SVENSKT NÄRINGSLIV
SWEDISH ENTERPRISE

AI-förordningen – en introduktion och guide

AUGUSTI 2024

Foto: iStock
Författare: Carolina Brånby

Innehåll

AI-förordningen

Sedan EU-kommissionen la fram förslaget om en AI-reglering i april 2021 har den ofta kallats AI-akten. I den slutgiltiga svenska lagtexten har den fått namnet förordning om artificiell intelligens (AI). I den här skriften förkortar vi den AIA, som är den engelska förkortningen av AI Act. Eftersom det är en EU-förordning gäller den i alla 27 medlemsstaterna.

AIA blev färdig i maj 2024. Den träder i kraft i juli 2024 men tillämpas med olika startdatum för olika delar inom de närmaste åren. AIA syftar till att främja användningen av AI genom gemensamma regler i hela EU och samtidigt säkerställa hälsa, säkerhet och grundläggande rättigheter i utvecklingen och användningen av AI-system och modeller. Den reglerar också hur innovation ska stöttas.

Viss AI-användning förbjuds; vissa AI-system och användningsområden klassas som högrisk och där har företag som är leverantörer och användare omfattande skyldigheter. För AI-system som interagerar med människor, till exempel chattbottar, och för generativ AI som skapar eller förändrar text, film, bild och ljud ska information lämnas så att användaren inte missbedömer eller tror att det är en människa man kommunicerar med eller att något AI-genererat är skapat av en person.

De flesta av dagens AI-system omfattas inte alls av reglerna. De typer av AI-system och modeller som omfattas berörs som huvudregel först när de tas i bruk eller sätts på marknaden. För forskning och utveckling gäller inte reglerna alls. När systemen tas i bruk för testning i verkliga förhållanden gäller dock AIA.

Samtidigt som AIA uppställer höga krav på leverantörer av vissa AI-system syftar regleringen även till att stödja småskaliga leverantörer och tillhandahållare. Bland annat ska myndigheter sprida information om tillämpningen av AIA anpassad till behoven hos de mindre företagen. Tanken är också att myndigheter ska vägleda och kommunicera med företagen.

AIA är framför allt en produktsäkerhetslag som utgör ett komplement till annan unionslagstiftning på produktsäkerhetsområdet. Det innebär att AI-system som används som säkerhetskomponenter i produkter som redan omfattas av sektorsspecifik lagstiftning, såsom produktsäkerhetslagar, både måste uppfylla kraven i AIA och kraven i tillämpliga produktsäkerhetslagar, innan de släpps ut på marknaden eller tas i bruk. Men viss lättnad ges för att minska dubbelregleringen för produkter som omfattas av bilaga I, avsnitt B.[1]

1 Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens, sidan 124

Vad är ett AI-system?

Definition: 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 de indata det tar emot, om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras.

Det är inte helt lätt att i lagtext definiera vad ett AI-system är, men den definition som är formulerad i AIA är central för att veta vad AIA reglerar. Helt klart är att programvara och algoritmiskt beslutsfattande inte generellt omfattas av lagen. AIA gäller en specifik typ av programvara, nämligen AI och konsekvenserna av AI-systemen. Fokus ligger inte bara på vilka beslut eller annan output som AI-systemet levererar, utan på resultat i en mer allmän mening. AIA reglerar inte hur AI-system ska skapas, utan den påverkan som sker genom AI-systemets leverans.

För företag som gör affärer utanför EU kan det vara bra att känna till att AIA-definitionen motsvarar OECD:s definition av AI-system:

An AI system is a machine-based system that can, for an explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

AI-teknik omfattar många olika tillvägagångssätt

Generativ AI är en teknik som fokuserar på att skapa nytt innehåll och används till exempel för text-, bild- och filmskapande, medan annan AI-teknik snarare gör förutsägelser eller klassificerar och sorterar befintliga data. Dessa AI-tekniker är bland annat maskininlärning (ML) med underkategorin djupinlärning (DL) som används till exempel i tjänster som Siri, Google Translate och bildigenkänning.

