Bolagsverket

AI-förordningen

Sambruk 2024-05-24

David Magård

Bakgrund och kontext

- Europeiska rådet (2017)
- Europeiska kommissionen (meddelande Artificiell intelligens för Europa, COM/2018/237)
- High-level expert group on artificial intelligence (AI HLEG) (2018)
- Europaparlamentet (2019)
- Vitboken om AI – En EU-strategi för spetskompetens och förtroende (COM (2020) 65)

Bakgrund och kontext

Digital suveränitet

EU först ut med AI-lagstiftning

The 2021 Coordinated Plan on Artificial Intelligence

Finanisering: Bl.a. Programmet för det digitala Europa (DIGITIAL) och Horizon Europe

“A European approach to AI”

Förordningen på övergripande nivå

Grund för reglering: Främst inre marknad 114 TFEU.

107 artiklar och 13 bilagor (och ett antal genomförandetakter).

Riskbaserat angreppssätt.

Höga böter.

Nya myndigheter, roller och aktörer.

Regulatoriska sandlådor och testverksamhet för AI.

Skyddslagslagstiftning
Produktlagstiftning

Europarlamentets korrigerade version från 16 april 2024.
Slutlig version publiceras i dagarna.

Generella undantag från förordningen

- Områden där EU inte har kompetens men särskilt förtydligat att detta gäller AI-system och utdata (*output*) som används för nationell säkerhet, militära ändamål och nationellt försvar
- AI-system som används av myndigheter i tredjeland eller internationella organisationer (vissa förbehåll) i EU
- AI-system och modeller inklusive utdata som endast utvecklats och använts för vetenskaplig forskning och utveckling.
- Forskning, utveckling, test av AI-system eller modeller innan systemet släpps ut på marknaden
- Användning av AI-system helt för personligt bruk.

ett antal specifika undantag finns

Centrala begrepp – AI rättsligt definierat!

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.

- Utsläppande, tillhandhållande, ibruktagande av AI-system på marknaden
- Avsett ändamål för ett AI-system
- Ex-ante (förhandsprövning)

Aktörer som omfattas

- *leverantör*: en fysisk eller juridisk person, en offentlig myndighet, en byrå eller ett annat organ som utvecklar ett AI-system eller en AI-modell för allmänna ändamål eller som har ett AI-system eller en AI-modell för allmänna ändamål och släpper ut det eller den på marknaden eller tar AI-systemet i bruk i eget namn eller under eget varumärke, antingen mot betalning eller kostnadsfritt

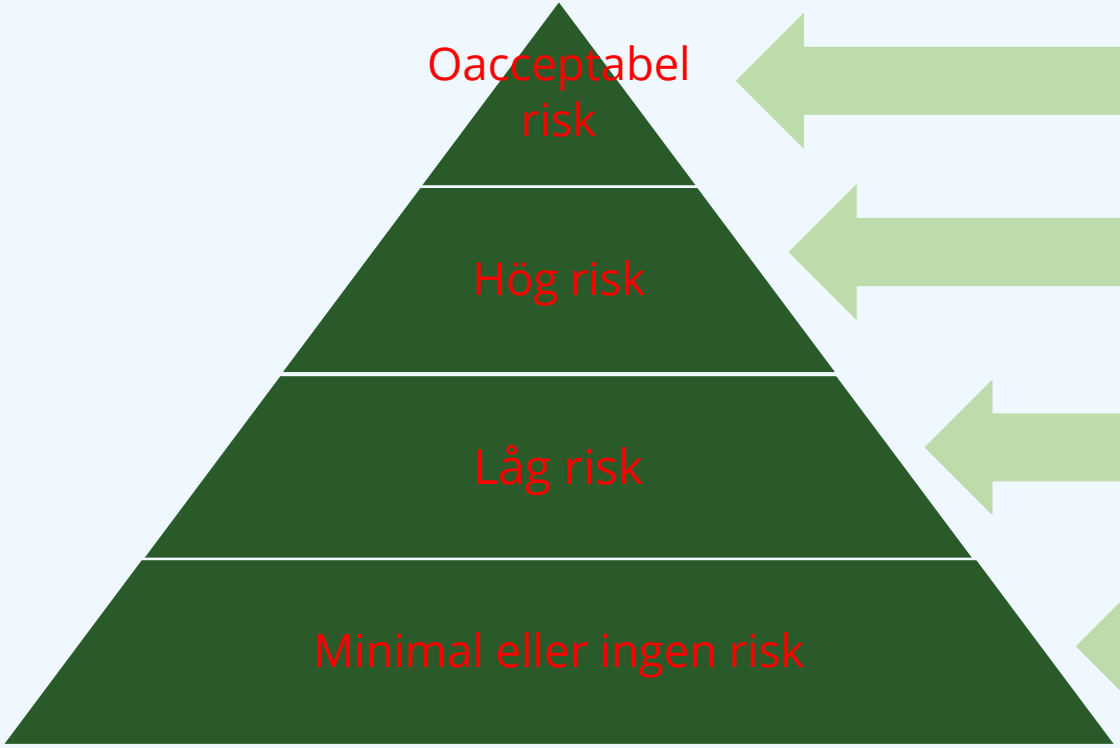
- *tillhandahållare*: en fysisk eller juridisk person, offentlig myndighet, en byrå eller annat organ som under eget överinseende använder ett AI-system, utom när AI-systemet används inom ramen för en personlig icke-yrkesmässig verksamhet.

