Gemensamt yttrande 5/2021

från EDPB och EDPS

om förslaget till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens)

18 juni 2021

Sammanfattning

Den 21 april 2021 lade Europeiska kommissionen fram sitt förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (nedan kallat *förslaget*). Europeiska dataskyddsstyrelsen (EDPB) och Europeiska datatillsynsmannen (EDPS) välkomnar lagstiftarens oro över användningen av artificiell intelligens (AI) inom EU och betonar att förslaget har ytterst viktiga **följder för dataskyddet**.

EDPB och EDPS noterar att den **rättsliga grunden** för förslaget i första hand finns i artikel 114 i fördraget om Europeiska unionens funktionssätt. Dessutom är förslaget baserat på artikel 16 i fördraget om Europeiska unionens funktionssätt i den mån det innehåller särskilda regler om skydd för enskilda vid behandling av personuppgifter, särskilt begränsningar av användningen av AI-system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser i brottsbekämpande syfte. EDPB och EDPS erinrar om att artikel 16 i fördraget om Europeiska unionens funktionssätt, i linje med rättspraxis vid Europeiska unionens domstol, ger en korrekt rättslig grund i de fall där skyddet av personuppgifter tillhör de väsentliga målen eller komponenterna i de bestämmelser som antagits av unionslagstiftaren. Tillämpningen av artikel 16 i fördraget om Europeiska unionens funktionssätt medför även **behovet av att säkerställa en oberoende övervakning av efterlevnad** av kraven vad gäller behandling av personuppgifter, vilket även krävs enligt artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna.

Vad gäller **förslagets tillämpningsområde** välkomnar EDPB och EDPS att det utvidgas till tillhandahållandet och användningen av AI-system av EU:s institutioner, organ eller byråer. **Att utestänga internationellt samarbete inom brottsbekämpning från tillämpningsområdet** för förslaget ger dock upphov till starka betänkligheter för EDPB och EDPS, eftersom sådan utestängning skapar en avsevärd risk för kringgående (t.ex. av tredje länder eller internationella organisationer som driver högrisktillämpningar som offentliga myndigheter inom EU litar på).

EDPB och EDPS **välkomnar den riskbaserade metod** som ligger till grund för förslaget. Denna metod bör dock förtydligas och begreppet ”risk för de grundläggande rättigheterna” anpassas till den allmänna dataskyddsförordningen och förordning (EU) 2018/1725, eftersom aspekter som hör till skyddet av personuppgifter gör sig gällande.

EDPB och EDPS stöder angivelsen i förslaget att klassificeringen av ett **AI-system som hög risk inte nödvändigtvis innebär att det är lagligt** och kan tillämpas av användaren som ett sådant. Den personuppgiftsansvarige **kan behöva efterleva ytterligare krav till följd av EU:s dataskyddslagstiftning**. Efterlevnaden av rättsliga förpliktelser till följd av unionslagstiftningen (inräknat om skydd av personuppgifter) bör vidare vara en förutsättning för att tillåtas komma in på den europeiska marknaden som en CE-märkt produkt. EDPB och EDPS anser därför att **kravet att säkerställa efterlevnad av den allmänna dataskyddsförordningen och förordning (EU) 2018/1725 bör ingå i kapitel 2 i avdelning III**. EDPB och EDPS finner det dessutom nödvändigt att anpassa förfarandet för bedömning av överensstämmelse i förslaget så att tredje parter alltid utför förhandsbedömningar av överensstämmelse för AI-system med hög risk.

Med tanke på den stora risken för diskriminering förbjuds ”social poängsättning” i förslaget när denna utförs ”under en viss tidsperiod” eller av ”offentliga myndigheter, eller på deras vägnar”. Emellertid kan privata företag, t.ex. leverantörer inom ramen för sociala medier och molntjänster, också behandla stora mängder personuppgifter och utföra social poängsättning. Följaktligen **bör alla former av social poängsättning förbjudas i den framtida AI-förordningen**.

Biometrisk fjärridentifiering av enskilda personer på allmänt tillgängliga platser innebär en hög risk för intrång i enskilda personers privatliv, med allvarliga följder för befolkningens förväntan att vara anonym på allmänna platser. Av dessa anledningar föreslår EDPB och EDPS **ett allmänt förbud mot all användning av AI för automatiserad igenkänning av mänskliga särdrag på allmänna platser** – t.ex. av ansikten men även av gångstil, fingeravtryck, DNA, röst, tangenttryckningar och andra biometriska eller beteendemässiga kännetecken – i alla sammanhang. Ett **förbud** rekommenderas även **mot AI-system som med hjälp av biometri kategoriserar enskilda personer i kluster** utifrån etniskt ursprung, kön, politisk åskådning eller sexuell läggning, eller andra skäl för diskriminering enligt artikel 21 i stadgan. Dessutom finner EDPB och EDPS att användningen av AI för att **uttyda fysiska personers känslor är högst ovälkommet och bör förbjudas.**

EDPB och EDPS välkomnar **att EDPS utses till behörig myndighet och marknadskontrollmyndighet för övervakningen av unionens institutioner, organ och byråer**. EDPS roll och uppgifter bör dock klargöras närmare, särskilt vad gäller dess roll som marknadskontrollmyndighet. Vidare bör en framtida AI-förordning tydligt fastslå **tillsynsmyndigheternas oberoende** i utförandet av sina uppgifter gällande övervakning och verkställande.

