Physical AI och regelefterlevnad i EU

Georgia & Molly | September *2026*

En sammanfattande genomgång av tillämplig AI-, produktsäkerhets-, cybersäkerhets- och dataskyddsreglering för uppkopplade fysiska produkter med AI-komponenter

BAKGRUND OCH SYFTE

Denna artikel sammanfattar en juridisk genomgång som behandlar regelefterlevnad för produkter som marknadsförs under begreppet "Physical AI" – fysiska produkter, såsom robotar, drönare, industrimaskiner och konsumentelektronik, som innehåller AI-komponenter och i vissa fall är uppkopplade till nätverk. Genomgången är avgränsad till EU-rätten, med särskilt fokus på AI-förordningen, maskinförordningen, cyberresiliensakten och GDPR.

1. VAD ÄR PHYSICAL AI?

"Physical AI" är inte en definierad juridisk term i EU:s regelverk, utan ett branschbegrepp för AI-system som är fysiskt förkroppsligade och agerar i den verkliga världen – robotar, autonoma fordon, drönare och andra fysiska produkter som använder AI för att uppfatta sin omgivning och agera i den. Detta skiljer sig från "digital AI", som producerar text, bilder eller rekommendationer i en digital miljö utan fysisk verkan.

Eftersom termen saknar egen juridisk status måste den rättsliga bedömningen i stället utgå från EU:s AI-förordning (Regulation (EU) 2024/1689), som definierar ett "AI-system" på ett teknikneutralt sätt: ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi och som, utifrån de indata det tar emot, kan generera utfall som prognoser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer. Denna definition omfattar alltså både digital AI och Physical AI som samma juridiska kategori.

Physical AI-produkter fångas i praktiken upp av flera samverkande regelverk: AI-förordningens riskklassificering, maskinförordningen (för maskiner och robotar), cyberresiliensakten (för uppkopplade produkter), produktansvarsdirektivet, samt sektorsspecifik lagstiftning som radioutrustningsdirektivet, EMC-direktivet och lågspänningsdirektivet.

2. AI-FÖRORDNINGEN: KLASSIFICERING OCH RISKBEDÖMNING

AI-förordningen följer en riskbaserad modell där högre risk för skada utlöser strängare krav. Två separata vägar leder till högriskklassificering: dels artikel 6(1), som gäller AI-system som är säkerhetskomponenter i eller själva utgör produkter som omfattas av harmoniseringslagstiftning i bilaga I, dels artikel 6(2), som gäller fristående AI-system förtecknade i bilaga III (till exempel biometri, rekrytering och kreditbedömning), oavsett koppling till en fysisk produkt. Endast den första vägen är direkt relevant för Physical AI i egentlig mening.

En "säkerhetskomponent" definieras i artikel 3(14) som en komponent i en produkt eller i ett AI-system som fyller en säkerhetsfunktion, eller vars fel eller felfunktion äventyrar människors hälsa och säkerhet eller egendom. En komponent fyller en säkerhetsfunktion när dess avsedda syfte är att förebygga eller minska sådana risker. Genom Digital Omnibus on AI (Regulation (EU) 2026/1744) förtydligades att enbart det förhållandet att ett AI-system är integrerat i en produkt som omfattas av harmoniseringslagstiftning inte i sig gör det till en säkerhetskomponent, och att AI-system som enbart används för användarstöd, prestandaoptimering eller bekvämlighet inte räknas som säkerhetskomponenter – såvida inte deras fel eller felfunktion skulle äventyra hälsa och säkerhet, i vilket fall de alltid räknas som säkerhetskomponenter.

2.1 Maskininlärningens och adaptivitetens roll i klassificeringen

Maskininlärning och adaptivitet är inte i sig avgörande för klassificeringen. Adaptivitet (förmågan att uppvisa anpassningsförmåga efter driftsättning) är enligt AI-systemdefinitionen en möjlig men inte nödvändig egenskap – ett statiskt, färdigtränat system kan fortfarande vara ett AI-system om det infererar utfall från indata. Klassificeringen som högrisk styrs i stället av säkerhetsfunktionen: en icke-adaptiv AI-modell som styr en säkerhetskritisk funktion kan vara en säkerhetskomponent, medan en kontinuerligt lärande men rent bekvämlighetsinriktad funktion kan vara helt undantagen.