- Importörer, distributörer, ombud, operatörer.

Utvecklare/de som utvecklar systemet

Förordningen gäller även leverantörer utanför EU. Dessutom leverantörer och användare om utdata producerat av ett AI-system används i EU

Riskbaserat angreppssätt = risk för individers säkerhet och risk för kränkningar av fri- och rättigheter



Förbjudet

Får användas, men under vissa förutsättningar

Transparenskrav

Inga krav enligt förordningen (men frivilliga uppförandekoder)

Bolagsverket

Tänk på

Risken är förutbestämd

Det är inte ni som organisation som avgör risken med ett AI-system, det avgörs av förordningen.

Prövningen görs av er (självständigt eller via tredjepart) men ska ske innan systemet släpps ut, tas i bruk eller tillhandahålls på marknaden

Minimal eller ingen risk

Inga krav.

Men, utarbetande och användandet av uppförandekoder som syftar till att främja frivillig tillämpning av kraven för hög risk uppmuntras.

Låg risk

I princip transparenskrav (användaren ska förstå att det är en AI som den interagerar med eller som skapat materialet)

Utarbetande och användandet av uppförandekoder som syftar till att främja frivillig tillämpning av kraven för hög risk uppmuntras.

Riskbaserat angreppssätt = risk för individers säkerhet och risk för kränkningar av fri- och rättigheter

Förbjudet (typ)

Får användas, men under vissa förutsättningar

Transparenskrav

Inga krav enligt förordningen (men frivilliga uppförandekoder)

Förbjudna AI-system, AI-system (1)

- som använder subliminala, manipulativa eller vilseledande tekniker för att snedvrida beteendet hos en person eller en grupp personer så de påverkade fattar beslut som de normalt inte skulle fatta och det leder till betydande skada.
- som utnyttjar sårbarheter hos en person eller en grupp personer relaterade till ålder, funktionshinder eller socioekonomiska situation för att snedvrida beteendet så att det leder till betydande skada.
- som används för biometriska kategoriseringssystem av människor och kategoriserar människor utifrån ras, politiska åsikter, medlemskap i fackföreningar, religiös eller filosofisk övertygelse, sexliv eller sexuell läggning, förutom märkning eller filtrering av lagligen förvärvade biometriska datauppsättningar eller när brottsbekämpande myndigheter kategoriserar biometriska data.
- som används för att poängsätta (*social scoring*) personer eller grupper av personer utifrån socialt beteende eller personliga egenskaper och detta orsakar skadlig eller ogynnsam behandling av dessa personer.