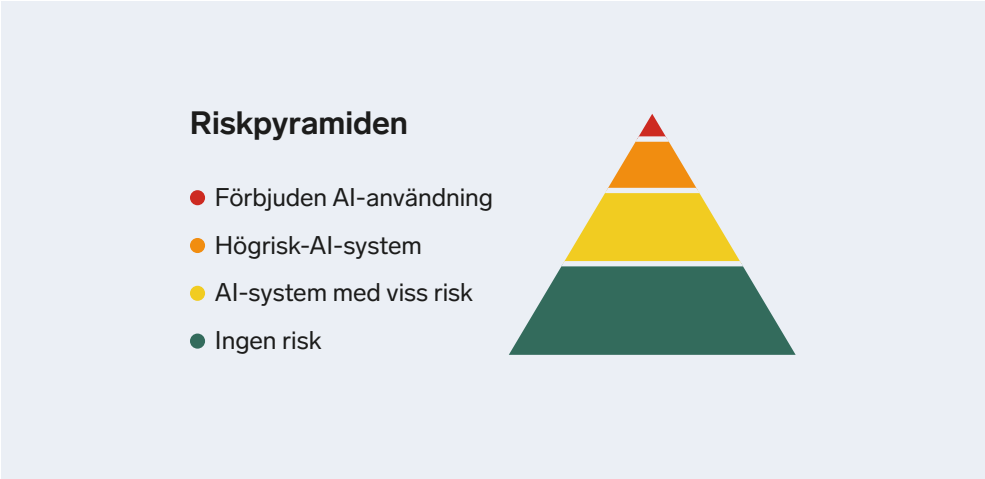
Riskindelning av AI-användning

AIA sorterar AI-system och modeller efter hur riskfyllda de anses vara. Beroende på risknivån finns olika regler att följa. Det är av vikt för såväl utvecklare som användare av AI-system att veta vilken risknivå deras system tillhör eftersom det styr vilka krav som ställs.

AI-systemens fyra risknivåer är

1. oacceptabel risk som blir förbjuden
2. hög risk som medför ett antal krav både på AI-systemleverantörer och produkt- och tjänsteleverantörer där högrisksystem ingår samt användare

3. AI-modeller och system med viss risk som medför krav på
   - information till den som interagerar med ett AI-system, till exempel en chattbot
   - märkning i maskinläsbart format när AI-systems utdata är syntetiskt ljud-, bild-, video- eller textinnehåll som är artificiellt genererat eller manipulerat
   - att informera personer som exponeras för AI-system för känsloigenkänning eller biometrisk kategorisering om systemets drift
   - upplysning om innehåll som är så kallade deepfakes (om innehållet utgör en del av ett uppenbart konstnärligt, kreativt, satiriskt, skönlitterärt eller liknande verk eller program, begränsas transparenskraven till att upplysa om förekomsten av sådant genererat eller manipulerat innehåll på ett lämpligt sätt som inte hindrar visningen eller åtnjutandet av verket)
   - upplysning om text som offentliggörs i syfte att informera allmänheten om frågor av allmänt intresse har genererats artificiellt eller manipulerats
4. ingen eller minimal risk som inte medför några krav, men leverantörer av sådana system kan ändå välja att följa reglerna på frivillig basis.



Vad är en AI-modell?

AI-modeller utgör inte ett AI-system i sig utan är vanligtvis integrerade i och utgör en del av ett AI-system. En AI-modell kräver tillägg av ytterligare komponenter, till exempel ett användargränssnitt, för att bli ett AI-system.

AI-modeller tränas vanligtvis med stora mängder data. Det är AI-modeller för allmänna ändamål som regleras av AIA och de ska uppvisa betydande generalitet och kunna utföra ett brett spektrum av uppgifter och kunna integreras i en rad system eller tillämpningar.

Generativa AI-modeller kan inte bara bearbeta och analysera enorma mängder data utan även generera nytt innehåll baserat på de mönster och den kunskap de har lärt sig av de data de tränats på.

AI-modeller som används för forsknings-, utvecklings- eller prototypverksamhet innan de släpps ut på marknaden behöver inte följa AIA.

Datum för när olika delar av AIA börjar gälla

Datum	Vad gäller då?
1 augusti 2024	AIA träder i kraft.
1 februari 2025 6 månader efter ikraftträdande	**Förbud införs mot AI med oacceptabel risk.** Förbudet gäller även system som tidigare tagits i bruk.
1 augusti 2025 12 månader efter ikraftträdande	**Särskilda regler för nya AI-modeller** för allmänna ändamål samt AI-modeller för allmänna ändamål med systemrisk börjar gälla, med undantag för böter för leverantörer av dessa modeller. Modeller som innan detta datum släppts ut på marknaden ska uppfylla kraven inom tre år, senast sensommaren 2027.
1 augusti 2026 24 månader efter ikraftträdande	**AIA börjar gälla generellt,** till exempel regler för AI system med viss risk och **nya AI-system som används inom högriskområden** listade i bilaga III. AIA **omfattar inte AI-system med hög risk som tagits i bruk eller släppts ut på marknaden före detta datum** (augusti 2026), såvida inte en större ändring av systemet har gjorts därefter.
1 augusti 2027 36 månader efter ikraftträdande	**Regler för högrisk-AI-system som finns i nytillverkade produkter** som regleras i sektorspecifik produktsäkerhetslagstiftning börjar gälla, till exempel i leksaker, hissar och maskiner, se AIA, bilaga I, avsnitt A. Skyldigheter kommer att konkretiseras och specificeras i harmoniserade standarder som produkterna förväntas efterleva. Olika produkter som motorfordon, luftfartyg och marin utrustning som omfattas av lagar som förtecknas i AIA, bilaga I, avsnitt B, regleras huvudsakligen av sektorspecifik lagstiftning.
2030	**Offentlig sektors gamla högrisk-AI system,** enligt bilagorna I och III, måste uppfylla kraven sex år efter ikraftträdandet, 1 augusti 2030, artikel 111.2. **Storskaliga IT-system** inom området frihet, säkerhet och rättvisa, som tagits i bruk eller släppts ut på marknaden före augusti 2027 och som förtecknas i bilaga X måste uppfylla vissa krav i AIA senast den 31 december 2030, artikel 111.1. Ett exempel är Schengens informationssystem.