Att dataskyddsmyndigheter utnämns till nationella tillsynsmyndigheter skulle säkerställa en mer harmoniserad regleringsmetod, bidra till en konsekvent tolkning av bestämmelserna om databehandling och undvika motstridigheter i verkställandet i de olika medlemsstaterna. EDPB och EDPS finner följaktligen att **dataskyddsmyndigheter bör utses till nationella tillsynsmyndigheter i enlighet med artikel 59 i förslaget.**

I förslaget tilldelas kommissionen en tongivande roll i den europeiska nämnden för artificiell intelligens. En sådan roll står i strid med behovet av ett europeiskt AI-organ som är oberoende av allt politiskt inflytande. För att säkra dess oberoende bör den framtida AI-förordningen ge **den europeiska nämnden för artificiell intelligens större autonomi** och säkerställa att nämnden kan agera på eget initiativ.

Med tanke på AI-systemens spridning över den inre marknaden och sannolikheten för gränsöverskridande fall finns det ett stort behov av ett harmoniserat verkställande och vederbörlig tilldelning av befogenheter mellan nationella tillsynsmyndigheter. EDPB och EDPS föreslår **att en mekanism införs som för varje AI-system garanterar en enda kontaktpunkt för enskilda personer som berörs av lagstiftningen, såväl som för företag.**

Vad gäller **sandlådorna rekommenderar** EDPB och EDPS **att deras tillämpningsområde och målsättningar förtydligas**. I förslaget ska det även tydligt anges att den rättsliga grunden för sådana sandlådor ska uppfylla kraven i den befintliga ramen för dataskydd.

Det **certifieringssystem** som beskrivs i förslaget **saknar en tydlig koppling till EU:s dataskyddslagstiftning** såväl som till EU:s och medlemsstaternas övriga lagstiftning för varje ”område” av AI-system med hög risk och beaktar inte **principerna om uppgiftsminimering och inbyggt dataskydd** som en av de aspekter som bör övervägas **före erhållandet av CE-märkning**. EDPB och EDPS rekommenderar därför att förslaget ändras för att förtydliga sambandet mellan intyg som utfärdas enligt den nämnda förordningen och certifieringar, förseglingar och märkningar för dataskydd. Slutligen bör

dataskyddsmyndigheterna involveras för att utarbeta och införa harmoniserade standarder och gemensamma specifikationer.

Vad gäller **uppförandekoderna** finner EDPB och EDPS det **nödvändigt att klargöra** om skyddet av personuppgifter ska tillhöra de ”ytterligare krav” som kan hanteras genom dessa uppförandekoder, liksom att säkerställa att ”tekniska specifikationer och lösningar” inte strider mot reglerna och principerna i EU:s befintliga ram för dataskydd.

INNEHÅLLSFÖRTECKNING

Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen har antagit detta gemensamma yttrande

med beaktande av artikel 42.2 i Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG[1],

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[2],

med beaktande av begäran om ett gemensamt yttrande från Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen av den 22 april 2021 om förslaget till förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens).

HÄRIGENOM FRAMFÖRS FÖLJANDE.

1 INLEDNING

1. Tillkomsten av system för artificiell intelligens (AI) är ett mycket viktigt steg i den tekniska utvecklingen och för hur människor samspelar med den. AI är en uppsättning viktiga tekniker som i grunden kommer att förändra våra dagliga liv, både ur ett socialt och ekonomiskt perspektiv. Under de närmaste åren väntas avgörande beslut för AI, som hjälper oss att övervinna några av de största utmaningarna vi står inför idag, allt ifrån hälsa till mobilitet, eller från offentlig förvaltning till utbildning.

2. Dessa utlovade framsteg är dock inte helt riskfria. Riskerna är faktiskt mycket relevanta med tanke på att AI-systemens effekter på individ- och samhällsnivå till stor del ännu inte har upplevts. Att skapa innehåll, upprätta prognoser eller fatta beslut på ett automatiserat sätt, som AI-systemen gör, genom maskininlärningstekniker eller logisk och sannolikhetsbaserad slutledning, sker inte på samma sätt som när människor gör samma sak, med hjälp av kreativa eller teoretiska resonemang, där fullt ansvar tas för följderna.

3. AI kommer att öka antalet prognoser som kan utföras inom många områden genom mätbara korrelationer mellan data som är osynliga för människoögat men synliga för maskiner. Detta kommer att göra våra liv lättare och lösa många problem, men kommer samtidigt att undergräva vår förmåga att ge resultaten ett orsakssamband. Som en följd av detta kommer begreppen transparens, mänsklig kontroll, ansvarsskyldighet och ansvarighet för resultat att ställas inför stora utmaningar.

[1] EUT L 295, 21.11.2018, s. 39–98.
[2] Hänvisningar till ”medlemsstater” som görs i hela detta dokument ska förstås som hänvisningar till ”EES-medlemsstater”.

4. Data (både personuppgifter och icke-personuppgifter) inom AI är i många fall den centrala förutsättningen för självständiga beslut, vilket oundvikligen kommer att påverka enskilda personers liv på olika nivåer. Det är av denna anledning som EDPB och EDPS, redan på detta stadium, med kraft hävdar att förslaget till förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) (nedan kallat *förslaget*)[3] har **viktiga följder för dataskyddet**.