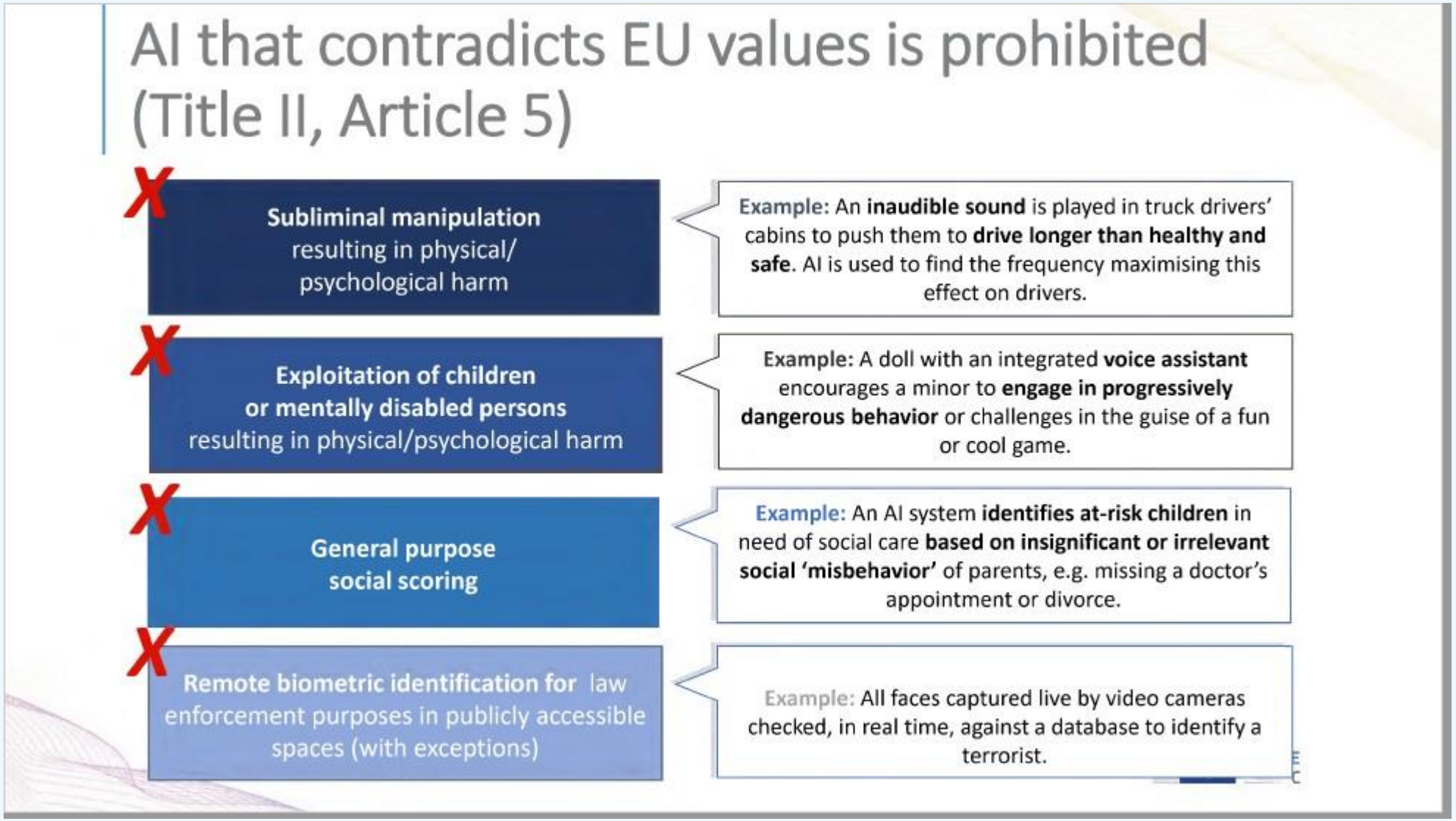
Förbjudna AI-system, AI-system (2)

- som används för att bedöma risken för att en individ begår brott enbart baserat på profilering eller personlighet egenskaper, utom när de används för att förstärka mänskliga bedömningar baserade på objektiva, verifierbara fakta och de fakta är direkt kopplade till kriminell verksamhet.
- som sammanställer databaser för ansiktsigenkänning genom oriktad skrapa av ansiktsbilder från internet eller CCTV övervakningssystem.
- som används för att utvärdera/deducera en persons känslor på arbetsplatser eller utbildningsinstitutioner, förutom av medicinska eller säkerhetsmässiga skäl.