Vem berörs av reglerna?

AIA ställer främst krav på de som utvecklar AI-modeller och system i EU och i tredje land, det vill säga utanför EU. I vissa fall berörs även de som importerar, säljer och använder AI-systemen. Aktörerna som åläggs skyldigheter kallas operatörer och kan vara en leverantör, en produkttillverkare som använder AI-system i sina produkter, en tillhandahållare, ett ombud, en importör eller en distributör. Nedan återfinns en redogörelse av de mest centrala aktörerna som omfattas samt deras huvudsakliga skyldigheter enligt AI-förordningen.

Leverantör: Den som utvecklat ett AI-system eller en AI-modell för allmänna ändamål och släpper ut systemet eller modellen på marknaden, eller tar systemet i bruk i eget namn eller varumärke. Leverantören ska säkerställa att deras AI-system eller AI-modell uppfyller kraven i förordningen.

Tillhandahållare: Den som använder ett AI-system under sin egen tillsyn, förutom när detta sker för personligt och privat bruk. Tillhandahållare ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att systemet används på ett korrekt sätt.

Distributör: En fysisk eller juridisk person i leveranskedjan som tillhandahåller ett AI-system på unionsmarknaden. Distributören ska bland annat kontrollera att importören och leverantören uppfyller sina krav enligt förordningen.

Importör: Den som släpper ut ett AI-system på marknaden och som bär namn eller varumärke för en fysisk eller juridisk person som är etablerad i tredje land. Importören ska kontrollera att leverantören uppfyller kraven i förordningen. Därutöver ska importören, om det finns skäl att tro att förordningens krav inte är uppfyllda, bland annat hindra att systemet släpps ut på marknaden samt informera ansvarig myndighet.

Checklista – regelefterlevnad

Här är en checklista i fem steg för leverantörer av AI-system och AI-modeller för att kontrollera att de uppfyller AIA.

Kraven gäller från början för nya AI-system och modeller som ska släppas ut på marknaden eller tas i bruk, och med viss tidsfrist för vissa AI-system som redan finns på marknaden. För sådan AI är systemets typ avgörande för om AIA gäller.

AI-system som är komponenter i vissa stora it-system som tidigare har släppts ut på marknaden måste innan 2031 följa kraven i förordningen. Motsvarande gäller för AI-modeller för allmänna ändamål som måste följa kraven till sommaren 2027.

För högrisk-AI-system som tidigare är tagna i bruk är AIA enbart tillämplig ifall systemet förändras betydligt i sin utformning efter det att AIA generellt börjat tillämpas sommaren 2026.

Offentlig sektors användning av gamla högrisk-AI-system måste från 2030 följa AIA:s regler.

Inga undantag gäller dock de AI-system som innebär en oacceptabel risk och är förbjudna enligt AI-förordningen. De förbjudna systemen ska fasas ut under 2024 och får sedan inte användas. Notera dock att vissa förbjudna AI-system kan få användas i undantagsfall, som till exempel vid sökning av försvunna barn.

Inom vilken risknivå klassificeras AI?

1. Oacceptabel risk

AI-system med oacceptabel risk är helt förbjudna enligt förordningen. Denna risknivå berör ett begränsat antal AI-system:

- AI som använder dolda eller vilseledande tekniker för att påverka människors beslut och orsaka skada
- AI som utnyttjar sårbarheter hos personer på ett otillbörligt sätt som orsakar skada
- AI som poängsätter individer på ett sätt som leder till skadlig eller ogynnsam behandling
- AI som används för brottsprofileringsändamål utan stöd av objektiva fakta med direkt koppling till brottslig verksamhet
- AI som skapar ansiktsigenkänningsdatabaser genom att inhämta bilder från internet eller från övervakningskameror
- AI som tolkar känslor på arbetsplatsen eller skolor och universitet, utom för medicinska eller säkerhetsskäl
- AI som kategoriserar personer biometriskt för att dra slutsatser om deras känsliga personuppgifter, bland annat etnicitet, sexuell läggning eller politiska åsikter
- biometrisk fjärridentifiering på allmänna platser i brottsbekämpande syfte, med strikta undantag för vissa allvarliga brott.

