

Infrastrukturdepartementet

## Europeiska kommissionens förslag till förordning om harmoniserade regler för artificiell intelligens

### Sammanfattning

Vinnovas övergripande ställningstagande är att förslaget har en rimlig intention och ansats men att det uppvisar brister och otydligheter av sådan karaktär att förslaget med stor sannolikhet får en oproportionell och obalanserad negativ inverkan på EUs konkurrens- och innovationskraft.

### Baserat på förslagens styrkor och svagheter samt lärdomar från liknande processer är Vinnovas övergripande slutsats att Sverige och särskilt Regeringskansliet behöver arbeta för att

- förslaget revideras så att det får en mer ändamålsenlig balans mellan risker och möjligheter.
- rätt förutsättning finns för innovation och sandboxes inom AI-området. Regeringskansliet har en särskilt viktig roll då sandboxes skapar möjligheter för Sverige att ligga i framkant inom EU genom att framstående företag utvecklar innovativa lösningar på ett kontrollerat sätt inom högriskområden.
- säkerställa att stödsystemet är redo i god tid för införandet av ny lagstiftning. Det finns många lärdomar att dra av införandet av GDPR-lagstiftningen där stöd och tolkningar saknades i stor utsträckning vilket ökade den upplevda risken och de faktiska kostnaderna i innovationssystemet.

### Vinnova identifierar följande styrkor och positiva delar i förslaget:

- Det är rimligt att anta att EU kan ha en positiv påverkan på den globala utvecklingen av mer etisk AI genom att ligga i framkant vad gäller utveckling av policy- och lagstiftning.
- Det är nödvändigt att ta ett helhetsgrepp vad gäller reglering inom digitaliseringsområdet då det finns flera exempel på tvivelaktiga lösningar på marknaden som inte ligger i linje med "Union values".
- Den riskbaserade ansatsen, med fyra nivåer, är konceptuellt tydlig och väl avvägd i sin utgångspunkt. Modellen ger direktionalitet för utveckling och implementering av AI-system genom att tydliggöra vad som är förbjudet respektive hur olika risknivåer ska hanteras.

**Vinnova identifierar följande svagheter och negativa delar i förslaget:**

- Det är oklart varför inte utgångspunkten är ett teknikneutralt lagstiftningsförslag som förvisso riskerar att bli vagare men som samtidigt blir mer framtidsäktrat.
- Definitionen av AI-tekniker och ansatser är högst bristfällig då den i princip täcker in all datadriven mjukvaruutveckling och mer därtill. En sådan bred definition är knappast förenlig med det bakomliggande motivet att just AI-området måste begränsas och inte digitalisering eller innovation i en vidare mening.
- Det finns tveksamheter gällande demokratiska aspekter av förslaget att KOM ska kunna utveckla och anpassa listan över AI-tekniker och ansatser, särskilt som processen inte preciseras nämnvärt.
- I förslaget lyfts vid olika tillfällen vikten av att särskilt beakta startups respektive mikrobolag (t.ex. vad gäller avgifter) vilket förvisso är positivt men i realiteten kommer förslaget innebära en substantiell ökning av såväl kostnader som administration. Vinnova bedömer att särskild hänsyn även bör tas till medelstora företag.
- Föregående punkt i kombination med uppenbara risker för att flaskhalsar uppstår (kompetens- och kapacitetsmässigt på såväl organisations som systemnivå) kan leda till allvarligt försvagad konkurrenskraft. Det kan även leda till att målgruppen inte utvecklar datadrivna lösningar som såväl samhälle som individer efterfrågar.

**Baserat på lärdomar från införandet av GDPR är Vinnovas övergripande ställningstagande att**

- Det finns väldigt många gråzoner i förslaget som kommer att kräva vägledning för de som utvecklar datadrivna lösningar. Det är ytterst centralt att vi som land implementerar EU-regelverk på ett enhetligt sätt, och på sätt som skapar trygghet i näringslivet gällande spelregler (inklusive tillämpning och uppföljning). Det räcker med andra ord inte att enbart lagstiftningen i sig är tydlig utan det gäller minst lika mycket vad implementeringen innebär i praktiken.
- Det kommer att krävas resurser att (i) införa, (ii) följa upp och (iii) att ge stöd till företag om lagstiftningen inte ska ha oproportionerligt negativ påverkan på konkurrens- och innovationskraft. De myndigheter som kommer att få utökat ansvar behöver därför erhålla budget för att ta in AI-teknisk kompetens.
- Det är särskilt kritiskt att tidigt säkerställa att certifierings/bedömningsorgan inte blir en flaskhals.
- Det är oklart varför högre bestraffningsnivåer krävs jämfört med GDPR.

## **Andra aspekter som bör beaktas**

Vinnovas bedömning är att förslaget har en allt för kraftig slagsida mot riskminimering som diskriminerar näringslivet samt hämmar EUs konkurrens- och innovationskraft i allt för stor utsträckning. Det är även oklart varför offentlig sektor såväl som EUs egna institutioner inte hanteras på ett likvärdigt sätt som näringslivet i lagstiftningen, annat än i undantagsfall.

Givet tillgänglig tid för att lämna remissvar och lagförslagets komplexitet har Vinnova inte analyserat och bedömt huruvida det harmoniserar med existerande lagstiftning och strukturer såsom GDPR vad gäller datahantering.

## **Vinnovas ställningstaganden**

Utifrån ovanstående sammanfattning följer Vinnovas mer detaljerade ställningstaganden.

