
Secify
No nonsense security

Agenda

- AI-förordningens syfte, funktion, struktur
- Genomgång av riskklasserna
- Överflygning av AI-förordningens krav per riskkategori
- AI-kunnighet
- Våra 10 viktigaste medskick

Secify

Specialister inom informationssäkerhet, dataskydd, och cybersäkerhet

Gedigen erfarenhet och kunskap inom en mängd olika branscher, och nischade inom **vård**, **industri** och **tech**.

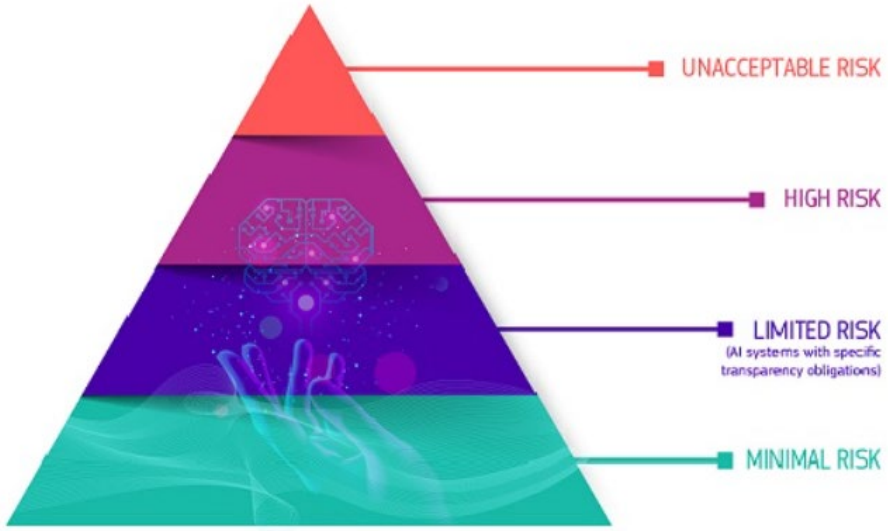
Vi gillar att förenkla och skala bort onödigt fluff – en filosofi vi har döpt till **no nonsense security.**

Flexibla & smidiga, anpassar kostymen efter er verksamhet, och stöttar inom hela området informationssäkerhet & dataskydd

Secify

AI-förordningens syfte

- Harmonisera AI-reglering inom hela EU
- Säkerställa fri rörlighet av AI-baserade varor och tjänster
- Säkerställa en hög skyddsnivå för hälsa, säkerhet och mänskliga rättigheter när AI används
- Förbjuda användning av AI som utgör *för stor risk* mot samhället, medan hög risk system regleras.
- Främja transparens för att öka förtroende



Vilka omfattas?

Olika roller i AI-förordningen

- Leverantörer
- Tillhandahållare
- Ombud
- Importör
- Distributör

Undantag: Användning för privat bruk.

Secify

Vad omfattas?

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-modell = Endast en komponent. Kräver fler komponenter för att kunna bli ett system.

