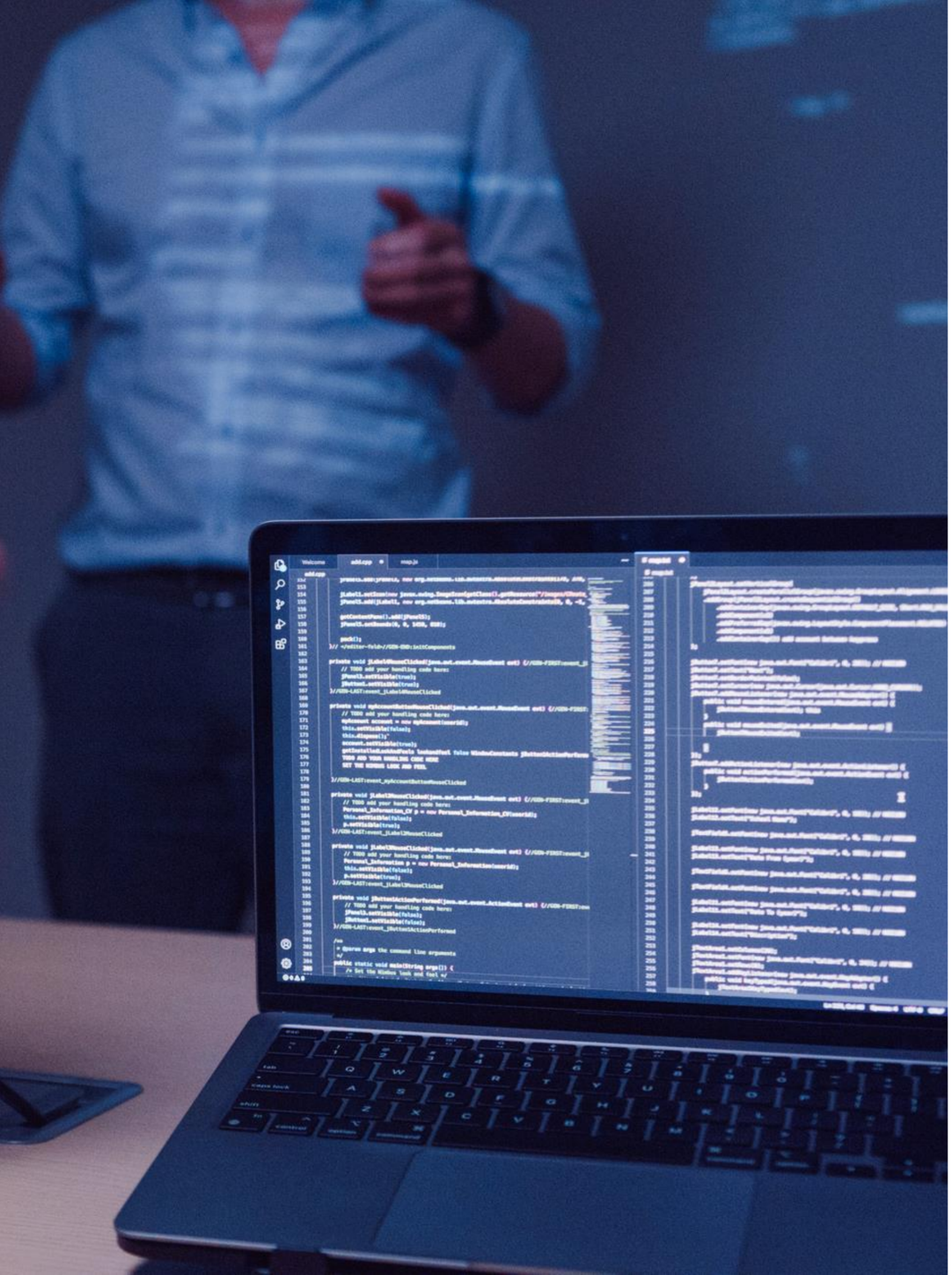
AI-förordningen i korthet

- EU:s allmänna reglering av artificiell intelligens (AI)
- Trädde i kraft den 1 augusti 2024
- 113 artiklar
- Målet är att skapa en trygg och etiskt hållbar miljö för AI-innovation samtidigt som man skyddar medborgarnas rättigheter och friheter



