

**Diarienummer:**  
DI-2021-4667

**Ert diarienummer:**  
I2021/01304

**Datum:**  
2021-06-24

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

Integritetsskyddsmyndigheten (IMY) har granskat förslaget huvudsakligen utifrån myndighetens uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter.

IMY lämnar följande synpunkter.

IMY anser att det är positivt att EU får en gemensam reglering rörande AI. Tekniken för AI-tillämpningar är här för att stanna och kommer att användas för allt fler samhällsfrämjande syften. Sverige har som uttalad ambition att Sverige ska vara ledande i att ta tillvara möjligheterna som användning av AI kan ge och samtidigt ha förmåga att hantera de risker som AI innebär<sup>1</sup>. Det remitterade förslaget syftar till att sätta ramarna för och bidra till att åstadkomma just detta.

**Relationen mellan de föreslagna reglerna gällande AI och dataskyddsreglerna**  
Förslaget är enligt IMY i huvudsak väl genomarbetat, men det finns stora brister vad gäller tydlighet mellan den föreslagna förordningen och dataskyddsregleringen. AI utvecklas snabbt, det är inte sällan stora uppgiftsmängder som behandlas och det är också ofta stora ekonomiska satsningar. Det är många gånger också fråga om att personuppgifter behandlas. Därför riskerar en osäkerhet om reglernas tillämpning att leda till såväl allvarliga integritetsrisker för de registrerade, som till allvarlig skada för de verksamheter som ska tillämpa förslaget.

I inledningen av det remitterade förslaget ("explanatory memorandum") anges att förslaget inte ska påverka utan komplettera dataskyddsförordningen<sup>2</sup>. Det är logiskt eftersom dataskyddsförordningen är det primära regelverket för behandling av personuppgifter. Samtidigt kan IMY konstatera att den föreslagna förordningen inte primärt är en kompletterande reglering till dataskyddsförordningen, utan en självständig reglering som riktar sig till såväl producenter som användare av AI-system. Hur dessa regleringar förhåller sig till varandra är i många delar svårt att

**Postadress:**  
Box 8114  
104 20 Stockholm

**Webbplats:**  
[www.imy.se](http://www.imy.se)

**E-post:**  
[imy@imy.se](mailto:imy@imy.se)

**Telefon:**  
08-657 61 00

<sup>1</sup>Nationell inriktning för artificiell intelligens, Publicerad 16 maj 2018, sid 4f,

[https://www.regeringen.se/49a828/contentassets/844d30fb0d594d1b9d96e2f5d57ed14b/2018ai\\_webb.pdf](https://www.regeringen.se/49a828/contentassets/844d30fb0d594d1b9d96e2f5d57ed14b/2018ai_webb.pdf)

<sup>2</sup>Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) vanligen förkortad GDPR.

förstå. Det gör det svårt att åstadkomma och säkerställa regelefterlevnad av båda regelverken.

I det följande beskriver IMY ett antal delar i förslaget som exempel på när vi ser att det finns risk för att förslaget kan leda till misstolkning eller bli vilseledande i förhållande till dataskyddsreglerna.

I förslaget delas AI-system in i olika nivåer beroende på dess risk för att vid användning inkräkta på grundläggande mänskliga rättigheter. Risknivåerna är *oacceptabel risk*, vars användning förbjuds, *hög risk*, som regleras strikt, och *låg eller minimal risk*, på vilka det inte läggs några särskilda krav, utöver vissa transparenskrav, i förslaget.

IMY har inget emot den uppdelningen utan delar uppfattningen att vissa tillämpningar av AI ska vara förbjudna och att "hög risk"-tillämpningar ska vara strikt reglerade. Såsom undantagen från förbuden i artikel 5 i förslaget är utformade riskerar de emellertid att på grund av vaga och otydliga formuleringar kunna bli tillämpliga i ett mycket stort antal situationer, särskilt på det brottsbekämpande området. De förutsättningar som gäller för att kvalificera vissa system som förbjudna är i vissa fall så vaga och otillräckliga att det i praktiken finns utrymme att kringgå förbudet, till exempel i fallet med "social scoring" och "remote biometric identification". Dessa förutsättningar behöver ses över så att de tydligt och klart blir förenliga med de krav på garantier för mänsklig värdighet och grundläggande värderingar som gäller inom EU och som också ligger till grund för EU:s dataskyddsreglering.

