Integritetsskydds myndigheten

27 september 2024

Värt att veta om AI-förordningen

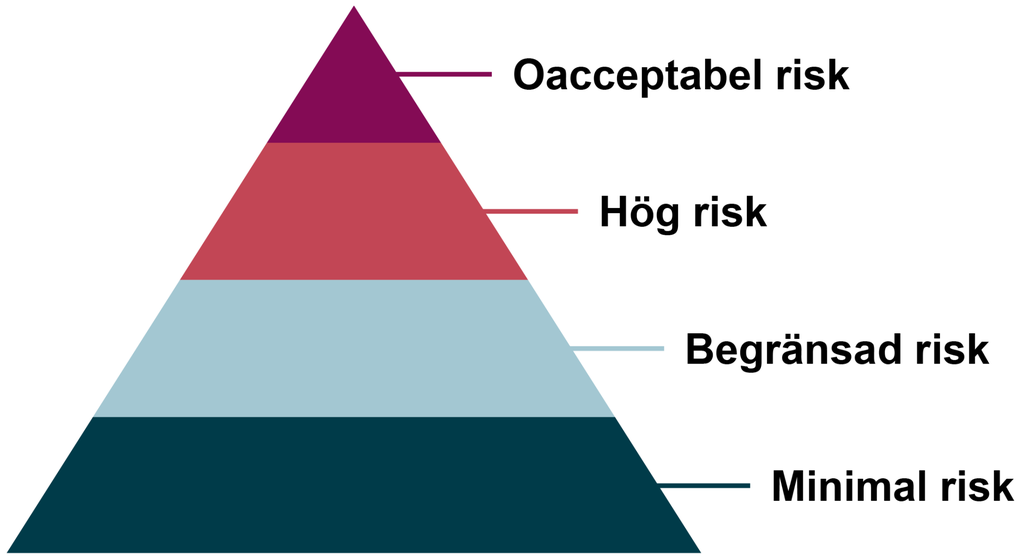
Agenda

- Introduktion till AI-förordningen
- Regulatoriska sandlådor för AI
- Frågor
- Avslutande ord