Av samma anledning räcker det i regel inte att stänga av inlärningsfunktionen för att undvika reglering. AI-status kräver inte aktiv inlärning, och högriskklassificeringen styrs av säkerhetsfunktionen och risken vid felfunktion, som normalt kvarstår oförändrad oavsett om den underliggande modellen är statisk eller lärande.

2.2 Exempel: robotdammsugare

En traditionell robotdammsugare som navigerar med fasta, förprogrammerade regler utan inferens från sensordata faller normalt helt utanför AI-förordningens tillämpningsområde. En AI-komponentbaserad robotdammsugare som använder datorseende eller sannolikhetsbaserad rumskartläggning uppfyller sannolikt AI-systemdefinitionen, men blir bara högriskklassificerad om AI-funktionen har ett avsett syfte att förebygga risk (till exempel hinder- eller trappdetektering för att undvika personskada), eller om dess felfunktion skulle äventyra säkerheten – oberoende av om funktionen enbart optimerar städmönster.

3. Tredjepartsbedömning av överensstämmelse

Högriskklassificering enligt artikel 6(1) kräver att två villkor är uppfyllda samtidigt: AI-systemet måste vara en säkerhetskomponent i en produkt som omfattas av harmoniseringslagstiftning i bilaga I, och produkten måste redan kräva tredjepartsbedömning av överensstämmelse enligt den underliggande produktlagstiftningen. Kravet på tredjepartsbedömning härrör alltså alltid från produktlagstiftningen själv – inte från AI-förordningen.

Genom Digital Omnibus on AI förtydligades att klassificeringen som högriskklassificerat AI-system enligt artikel 6(1) inte i sig tvingar fram tredjepartsbedömning: om den underliggande produktlagstiftningen tillåter tillverkarens egen försäkran, gäller detta fortsatt även med ett inbyggt högriskklassificerat AI-system.

För maskiner (inklusive robotar) styrs frågan av maskinförordningen (Regulation (EU) 2023/1230). Maskiner i bilaga I del A – de allvarligaste kategorierna – kräver alltid ett förfarande som involverar ett anmält organ. Maskiner i bilaga I del B kan bedömas genom tillverkarens egen försäkran, förutsatt att produkten är konstruerad enligt tillämpliga harmoniserade standarder; annars krävs ett tredjepartsförfarande. Maskiner som inte finns förtecknade i bilaga I omfattas alltid av intern produktionskontroll utan tredje part. Genom Digital Omnibus on AI flyttades maskinförordningen till avsnitt B i bilaga I till AI-förordningen för att samordna AI-relaterade säkerhetskrav direkt i maskinbedömningen, med tillämpning senast den 2 augusti 2028.

Ett särskilt undantag gäller om tredjepartsbedömning krävs enbart av skäl som inte rör hälsa och säkerhet, exempelvis radiospektrum- eller elektromagnetiska risker – detta räknas inte som att villkoret om tredjepartsbedömning i artikel 6(1) är uppfyllt.

4. CE-märkning och marknadsgodkännande

CE-märkning krävs i praktiken för nästan alla Physical AI-produktkategorier, men detta följer i första hand av den underliggande sektorslagstiftningen snarare än av AI-inslaget som sådant.

Robotar och industrimaskiner som utgör "maskiner" i maskinförordningens mening måste alltid CE-märkas innan de släpps på marknaden eller tas i drift, oavsett AI-innehåll. Drönare (obemannade luftfartsystem) omfattas av förordning (EU) 2019/945, som föreskriver en EU-försäkran om överensstämmelse och CE-märkning enligt viktbaserade riskklasser (C0–C6), med tillhörande klassidentifieringsetikett. Konsumentelektronik omfattas normalt av radioutrustningsdirektivet (om den har radiofunktion), EMC-direktivet och/eller lågspänningsdirektivet, som alla kräver CE-märkning.

AI-förordningen blir relevant för innehållet i CE-bedömningen – snarare än för själva märkningsplikten – när produktens AI-funktion kvalificerar som en säkerhetskomponent: i så fall ska AI-förordningens materiella krav (riskhantering, dokumentation, robusthet, mänsklig tillsyn) införlivas i den befintliga bedömningsprocessen, oavsett om denna sker genom egen försäkran eller ett anmält organ.