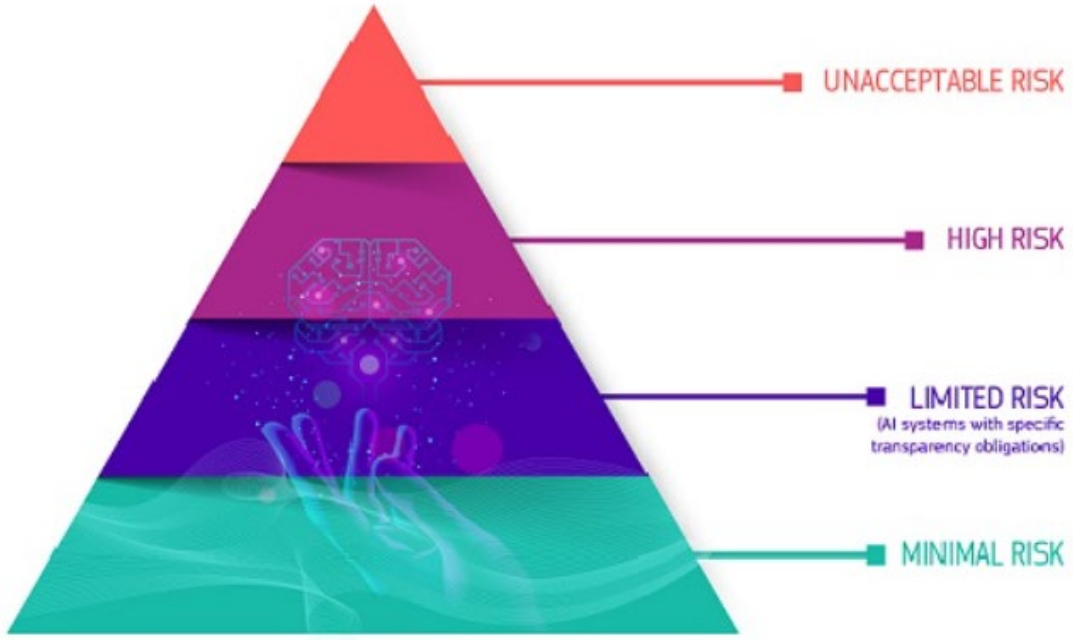
AI-modell för allmänna ändamål = AI-modell som uppvisar betydande generalitet och kapacitet att kompetent utföra ett brett spektrum av distinkta uppgifter och kan integreras i flertal AI-system eller applikationer.

AI-system för allmänna ändamål = AI-system som bygger på AI-modell för allmänna ändamål och som har kapacitet att tjäna en rad olika ändamål, både för direkt användning och för integrering i andra AI-system.

AI-förordningen i ett nötskal!

Riskbaserad modell

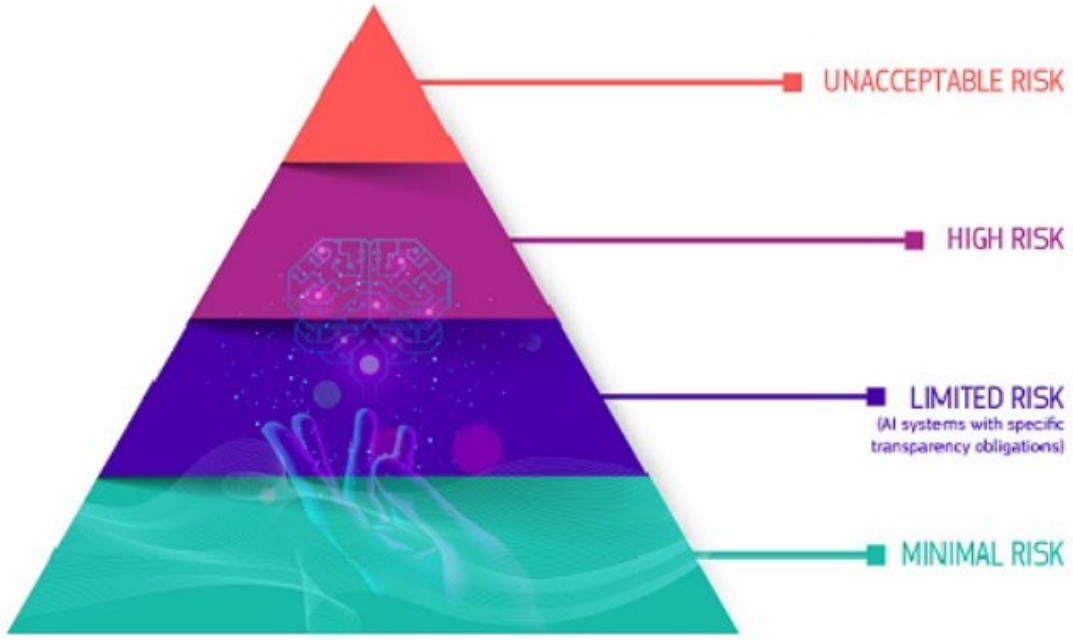
Ju högre risk, desto hårdare krav.