En introduktion till AI-förordningen

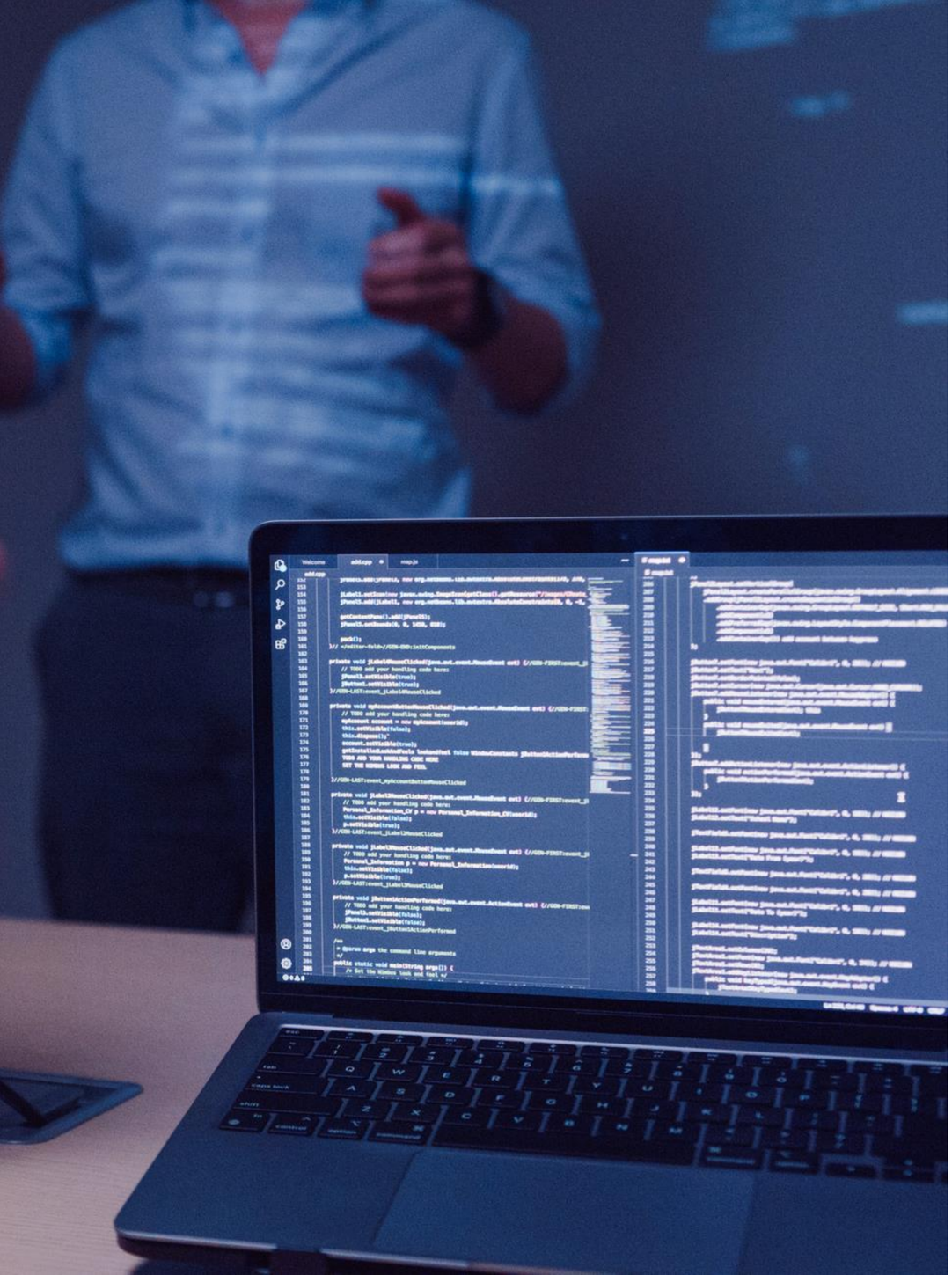
AI-förordningen i korthet

- 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 där AI-system klassificeras baserat på deras potentiella risk för samhället och individers rättigheter



