Bolagsverket

AI-förordningen Dataskydd och AI

Sambruk 2024-08-28

David Magård (Bolagsverket)
Per Nydén (IMY)

Agenda

AI-förordningen med fokus på högrisk

Dataskyddsförordningen och AI

Lärdomar från pilot av AI regulatory sandlåda

Frågor

Förordningen på övergripande nivå

Grund för reglering: Främst inre marknad 114 TFEU.

113 artiklar, 180 skäl och 13 bilagor (och ett antal genomförandetakter).

Riskbaserat angreppssätt.

Höga böter.

Nya myndigheter, roller och aktörer.

Regulatoriska sandlådor och testverksamhet för AI.

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

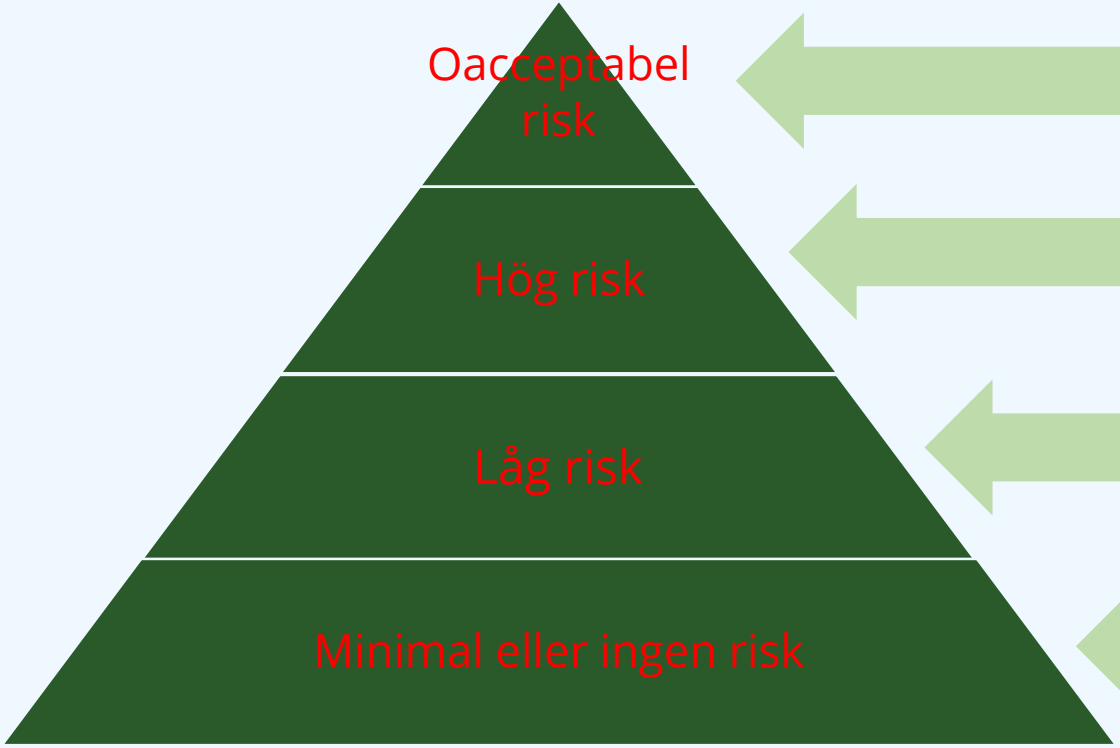
- *tillhandahållare*: en fysisk eller juridisk person, offentlig myndighet, en byrå eller annat organ som under eget överinseende använder ett AI-system, utom när AI-systemet används inom ramen för en personlig icke-yrkesmässig verksamhet.

- 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

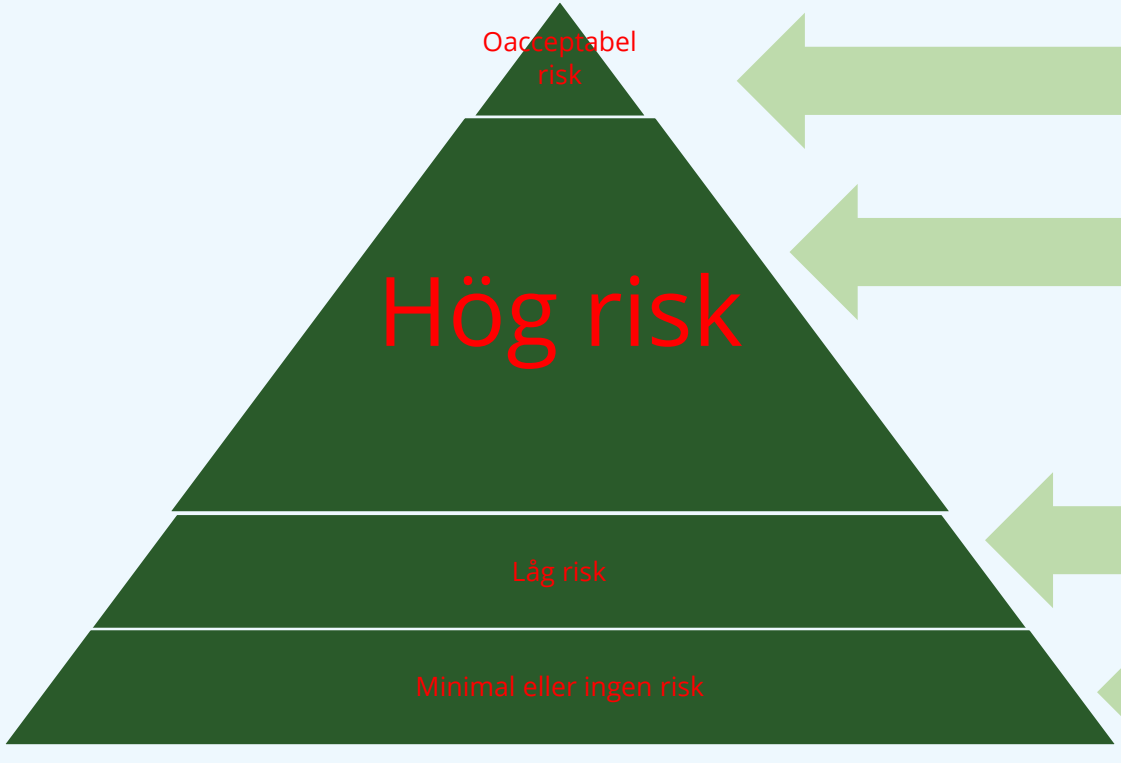
Risken är förutbestämd

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

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.

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

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