2. Hög risk

AI-system med hög risk är tillåtna, men endast om de uppfyller vissa tvingande krav. Det beror på att dessa system anses medföra en hög risk för fysiska personers hälsa, säkerhet eller grundläggande rättigheter. Sådana AI-system måste bedömas dels innan de släpps ut på marknaden eller tas i bruk, dels löpande för att säkerställa ett de fortsättningsvis uppfyller kraven i AI-förordningen. Det finns två kategorier av AI-system med hög risk:

Kategori 1 – AI-system som regleras av annan produktsäkerhetslagstiftning

Denna kategori innefattar AI-system som används som en säkerhetskomponent i en produkt, eller i sig är en produkt som redan regleras av EU-lagstiftning som uppräknas i bilaga I till AI-förordningen och som genom annan lag måste genomgå en tredjeparts-bedömning av överensstämmelse för att produkten ska få släppas ut på marknaden eller tas i bruk.

Exempel: hissar, olika fordon, medicintekniska produkter och leksaker.

Kategori 2 – AI-system som används inom vissa, specifikt angivna områden

Denna kategori innefattar AI-system som används inom områden listade i bilaga III till AIA. I bilaga III finns idag åtta områden där användningen av AI-systemens resultat medför signifikant risk som är identifierad som hög risk

1. biometrisk kategorisering, igenkänning eller fjärridentifiering (till exempel ansiktsigenkänning)
2. kritisk infrastruktur (till exempel kritisk digital infrastruktur, inom vägtrafik och infrastruktur som rör försörjning av vatten, gas, värme och el)
3. utbildning och yrkesutbildning (till exempel för antagning eller betygsättning)
4. anställning, arbetsledning och tillgång till egenföretagande (detta innefattar system avsedda för rekrytering eller urval av personer, särskilt för publicering av riktade platsannonser, analys och filtrering av platsansökningar samt utvärdering av kandidater. Därutöver inkluderas AI-system avsedda att användas för att fatta beslut som påverkar villkor för arbetsrelaterade förhållanden, befordringar och uppsägningar av arbetsrelaterade avtalsförhållanden, för uppgiftsfördelning baserat på individuellt beteende eller personlighetsdrag, och för övervakning och utvärdering av prestationer och beteende inom sådana förhållanden)[2]
5. tillgång till väsentliga privata och offentliga tjänster och förmåner: hälso- och sjukvård, utvärdering av kreditvärdighet för fysiska personer samt riskbedömning, prissättning i fråga om liv- och sjukförsäkringar och utvärdering och klassificering av nödsamtal
6. vissa system som används inom brottsbekämpning (till exempel lögndetektorer, bevisvärdering, prediktiv analys och profilering)
7. migration, analys och gränskontroll (bland annat bevisvärdering, biometrisk igenkänning och lögndetektorer)
8. rättskipning och demokratiska processer (till exempel inom domstolar och val).

När man bedömer om ett AI-system är högrisk ska man titta på dess syfte. Kommissionen kan lägga till fler system om de kan skada hälsa, säkerhet eller grundläggande rättigheter.

Vissa AI-system som används inom de åtta områdena ovan är trots allt inte högrisk-klassade, förutsatt att något av följande kriterier är uppfyllt:

- De utför en snäv processuell uppgift.
- De förbättrar resultatet av tidigare mänsklig verksamhet.
- De upptäcker beslutsmönster eller avvikelser från tidigare beslutsmönster och är inte avsedda att ersätta eller påverka tidigare slutförd mänsklig bedömning.
- De utför en förberedande uppgift som är relevant för de listade högrisksystemen.

Det ska dock noteras att ett AI-system alltid är att anse som ett högrisksystem om det profilerar fysiska personer.

2 Det räcker att AI-systemet används som beslutsstöd i och med att det används för att fatta beslut, enligt målet SCHUFA C-634/21. Där konstaterades att förberedande beslut i sig är att beakta som beslut enligt artikel 22 GDPR. Det räcker inte att en människa formellt tar beslutet utan att själv göra en självständig bedömning.

3. Vissa risker

Denna risknivå gäller AI-system som interagerar med personer och därför åläggs vissa krav på information och transparens. Exempel är chattbottar och generativa AI-verktyg som kan generera bilder, ljud och video. Dessa system omfattas av särskilda transparensskyldigheter:

1. AI-system som är utformade för att interagera med fysiska personer
2. AI-system för känsloigenkänning eller system för biometrisk kategorisering
3. AI-system som genererar eller ändrar text, bilder, ljud eller video för att skapa nytt innehåll.