4.1 Väsentlig ändring efter tredjepartsleverantörens CE-märkning

När en produkt redan är CE-märkt av en underleverantör men senare modifieras (till exempel genom mjukvaruändringar, tillägg av nya sensorer, eller tillägg av en connectivity-enhet), måste det bedömas om ändringen utgör en "väsentlig ändring" enligt artikel 3(16) i maskinförordningen. Definitionen har fyra kumulativa rekvisit: en ändring genom fysiska eller digitala medel, som sker efter att produkten släppts på marknaden, som inte var förutsedd eller planerad av den ursprungliga tillverkaren, och som skapar en ny risk eller ökar en befintlig risk på ett sätt som kräver tillägg av skyddsanordningar som kräver ändring av säkerhetsstyrsystemet, eller ytterligare stabilitets- eller hållfasthetsåtgärder.

Enligt artikel 18 blir den som utför en väsentlig ändring att betrakta som tillverkare i förordningens mening, med samtliga tillverkarskyldigheter enligt artikel 10 – ny teknisk dokumentation, nytt bedömningsförfarande, ny EU-försäkran om överensstämmelse och ny CE-märkning under eget namn. I en typisk situation med mjukvarumodifiering, nya sensorer och en redan CE-märkt connectivity-enhet är tillägget av säkerhetsrelaterade sensorer den ändring som oftast har störst sannolikhet att utgöra en väsentlig ändring, medan en fristående connectivity-komponent utan koppling till säkerhetsfunktioner har lägre sannolikhet att göra det enligt maskinförordningen – även om den kan utlösa separata skyldigheter enligt cyberresiliensakten. Bedömningen bör göras både för varje enskild ändring och för deras sammantagna effekt.

5. Cyberresiliensakten och uppkopplade produkter

Cyberresiliensakten (Regulation (EU) 2024/2847) gäller "produkter med digitala element" vars avsedda syfte eller rimligen förutsebara användning innefattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nätverk. En uppkopplad robot eller annan fysisk AI-produkt med en connectivity-funktion uppfyller normalt detta kriterium och omfattas därmed av förordningen, såvida inte ett sektorsundantag gäller (medicinteknik, fordonsgodkännande, certifierad civil luftfart, marin utrustning, eller produkter för nationell säkerhet och försvar).

Produkter vars kärnfunktion motsvarar en kategori i bilaga III räknas som "viktiga produkter med digitala element" och omfattas av striktare bedömningsförfaranden – detta gäller funktioner som är kritiska för cybersäkerheten hos andra produkter eller som kan störa, kontrollera eller skada ett stort antal andra produkter eller användares hälsa och säkerhet. Enbart det förhållandet att en sådan komponent integreras i en annan produkt gör dock inte i sig hela produkten till en "viktig produkt". De striktaste kategorierna, "kritiska produkter" enligt bilaga IV, kräver certifiering på hög tillitsnivå och är förbehållna produkter med central betydelse för samhällsviktiga entiteters cybersäkerhet.

Cyberresiliensakten har sin egen definition av "väsentlig ändring", fristående från maskinförordningens – en ändring efter marknadsintroduktion som påverkar överensstämmelsen med de väsentliga cybersäkerhetskraven eller ändrar det avsedda syftet. En ändring (till exempel tillägg av en connectivity-enhet) kan därför utgöra en väsentlig ändring enligt cyberresiliensakten även om den inte gör det enligt maskinförordningen, eftersom bedömningen där avser cybersäkerhetsrisk snarare än fysisk säkerhet.

6. Dataskyddskrav enligt GDPR

Uppkopplade fysiska AI-produkter med sensorer (kameror, mikrofoner, positions- och rörelsedata) samlar ofta in personuppgifter och aktualiserar därmed GDPR. Europeiska dataskyddsstyrelsens vägledning om uppkopplade fordon ger, i avsaknad av robotspecifik vägledning, den närmast tillämpliga referensramen: särskild uppmärksamhet bör ägnas platsdata, biometriska data och data som kan avslöja brott eller överträdelser, eftersom dessa kategorier är särskilt integritetskänsliga.

För varje behandlingsändamål måste en rättslig grund enligt artikel 6 fastställas. Inbyggt dataskydd och dataskydd som standard enligt artikel 25 kräver att den personuppgiftsansvarige, redan i produktens designfas, beaktar behandlingens art, omfattning, sammanhang och syfte samt riskerna för de registrerades rättigheter, och att skyddsåtgärderna hålls uppdaterade i takt med den tekniska utvecklingen ("state of the art"). Praktiska åtgärder som rekommenderas för uppkopplade produkter inkluderar datamminimering, integritetsvänliga standardinställningar, och – där möjligt – lokal databehandling i produkten snarare än överföring till externa system, vilket minskar både integritets- och cybersäkerhetsrisker.