IMY ser även en risk att det kan uppfattas som att AI-system med lägre risknivå inte överhuvudtaget är reglerade. I inledningen till förslaget anges att "Businesses or public authorities that develop or use any AI applications not classified as high risk would only have minimal obligations of information. However, they could choose to join others and together adopt a code of conduct to follow suitable requirements, and to ensure that their AI systems are trustworthy." (3.3.Impact assessment).

Kommissionens egen "Fråga och svar" om förslaget på deras webbplats<sup>3</sup> anger följande.

*Minimal risk: Alla andra AI-system får utvecklas och användas utan några ytterligare rättsliga skyldigheter. Den absoluta huvuddelen av de AI-system som i dag används i EU tillhör denna kategori. Leverantörerna av sådana system kan välja att frivilligt tillämpa kraven för beteckningen tillförlitlig AI och ansluta sig till frivilliga uppförandekoder.*

Kommissionens information om förslaget bekräftar att den föreslagna förordningen kan uppfattas som uttömmande och att andra regler inte behöver följas. Ett AI-system innehållande personuppgifter ska oavsett risknivå följa gällande dataskyddsregler.

Att en viss tillämpning av AI inte är förbjuden enligt förslaget anger exempelvis ingenting om att en eventuell personuppgiftsbehandling är laglig. För att en personuppgiftsbehandling ska vara laglig måste den ske i enlighet med principerna i artikel 5 i dataskyddsförordningen och ha en rättslig grund enligt artikel 6. Behandling av känsliga personuppgifter är inte tillåtet om behandlingen inte omfattas av något av undantagen i artikel 9.2 i dataskyddsförordningen. Den personuppgiftsansvarige måste också uppfylla de skyldigheter som följer av dataskyddsförordningen. I det ingår bland

<sup>3</sup> [https://ec.europa.eu/commission/presscorner/detail/sv/qanda\\_21\\_1683](https://ec.europa.eu/commission/presscorner/detail/sv/qanda_21_1683)

annat att uppfylla den registrerades rättigheter såsom exempelvis rätten till information. Den personuppgiftsansvarige ska också ansvara för säkerheten i samband med behandlingen och kan behöva göra en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen om behandlingen kan innebära en hög risk för fysiska personers rättigheter och friheter. Den personuppgiftsansvarige ansvarar också för att personuppgifter inte otillåtet förs över till ett land utanför EU och EES s.k. tredjeland.

IMY konstaterar att även andra regler än dataskyddsreglerna behöver beaktas, inte minst gäller det myndigheter som bland annat har särskilda utmaningar i krav på transparens mot landets medborgare. IMY anser att det behöver bli mycket mer tydligt att det enbart är i förhållande till reglerna i den föreslagna AI regleringen som de olika risknivåerna får betydelse och att den föreslagna AI-förordningen inte påverkar tillämpningen av andra regler. Ett förslag som kan bidra till ökad tydlighet är att det i en artikel infogas en erinran om att andra regelverk ska följas och att vid behandling av personuppgifter gäller dataskyddsförordningen, i likhet med till exempel artikel 110 i förordningen om medicintekniska produkter, (EU) 2017/745 eller artikel 1.5 i förslag till förordning om en inre marknad för digitala tjänster (rättsakten om digitala tjänster), (EU) 2020/0361.

Det är också helt centralt att klargöra hur olika i förslaget utpekade aktörer (user, provider, importör och distributor) förhåller sig till rollerna personuppgiftsansvarig och personuppgiftsbiträde i dataskyddsförordningen. Det är sannolikt att olika aktörer i olika skeden i en AI-tillämpnings livscykel kommer att agera i båda rollerna och då alltså ha att tillämpa dataskyddsförordningen. Till exempel kan en leverantör behöva behandla personuppgifter, som ett led i att träna och validera sin AI-tillämpning, så som personuppgiftsansvarig och senare komma att agera personuppgiftsbiträde till en användare av AI-tillämpningen. Viktigt att komma ihåg här är också att dataskyddsförordningen ska tillämpas i sin helhet även vid testverksamhet. Det kan också uppstå situationer som innebär ett gemensamt personuppgiftsansvar mellan aktörerna. Rollfördelningen är central då olika regler i dataskyddsförordningen blir tillämpliga i olika situationer. Som personuppgiftsansvarig har man bland annat ansvar för att visa att de grundläggande principerna i dataskyddsförordningen följs. Rollfördelningen kan också få betydelse vid överträdelse av förordningen om sanktionsavgifter aktualiseras.