Minimal risk eller ingen risk

Omfattas i princip inte av förordningen.

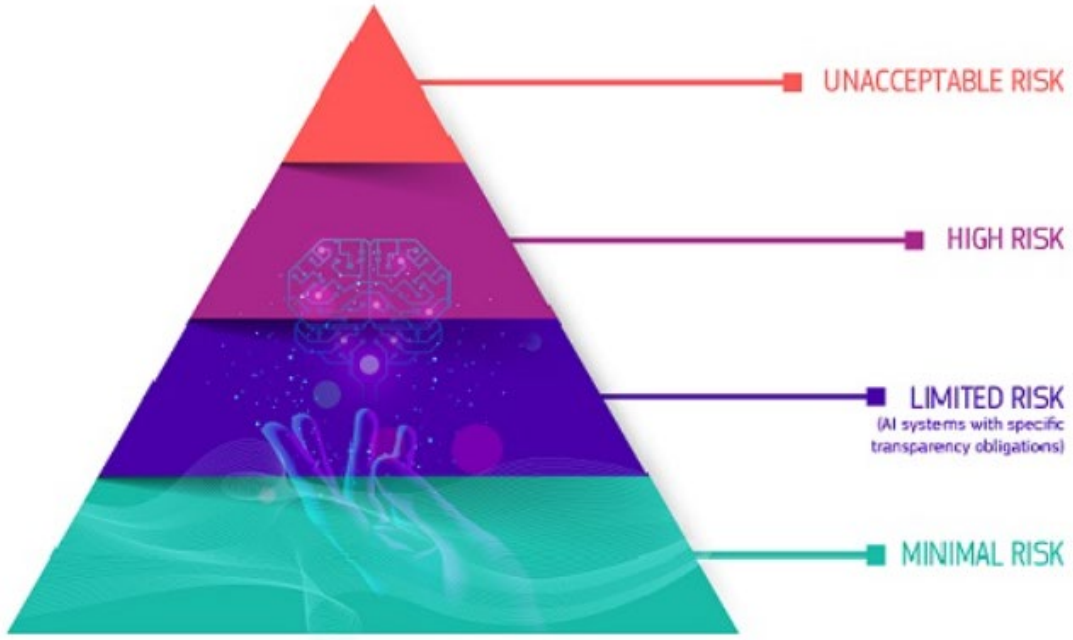
- Skräppostfilter,
- Rekommendations-algoritmer för musik
- Schemaläggning