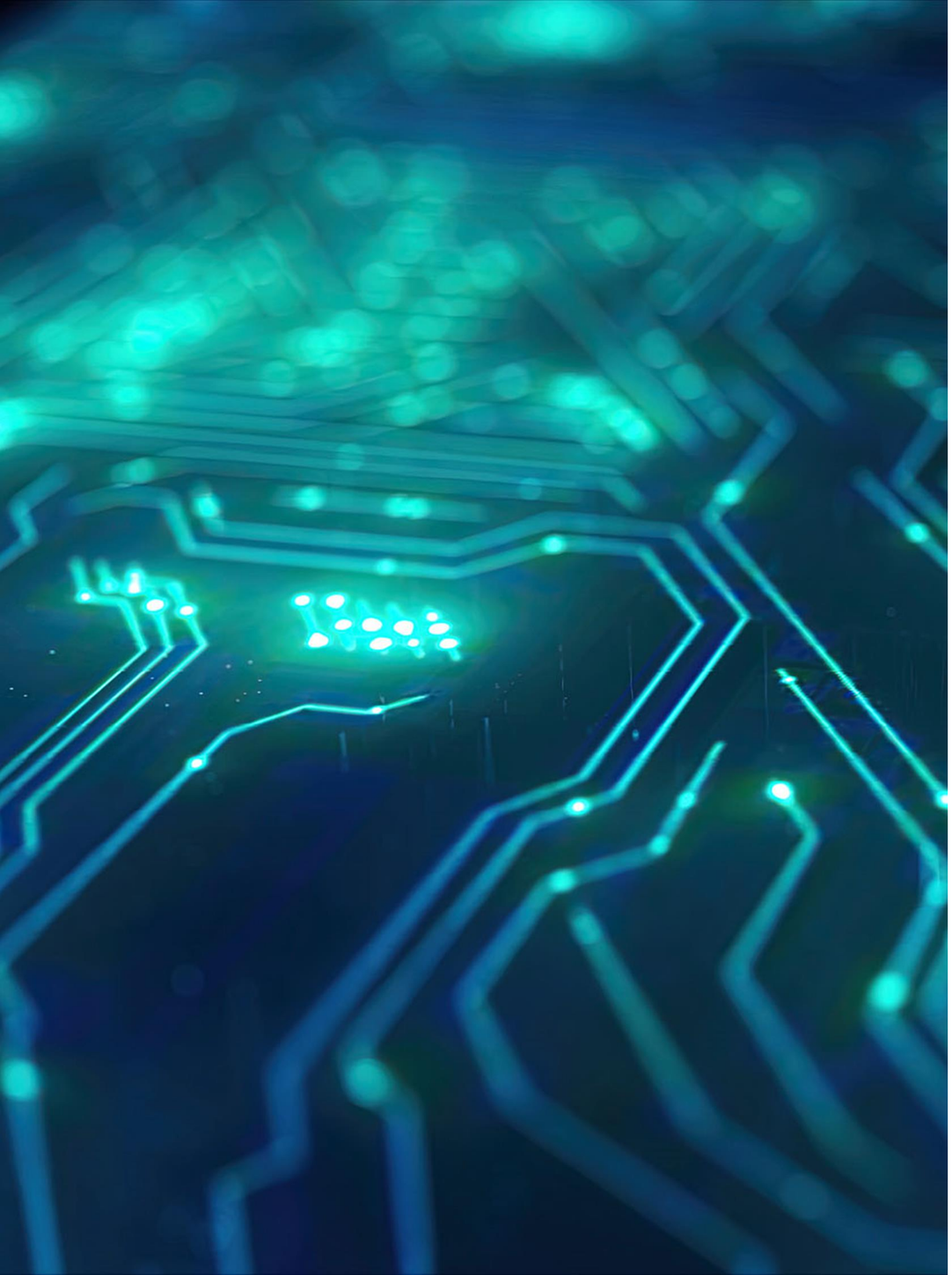
Riskbaserat tillvägagångssätt

- AI-system med oacceptabel risk (förbjuden)
- AI-system med hög risk (flertalet krav)
- AI-system med begränsad risk (krav på öppenhet)
- AI-system med minimal risk (AI-förordningen ställer inga krav)