En konsekvensbedömning avseende dataskydd (DPIA) enligt artikel 35 krävs när behandlingen sannolikt innebär en hög risk för registrerades rättigheter och friheter – vilket typiskt är fallet för produkter som kombinerar AI-driven sensorbehandling med fysisk närvaro i hem- eller arbetsmiljöer. Underlåtenhet att genomföra en DPIA när den krävs kan medföra administrativa sanktionsavgifter.

7. Prioriterade compliance-steg

Baserat på genomgången kan arbetet med att introducera en uppkopplad robot med AI-komponent på EU/EES-marknaden struktureras i fyra faser.

7.1 Fas 1 – Grundläggande klassificering

Klassificera AI-komponentens status enligt AI-förordningen (AI-system, säkerhetskomponent), klassificera produkten enligt maskinförordningens bilaga I, klassificera produkten enligt cyberresiliensaktens riskkategorier, och kartlägg all personuppgiftsbehandling med tillhörande rättslig grund.

7.2 Fas 2 – Design och dokumentation

Genomför en integrerad risk- och konsekvensbedömning som samordnat täcker fysisk säkerhet, AI-specifika risker, cybersäkerhet och dataskydd (DPIA), implementera inbyggt dataskydd och säkra standardinställningar, och upprätta teknisk dokumentation som täcker samtliga tillämpliga regelverk.

7.3 Fas 3 – Bedömning av överensstämmelse

Genomför det eller de relevanta bedömningsförfarandena enligt maskinförordningen och cyberresiliensakten, upprätta EU-försäkran om överensstämmelse och anbringa CE-märkning, och registrera produkten i relevanta EU-databaser om den är högriskklassificerad enligt AI-förordningen.

7.4 Fas 4 – Marknadslansering och löpande efterlevnad

Publicera integritetspolicy och användarinformation innan lansering, etablera processer för sårbarhetshantering och incidentrapportering enligt cyberresiliensakten samt personuppgiftsincidenter enligt GDPR, och etablera en process för att bedöma framtida ändringar mot begreppet väsentlig ändring i både maskinförordningen och cyberresiliensakten innan varje uppdatering rullas ut.

Ett viktigt observandum rör tidsplanen: AI-förordningens högriskregler för produktinbäddade AI-system enligt artikel 6(1) och bilaga I tillämpas, efter Digital Omnibus-ändringen, från den 2 augusti 2028, medan grundläggande skyldigheter (till exempel förbud mot vissa AI-metoder och krav på AI-kompetens) redan gäller. Maskinförordningens och cyberresiliensaktens egna tidsplaner löper oberoende av detta.

SAMMANFATTANDE SLUTSATS

Regelefterlevnad för Physical AI-produkter kräver en samordnad bedömning över flera regelverk som var för sig har olika utlösande kriterier och tillämpningsdatum. AI-förordningen adderar materiella krav ovanpå redan existerande produktsäkerhetsregler snarare än att ersätta dem, vilket innebär att den centrala uppgiften för en tillverkare är att korrekt kartlägga vilken kombination av maskinförordningen, cyberresiliensakten, sektorsspecifik produktlagstiftning och GDPR som är tillämplig för den specifika produkten, och att bygga en integrerad – snarare än fragmenterad – process för risk- och konsekvensbedömning, teknisk dokumentation och bedömning av överensstämmelse.

OM DENNA ARTIKEL

Artikeln sammanfattar en juridisk dialog fokuserad på EU-rätt (AI-förordningen 2024/1689, Digital Omnibus on AI 2026/1744, maskinförordningen 2023/1230, cyberresiliensakten 2024/2847, produktansvarsdirektivet 2024/2853, samt GDPR och tillhörande vägledning från Europeiska dataskyddsstyrelsen). Den täcker inte nationell implementeringslagstiftning, myndighetsvägledning från AI-byrån eller nationella tillsynsmyndigheter, eller regelverk utanför EU/EES. Slutsatserna är baserade på en generell produktbeskrivning och bör verifieras mot den specifika produktens tekniska specifikation innan de läggs till grund för en marknadsintroduktion.