Begränsad risk

Transparenskrav

- Deep fakes
- AI-kommunikation inom kundtjänst

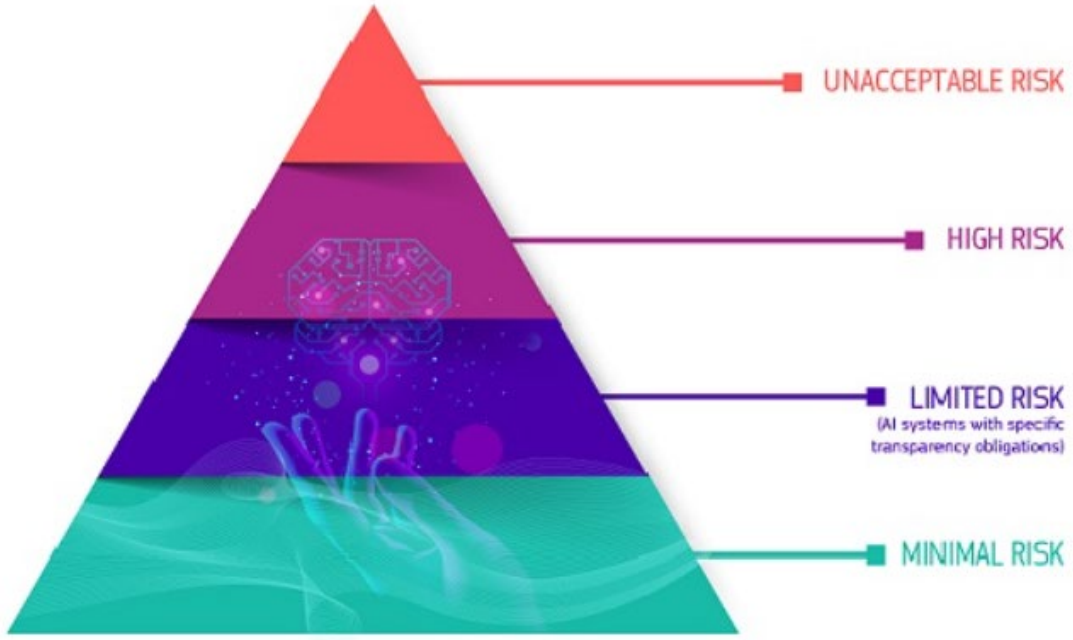


Hög risk

Strikta krav

Viss AI inom...

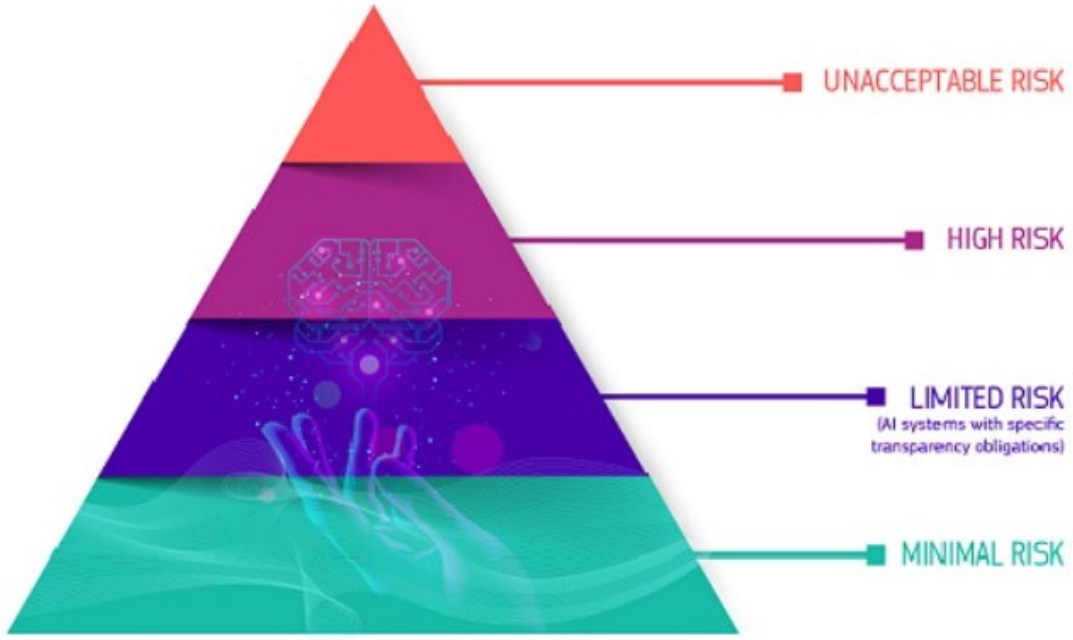
- Rekrytering,
- Kreditgivning,
- Brottsbekämpning,
- Medicinteknik



Oacceptabel risk

Helt förbjuden inom EU

- Sociala poängsystem
- AI som manipulerar människor
- Uttydning av känslor på arbetsplatsen



Digital Omnibus

Förslag på ändringar av EU:s digitala regelverk.
Bland annat: AI-förordningen, GDPR och NIS2.

November 2025

Syftet:

- Göra det enklare att följa reglerna
- Minska dubbelarbete

När börjar förordningen gälla?