Informationskraven är till för att enskilda ska vara medvetna om användningen av AI-systemet, eller att innehållet är AI-genererat (till exempel så kallade deepfakes). Dessa krav omfattar inte bara leverantörer, utan även de som använder AI-systemen. Observera att även högrisksystem kan omfattas av dessa krav, och då gäller transparenskraven även för de AI-systemen.

Exempel på AI-system med viss risk: Generativa AI-verktyg och ”chattbottar”. Det ska framgå för användare att materialet är AI-skapat eller att de interagerar med AI och inte med en fysisk person.

4. Ingen eller minimal risk

Denna risknivå berör sådana AI-system som utgör en så låg risk att den är minimal eller till och med obefintlig. Här återfinns den stora majoriteten av AI-system som hitintills använts. Framför allt hör traditionell och smal AI till denna grupp. Dessa AI-system får utvecklas och användas utan några rättsliga skyldigheter enligt AIA. Leverantörerna av sådana system kan däremot välja att frivilligt tillämpa kraven för att erhålla en beteckning om tillförlitlig AI, samt ansluta sig till frivilliga uppförandekoder. Ibland kan dock vissa kunder kräva att leverantörer av AI-system trots allt åtar sig att följa kraven.

Exempel på AI-system med minimal risk: spamfilter, AI i dataspel, transkribering av möten, automatiska kalenderbokningar, sortering av mejl, rättstavningsprogram, strukturering av filer med mera.

5. AI-modeller för allmänna ändamål med systemrisk

AI-modeller för allmänna ändamål berörs av särskilda regler i AIA. De generella kraven innefattar främst krav på transparens, såsom tillhandahållande av teknisk dokumentation, samt en skyldighet att informera när material är skapat av AI. Därutöver behöver leverantörer av AI-modeller för allmänna ändamål sammanställa och offentliggöra vilket upphovsrättsligt skyddat material som har använts för att träna upp AI-modellen.

AI-modeller för generella ändamål med systemrisk är så stora att de åläggs särskilda krav. Det avgörande för om en modell anses medföra systemrisker är ifall den har lärts upp med en beräkningskraft på över 10^25 flyttalsoperationer per sekund. För leverantörer av sådana system uppställs högre krav, bland annat ska de bedöma och begränsa risker samt utföra modellutvärderingar och säkerställa cybersäkerhet. I dagsläget beräknas endast två modeller uppnå detta tröskelvärde: Open AI:s GPT och Googles Gemini.

6. AI-modeller för allmänna ändamål (General Purpose AI Models)

AI-modeller för allmänna ändamål berörs av särskilda regler i AIA. De generella kraven innefattar främst krav på transparens, såsom tillhandahållande av teknisk dokumentation, samt en skyldighet att informera när material är skapat av AI. Därutöver behöver leverantörer av AI-modeller för allmänna ändamål sammanställa och offentliggöra vilket upphovsrättsligt skyddat material som har använts för att träna upp AI-modellen.

Undantag: En stor del av de särskilda reglerna för AI-modeller för allmänna ändamål gäller inte för sådana modeller som släpps ut kostnadsfritt med öppen källkod.

Vilka åtgärder krävs för olika risknivåer?

- Hög risk:
  - Om systemet klassificeras som ett högrisksystem måste det följa de tio stegen i checklistan på sidan 16 innan det släpps ut på marknaden eller tas i bruk.
- Viss risk:
  - Om systemet klassificeras som ett system som medför vissa risker uppställs krav på transparens och information, till exempel att det tydligt framgår för användare att de interagerar med ett AI-system och inte en fysisk person.
- Minimal risk:
  - System som utgör minimal risk får ansluta sig till frivilliga uppförandekoder – men i övrigt uppställer regleringen inga rättsliga förpliktelser för dessa system.
- AI-modeller för allmänna ändamål:
  - Om modellen klassificeras som en vanlig AI-modell för allmänna ändamål, det vill säga utan systemrisk, uppställs krav på att tillhandahålla teknisk dokumentation, att införa en policy för att följa unionens upphovsrättslag-stiftning samt att sammanfatta och tillgängliggöra information om hur modellen har tränats upp.
  - Om modellen klassificeras som en AI-modell för allmänna ändamål som medför systemrisk uppställs utöver det ovannämnda även krav på modellutvärdering, riskbedömning och riskminimering samt att säkerställa cybersäkerhet.