- som används för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser i brottsbekämpande ändamål

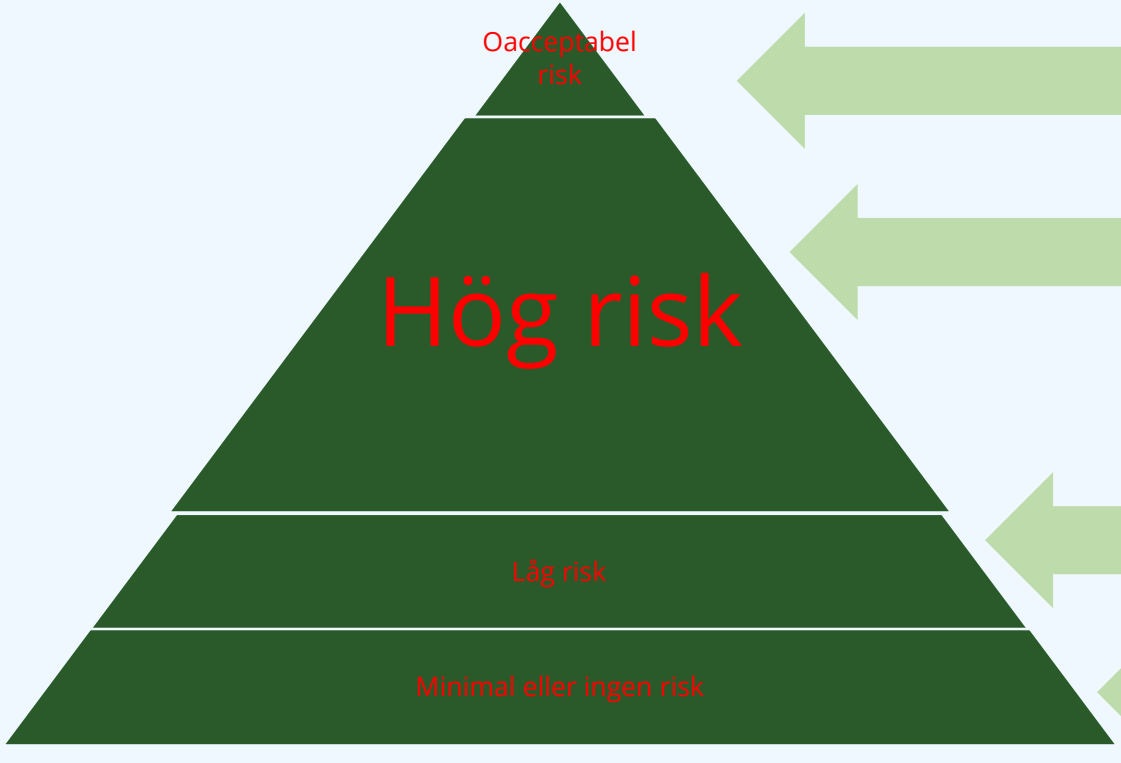
- men med flera undantag och flera olika ”ventiler” för möjliggöra men också stävja användningen.

Förbjudna AI-system (bild från KOM från grundförslaget)



Bolagsverket

Riskbaserat angreppssätt = risk för individers säkerhet och risk för kränkningar av fri- och rättigheter



Förbjudet

Får användas, men under vissa förutsättningar

Transparenskrav

Inga krav enligt förordningen (men frivilliga uppförandekoder)

AI-system som är av hög risk – kategori 1

AI-system som är tänkta att användas som en säkerhetskomponent i en produkt eller AI-system som i sig är en produkt och omfattas av rättsakterna i Bilaga II och som måste genomgå tredjepartsbedömning för att släppas ut på marknaden eller tas i bruk.

Det handlar om bl.a. leksaker, medicintekniska produkter och hissar.

Dock – I Art. 2 (2) finns undantag för rättsakter som tas upp Bilaga II sektion B, som bl.a. berör bilar och flygplan. I skäl (29) framgår att nämnda rättsakter bör ändras så att kraven i de rättsakterna harmoniseras med AI-förordningens krav på hög-risk system.

AI-system som är av hög risk – kategori 2

AI-system som omfattas av Bilaga III kategoriseras som högrisk-system.

Om inte

AI-systemet endast utför en begränsad administrativ uppgift, syftar till att förbättra ett resultat som en människa skapat, upptäcka mönster i beslutsfattande eller tidigare beslut och detta inte används för att utan mänskligt inflytande ändra i beslut eller systemet utför en förberedande uppgift i utvärderingen av ett användningsfall som listas i Bilaga III.

Men

AI-system som omfattas av Bilaga III är alltid att hög risk om systemet profilerar fysiska personer.