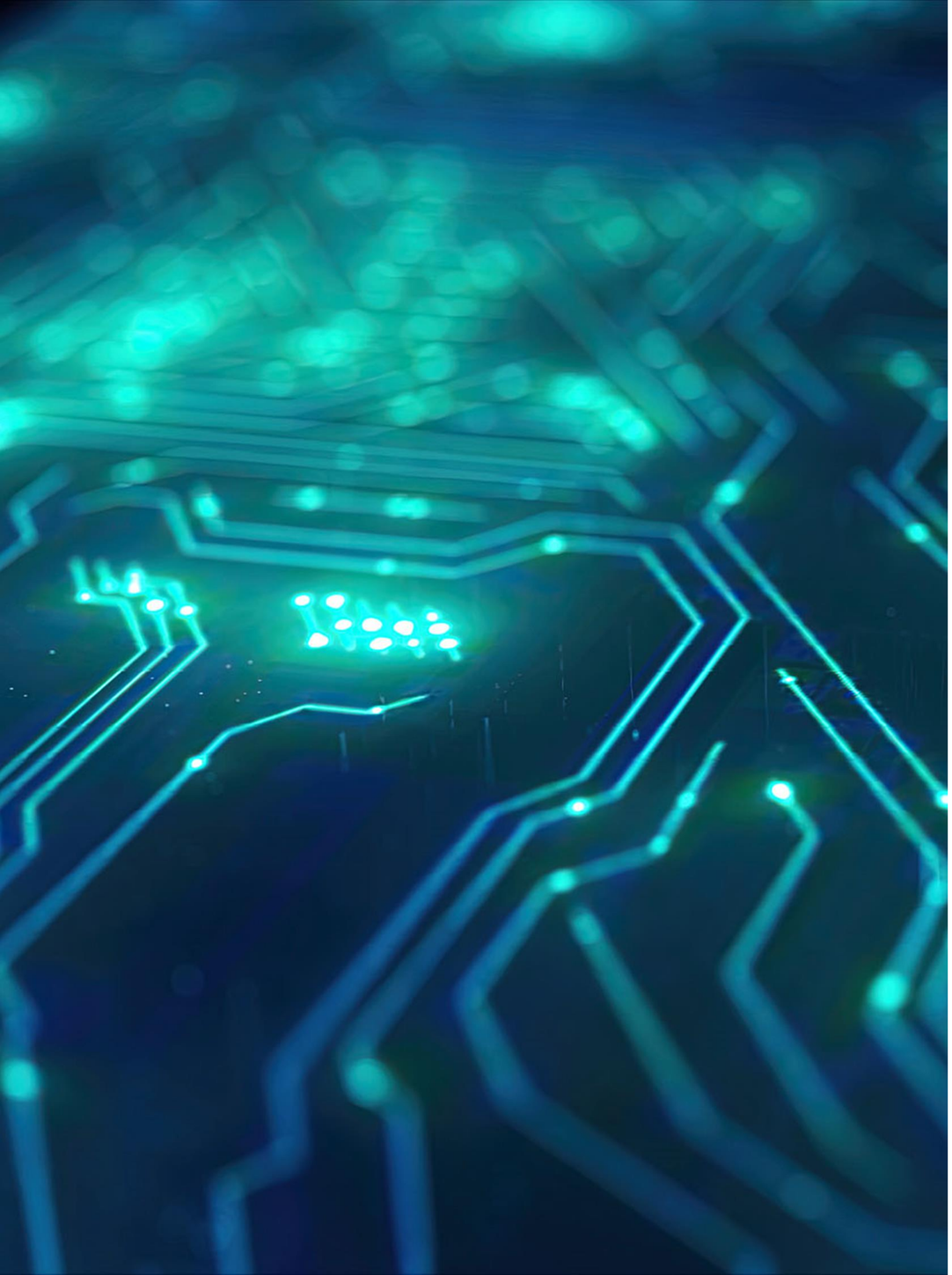
Riskbaserat förhållningssätt

- 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-förordningens krav 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 kategoriseringssystem

Ospecificerad skrapning av ansiktsbilder

Känsloigenkänning på arbetsplatser m.m.