5. Att på grundval av data tilldela maskiner en beslutande uppgift kommer att skapa risker för enskilda personers fri- och rättigheter, liksom påverka deras privatliv och eventuellt skada hela grupper eller till och med samhällen. EDPB och EDPS betonar att rätten till privatliv och skydd av personuppgifter, i strid med antagandet av maskiners förmåga till självständiga beslut som ligger till grund för AI-begreppet, utgör en pelare för EU:s värderingar, i enlighet med den allmänna förklaringen om de mänskliga rättigheterna (artikel 12), den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (artikel 8) samt Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) (artiklarna 7 och 8). Att förena det tillväxtperspektiv som erbjuds av AI-tillämpningar och människors avgörande roll och företräde gentemot maskiner är ett mycket ambitiöst men nödvändigt mål.

6. EDPB och EDPS välkomnar att alla intressenter i AI-värdekedjan involveras i regleringen och att särskilda krav införs för leverantörer av lösningar eftersom de spelar en avgörande roll i förhållande till de produkter för vilka deras system används. Det ansvar som de olika parterna – användaren, leverantören, importören eller återförsäljaren av ett AI-system – har måste dock tydligt anges och tilldelas. I synnerhet bör man vid behandling av personuppgifter särskilt beakta att dessa roller och ansvarsområden överensstämmer med begreppen personuppgiftsansvarig och personuppgiftsbiträde enligt ramen för dataskydd, eftersom de två normerna inte sammanfaller med varandra.

7. Förslaget ger begreppet mänsklig tillsyn en central plats (artikel 14), vilket EDPB och EDPS välkomnar. På grund av den potentiellt stora inverkan som vissa AI-system har på enskilda personer eller grupper av enskilda personer bör dock, som nämnts tidigare, människors verkligt avgörande roll bygga på högkvalificerad mänsklig tillsyn och laglig behandling. Detta ska ske i den mån som dessa system bygger på behandling av personuppgifter eller behandlar personuppgifter för att fullgöra sina uppgifter för att garantera att rätten att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling respekteras.

8. Eftersom många AI-tillämpningar är dataintensiva bör förslaget dessutom främja antagandet av ett inbyggt dataskydd och dataskydd som standard på alla nivåer, genom att uppmuntra till ett effektivt genomförande av principerna om dataskydd (enligt artikel 25 i den allmänna dataskyddsförordningen och artikel 27 i förordning (EU) 2018/1725) med hjälp av den senaste tekniken.

[3] COM(2021) 206 final.

9. Slutligen betonar EDPB och EDPS att detta gemensamma yttrande endast lämnas som en preliminär analys av förslaget, och att det inte påverkar eventuella andra bedömningar och yttranden om förslagets effekter och huruvida det strider mot EU:s dataskyddslagstiftning.

2 ANALYS AV FÖRSLAGETS CENTRALA PRINCIPER

2.1 Förslagets tillämpningsområde och förhållande till den befintliga rättsliga ramen

10. Enligt motiveringen är förslagets **rättsliga grund** i första hand artikel 114 i fördraget om Europeiska unionens funktionssätt, i vilken det föreskrivs att åtgärder ska vidtas för att säkerställa att den inre marknaden upprättas och fungerar[4]. Dessutom är förslaget baserat på artikel 16 i fördraget om Europeiska unionens funktionssätt *i den mån det innehåller särskilda regler om skydd för enskilda vid behandling av personuppgifter*, särskilt begränsningar av användningen av AI-system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser i brottsbekämpande syfte[5].

11. EDPB och EDPS erinrar om att artikel 16 i fördraget om Europeiska unionens funktionssätt, i linje med rättspraxis vid Europeiska unionens domstol, ger en korrekt rättslig grund i de fall där skyddet av personuppgifter tillhör de väsentliga målen eller komponenterna i de bestämmelser som antagits av unionslagstiftaren[6]. Tillämpningen av artikel 16 i fördraget om Europeiska unionens funktionssätt medför även behovet av att säkerställa en oberoende övervakning av efterlevnad av kraven vad gäller behandling av personuppgifter, vilket även krävs enligt artikel 8 i stadgan.

12. EDPB och EDPS erinrar om att en övergripande ram för dataskydd redan antagits på grundval av artikel 16 i fördraget om Europeiska unionens funktionssätt, bestående av den allmänna dataskyddsförordningen[7], förordning (EU) 2018/1725[8] och direktivet om dataskydd vid brottsbekämpning[9]. Enligt förslaget är det bara de extra begränsningarna avseende behandlingen av biometriska data i förslaget som kan anses vara baserade på artikel 16 i fördraget om Europeiska unionens funktionssätt och som därför kan anses ha samma rättsliga grund som den allmänna dataskyddsförordningen, förordning (EU) 2018/1725 eller direktivet om dataskydd vid brottsbekämpning. Mer allmänt har detta viktiga följder för förslagets

[4] Motiveringen, s. 5.
[5] Motiveringen, s. 6. Se även skäl 2 i förslaget.
[6] Yttrande av den 26 juli 2017, *PNR Canada*, förfarande för yttrande 1/15, ECLI:EU:C:2017:592, punkt 96.
[7] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 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) EUT L 119, 4.5.2016, s. 1–88.
[8] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG, EUT L 295, 21.11.2018, s. 39–98.
[9] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, EUT L 119, 4.5.2016, s. 89–131.

förhållande till den allmänna dataskyddsförordningen, förordning (EU) 2018/1725 och direktivet om dataskydd vid brottsbekämpning, enligt vad som anges nedan.