1 augusti 2024 – Förordningen trädde i kraft

2 februari 2025 – Oacceptabel risk + AI-kunnighet

~~2 augusti 2026~~ 2 december 2027 – AI med hög risk på grund av dess särskilda användningsområde/syfte (bilaga III)

~~*2 augusti 2026*~~ *2 december 2026* – Krav på Vattenmärkning

~~2 augusti 2027~~ 2 augusti 2028 – AI med hög risk som utgör säkerhetskomponenter i produkter (bilaga I) inom vissa särskilda områden och som kräver tredjepartsbedömning innan utsläppande på marknaden.

+ Undantag för system som redan finns på marknaden vid ”cut off date”

Några förändringar

- Krav på vattenmärkning skjuts upp
- Nudifier-appar förbjuds
- Större möjlighet att behandla personuppgifter för att upptäcka och korrigera bias

I väntan på högrisk-reglerna…

- Riskklassificera AI-system
- Analysera vilken roll ni har
- Om hög risk, granska leverantören!
  - *Förbereder de sig för reglerna?*
  - *Hur?*
  - *Finns bevis?*
- Bedöm vilka andra lagar som är tillämpliga på systemet

Vad gäller nu?

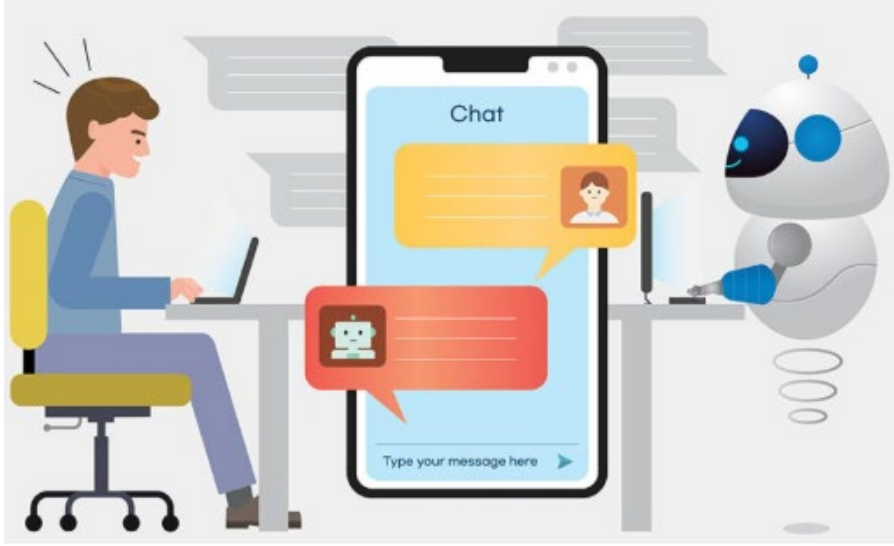
- AI-kunnighet, utbilda medarbetare (artikel 4)
- Reglerna som förbjuder viss typ av AI (artikel 5)

Vad gäller snart?

- Transparenskraven (artikel 50)

Transparenskraven

- Syftar till att upprätthålla förtroende för myndigheter / samhället samt motverka falsk nyhetsspridning
- Människor ska inte luras att de samtalar med AI
- Deepfakes ska enkelt kunna identifieras som fejkat material
- Det ska vara tydligt att AI-genererade nyheter är just AI-genererade
- Informera om känsloigenkänning används



AI-kunnighet

Gäller för alla typer av AI-system oavsett risknivå

Def: färdigheter, kunskaper och den förståelse som gör det möjligt för tillhandahållare och andra aktörer att göra välgrundade val vid användning av AI-system, samt att bli medvetna om de möjligheter och risker som AI medför

Utbildningen ska vara anpassad efter vad som är nödvändigt för användare att känna till

- Beroende på risknivå
- Beroende på roll

Det räcker inte att hänvisa till bruksanvisningen för systemet - det måste göras en (pedagogisk) insats.