Bedömningen görs av leverantör och ska dokumenteras + registreras i EU databas innan systemet tas i bruk

AI-system som är av hög risk – kategori 2 - Områden

- Biometrisk identifiering och kategorisering av fysiska personer
- Förvaltning och drift av kritisk infrastruktur
- Utbildning och yrkesutbildning
- Sysselsättning, arbetsledning och tillgång till egenföretagande
- Tillgång till och åtnjutande av grundläggande privata tjänster och offentliga tjänster och förmåner
- Brottsbekämpning
- Migrations-, asyl- och gränskontrollförvaltning
- Rättskipning och demokratiska processer

Bilaga III kan ändras genom delegerad förordning ←-----Gissningsvis kommer listan att utökas

AI-system som är av hög risk – kategori 2 - Nedslag

- a) AI-system som är avsedda att användas för rekrytering eller urval av fysiska personer, särskilt för att publicera riktade platsannonser, analysera och filtrera platsansökningar och utvärdera kandidater.

- b) AI-system som är avsedd att användas för att fatta beslut som påverkar villkoren för arbetsrelaterade förhållanden, befordringar och uppsägningar av arbetsrelaterade avtalsförhållanden, för uppgiftsfördelning på grundval av individuellt beteende eller personlighetsdrag eller egenskaper eller för att övervaka och utvärdera personers prestationer och beteende inom ramen för sådana förhållanden

- AI-system som är avsedda att användas av offentliga myndigheter eller för offentliga myndigheters räkning för att utvärdera fysiska personers rätt till väsentliga förmåner och tjänster i form av offentligt stöd, inbegripet hälso- och sjukvårdstjänster, samt för att bevilja, minska, upphäva eller återkalla sådana förmåner och tjänster.

Om AI-systemet anses vara hög risk ska leverantören enligt huvudregeln säkerställa överenstämmelse med förordningen innan systemet får användas

(grund)Krav på:

- Riskhanteringssystem
- Datahantering/dataförvaltning
- Teknisk dokumentation
- Arkivering/registrering av loggar
- Dokumentation, transparens och information
- Effektiv mänsklig tillsyn
- Lämplig nivå av noggrannhet, robusthet och cybersäkerhet
- Kvalitetsstyrningssystem

Även vissa krav på att övervaka/följa systemet efter det tagits i bruk/släppts ut på marknaden

Leverantörens process för visad överenstämmelse

Innan systemet släpps ut/tas i bruk:

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

Intern kontroll

Tredjepartsbedömning

Överenstämmelse kan ibland presumeras, om leverantören följer vissa standarder, gemensamma specifikationer, använder vissa dataset

- Upprätta en EU-deklaration om överenstämmelse.
- Registrera systemet i EU:s öppna databas för högrisk (för vissa system finns en databas som med begränsad insyn).
- ”Fästa” en CE-märkning till systemet.

Även krav på *tillhandhållare*

- Tillförsäkrat att leverantören har genomfört förfarandet för överenstämmelse.
- Ha tillräcklig kompetens för att följa instruktionerna som följer med systemet.
- Säkerställa mänsklig tillsyn.
- Använda sig av relevant och tillräcklig input data om användaren använder sig av input data
- Viss krav på monitorering och informationskrav vid fel
- Arkivering av loggar
- I vissa fall genomföra en påverkansanalys utifrån grundläggande rättigheter.
- Myndigheter ska i den öppna databasen registrera att de använder sig av ett, och vilket, högrisk-system.

För övriga aktörer såsom importörer och distributörer gäller i princip att säkerställa att systemet har genomgått förfarandet för överenstämmelse och hålla relevant information

General purpose AI (GPAI) – AI-system för allmänna ändamål

‘AI-modell för allmänna ändamål: en AI-modell, även när en sådan AI-modell tränas med en stor mängd data med hjälp av självövervakning i stor skala, som uppvisar betydande generalitet och på ett kompetent sätt kan utföra ett brett spektrum av distinkta uppgifter oavsett hur modellen släppts ut på marknaden och som kan integreras i en rad system eller tillämpningar i efterföljande led, utom AI-modeller som används för forsknings-, utvecklings- eller prototypverksamhet innan de släpps ut på marknaden.

‘AI-system för allmänna ändamål: ett AI-system som bygger på en 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

En klassificeringsprocess införs varigenom en GPAI kan anses vara av ”systemrisk”. I dagsläget främst beroende på beräkningskapacitet men kraven ska utvecklas av AI Office.

General purpose AI (GPAI) – Krav på leverantörer

Generella krav på efterlevnad av Upphovsrättsdirektivet 2019/790 och tillhandahållande av detaljerad dokumentation gällande träningsdata. Även transparenskrav i förhållande till användare.