13. Vad gäller **förslagets tillämpningsområde** välkomnar EDPB och EDPS att det utvidgas till användningen av AI-system av EU:s institutioner, organ eller byråer. Med tanke på att dessa enheters användning av AI-system också kan ha en betydande effekt på enskilda personers grundläggande rättigheter, liknande användningen inom EU:s medlemsstater, är det absolut nödvändigt att den nya rättsliga ramen för AI både gäller för EU:s medlemsstater och för EU:s institutioner, organ och byråer för att garantera ett enhetligt synsätt inom hela unionen. Eftersom EU:s institutioner, organ och byråer både kan agera leverantörer och användare av AI-system finner EDPB och EDPS det helt lämpligt att låta dessa enheter ingå i förslagets tillämpningsområde på grundval av artikel 114 i fördraget om Europeiska unionens funktionssätt.

14. EDPB och EDPS har dock starka betänkligheter mot att internationellt samarbete inom brottsbekämpning utestängs från tillämpningsområdet i enlighet med artikel 2.4 i förslaget. Denna utestängning skapar en betydande risk för kringgående (t.ex. tredje länder eller internationella organisationer som driver högrisktillämpningar som offentliga myndigheter inom EU litar på).

15. Utvecklingen och användningen av AI-system leder ofta till behandling av personuppgifter. Det är ytterst viktigt att säkerställa klarhet i detta förslags förhållande till den befintliga EU-lagstiftningen om dataskydd. Förslaget kompletterar, utan att påverka tillämpningen av, den allmänna dataskyddsförordningen, förordning (EU) 2018/1725 och direktivet om dataskydd vid brottsbekämpning. Även om skälen i förslaget klargör att användningen av AI-system fortfarande bör överensstämma med dataskyddslagstiftningen **rekommenderar EDPB och EDPS att det i artikel 1 i förslaget klargörs att unionens lagstiftning för skydd av personuppgifter**, särskilt den allmänna dataskyddsförordningen, förordning (EU) 2018/1725, direktivet om integritet och elektronisk kommunikation[10] och direktivet om dataskydd vid brottsbekämpning, ska gälla för all behandling av personuppgifter som ingår i förslagets tillämpningsområde. Ett motsvarande skäl bör likaså klargöra att förslaget inte syftar till att påverka tillämpningen av den befintliga EU-lagstiftning som reglerar behandlingen av personuppgifter, däribland arbetsuppgifterna och befogenheterna för den oberoende tillsynsmyndighet som är behörig att övervaka efterlevnaden av dessa instrument.

2.2 Riskbaserad metod

16. EDPB och EDPS **välkomnar den riskbaserade metod** som ligger till grund för förslaget. Förslaget skulle tillämpas på alla AI-system, inräknat de som inte inbegriper behandling av personuppgifter men som fortfarande kan påverka intressen eller grundläggande rättigheter och friheter.

[10] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), ändrat genom direktiv 2006/24/EG och direktiv 2009/136/EG.

17. EDPB och EDPS noterar att vissa av förslagets bestämmelser utelämnar riskerna för grupper av enskilda personer eller samhället som helhet (t.ex. kollektiva effekter av särskild relevans, såsom gruppdiskriminering eller politiska åsiktsyttringar på allmänna platser). EDPB och EDPS rekommenderar att de risker på samhälls-/gruppnivå som AI-systemen medför också bör bedömas och begränsas.

18. EDPB och EDPS anser att den riskbaserade metoden i förslaget bör förtydligas och begreppet ”risk för de grundläggande rättigheterna” **anpassas till den allmänna dataskyddsförordningen**, eftersom aspekter som hör till skyddet av personuppgifter gör sig gällande. Oavsett om det rör sig om slutanvändare, registrerade eller andra personer som berörs av AI-systemet anses avsaknaden av hänvisning i texten till enskilda personer som påverkas av AI-systemet vara en brist i förslaget. De skyldigheter som åläggs aktörer gentemot de personer som påverkas bör framträda mer konkret från skyddet för enskilda personer och deras rättigheter. EDPB och EDPS uppmanar därför lagstiftarna att i förslaget uttryckligen ta upp de **rättigheter och åtgärder som finns tillgängliga för enskilda personer** som utsätts för AI-system.

19. EDPB och EDPS noterar alternativet att tillhandahålla en uttömmande förteckning över **AI-system med hög risk**. Detta alternativ skulle kunna skapa en svart-vit effekt, där högrisksituationer har låg attraktionsförmåga, och undergräva den övergripande riskbaserade metod som ligger till grund för förslaget. I denna förteckning över AI-system med hög risk, som beskrivs i bilagorna II och III i förslaget, saknas även vissa typer av användningsfall som innebär betydande risker, såsom användning av AI för bestämning av försäkringspremier, eller bedömning av medicinsk behandling eller för hälsoforskning. EDPB och EDPS betonar även att dessa bilagor måste uppdateras regelbundet för att deras tillämpningsområde ska vara korrekt.