Fall: Chattbotar

Exempel på hur AI-kunnighetskravet kan efterlevas

Det som genereras är baserad på matematik, inte riktig kunskap

Hallucinationer kan inträffa, faktapåståenden behöver verifieras

Tydliggör vilken information som är godkänd att mata in, när försiktighet ska vidtas och vilken information som är strikt förbjuden

Utdata måste alltid granskas – ansvar ligger på individen och organisationen

Hög risk

Bilaga I
Reglerar AI som finns i produkter som omfattas av sektorspecifik lagstiftning, ex. MDR

Bilaga III
Reglerar AI som används för visa typer av ändamål

- Rekrytering och anställning
- Utbildning
- Känslodetektering
- Offentliga tjänster
- Kreditvärdighet

Hög risk – Leverantörers skyldigheter

Sammanfattning av leverantörskraven

- Personalen ska ha AI-kunnighet
- Riskhanteringssystem
- Säkerställa god datakvalitet i alla led
- Upprätta teknisk dokumentation över systemet som möjliggör tillsyn
- Loggkrav enligt vissa kriterier
- Upprätta en bruksanvisning för Tillhandahållare i hur systemet ska användas
- Upprätta lättbegriplig information till Tillhandahållare om systemets funktionalitet, syfte, prestanda och begränsningar.

Hög risk – Leverantörers skyldigheter
Fortsättning

- Möjliggöra för Tillhandahållaren att utöva mänsklig kontroll över systemet när det är i bruk
- Säkerställa en lämplig nivå av riktighet, robusthet och cybersäkerhet
- Kvalitetsledningssystem
- Rapportera allvarliga incidenter till kontrollmyndighet
- Registrera systemet i EU-databas
- Konformitetsbedömning
- CE-märkning i vissa fall

Hög risk – Tillhandahållares skyldigheter

- Följa bruksanvisningen
- Säkerställa AI-kunnighet
- Utöva mänsklig tillsyn/kontroll
- Informera individer som blir direkt utsatta för systemet
- På arbetsplats: Informera arbetstagarrepresentanterna
- Kvalitetssäkra indata, i den mån den står under tillhandahållarens kontroll
- Driftövervakning

Hög risk – Tillhandahållares skyldigheter

- Loggning
- Incidentrapportering
- Upprätta DPIA om personuppgifter ska behandlas
- Upprätta FRIA om myndighet eller privat bolag som utför offentlig tjänst, ex. socialjtänst
- Samarbeta med myndigheter

Ansvar längs AI-värdekedjan

Undvik att bli leverantör av misstag.

- Sätter sitt namn eller varumärke på AI-systemet som redan finns på marknaden
- Gör en väsentlig ändring av AI-systemet som redan finns på marknaden (som var hög risk och fortfarande är hög risk)
- Ändrar det avsedda ändamålet med ett AI-system, som inte var klassat som hög risk, men som på grund av det ändrade ändamålet blev ett hög risk system

Sanktionsbelopp

Brott mot bestämmelser inom:

Det förbjudna området (artikel 5) → 7% av totala globala årsomsättningen eller 35 miljoner Euro

Hög risk området eller transparensreglerna → 3% av totala globala årsomsättningen eller 15 miljoner Euro

Avslutande medskick

1. Klassificera riskkategori för alla AI-system
2. Klassificera er roll enligt förordningen (tillhandahållare/leverantör). Undvik att bli leverantör av misstag.
3. Upphör med all användning av AI med Oacceptabel risk
4. Hög risk: Skapa en plan för efterlevnad
5. Säkerställ AI-kunnighet på systemnivå / användningsområde. Dokumentera alla utbildningsinsatser.
6. Var transparent i när AI används
7. AI Compliance Officer för att hålla ihop arbetet med regelefterlevnad (likt DSO)
8. Kartlägg vilka regelverk som er AI-användning träffas av
9. Omvärldsbevaka kontinuerligt
10. Se över systemportföljen i takt med förändringar

Tack för er uppmärksamhet!