Lättare krav om modellen är open source. Om inte, krav på teknisk dokumentation

Om modellen är GPAI med systemisk risk och inte open source gäller fler krav. Förtydliganden ska tas fram av AI Office. Eventuellt fler krav.

Regulatoriska sandlådor och ”real world testing”

Krav på att varje medlemsstat ska tillhandahålla minst en regulatorisk sandlåda i enlighet med förordningen.

En kontrollerad miljö för utveckling, 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 plan. Medlemsstaterna ska särskilt underlätta för SME:s.

Upprättas av behörig(a) myndighet(er). Vissa begränsade möjligheter att vidarebehandla personuppgifter.

Real world testing – Test av system under verkliga förhållanden.

Sanktioner

- I huvudsak böter men medlemsstaterna ska ta fram egna regler. Höga böter möjliga men olika nivåer beroende på systemet, vilken sorts aktör som misskött sig och graden av misskötsel.

Flera nya myndigheter och aktörer

EU-nivå

- AI Office - inom kommissionen
- European Artificial Intelligence Board – En representant per medlemsstat
- Advisory forum – Näringsliv, akademi, standardinseringorgan mfl.
- Scientific panel of independent experts

Nationell nivå

- Minst en marknadskontrollsmyndighet
- Minst en anmälande myndighet för anmälande organ (inriktat på tredjepartsbedömningar)
- Ansvar för vissa behöriga myndigheter enligt utpekande i existerande rättsakter

Ikraftträdande och tillämpningsperioder

Träder i kraft 20 dagar efter att förordningen publicerats i Europeiska unionens officiella tidning

Antagligen i maj 2024

Efter 6 månader gäller kraven för de förbjudna system.

Efter 12 månader gäller kraven på GPAI modeller

Efter 24 månader gäller i princip övriga krav

Efter 36 månader gäller kraven för hög risk system som omfattas av andra EU-rättsakter.

AI-system i bruk inom offentlig sektor ska leva upp till förordningen inom 4 år från ikraftträdande

Användning av ett AI-system för ett annat syfte eller att systemet genomgår en väsentligt förändring?

- Om det inte var avsikten från början (bevisa) - börja om från början!
- Om du inte är leverantör kan du bli klassad som leverantör, utifall du gör större ändringar eller sätter ditt namn/varumärke på ett system.

Vad händer om en GPAI används som högrisk?

- Då är användningen högrisk… Ansvaret hamnar på aktören som använder systemet på det sättet. Gissningsvis kommer leverantörer snäva av det ”avsedda andamålet” .

Behövs kompletterande regler, vägledningar osv

- Ja. På EU-nivå och nationell nivå.

Hur kommer myndighetsstrukturen i Sverige att se ut?

- Vi vet inte än. IMY kommer ha en roll. Behöriga myndigheter i vissa sektorer som t.ex. PTS kommer ha en roll.

Gäller GDPR?

- Ja. Och alla andra regelverk, det är nog i att få en samlad bild där det främsta utmaningarna finns.

Bolagsverket

Några tankar

- Mycket kommer att hamna inom definitionen av AI enligt förordningen, men i många fall kommer det inte betyda merarbete.
- I huvudsak en dokumentera, registrera och visa upp-reglering – vi kan detta i offentlig sektor men det kommer att krävas mer resurser.
- Inte orimligt att näringslivet kommer att fokusera på systemet som inte är högrisk vilket kan innebära att offentlig sektor behöver utveckla mer själva. Open source och förvaltningsgemensamma infrastrukturen blir då viktigare.
- Ni bestämmer själva när ni omfattas av förordningen… Det är inte förrän systemet sätts använts på marknaden/tas i bruk som förordningen gäller. Oavsett om ni upphandlar eller utvecklar själva. Fyra år för de system som redan finns så tid finns.
- Förbered upphandlingsavdelningen.
- Förbered verksamheten men särskilt jurister och utvecklare.
- Förväntar mig att det kommer att komma bra stöd från de olika nationella och EU-aktörerna. Därtill eSAM. Lite is i magen är bra.

Tack! Frågor?

I mitten av juni planerar Arbetsförmedlingen, Bolagsverket, Skatteverket och IMY att publicera en första rapport inom ramen för eSAM gällande vårt arbete med en pilot av en AI-regulatorisk sandlåda

David.Magard@Bolagsverket.se