20. I förslaget föreskrivs att AI-systemets **leverantörer** ska utföra en riskbedömning. I de flesta fall kommer dock de personuppgiftsansvariga att vara AI-systemens **användare** snarare än leverantörer (en användare av ett system för ansiktsigenkänning är t.ex. en ”personuppgiftsansvarig” och är därför enligt förslaget inte bunden av kraven för leverantörer av AI med hög risk).

21. Vidare kommer **en leverantör inte alltid kunna bedöma samtliga användningar** för AI-systemet. Därför kommer den inledande riskbedömningen att vara av mer allmän typ än den som utförs av AI-systemets användare. Även om leverantörens inledande riskbedömning inte visar att AI-systemet utgör ”hög risk” enligt förslaget ska detta inte utesluta **en efterföljande (mer utförlig) bedömning** (konsekvensbedömning avseende dataskydd enligt artikel 35 i den allmänna dataskyddsförordningen, artikel 39 i förordning (EU) 2018/1725 eller enligt artikel 27 i direktivet om dataskydd vid brottsbekämpning) **som ska utföras av systemets användare**, där användningens sammanhang och de specifika användningsfallen övervägs. Tolkningen av huruvida en viss behandling enligt den allmänna dataskyddsförordningen, förordning (EU) 2018/1725 och direktivet om dataskydd vid brottsbekämpning sannolikt resulterar i en hög risk ska göras oberoende av förslaget. Klassificeringen av ett AI-system som

”hög risk” på grund av dess effekt på grundläggande rättigheter[11] **utlöser ett ”hög risk”-antagande enligt den allmänna dataskyddsförordningen, förordning (EU) 2018/1725 och direktivet om dataskydd vid brottsbekämpning, i den utsträckning som personuppgifter behandlas.**

22. **EDPB och EDPS stöder angivelsen i förslaget att klassificeringen av ett AI-system som hög risk inte nödvändigtvis innebär att det är lagligt och kan tillämpas av användaren som ett sådant. Den personuppgiftsansvarige kan behöva efterleva ytterligare krav till följd av EU:s dataskyddslagstiftning.** Vidare är det nödvändigt att ta upp och ta bort det underliggande resonemanget i artikel 5 i förslaget, enligt vilket högrisksystemen, till skillnad från förbjudna system, i princip kan vara tillåtna, särskilt eftersom den föreslagna CE-märkningen inte innebär att den åtföljande behandlingen av personuppgifter är laglig.

23. Efterlevnaden av rättsliga förpliktelser till följd av unionslagstiftningen (inräknat om skyddet av personuppgifter) bör dock vara en förutsättning för att tillåtas komma in på den europeiska marknaden som en CE-märkt produkt. EDPB och EDPS **rekommenderar därför att kapitel 2 i avdelning III i förslaget ska innehålla kravet att säkerställa efterlevnad av den allmänna dataskyddsförordningen och förordning (EU) 2018/1725**. Dessa krav ska revideras (genom tredje parts revision) före CE-märkningen i enlighet med ansvarsprincipen. I samband med denna tredje parts bedömning kommer den inledande konsekvensbedömningen som ska utföras av leverantören att vara särskilt relevant.

24. Med beaktande av de sammansatta problem som utvecklingen av AI-system utlöser bör det påpekas att AI-systemens tekniska kännetecken (t.ex. typ av AI-metod) kan medföra större risker. Därför ska alla riskbedömningar av ett AI-system beakta **de tekniska egenskaperna** vid sidan av **dess specifika användningsfall och det sammanhang** i vilket systemet är i drift.

25. EDPB och EDPS rekommenderar därför att det i förslaget anges att **leverantören** ska utföra en inledande riskbedömning av det berörda AI-systemet **med tanke på användningsfallen** (ska anges i förslaget – t.ex. komplettera bilaga III punkt 1 a, där användningsfallen avseende biometriska AI-system inte nämns). Dessutom ska AI-systemets **användare**, i rollen som personuppgiftsansvarig enligt EU:s dataskyddslagstiftning (om så är relevant), utföra konsekvensbedömningen avseende dataskydd enligt beskrivning i artikel 35 i den allmänna dataskyddsförordningen, artikel 39 i förordning (EU) 2018/1725 och artikel 27 i direktivet om dataskydd vid brottsbekämpning, inte bara med tanke på tekniska kännetecken och **användningsfallet**, utan **också det specifika sammanhang** i vilket AI-systemet kommer att användas.

[11] Europeiska unionens byrå för grundläggande rättigheter (FRA) har redan tagit upp behovet av att utföra konsekvensbedömningar för grundläggande rättigheter vid användning av AI eller tillhörande tekniker. I sin rapport från 2020, *Getting the future right – Artificial intelligence and fundamental rights*, identifierade FRA ”fallgropar vid användningen av AI, till exempel vid prognostiserat polisarbete, medicinska diagnoser, sociala tjänster och riktad reklam” och betonade att ”[p]rivata och offentliga organisationer bör göra bedömningar av hur AI skulle kunna skada de grundläggande rättigheterna” för att minska de negativa effekterna på enskilda personer.