Artikel 10.5 i förslaget anger att känsliga personuppgifter ska få behandlas i syfte att säkerställa övervakning, upptäckt och korrigerande av partiskhet (bias) hos högrisk AI-system. Eftersom undantagen i artikel 9.2 i dataskyddsförordningen är uttömmande i förhållande till det principiella förbudet mot att behandla känsliga personuppgifter (särskilda kategorier av personuppgifter) i artikel 9.1 behöver regleringen i förslaget tydligt utgå från något av de undantag som anges i 9.2 för att en sådan behandling ska vara tillåten.

Enligt artikel 54.1 i förslaget ska personuppgifter som lagligen insamlats för andra ändamål under vissa förutsättningar få behandlas även för ändamålen utveckla och testa vissa AI-system inom ramen för en regulatorisk sandlåda. En regulatorisk sandlåda ska tillhandahålla en kontrollerad miljö som underlättar utveckling, testning och validering av innovativa AI-system. Möjligheten till vidarebehandling av personuppgifter regleras, med utgångspunkt i rättslig grund i artikel 6 i dataskyddsförordningen, av ändamålsbegränsningen i artikel 5.1 b (finalitetsprincipen). Det innebär att vidarebehandling ska vara förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in. Även detta förslag är otydligt i förhållande till dataskyddsförordningen och behöver klargöras.

Sammanfattningsvis kan sägas att bristen på tydlighet i förslaget medför uppenbara risker för att de registrerades grundläggande fri- och rättigheter enligt dataskyddsförordningen överträds, vilket kan få stora konsekvenser för såväl de registrerade som för inblandade aktörer. Det föreslagna regelverket gällande AI måste således förtydligas och förhållandet till dataskyddsreglerna, när det är fråga om personuppgiftsbehandling, klargöras.

#### **IMY:s roll**

Delar av förslaget berör också IMY:s roll. Så innehåller exempelvis artikel 53, om regulatoriska sandlådor, ett förslag att de nationella kompetenta myndigheterna, som kan vara dataskyddsmyndigheterna, ska övervaka utveckling, testning och validering av AI-tillämpningar och i samband därmed ge vägledning i syfte att säkerställa regelefterlevnad. Hur det förhåller sig till uppgiften att övervaka tillämpningen av dataskyddsförordningen anges inte och kravet på oberoende kommenteras inte. Förslaget om regulatoriska sandlådor behöver utredas ytterligare och förtydligas, inte bara avseende de nationella dataskyddsmyndigheternas roll utan även i fråga om teknisk infrastruktur och systemresurser ska tillhandahållas i sandlådan.

I artikel 59 beskrivs hur de nationella kompetenta myndigheterna ska utses. I artikel 63.5 anges att marknadsövervakande myndighet för vissa AI-tillämpningar ska vara tillsynsmyndigheten enligt dataskyddsförordningen eller den myndighet som bedriver tillsyn över polisväsendets eller migrations- eller asylmyndighetens verksamhet.

IMY delar förslaget i artikel 59.1 och 2 att medlemsländerna själva ska få besluta om vilka myndigheter som ska tilldelas vilka roller. Det är viktigt att utgå från myndigheternas befintliga roll och kompetens när olika behöriga myndigheter utses. För IMY skulle det vara en ny och annorlunda roll att vara sammanhållande myndighet, marknadsövervakande myndighet och "notifying authority" för framtagande och användande av AI-system. Till följd av den snabba digitala utveckling som sker och en successivt ökande användning av AI-system i både offentlig och privat verksamhet kan det antas att det blir ett omfattande uppdrag. Det skulle krävas både omfattande resurser och en annan kompetens än den myndigheten har idag utifrån sitt uppdrag att se till att den personliga integriteten skyddas vid behandling av personuppgifter. Om dataskyddsmyndigheterna inom EU/EES i det fortsatta arbetet pekas ut som nationella kompetenta myndigheter, eller om Sverige väljer att peka ut IMY som sådan, krävs att nödvändiga och tillräckliga resurser tillförs myndigheten för uppdraget.

Detta yttrande har beslutats av generaldirektören Lena Lindgren Schelin efter föredragning av it- och informationssäkerhetsspecialisten Magnus Bergström. Vid den slutliga handläggningen har även enhetschefen Katarina Tullstedt och juristen Elisabeth Jilderyd medverkat.

*Lena Lindgren Schelin, 2021-06-24 (Det här är en elektronisk signatur)*