Om AI-systemet är att anse som högrisksystem

Krav för leverantörer

Om AI-systemet klassificeras som ett högrisksystem måste systemet uppfylla ett antal krav; se checklista på nästa sida. När dessa tio krav är uppfyllda kan AI-systemet släppas ut på marknaden eller tas i bruk. På motsatt vis måste leverantörer – som anser att deras AI-system som faller under områden listade i AI-förordningens förteckning över AI-system med hög risk trots allt inte utgör ett högrisksystem – göra samt dokumentera en riskbedömning innan de släpper ut systemet på marknaden. Varje distributör, importör, tillhandahållare eller annan tredje part kommer att klassas som en leverantör om de förser ett AI-system med sitt namn eller varumärke, eller om de gör väsentliga ändringar av AI-system med hög risk.

CHECKLISTA – Tio krav för leverantörer av AI-system med hög risk

- [ ] **1. Riskhanteringssystem**
  Ett riskhanteringssystem för AI-systemet ska inrättas för att identifiera, analysera och åtgärda risker med systemet.
- [ ] **2. Metoder för hantering av data och dataförvaltning**
  Dessa metoder ska säkerställa bland annat att de data som används är lämpliga för ändamålet, spårbara och klassificerade. Särskilda krav gäller för känsliga uppgifter.
- [ ] **3. Teknisk dokumentation**
  Teknisk dokumentation för att demonstrera att systemet uppfyller kraven i AI-rättsakten behöver upprättas. Denna tekniska dokumentation ska sedan hållas uppdaterad under systemets livscykel.
- [ ] **4. Arkivering och transparens**
  Leverantörer behöver förse användarna med korrekt och tydlig information om AI-systemet, bland annat avseende prestanda, avsedda ändamål och eventuella risker med användningen. Därutöver finns det krav på att logga och registrera relevanta händelser.
- [ ] **5. Mänsklig tillsyn**
  Fysiska personer ska kunna kontrollera hur systemet fungerar.
- [ ] **6. Noggrannhet, robusthet och cybersäkerhet**
  Systemen ska vara motståndskraftiga mot felaktigheter, funktionsfel och inkonsekvenser.
- [ ] **7. Kvalitetsstyrningssystem**
  Kvalitetsstyrningssystemet ska innefatta strategier för efterlevnad av regelverket, utveckling, undersökningar och tester, riskhantering, övervakning, datahantering och incidentrapportering.

- [ ] **8. EU-försäkran om överensstämmelse och informationsplikt**
Leverantören ska upprätta en skriftlig EU-försäkran om överensstämmelse för AI-systemet och kunna uppvisa den för de nationella myndigheterna i tio år efter det att systemet har släppts ut på marknaden eller tagits i bruk. Finns det skäl att tro att kraven inte uppfylls måste leverantören åtgärda problemen omedelbart och informera användarna.

- [ ] **9. CE-märkning om överensstämmelse**
En synlig CE-märkning ska placeras på AI-systemet. För AI-system som är integrerade i en fysisk produkt bör en CE-märkning placeras på produkten som kan kompletteras med en digital CE-märkning, medan enbart digitala AI-system förses med digitala CE-märkningar.

- [ ] **10. Registreringsåtgärder**
Innan ett AI-system med hög risk släpps ut på marknaden eller tas i bruk ska leverantören registrera detta system i en EU-databas.

Harmoniserade standarder

Ett viktigt komplement till AI-förordningen är införandet av harmoniserade standarder på EU-nivå. Dessa utvecklas av de europeiska standardiseringsorganisationerna för att underlätta tolkningen av AI-förordningen, och avser att förtydliga och exemplifiera hur kraven i rättsakten kan tolkas på en detaljerad, mer teknisk nivå. När ett AI-system med hög risk eller en AI-modell för allmänt ändamål överensstämmer med relevanta harmoniserade standarder föreligger en presumtion om att systemet uppfyller kraven i AI-förordningen. Detta innebär att även om AI-förordningen inte uppställer krav på att systemen måste uppfylla de harmoniserade standarderna, så kommer leverantören av sådana system sannolikt stödja sig och vara beroende av dem. Detta då specifikationerna utgör ett säkert kort för vägledning till hur AI-förordningen kommer att tolkas i praktiken. De harmoniserade standarderna utgör därmed ett verktyg för leverantörer av AI-system för att säkerställa att de efterlever kraven i förordningen.

Krav för tillhandahållare

Det är inte bara leverantörer av AI-system med hög risk som omfattas av krav. Även de som köper in och använder AI-system och är tillhandahållare enligt förordningen, behöver uppfylla vissa krav då de använder AI-system med hög risk. Framför allt ska de ha system på plats för att fånga upp eventuella risker med användningen av AI-systemet, och i så fall informera både leverantören och marknadskontrollsmyndigheten.