AI-förordningen i korthet

- Krav på **CE-märkning** av AI-system med hög risk
- Vissa AI-system är **undantagna** från AI-förordningen
- **Utredning** för att se över behovet av nationella anpassningar till följd av AI-förordningen
- **GDPR** ska gälla parallellt med AI-förordningen



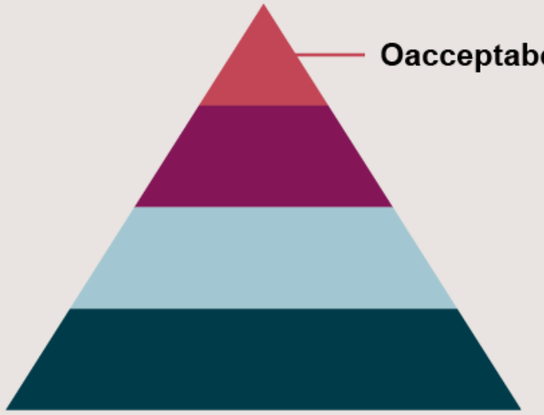
Vad är ett AI-system?

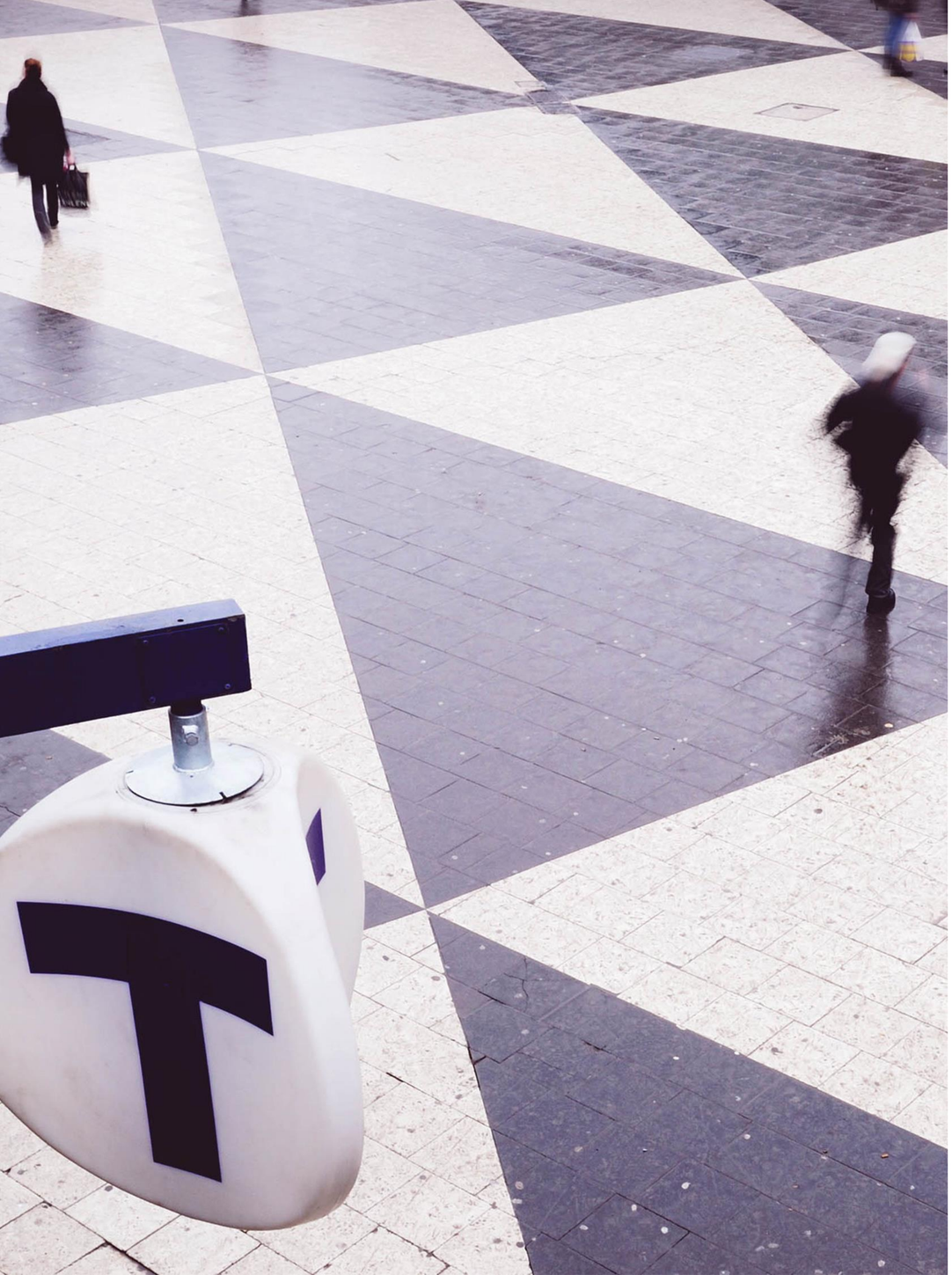
- **Ett maskinbaserat system** som är utformat för att fungera med varierande grad av autonomi och som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, drar slutsatser härledda från den indata det tar emot, om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras.