### **Avsnitt ” EXPLANATORY MEMORANDUM”**

Vinnovas ställningstagande är att förslaget troligen underskattar de kostnader som uppskattas för högrisksystem och compliance (3.3).

Skälen för ställningstagandet är att lagstiftningen kräver såväl omfattande som detaljrik dokumentation för AI-system i denna riskgrupp. Kostnaden kan bli särskilt kännbar för små- och medelstora företag som i relativt stor omfattning lär vara beroende av konsulter.

### **Avsnitt ”TITLE I – GENERAL PROVISIONS”**

Vinnovas ställningstagande är att definitionen gällande företag behöver utvidgas från ”micro or small enterprises” till ”micro or small or medium sized enterprises” i enlighet med EUs standarddefinition.

Vinnovas skäl för ställningstagandet är att medelstora företag utgör en viktig grupp som liksom mikro- och småföretag har begränsade resurser och ekonomiska förutsättningar. Genom att utvidga definitionen ges bättre möjligheter för skalande bolag att nå en kritisk nivå.

### **Avsnitt ” TITLE III – HIGH-RISK AI SYSTEMS”**

#### *Chapter 2: Requirements for high-risk AI systems*

Vinnovas ställningstagande är att kapitlet är väl artikulärt men väcker ett stort antal praktiska följdfrågor som kräver förtydliganden och riktlinjer. Exempel på frågetecken är vad som är en acceptabel nivå av teknisk dokumentation och record keeping samt vad human oversight innebär i praktiken.

Vinnovas skäl till ställningstagandet är att utvecklingen riskerar att mer eller mindre stanna av om inte förtydliganden och stöd finns på plats, särskilt för små- och medelstora företag.

*Chapter 3 Obligations of providers and users of high-risk AI systems and other parties*

Givet krav på dokumentation, och tillhörande kostnad, som krävs för högrisk AI-system är Vinnovas ställningstagande att lagförslaget i allt för hög utsträckning riskerar att hindra innovationer.

Vinnovas skäl till ovanstående anmärkning är att det inom utveckling av mjukvara ofta behövs tidiga och begränsade tester med mer eller mindre riktiga individer och/eller miljöer för att identifiera potential och affärsvärde. Frågan är om detta iterativa angreppssätt blir möjligt givet dokumentation, kostnader och definitionen av begreppen ”placing on the market” respektive ”putting into service”.

*Chapter 5 Standards, conformity, certifications, registration*

Vinnovas ställningstagande är att förslaget i högre utsträckning behöver exemplifiera vad som avses med ”substantially modified” (Article 43).

Vinnovas skäl till att anmärka på ovanstående är att all mjukvara och särskilt de som bygger på AI-tekniker och ansatser kommer att modifieras varpå mer precis vägledning behövs givet den begreppsdefinition som har artikulerats.

**Avsnitt ” TITLE V – MEASURES IN SUPPORT OF INNOVATION”**

*Article 55*

Vinnovas ställningstagande är positivt till de insatser som föreslås i artikeln men är tveksamma till att ”market size” utgör en rimlig och praktisk variabel att beakta vid avgiftsbeläggning då det kan vara svårt att bedöma skalbarhet i såväl rum som tid.

**Avsnitt ” TITLE VII – EU DATABASE FOR STAND-ALONE HIGH-RISK AI SYSTEMS”**

Vinnovas ställningstagande är positivt till upprättande av en EU-databas för högrisk AI-system men myndigheten noterar vikten att följa upp mer i detalj vilken data som ska loggas.

Vinnovas skäl till anmärkningen är att det behöver finnas en balans mellan vilken information som offentliggörs och företagens affärshemligheter.

**AVSNITT: "ANNEX I ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES"**

I Article 3 presenteras en definition där det framgår att en mjukvara ska räknas som ett AI-system om det bygger på en eller flera av de tekniker och ansatser som presenteras i Annex I. Vinnovas ställningstagande är att arbetet med att operationalisera, konkretisera och exemplifiera definitionen av AI i Annex I uppvisar mycket allvarliga brister. Definitionen är på gränsen till obegriplig.

Skälen till ställningstagandet är att hela rationalen bakom lagstiftningen utgår ifrån att utvecklingen och användandet av AI behöver regleras eftersom teknologierna som ingår i området har så pass, potentiellt, allvarliga konsekvenser för och inverkan på samhället och individer. Det är då ytterst problematiskt att utgångspunkten gällande denna specificitet inte möts upp i Annex I. I synnerhet är kategori C svår att kontextualisera och förstå. Med föreslaget Annex så blir definitionen så pass omfattande att i princip all datadriven mjukvaruutveckling kommer att täckas in. Detta kommer i sin tur att skapa oacceptabla otydligheter och hinder för de som vill utveckla och använda mjukvara.

**AVSNITT: "ANNEX III HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)"**

Vinnovas ställningstagande är att områdena som identifieras är relevanta utifrån ett samhälls- och individperspektiv. Beskrivningarna är i vissa avseenden väldigt breda vilket skapar gråzoner. Ett exempel är vilken risknivå en applikation skulle hamna på som nyttjar AI i utbildningssystemet för att "guida" studenterna i lärandet (t.ex. AI och gamification) men som inte används för intag till en kurs eller för betygssättande.

I detta ärende har Generaldirektör Darja Isaksson beslutat. Biträdande områdesansvarig för Digital omställning Daniel Rencrantz har varit föredragande. I den slutliga handläggningen har också Områdesansvarig för Digital omställning Andreas Aurelius, Områdesledare för Digital omställning Jessica Svennebring och Direktör Göran Marklund deltagit.

Darja Isaksson