Välkomna till

EU AI-act: Hur påverkas energibranschen?

Tilde Skånvik

Legal counsel and Compliance officer

På Lindholmen Science Park and AI Sweden

Certifierat Dataskyddsombud

Konsult/rådgivning

IT-säkerhetsföretag och advokatbyrå

Juristexamen

Inriktning inom Cyber law and Cyber crime och immaterialrätt

Agenda

- Bakgrund och syfte
- Tillämpningsområde
- Riskbaserat tillvägagångssätt
- Förbjuden AI
- Högrisk AI-system
- Skyldigheter för leverantörer och användare av högrisk AI-system
- Skyldigheter för leverantörer och användare av AI-system med begränsad risk
- Påföljder

Varför behövs en reglering av Artificiell Intelligens?

Möjligheter och risker med AI-System

Möjligheter

- Samhällsnytta
  - Hälsovård, smarta städer, utbildning
- Ekonomisk tillväxt
  - Effektivitet genom automatisering
- Innovation och global konkurrenskraft
  - Energi, finansiella tjänster, grön teknologi

Risker

- Individers hälsa, säkerhet och grundläggande rättigheter
  - Felaktig tolkning av medicinska data, programmeringsfel eller felaktiga beslut
- Demokrati och rättsstatens principer
  - Polarisering, bias, diskriminering, manipulation, deepfakes

Problematisk användning av AI

- Social scoring
  - Bedömning av medborgares beteende och tilldelar dem poäng baserat på deras handlingar, inklusive betalningshistorik, sociala interaktioner och till och med åsikter som uttrycks på sociala medier.
- Manipulativa annonseringstekniker
  - Manipulera konsumenter att köpa produkter genom dolda eller subliminala meddelanden.
- Deepfake-teknologi
  - Individer verkar säga eller göra saker de inte har gjort.

Vad är ett AI-system?

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.

Har min AI följande egenskaper?

✓ Maskinbaserad

✓ Viss autonomi

✓ Anpassningsförmåga

✓ Uttryckliga eller underförstådda mål

✓ Utdata baserat på indata

Artikel 3.1 AI Act

Vad har AI Act för bakgrund och syfte?

Vilka intressen är det AI Act ska skydda?

Syftet är att säkerställa att användningen av AI-system på EU:s inre marknad är säker, respekterar mänskliga rättigheter och underlättar innovation och investeringar i AI.

Artikel 1 AI Act

Vilka aktörer omfattas av AI Act?

Första frågan

Är AI-systemet tillgängligt på unionens marknad eller påverkar det individer som befinner sig inom EU?

Förordningen är tillämplig på både offentliga och privata aktörer, inom och utanför EU, så länge AI-systemet

1. finns på unionens marknad,
2. eller dess användning påverkar personer som befinner sig i EU.

Andra frågan

Har er organisation någon av följande roller:

- **Leverantör,**
- **Tillhandahållare,**
- **Importör, eller**
- **Distributör?**

Olika aktörer

1. Leverantör/Provider

De som utvecklar AI-system eller modeller och lanserar dem på marknaden.
De som utvecklar och använder dem under eget namn. (Exempelvis en utvecklare av ett verktyg för CV-screening)

2. Tillhandahållare/Deployer

De som använder ett AI-system.
(Exempelvis en bank som köper detta screeningverktyg).

3. Importör/Importer

Importerar och gör tillgängligt på marknaden.

4. Distributör/Distributor

Gör det tillgängligt på marknaden på ett sätt som skiljer sig från de tidigare parterna i leveranskedjan.

Artikel 2 AI Act

Några undantag när AI Act inte är tillämplig

Vetenskapligt forsknings- och utvecklingssyfte

AI-system eller AI-modeller, inbegripet deras utdata, som specifikt utvecklas och tas i bruk enbart i vetenskapligt forsknings- och utvecklingssyfte.

Forsknings-, testnings- eller utvecklingsverksamhet för AI-system eller AI-modeller innan de släpps ut på marknaden eller tas i bruk

Militär-, försvar- eller ändamål som rör nationell säkerhet

AI-system som är uteslutande utformade för dessa aktiviteter är undantagna, oavsett vilken typ av enhet som utför dessa aktiviteter.