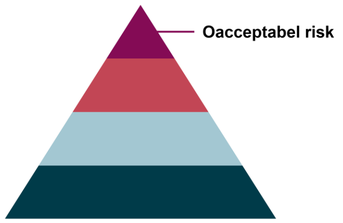
Social poängsättning

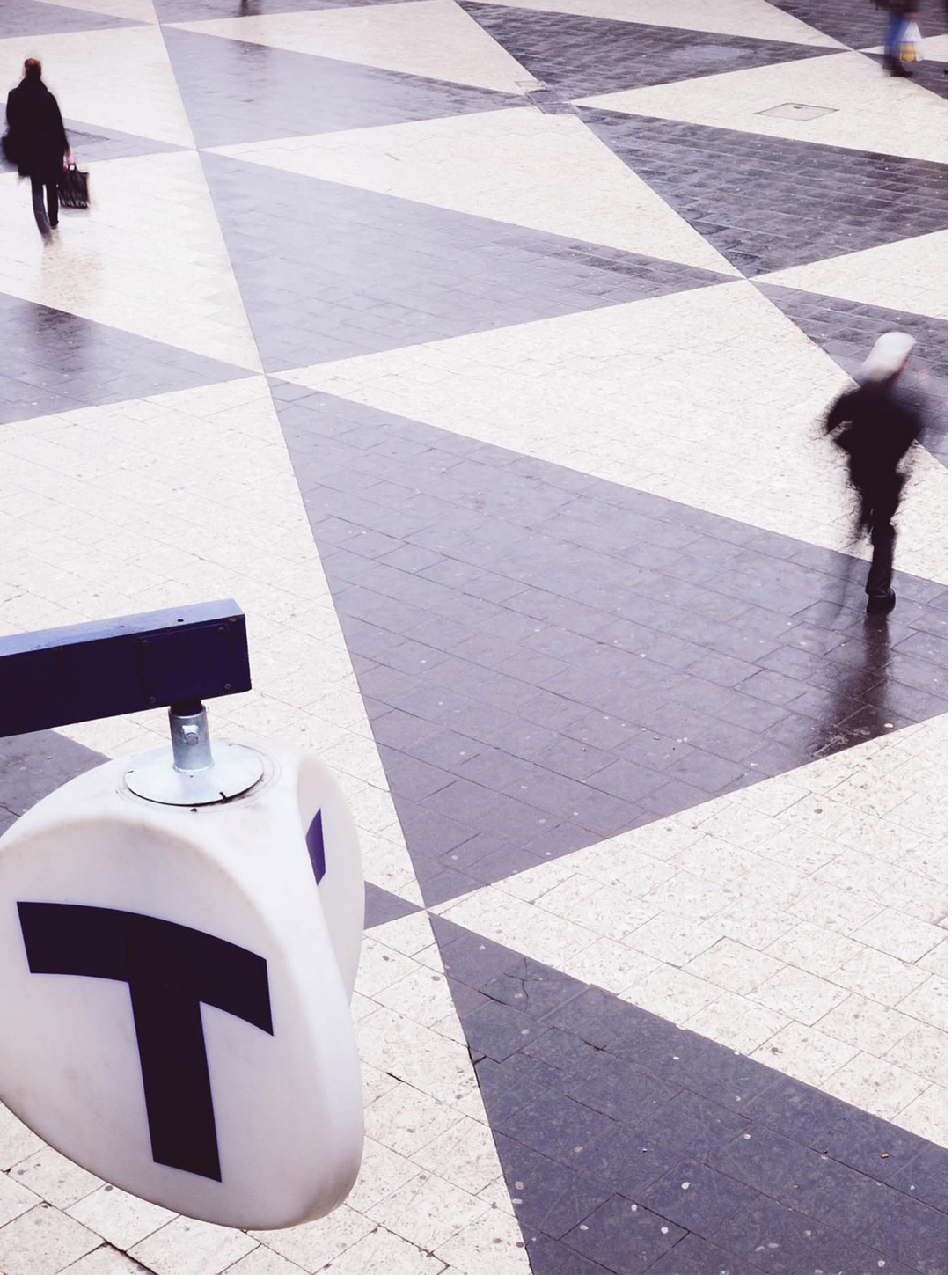
Manipulerar människors beteende

Utnyttjar människors sårbarhet

Bedömer risken för en individ att begå brott

Biometrisk fjärridentifiering i realtid

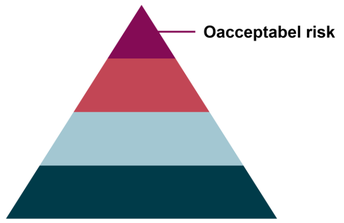




Biometrisk fjärridentifiering i realtid

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

- **Möjligt i följande fall:**
  1. Riktade sökningar efter offer som utsatts för vissa brott
  2. Förebyggande av ett specifikt och aktuellt terroristhot
  3. Lokalisera eller identifiera en person som misstänks ha begått något av de 16 brott som nämns i AI-förordningens bilaga II



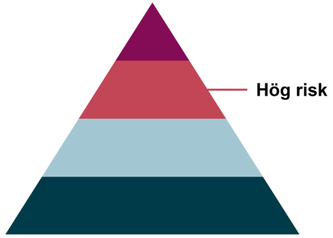
AI-system med hög risk

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

Utbildning och yrkesutbildning

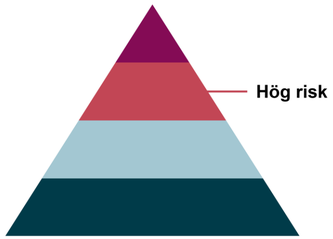
Anställning, arbetsledning och tillgång till egenföretagande

Tillgång till och åtnjutande av väsentliga privata tjänster och väsentliga offentliga tjänster och förmåner

Brottsbekämpning

Migration, asyl och gränskontrollförvaltning

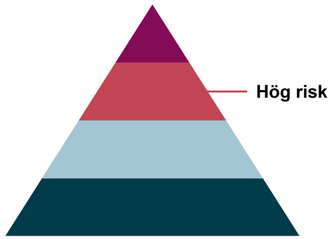
Rättskipning och demokratiska processer



AI-system som omfattas av bilaga III i 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