CHECKLISTA – Sju krav för tillhandahållare av AI-system med hög risk

- [ ] **1. Följa bruksanvisningen**
  Tillhandahållare behöver vidta lämpliga åtgärder för att säkerställa att de följer systemets bruksanvisningar.
- [ ] **2. Säkra tillräcklig kompetens**
  De som använder systemen ska ha nödvändig kompetens, utbildning och auktoritet för att utöva mänsklig tillsyn.
- [ ] **3. Informera leverantören och myndigheter om risker**
  Om tillhandahållaren identifierar en risk för hälsa, säkerhet eller grundläggande rättigheter ska de informera leverantören eller distributören och marknadskontrollsmyndigheten om risken.
- [ ] **4. Spara loggar**
  De loggar som genereras automatiskt ska sparas i sex månader.
- [ ] **5. Informera arbetstagare om AI på arbetsplatsen**
  Arbetstagare och deras representanter ska informeras om de blir föremål för AI-system med hög risk.
- [ ] **6. Informera om automatiserat beslutsfattande**
  De som blir föremål för automatiserat beslutsfattande har rätt att bli informerade.
- [ ] **7. Konsekvensbedömning avseende grundläggande rättigheter**
  Tillhandahållare behöver bedöma hur systemet inverkar på grundläggande rättigheter. Marknadskontrollsmyndigheten ska underrättas om resultatet.

Att följa lagstiftningen; hjälp, rättigheter, sanktioner m.m.

Hjälp med regelefterlevnad

- Regulatoriska sandlådor för AI:
  - Medlemsstaterna ska säkerställa att minst en regulatorisk sandlåda för AI inrättas på nationell nivå.
  - De regulatoriska sandlådorna för AI ska tillhandahålla en kontrollerad miljö som främjar innovation och underlättar utveckling, träning, testning och validering av AI-system under en begränsad tid innan de släpps ut på marknaden.
- Riktlinjer och exempel. EU-kommissionen ska bland annat tillhandahålla riktlinjer som
  - specificerar hur AI-system klassas som hög risk och även inkludera praktiska exempel på system som faller innanför respektive utanför högrisk-klassificeringen
  - preciserar hur kraven på AI-system med hög risk ska efterlevas
  - redogör för de förenklade kvalitetsstyrningssystem som mikroföretag kan följa
  - specificerar hur incidentrapportering ska gå till
  - redogör för hur transparensskyldigheterna ska uppfyllas.
- Standarder (se ovan):
  - AI-system som tillämpat harmoniserande standarder förutsätts överensstämma med kraven som ställs på högrisksystem – i den mån dessa standarder omfattar dessa krav eller skyldigheter.
  - Standarder som utvecklas i de olika sektorerna måste vara tydliga och samstämmiga så att företag vet hur kraven och skyldigheterna ska efterlevas.
- Vissa åtgärder för småskaliga leverantörer och tillhandahållare:
  - Små och medelstora företag[3], inbegripet uppstartsföretag, bör få prioriterad åtkomst till de regulatoriska sandlådorna för AI.
  - Mikroföretag bör kunna inrätta förenklade kvalitetsstyrningssystem.
  - Myndigheter ska sprida information om tillämpningen av AI-förordningen som är anpassad till behoven hos småskaliga leverantörer och tillhandahållare.
  - Myndigheter ska vägleda och kommunicera med småskaliga leverantörer, tillhandahållare och andra innovatörer.
  - Sanktionsavgifters storlek bedöms enligt en särskild måttstock där deras intressen och ekonomiska bärkraft ska beaktas.

3 Mikroföretag samt små och medelstora företag (SMF) är företag som sysselsätter färre än 250 personer och vars årsomsättning inte överstiger 50 miljoner euro eller vars balansomslutning inte överstiger 43 miljoner euro per år.

Rättigheter för individer

- Rätt att lämna in klagomål:
  - Var och en som har skäl att anse att AI-förordningen har överträtts har rätt att lämna in klagomål till den berörda marknadskontrollsmyndigheten.
- Rätt till förklaring av individuellt beslutsfattande:
  - Varje berörd person som är föremål för automatiserat beslutsfattande av ett högrisksystem, och som har rättslig eller motsvarande verkan på den personen på ett negativt sätt, har rätt att få förklaringar av AI-systemets roll i beslutsprocessen.

Sanktionsavgifter vid regelbrott

Vid bristande uppfyllnad av AI-förordningen uppställs tre olika sanktionsavgifter, beroende på vilken typ av överträdelse av förordningen det är fråga om.

Bristande efterlevnad av reglerna avseende förbjudna AI-system

Om ett företag släpper ut förbjudna AI-system på marknaden kan det medföra sanktionsavgifter på upp till 35 miljoner euro eller 7 procent av den totala globala omsättningen under föregående räkenskapsår, beroende på vilket som är högst.