AI-system med oacceptabel risk

AI-system med oacceptabel risk (förbjuden)

- Biometriska kategoriserings-system
- Biometrisk fjärridentifiering i realtid
- Bedömer risken för en individ att begå brott
- Ospecificerad skrapning av ansiktsbilder
- Utnyttjar människors sårbarhet
- Känslo-igenkänning på arbetsplatser m.m.
- Social poängsättning
- Manipulerar människors beteende

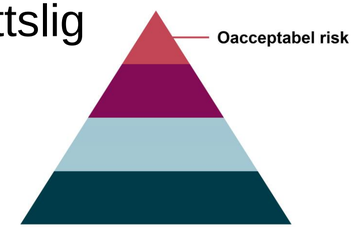




Biometrisk fjärridentifiering i realtid

- **Huvudregel: Förbjudet på allmänt tillgängliga platser för brottsbekämpande ändamål**

- **Möjligt i följande fall:**
  1. Riktade sökningar efter offer som utsatts för vissa brott samt sökning efter försvunna personer.
  2. Förhindra allvarliga hot mot människors liv och säkerhet.
  3. Lokalisera eller identifiera en person som misstänks ha begått något av de 16 brott som nämns i AI-förordningens bilaga II, eller för att verkställa en straffrättslig påföljd för något av dessa brott.



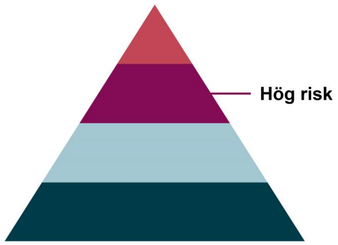
AI-system med hög risk

AI-system med hög risk – Kategori 1

- Ett AI-system som är tänkt att användas som en säkerhetskomponent i en produkt, eller AI-systemet i sig är en produkt, som **omfattas av en rättsakt i bilaga I**

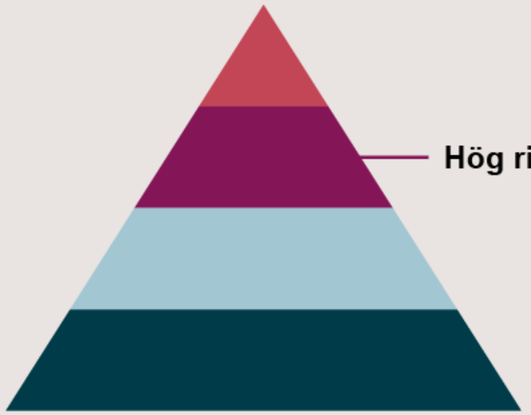
OCH

- Denna produkt måste genomgå en **tredjepartsbedömning** för att få släppas ut på marknaden eller tas i bruk.



AI-system med hög risk – Kategori 2

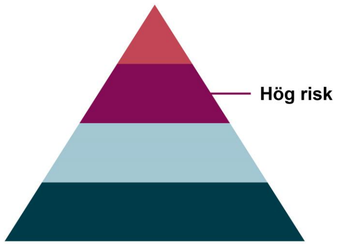
- Biometri
- Kritisk infrastruktur
- Väsentliga privata tjänster och väsentliga offentliga tjänster och förmåner
- Brotts-bekämpning
- Utbildning och yrkes-utbildning
- Migration, asyl och gränskontroll-förvaltning
- Rättskipning och demokratiska processer
- Anställning, arbetsledning och tillgång till egen-företagande