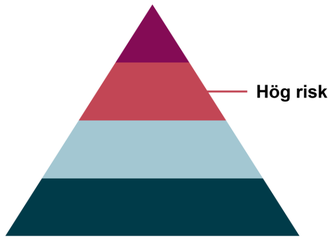
Innan ett AI-system med hög risk släpps ut på marknaden eller tas i bruk:

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

Intern kontroll

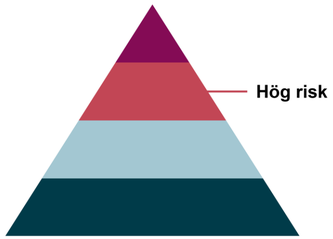
Tredjeparts-bedömning

- 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

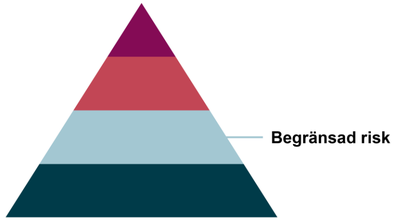
AI-system med begränsad risk

AI-system som interagerar med människor

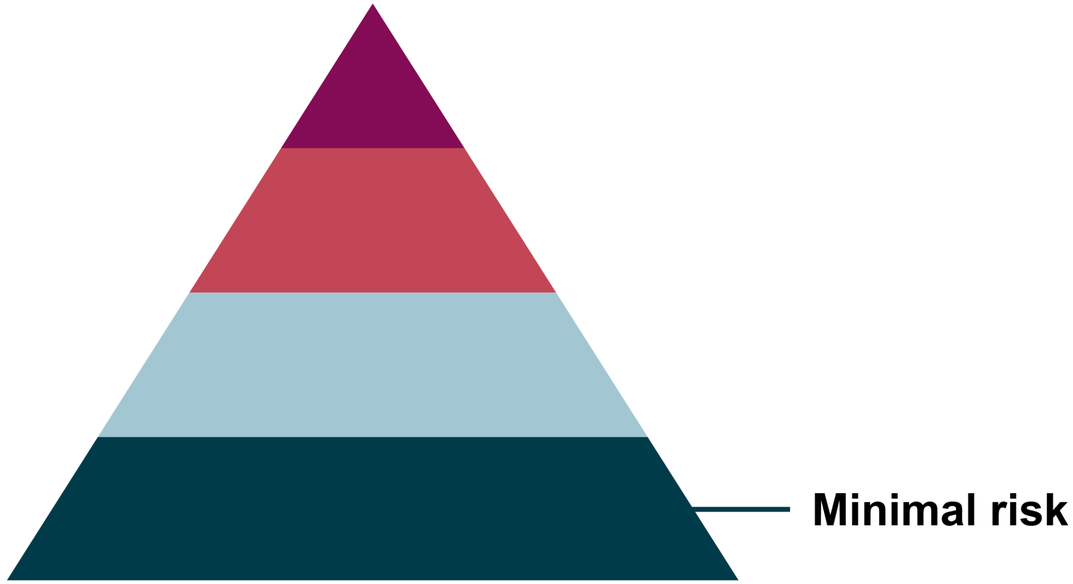
Transparenskrav som innebär att användaren ska förstå att hen interagerar med ett AI-verktyg

AI-system som genererar texter, bilder mm

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-modeller för allmänna ändamål

Vad är AI-modeller för allmänna ändamål?

- På engelska: *General Purpose AI models (GPAI models)*
- Generativ AI, inklusive stora språkmodeller (LLM)

AI-modeller för allmänna ändamål med systemrisk

- Modeller med stor beräkningskapacitet
  Exempel: *OpenAI:s GPT-4 och Googles Gemini*

- Ännu fler krav att leva upp till än vad som gäller för ”vanliga” AI-modeller för allmänna ändamål

Sanktioner m.m.

Sanktioner

- **35M EUR eller 7 procent** av den globala årsomsättningen vid överträdelser av bestämmelserna om förbjudna AI-användningsområden
- **15M EUR eller 3 procent** av den globala årsomsättningen vid överträdelser av bestämmelserna om leverantörers och tillhandahållares skyldigheter
- **7,5M 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 (förbjudna)

2 augusti 2025

Kraven på AI-modeller för allmänna ändamål

2 augusti 2026

I princip alla regler 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!