26. En del av de termer som nämns i bilaga III till förslaget, t.ex. termen ”grundläggande privata tjänster” eller småskaliga leverantörer som använder AI-system för kreditprövning för egen användning, bör förtydligas.

2.3 Förbjudna användningar av AI

27. EDPB och EDPS finner att **inkräktande former av AI** – särskilt de som kan påverka människans värdighet – bör betraktas som förbjudna AI-system enligt artikel 5 i förslaget i stället för att bara klassificeras som system ”med hög risk” i bilaga III till förslaget, såsom under nr 6. Detta gäller särskilt uppgiftsjämförelser som i stor skala också påverkar personer som inte har gett polisen någon eller bara liten anledning till observation, eller behandling som skadar principen för ändamålsbegränsning enligt dataskyddslagstiftningen. Användning av AI inom polis- och brottsbekämpningsområdet förutsätter områdesspecifika, exakta, förutsägbara och proportionerliga regler med hjälp av vilka de berörda personernas intressen och effekterna för ett fungerande demokratiskt samhälle måste övervägas.

28. Artikel 5 i förslaget riskerar bara att utgöra tomma ord vad gäller ”värdena” och förbudet av AI-system som strider mot sådana värden. De kriterier som används i artikel 5 för att ”klassificera” AI-systemen som förbjudna **begränsar faktiskt förbudets tillämpningsområde** i sådan grad att det kan bli meningslöst i praktiken (t.ex. ”orsakar eller sannolikt kommer att orsaka fysisk eller psykisk skada” i artikel 5.1 a och b; begränsning till offentliga myndigheter i artikel 5.1 c; en vag ordalydelse i led c i och ii; begränsning av biometrisk fjärridentifiering i ”realtid” men utan klar definition osv.).

29. Användningen av AI för social poängsättning, i enlighet med artikel 5.1 c i förslaget, kan i synnerhet leda till diskriminering och strider mot EU:s grundläggande värden. I förslaget förbjuds bara dessa åtgärder när de utförs ”under en viss tidsperiod” eller av ”offentliga myndigheter, eller på deras vägnar”. Privata företag, särskilt leverantörer inom ramen för sociala medier och molntjänster, kan behandla stora mängder personuppgifter och utföra social poängsättning. Följaktligen **bör alla former av social poängsättning förbjudas i förslaget**. Med avseende på brottsbekämpning bör det noteras att artikel 4 i direktivet om dataskydd vid brottsbekämpning redan avsevärt begränsar – om inte i praktiken förbjuder – denna typ av verksamhet.

30. **Biometrisk fjärridentifiering** av enskilda personer på allmänt tillgängliga platser innebär en hög risk för intrång i enskilda personers privatliv. Därför finner EDPB och EDPS **att ett striktare tillvägagångssätt är nödvändigt**. Användningen av AI-system skulle kunna vara ett allvarligt problem för proportionalitetsprincipen, eftersom de kan involvera behandling av data från ett urskillningslöst och oproportionerligt antal registrerade men bara identifiera ett fåtal enskilda personer (t.ex. passagerare på flygplatser och tågstationer). Den **friktionsfria** användningen av biometriska fjärridentifieringssystem leder även till transparensproblem och frågor gällande behandlingens rättsliga grund enligt EU:s lagstiftning (direktivet om dataskydd vid brottsbekämpning, den allmänna dataskyddsförordningen, förordning (EU) 2018/1725 och annan tillämplig lagstiftning). Problemet gällande det rätta sättet att informera enskilda personer om denna behandling är fortfarande olöst liksom hur enskilda personers rättigheter ska utövas effektivt och snabbt. Detsamma gäller **dess irreversibla, kraftiga effekt på**

befolkningens (skäliga) **förväntan att vara anonym på allmänna platser**, vilket ger en direkt negativ effekt på yttrandefriheten, mötesfriheten, föreningsfriheten och den fria rörligheten.

31. I artikel 5.1 d i förslaget finns en omfattande **förteckning över undantagsfall** då biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser är tillåtet i brottsbekämpande syfte. EDPB och EDPS finner att **denna metod är felaktig** vad gäller flera aspekter: För det första är det oklart vad som ska förstås som ”en betydande fördröjning” och hur den ska anses vara en begränsande faktor, med tanke på att massidentifieringssystem förmår identifiera tusentals enskilda personer på ett fåtal timmar. Dessutom är den grad i vilken behandlingen är inkräktande inte alltid beroende av om identifieringen utförs i realtid eller inte. Biometrisk fjärridentifiering inom ramen för en politisk protest har troligtvis en betydande nedkylande effekt på utövandet av grundläggande rättigheter och friheter, såsom mötesfrihet och föreningsfrihet och demokratins grundprinciper mer i allmänhet. För det andra är den grad i vilken behandlingen är inkräktande inte nödvändigtvis beroende av dess syfte. Att använda detta system för andra ändamål såsom privata bevakningstjänster utgör samma hot mot den grundläggande rätten till respekt för privatlivet och familjelivet och skydd av personuppgifter. Slutligen, även med de förutsedda begränsningarna, kommer det potentiella antalet misstänkta eller förövare av brott nästan alltid att vara ”tillräckligt högt” för att motivera en kontinuerlig användning av AI-system för att avslöja misstänkta personer, trots de ytterligare villkoren i artikel 5.2 och 5.4 i förslaget. Vid övervakning av öppna områden verkar resonemanget bakom förslaget förbise att skyldigheterna enligt EU:s dataskyddslagstiftning inte bara måste uppfyllas för misstänkta personer, utan för alla som övervakas i praktiken.