Privat bruk
(icke yrkesmässig verksamhet) omfattas inte

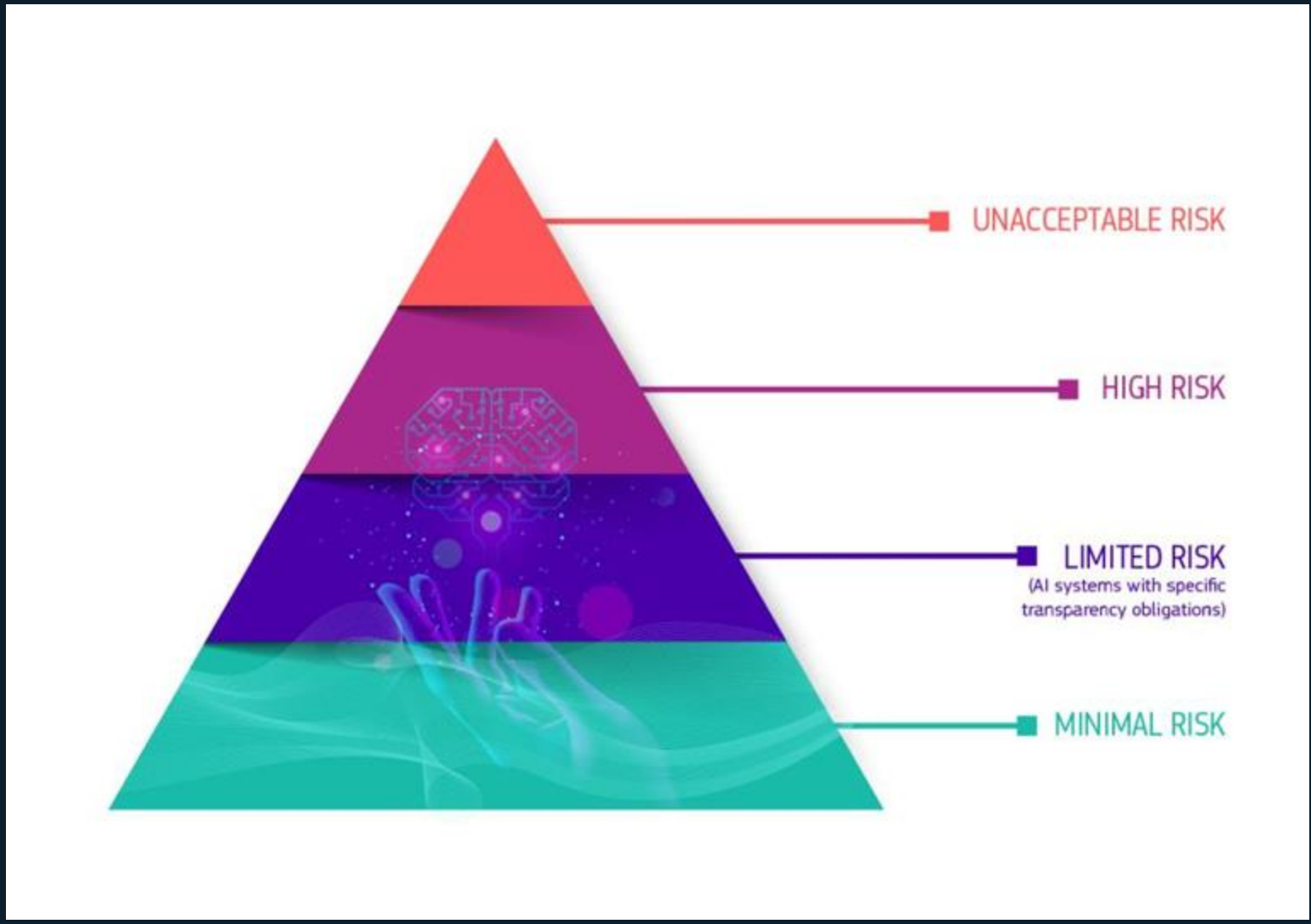
Artikel 2 AI Act

Varför klassificera “Risken” av ett AI-System?

Varför klassificera “Risken” av ett AI-System?

1. AI Act har 4 riskklasser.
2. Aktörens skyldigheter beror på riskklassen för ett AI-system.
3. Aktörens hantering av leverantörer kommer att påverkas av riskklassen för AI-systemet.

Vilka är riskkategorierna?



Vad är förbjuden AI?

Förbjuden AI

- Utnyttja människors sårbarheter
- Manipulerande eller vilseledande
- Socialt kreditsystem
- Individuell prediktiv polisarbete (profilering av personer)
- Oriktad skrapning/datainsamling (internet, CCTV för databaser)
- Emotionell igenkänning på arbetsplatsen och inom utbildningsinstitutioner
- Biometrisk kategorisering (ras, politiska åsikter, etc.)
- Fjärridentifiering i realtid med biometriska data på offentliga platser av brottsbekämpande myndigheter

Hur klassificerar man om ett AI-system är högrisk?

1. Hur klassificerar man om ett AI-system är högrisk?

A) **Säkerhetskomponent** i produkter som omfattas av befintlig produktlagstiftning (Bilaga I) eller

B) **utgöra sådana produkter** i sig själva.

Detta kan exempelvis vara AI-baserad medicinsk programvara.

2. Hur klassificerar man om ett AI-system är högrisk?

C) high-risk use case, listade i bilaga III till AI-förordningen. Specifika användningsområden utgör hög risk (8 områden).

- **Kritisk infrastruktur**
- **Biometrisk kategorisering m.m**
- **Utbildning**
- **Anställning**
- **Brottsbekämpning**
- **Hälso- och sjukvård**
- **Migration**
- **Rättsskipning och demokratiska processer**

2. Hur klassificerar man om ett AI-system är högrisk?

Kritisk infrastruktur

Till exempel kritisk digital infrastruktur, inom vägtrafik och infrastruktur som rör försörjning av vatten, gas, värme och el.