Styrning på EU-nivå

Styrning på EU-nivå

AI-byrån

- Inrättats inom EU-kommissionen
- Ska arbeta för att utveckla EU:s sakkunskap och kapacitet på AI-området
- Ska bland annat verkställa och övervaka bestämmelserna som rör AI-modeller för allmänna ändamål

Europeisk styrelse för AI

- Ska bestå av en företrädare per medlemsstat
- Ska ge råd till och bistå EU-kommissionen och medlemsstaterna för att underlätta en konsekvent och effektiv tillämpning av AI-förordningen

Tillsyn

Tillsynen över AI-förordningen

- AI-byrån
- Europeiska datatillsynsmannen (EDPS)
- Nationella myndigheter

IMY:s tillsynsområde

Biometri

Kritisk infrastruktur

Utbildning och yrkesutbildning

Anställning, arbetsledning och tillgång till egenföretagande

Tillgång till och åtnjutande av väsentliga privata tjänster och väsentliga offentliga tjänster och förmåner

Brottsbekämpning

Migration, asyl och gränskontrollförvaltning

Rättskipning och demokratiska processer

AI-system som omfattas av bilaga III i 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

Regulatoriska sandlådor för AI

Regulatoriska sandlådor för AI

En översikt,
och någon lärdom från den svenska piloten

IMY webinarium 27 september 2024

AI-regulatoriska sandlådor – vad

Art. 3 (55) definition:

en kontrollerad ram som inrättats av en behörig myndighet och **som erbjuder leverantörer eller potentiella leverantörer** av AI-system möjlighet att utveckla, träna, validera och testa, när så är lämpligt under verkliga förhållanden, ett innovativt AI-system, enligt en specifik sandlådeplan för en begränsad tid under regulatorisk tillsyn.

Art. 57 (5)
… en **kontrollerad miljö** som främjar innovation och underlättar utveckling, träning, testning och validering av innovativa AI-system under en **begränsad tid** innan de släpps ut på marknaden eller tas i bruk i enlighet med en särskild **sandlådeplan** som leverantörerna eller de potentiella leverantörerna och den behöriga myndigheten kommer överens om. Sådana sandlådor får omfatta testning under verkliga förhållanden under tillsyn i sandlådorna.

Bolagsverket

AI-regulatoriska sandlådor – vem

Art 57 (1) Medlemsstaterna ska säkerställa att deras **behöriga myndigheter** inrättar minst en regulatorisk sandlåda för AI på nationell nivå, som ska vara **i drift senast den 2 augusti 2026**. Denna sandlåda får också inrättas tillsammans med de behöriga myndigheterna i andra medlemsstater. Kommissionen får tillhandahålla tekniskt stöd, rådgivning och verktyg för inrättande och drift av regulatoriska sandlådor för AI.

Skyldigheten enligt första stycket får också fullgöras genom deltagande i en befintlig sandlåda i den mån deltagandet ger en likvärdig nivå av nationell täckning för de deltagande medlemsstaterna.

2. Ytterligare regulatoriska sandlådor för AI får också inrättas på regional eller lokal nivå eller tillsammans med andra medlemsstaters behöriga myndigheter.

Bolagsverket

AI-regulatoriska sandlådor – varför

Art. 57 (9) Inrättandet av regulatoriska sandlådor för AI ska syfta till att bidra till följande **mål**

a)Förbättra rättssäkerheten för att uppnå efterlevnad av denna förordning eller, i förekommande fall, annan tillämplig unionsrätt och nationell rätt.

b)Stödja utbyte av bästa praxis genom samarbete med de myndigheter som deltar i den regulatoriska sandlådan för AI.

c) Främja innovation och konkurrenskraft och underlätta utvecklingen av ett AI-ekosystem.

d) Bidra till evidensbaserat regulatoriskt lärande.

e)Underlätta och påskynda tillträdet till unionsmarknaden för AI-system, särskilt när de tillhandahålls av små och medelstora företag, inbegripet uppstartsföretag.