32. Av alla dessa anledningar föreslår EDPB och EDPS **ett allmänt förbud mot all användning av AI för automatiserad igenkänning av mänskliga särdrag på allmänna platser – t.ex. av ansikten men även av gångstil, fingeravtryck, DNA, röst, tangenttryckningar och andra biometriska eller beteendemässiga kännetecken – i alla sammanhang**. Den metod som för närvarande används i förslaget är att identifiera och lista alla AI-system som bör förbjudas. För konsekvensens skulle bör därför **AI-system för storskalig fjärridentifiering på onlineplatser** förbjudas enligt artikel 5 i förslaget. Med beaktande av direktivet om dataskydd vid brottsbekämpning, förordning (EU) 2018/1725 och den allmänna dataskyddsförordningen kan inte EDPS och EDPB fastställa hur denna typ av praxis skulle kunna uppfylla nödvändighets- och proportionalitetskraven, vilket slutligen härrör från vad som betraktas som godtagbart åsidosättande av de grundläggande rättigheterna vid Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna.

33. Vidare rekommenderar EDPB och EDPS **ett förbud**, för både offentliga myndigheter och privata enheter, mot **AI-system som med hjälp av biometri kategoriserar enskilda personer (till exempel genom ansiktsigenkänning) i kluster utifrån etniskt ursprung, kön, politisk åskådning eller sexuell läggning, eller andra skäl för diskriminering enligt artikel 21 i stadgan, eller** AI-system vars vetenskapliga värde inte är bevisat eller som strider mot EU:s grundläggande värden (t.ex. lögndetektor, bilaga III punkterna 6 b och 7 a). Följaktligen bör ”**biometrisk kategorisering**” **förbjudas enligt artikel 5**.

34. Det **påverkar även människans värdighet att bli bedömd eller klassificerad av en dator vad gäller framtida beteende oberoende av ens egen fria vilja**. AI-system som är avsedda att användas av brottsbekämpande myndigheter för att utföra individuella riskbedömningar av fysiska personer i syfte att bedöma en fysisk persons risk för brott eller återfall, jämför bilaga III punkt 6 a, eller för att förutse förekomst eller upprepning av ett faktiskt eller potentiellt brott baserat på profilering av fysiska personer, eller bedöma personlighetsdrag och egenskaper eller tidigare brottsligt beteende, jämför bilaga III punkt 6 e, och som används i enlighet med deras avsedda syfte kommer att leda till att polisen och det rättsliga beslutsfattandet på ett avgörande sätt underkastas dem, vilket objektifierar den berörda personen. Sådana AI-system som berör det centrala i rätten till människans värdighet bör förbjudas enligt artikel 5.

35. Dessutom finner EDPB och EDPS att användningen av AI för att **uttyda fysiska personers känslor är högst ovälkommet och bör förbjudas,** utom i vissa väl angivna fall, dvs. i hälso- eller forskningssyfte (t.ex. patienter hos vilka känsloigenkänning är viktigt), alltid med lämpliga skyddsåtgärder på plats och givetvis med beaktande av alla andra villkor för dataskydd och begränsningar, inräknat ändamålsbegränsning.

2.4 AI-system med hög risk

2.4.1 Behov av externa tredje parters förhandsbedömning av överensstämmelse

36. EDPB och EDPS välkomnar att de AI-system som utgör en hög risk först måste bedömas avseende överensstämmelse innan de kan släppas ut på marknaden eller på annat sätt tas i drift inom EU. Denna regulatoriska modell är i princip välkommen eftersom den ger en bra balans mellan innovationsvänlighet och en hög nivå av proaktivt skydd för de grundläggande rättigheterna. För att tas i bruk i specifika miljöer såsom beslutsprocesser i offentliga institutioner eller kritisk infrastruktur måste sätt att undersöka den fullständiga källkoden läggas ut.

37. EDPB och EDPS förespråkar dock anpassning av förfarandet för bedömning av överensstämmelse enligt artikel 43 i förslaget så att **tredje part i allmänhet måste utföra en förhandsbedömning av överensstämmelse för högrisk-AI**. Även om tredje parts bedömning av överensstämmelse för högriskbehandling av personuppgifter inte är ett krav i den allmänna dataskyddsförordningen eller förordning (EU) 2018/1725 är AI-systemens risker ännu inte helt utredda. Det allmänna införandet av en skyldighet för tredje part att utföra bedömning av överensstämmelse skulle därför stärka rättssäkerheten och tilliten för alla AI-system med hög risk.

2.4.2 Förordningens tillämpningsområde måste även täcka AI-system som redan är i bruk

38. Enligt artikel 43.4 i förslaget ska AI-system med hög risk alltid genomgå ett nytt förfarande för bedömning av överensstämmelse när de ändras väsentligt. Det ska säkerställas att AI-systemen uppfyller kraven i AI-förordningen under hela deras livscykel. AI-system som har släppts på marknaden eller tagits i bruk innan den föreslagna förordningen träder i kraft (eller 12 månader därefter för stora it-system som förtecknas i bilaga IX) utestängs från sitt tillämpningsområde,

om inte dessa system genomgår ”betydande ändring” av utformningen eller det avsedda ändamålet (artikel 83).