AI-system som omfattas av bilaga III till AI-förordningen

Skyldigheter för leverantörer av AI-system med hög risk

- Riskhanteringssystem
- Data och dataförvaltning
- Teknisk dokumentation
- Loggning
- Transparens och tillhandahållande av information
- Mänsklig kontroll
- Riktighet, robusthet och cybersäkerhet
- Kvalitetsstyrningssystem
- Övervakning efter utsläppande på marknaden



En leverantörs process för visad överenstämmelse

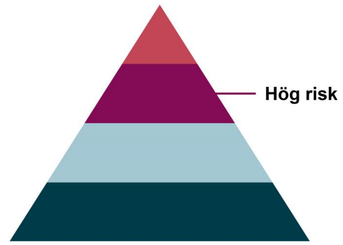
Innan ett AI-system med hög risk släpps ut på marknaden eller tas i bruk:

Genomgå förfarandet för bedömning av överenskommelse (*i princip säkerställa att kraven som tas upp på föregående sida uppfylls*)

Intern kontroll

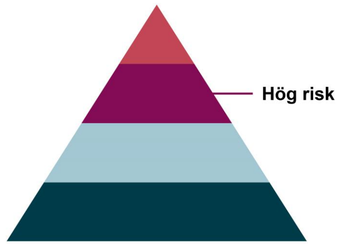
Tredjeparts-bedömning

- Upprätta en EU-deklaration om överenstämmelse
- Registrera AI-systemet i EU:s databas för högrisk-AI-system
- CE-märka AI-systemet



Skyldigheter för tillhandahållare av AI-system med hög risk

- Följa bruksanvisningen för AI-systemet
- Säkerställa AI-kompetens
- Informera leverantören och behörig myndighet om risker
- Spara loggar
- Informera berörda arbetstagare och fackförbund
- I vissa fall genomföra en **konsekvensbedömning avseende grundläggande rättigheter**



AI-system med begränsad risk

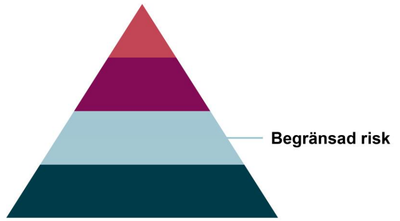
AI-system med begränsad risk

AI-system som interagerar med människor

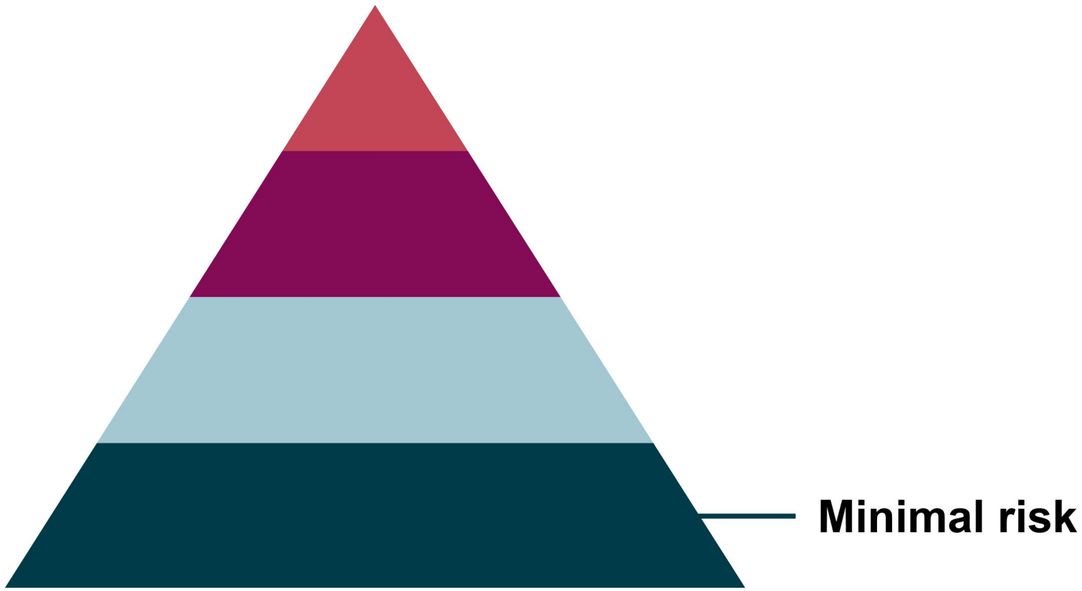
Transparenskrav som innebär att användaren ska förstå att hen interagerar med ett AI-verktyg