Bristande efterlevnad av andra krav enligt förordningen

Om leverantören eller, i tillämpliga fall, tillhandahållaren brister i efterlevnad av andra krav kan det medföra sanktionsavgifter på upp till 15 miljoner euro eller 3 procent av den totala globala omsättningen under föregående räkenskapsår, beroende på vilket som är högst.

Tillhandahållande av felaktig information

Om ofullständig, felaktig eller falsk information lämnas till anmälda organ och nationella myndigheter som svar på begäran kan detta medföra sanktionsavgifter på upp till 7,5 miljoner euro eller 1 procent av den totala globala omsättningen under föregående räkenskapsår, beroende på vilket som är högst.

Små och medelstora företag: Vad gäller små och medelstora företag, inbegripet uppstartsföretag, gäller särskilda utgångspunkter vid bedömning av sanktionsavgift. Samma procentsatser och belopp som stadgas ovan gäller, men det avgörande blir i stället vilket av de två som är *lägst.*

Förhållandet mellan AI-förordningen och annan lagstiftning

AI-förordningen och dataskyddsförordningen, GDPR

AIA och GDPR har en nära koppling, särskilt vad gäller AI som tränas upp på personuppgifter. Leverantörer av sådana system eller modeller måste därför förhålla sig till båda regelverken. Värt att notera är att GDPR alltid gäller. En betydande skillnad mellan tillämpningen av de två regelverken är att AIA undantar forskning och utveckling av AI, varför dessa områden är undantagna från AIAs tillämplighet. Dessa undantag finns inte i GDPR, utan där blir reglerna alltjämt gällande vid AI-utveckling. Sverige saknar ett generellt FoU-undantag för behandling av känsliga personuppgifter vilket gör det mer komplicerat än i andra länder att använda dessa uppgifter för träning av AI-systemen. För att få använda känsliga personuppgifter behöver de registrerades samtycke inhämtas även vid forskning och utveckling av AI.

I övrigt utgör kraven i AI-förordningen inte någon rättslig grund för behandling av personuppgifter, vilket innebär att utvecklare av AI-system och AI-modeller behöver säkerställa att det finns en rättslig grund enligt GDPR för behandlingen inom ramen för utvecklingen och testningen av AI-systemet eller AI-modellen. I skälen till AIA preciseras det dock att det är möjligt att förlita sig på den rättsliga grunden ”viktigt allmänt intresse” som anges i artikel 9.2 g i GDPR för att upptäcka och korrigera bias i högrisksystem. Detta undantag ska tolkas väldigt restriktivt och är endast tillämpligt om det är ”absolut nödvändigt”.

AIA ställer krav på transparens gentemot de som berörs av AI-system, men GDPR ställer generella krav på informationsgivning som kan påverka både leverantörers och tillhandahållares skyldigheter att informera individer om hur personuppgifter används av AI-system. Vissa tillsynsmyndigheter, till exempel den italienska dataskyddsmyndigheten, anser även att artikel 13–14 i GDPR uppställer krav på att individer dessutom har rätt att ta del av logiken bakom AI-system. Om denna tolkning etableras inom EU skulle det innebära att GDPR indirekt uppställer krav på att logiken bakom ett AI-system ska kunna förklaras för användarna, och speciellt för de registrerade vars personuppgifter använts för att träna upp systemet.

AIA påverkar inte de skyldigheter som leverantörer av AI-system har enligt GDPR. Däremot innehåller AIA i sin tur särskilda krav då AI-systemen behandlar vissa personuppgifter, och speciellt känsliga sådana. AIA kräver till exempel att känsliga personuppgifter inte får göras tillgängliga för andra parter. En annan koppling är att AI-system i många fall behöver analyseras i en konsekvensbedömning enligt GDPR, och denna bedömning kan ligga till grund för konsekvensbedömningen avseende grundläggande rättigheter som behöver upprättas för AI-system med hög risk och som används inom offentlig sektor.

AI-förordningen och upphovsrätt

Upphovsrättsliga frågor aktualiseras då AI-modeller tränas upp på material som andra äger rätten till, så kallad proprietära data. Oftast är det då fråga om upphovsrättsskyddat material, men även hela databaser kan vara skyddade enligt databasrätten. AIA ställer krav på leverantörer av AI-modeller för allmänna ändamål att sammanställa en sammanfattning av det innehåll som används för träning av AI-modellen, samt en skyldighet att införa en policy för efterlevnad av bland annat upphovsrättsdirektivet (som i Sverige genomförts genom upphovsrättslagen).

www.svensktnaringsliv.se
Storgatan 19, 114 82 Stockholm
Telefon 08-553 430 00