De är klassade som högrisk eftersom felaktigheter i deras beslut eller funktion kan leda till allvarliga konsekvenser, såsom strömavbrott, överbelastningar eller till och med säkerhetsrisker för kritisk infrastruktur.

Exempel

- **Vattenrening och distribution**
- **Gasdistributionssystem**
- **Fjärrvärmesystem**

Några undantag när det inte är frågan om högrisk AI för energisektorn

- **Snäv processuell uppgift.**
- **Används för att förbättra resultat som är av mänsklig verksamhet.**

- **Används för att upptäcka beslutsmönster eller avvikelser och vare sig ersätter eller påverkar tidigare mänsklig bedömning.**
- **Används för förberedande syfte som är relevant för de listade högrisksystemen.**

Riskklassificering: Bästa Praxis

1. Dokumentera och registrera era system i hela organisationen
2. Definiera ert avsedda syfte noggrant och tillämpa det konsekvent i hela organisationen
3. Utveckla en standardmetod för riskklassificering
4. Stärk kompetensen i era organisationer
5. Använd verktyg för automatisering och skalbarhet

Vilka är skyldigheterna för leverantörer av högrisk AI-system?

Vilka är skyldigheterna för leverantörer av högrisk AI-system?

Conformity assessment

Är AI-systemet pålitligt?

- Datakvalitet
- Dokumentation och spårbarhet
- Transparens
- Mänsklig tillsyn
- Noggrannhet
- Cybersäkerhet
- Robusthet

Quality and risk management systems

Efterlevnad av nya krav och riskminimering efter att produkten lanserats på marknaden.

Registered in a public EU database

Om det används av offentliga myndigheter eller enheter som agerar på deras vägnar.

CE-märkning synlig på produkten eller digitalt.

Upcoming!

Europeiska standardiserings organisationen utvecklar en standard

AI-system som utvecklas i enlighet med standarderna kommer att ges "presumtion om överensstämmelse".

Förväntas vara tillgängliga i slutet av april 2025.

Vilka är skyldigheterna för användare av högrisk AI-system?

Krav för användare av AI-system

1. Följ AI-systemets instruktioner
2. Säkerställ att användaren har nödvändig kompetens och befogenhet för att utöva mänsklig tillsyn
3. Informera leverantören och myndigheter om risker
    a. Om användaren identifierar en risk för hälsa, säkerhet eller grundläggande rättigheter, måste de informera leverantören eller distributören samt tillsynsmyndigheten om risken.
4. Spara automatiserade loggar i 6 månader
5. Informera anställda om AI på arbetsplatsen
6. Informera beörda om automatiserat beslutsfattande
7. Konsekvensbedömning gällande grundläggande rättigheter (FRIA)
    a. Användare måste bedöma hur systemet påverkar grundläggande rättigheter. Marknadstillsynsmyndigheten bör informeras om resultaten.

Vilka är skyldigheterna för leverantörer och användare av AI-system med begränsad risk?

Interagerar AI-systemet med individer?

Om JA, finns det ett krav på information och transparens.

Syftet är att informera individen om användningen av AI-system.

Exempel:
Generativa AI-verktyg och "chattbotar". Det måste vara tydligt för användarna att materialet är AI-genererat eller att de interagerar med AI och inte med en fysisk person.

Article 50 AI Act

Vad är konsekvenserna om organisationen inte följer AI-förordningen?

Vad händer om man inte följer lagstiftningen?

Förbjuden AI

Böterna kan vara upp till 35 miljoner euro eller 7% vid överträdelser av förbjudna AI-applikationer.

Skyldigheter enligt förordningen

Böterna kan vara upp till 15 miljoner euro eller 3% vid överträdelser av skyldigheterna enligt AI-lagen.

Felaktig information

Böterna kan vara upp till 7,5 miljoner euro eller upp till 1% för tillhandahållande av felaktig information efter tillsynsbeslut..

(Artikel 99 AI Act)

Viktiga datum att förbereda sig för

Timeline


AI Act träder i kraft
1 Aug 2024
Otillåten AI, definitioner och regler om AI-kunnighet
2 Feb 2025
AI för allmänna ändamål m.m.
2 Aug 2025
Den största delen av AI Act börjar gälla
2 Aug 2026
AI-system med hög risk som är inbyggda i reglerade produkter
2 Aug 2027
Krav för offentliga sektorns högrisk AI-system
2030

Key Takeaways

- Identifiera om AI-systemet är placerat i EU eller påverkar individer i EU.
- Identifiera vilken typ av aktör organisationen är.
- Identifiera AI-systemets riskklassificering.
- Identifiera skyldigheterna för den aktuella riskklassificeringen.
- Planera arbetet med efterlevnad av AI-förordningen enligt tidslinjen.

Thank you!

And don’t forget: my.ai.se and ai.se/newsletter.

Connect with me on LinkedIn to discuss AI Act

- ai.se
- my.ai.se
- ai.se/newsletter
- youtube.com/c/aisweden
- linkedin.com/company/aisweden