AI-system som genererar bild, ljud och video

Transparenskrav som innebär att man ska förstå att materialet är AI-genererat (*deepfake*)



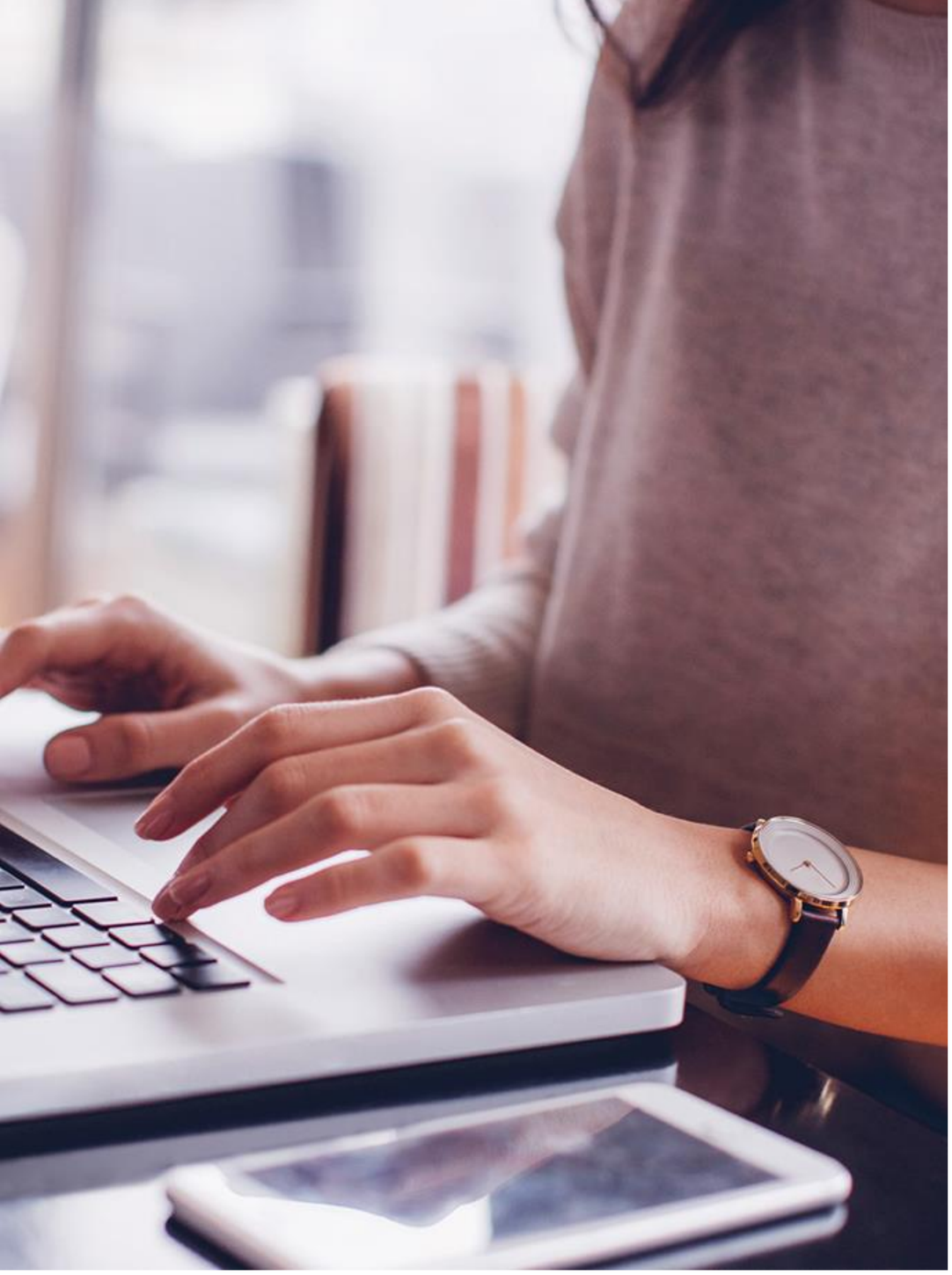
AI-system med minimal risk



AI-system med minimal risk

- AI-förordningen ställer inga krav
- Verksamheter kan på frivillig basis förbinda sig till uppförandekoder för AI-system
- GDPR gäller

AI-kunnighet



AI-kunnighet

- Personal och andra som arbetar med AI ska ha tillräcklig kunskap om AI utifrån deras tekniska kompetens, erfarenhet och utbildning

- Kompetenskraven ska anpassas efter hur AI används och vilka personer eller grupper som påverkas

Sanktioner m.m.