Bolagsverket

AI-regulatoriska sandlådor – varför

Art. 57 (6)

De behöriga myndigheterna ska, beroende på vad som är lämpligt, tillhandahålla **vägledning, tillsyn och stöd** inom den regulatoriska sandlådan för AI i syfte att identifiera risker, särskilt när det gäller grundläggande rättigheter, hälsa och säkerhet, testning, riskreducerande åtgärder och deras effektivitet i förhållande till skyldigheterna och kraven i denna förordning samt, i förekommande fall, annan unionsrätt och nationell rätt som är föremål för tillsyn inom sandlådan.

Art. 57 (7)

De behöriga myndigheterna ska ge leverantörer och potentiella leverantörer som deltar i den regulatoriska sandlådan för AI **vägledning** om rättsliga förväntningar och hur de krav och skyldigheter som fastställs i denna förordning ska uppfyllas.

På begäran av leverantören eller den potentiella leverantören av AI-systemet ska den behöriga myndigheten tillhandahålla ett **skriftligt bevis** på den verksamhet som framgångsrikt utförts i sandlådan. Den behöriga myndigheten ska också tillhandahålla en slutrapport med uppgifter om den verksamhet som bedrivs i sandlådan och tillhörande resultat och lärdomar.

Leverantörer får använda sådan dokumentation för att **visa att de uppfyller kraven i denna förordning** genom förfarandet för bedömning av överensstämmelse eller relevant marknadskontroll. I detta avseende ska marknadskontrollmyndigheter och anmälda organ beakta slutrapporterna och de skriftliga bevis som tillhandahålls av den nationella behöriga myndigheten på ett positivt sätt, i syfte att påskynda förfaranden för bedömning av överensstämmelse i rimlig utsträckning.

Bolagsverket

GDPR gäller men

Art. 59 - Ytterligare behandling av personuppgifter för utveckling av vissa AI-system i allmänhetens intresse i den regulatoriska sandlådan för AI

1. Personuppgifter som lagligen samlats in för andra ändamål får behandlas i den regulatoriska sandlådan för AI enbart i syfte att utveckla, träna och testa vissa AI-system i sandlådan om samtliga följande villkor är uppfyllda:

tekniska

utvecklas för att ett viktigt allmänt intresse ska skyddas

rättsliga (även nationella)

dokumentation

Ytterligare nedslag

- Genomförandeförordningar ska specificera och förtydliga
- Tillgången till sandlådorna ska vara kostnadsfri för små och medelstora företag, inbegripet uppstartsföretag
- Tillsynsmyndigheter (såsom nationella dataskyddsmyndigheter) ska delta under vissa förutsättningar
- Krav på behörig myndighet gällande personal, resurser och kompetens,
- Krav på samarbete mellan behöriga myndigheter

Bolagsverket

Testning av AI-system med hög risk under verkliga förhållanden utanför regulatoriska sandlådor för AI

En särskild plan

Leverantörer eller potentiella leverantören av system med hög risk innan det tas i bruk eller släpps ut på marknaden

Genomförandeföro rdningar ska förtydliga

Sammanfattning gällande AI-regulatoriska sandlådor

- Mycket är oklart – antagligen finns stor variation i hur de kan fungera.
- Kommer sannolikt kräva en hel del specificeringar på EU-nivå och nationell nivå.

Ny utredning beslutad 19 september 2024 ”för trygg och tillförlitlig användning av AI i Sverige” tillsatt
Redovisas senast 30 september 2025

Pilot AI-regulatorisk sandlåda

Första iterationen

eSam

Bolagsverket

Första rapporten

En första rapport, fler kommer

Svensk pilot för AI-regulatorisk sandlåda – eSamverka

Bolagsverket

Lärdomar

Om AI-förordningen

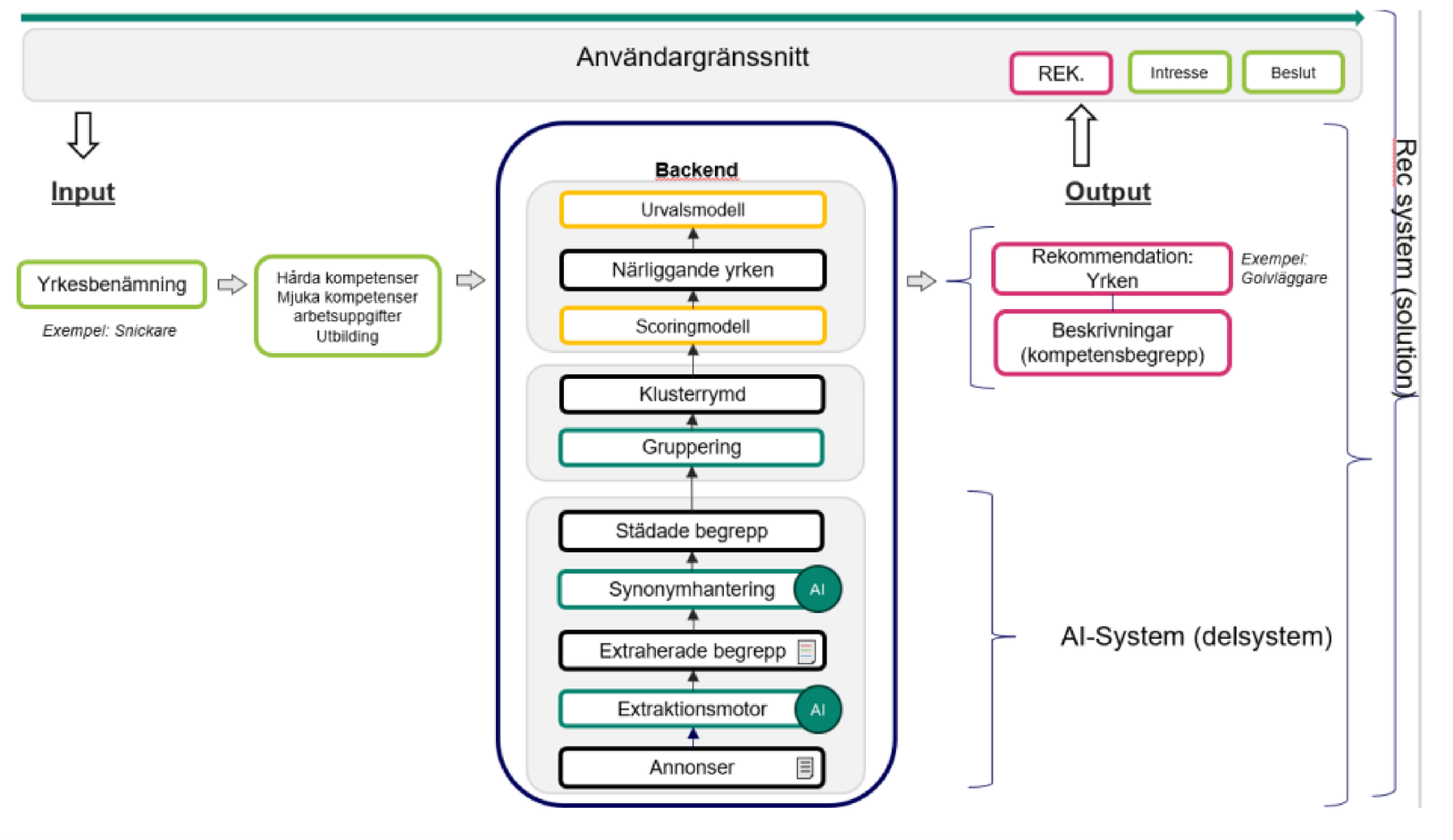
Många it-system kommer att utgöra ett AI-system. Sannolikt kommer det mesta som inte är helt regelbaserad it att kunna omfattas av AI-förordningens definition av AI-system.

Gränsdragningen av omfattningen av systemet, dvs. vad som ska ingå i systemet och vad som inte är en del av systemet, är komplicerad. Det **avsedda ändamålet** bör stå i centrum. Detta sätter ramen för systemet och gör att ett AI-system kan innehålla flera komponenter, modeller och data som behöver beaktas i bedömningen av systemets omfattning.

För att göra bedömningen om vad som innefattas i ett AI-system krävs en **god helhetsbild** över it- och AI-arkitekturen.

Bolagsverket

Gränsen för vad ett AI-system är?



Frågor

Läs mer om vårt AI-arbete
imy.se/ai

Mejla till: innovation@imy.se

IMY. Integritetsskydds myndigheten

www.imy.se