Sanktioner

- **35 miljoner EUR eller 7 procent** av den globala årsomsättningen vid överträdelser av bestämmelserna om förbjudna AI-användningsområden
- **15 miljoner EUR eller 3 procent** av den globala årsomsättningen vid överträdelser av bestämmelserna om leverantörers och tillhandahållares skyldigheter
- **7,5 miljoner EUR eller 1 procent** av den globala årsomsättningen vid överträdelser av bestämmelserna om att tillhandahålla myndigheterna med korrekt information mm.
- Lättnader för små- och medelstora företag
- Offentliga myndigheter

När börjar AI-förordningen gälla?

1 augusti 2024

AI-förordningen trädde i kraft

2 februari 2025

AI-system med oacceptabel risk (förbjuden)

2 augusti 2025

Kraven på AI-modeller för allmänna ändamål

2 augusti 2026

I princip alla reglerna i AI-förordningen blir tillämpliga

AI-förordningen är inte tillämplig på AI-system med hög risk som redan släppts ut på marknaden eller tagits i bruk före den 2 augusti 2026. Undantag finns dock!

Regulatoriska sandlådor för AI

Regulatoriska sandlådor för AI

- Medlemsstaterna ska säkerställa att deras behöriga myndigheter inrättar **minst en regulatorisk sandlåda för AI**
- Sandlådan ska vara i drift senast **den 2 augusti 2026**
- SME:er ska ha företräde till sandlådan
- Personuppgiftsbehandling?! **Dataskyddsmyndigheten** ska involveras

IMY:s roll och medskick

IMY:s tillsynsområde

Biometri

Kritisk infrastruktur

Väsentliga privata tjänster och väsentliga offentliga tjänster och förmåner

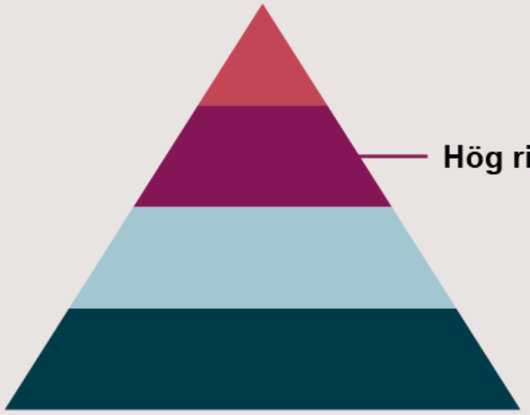
Brotts-bekämpning

Utbildning och yrkes-utbildning

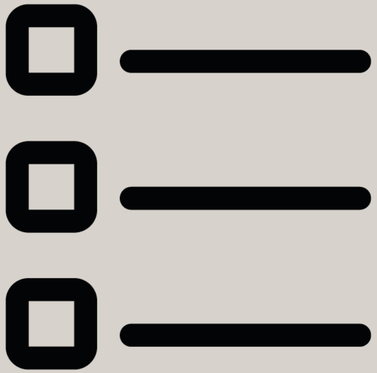
Migration, asyl och gränskontroll-förvaltning

Rättskipning och demokratiska processer

Anställning, arbetsledning och tillgång till egen-företagande



AI-system som omfattas av bilaga III till AI-förordningen



Tre medskick

1. Inventera vilka AI-system som ni använder idag eller kan komma att använda inom en snar framtid

2. Tekniker och jurister behöver jobba tätt tillsammans

3. GDPR kommer att gälla parallellt med AI-förordningen

Frågor?

Läs mer om vårt AI-arbete:
imy.se/ai

Mejla till:
innovation@imy.se

Tack för att du lyssnat!
Svara gärna på vår utvärdering

Integritetsskydds myndigheten

www.imy.se