39. Tröskeln för ”betydande ändring” är dock oklar. I skäl 66 i förslaget anges en lägre tröskel för förnyad förhandsbedömning av överensstämmelse ”vid varje ändring som kan påverka systemets överensstämmelse”. En liknande tröskel skulle vara lämplig för artikel 83, åtminstone för AI-system med hög risk. För att ytterligare åtgärda eventuella brister i skyddet är det vidare nödvändigt att AI-system som redan släppts ut på marknaden eller tagits i bruk – efter en viss genomförandefas – också uppfyller alla kraven i AI-förordningen.

40. AI-systemens säkerhet påverkas också av de talrika möjligheterna till behandling av personuppgifter och externa risker. I artikel 83 finns ingen hänvisning till ändring av externa risker i dess inriktning på ”betydande ändring av [...] utformning eller avsedda ändamål”. En hänvisning till ändringar av hotscenariot, till följd av externa risker, t.ex. it-angrepp, adversariellt angrepp och styrkta klagomål från konsumenter, bör därför ingå i artikel 83 i förslaget.

41. Eftersom tillämpningen är inplanerad att starta 24 månader efter den framtida förordningens ikraftträdande finner EDPB och EDPS det heller inte lämpligt att undanta AI-system som redan släppts ut på marknaden för en ännu längre tidsperiod. Eftersom det i förslaget även fastställs att kraven i förordningen ska beaktas vid utvärderingen av alla stora it-system i enlighet med de rättsakter som förtecknas i bilaga IX, finner EDPB och EDPS att kraven vad gäller ibruktagande av AI-system ska gälla från den dag då den framtida förordningen träder i kraft.

2.5 Styrning och den europeiska AI-nämnden

2.5.1 Styrning

42. EDPB och EDPS välkomnar att EDPS utses till behörig myndighet och marknadskontrollmyndighet för övervakningen av unionens institutioner, organ och byråer när de omfattas av detta förslags tillämpningsområde. EDPS är redo att fullgöra sin nya roll som AI-tillsynsmyndighet för EU:s offentliga förvaltning. Vidare beskrivs inte EDPS roll och uppgifter tillräckligt utförligt och bör klargöras närmare i förslaget, särskilt vad gäller dess roll som marknadskontrollmyndighet.

43. EDPB och EDPS bekräftar fördelningen av finansiella medel, som förutses för nämnden och EDPS, som fungerar som anmälande organ, i förslaget. Uppfyllandet av de nya skyldigheter som förutses för EDPS, oavsett om denne agerar anmält organ eller inte, skulle dock kräva betydligt mer finansiella medel och mänskligt kapital.

44. För det första eftersom artikel 63.6 är formulerad så att EDPS ”ska fungera som marknadskontrollmyndighet” för unionens institutioner, byråer och organ som omfattas av förordningens tillämpningsområde, vilket inte klargör om EDPS ska betraktas som en fullständigt auktoriserad marknadskontrollmyndighet, i enlighet med förordning (EU) 2019/1020. Detta väcker frågor om skyldigheter och befogenheter för EDPS i praktiken. För det andra, och förutsatt att denna fråga besvaras jakande, är det oklart hur EDPS roll, i enlighet med förordning (EU) 2018/1725, kan tillgodose uppgiften i artikel 11 i förordning (EU)

2019/1020, som omfattar ”effektiv marknadskontroll inom deras territorium av produkter som görs tillgängliga på [...] internet” eller ”fysiska kontroller eller kontroller i laboratorium baserat på ett adekvat urval”. Om den nya uppsättningen uppgifter antas utan närmare förklaring i förslaget finns det en risk för att fullgörandet av dess skyldigheter som datatillsynsman kan äventyras.

45. EDPB och EDPS betonar dock att vissa bestämmelser i förslaget i vilka de olika behöriga myndigheternas uppgifter och befogenheter fastställs enligt AI-förordningen, liksom deras förhållanden, deras funktion och garantin att de är oberoende, verkar vara oklara i detta skede. Medan det i förordning (EU) 2019/1020 anges att marknadskontrollmyndigheten måste vara oberoende, krävs det inte i utkastet till förordning att tillsynsmyndigheter ska vara oberoende, och de ska till och med rapportera till kommissionen om vissa uppgifter som utförs av marknadskontrollmyndigheter, som kan vara andra institutioner. Eftersom det i förslaget även anges att dataskyddsmyndigheterna kommer att vara marknadskontrollmyndigheter för AI-system som används för brottsbekämpande ändamål (artikel 63.5) innebär detta att de, möjligen via sin nationella tillsynsmyndighet, också ska ha rapporteringsskyldigheter till kommissionen (artikel 63.2), vilket förefaller oförenligt med deras oberoende.

46. Därför finner EDPB och EDPS att dessa bestämmelser måste förtydligas så att de överensstämmer med förordning (EU) 2019/1020, förordning (EU) 2018/1725 och den allmänna dataskyddsförordningen, samt att det i förslaget tydligt fastslås att tillsynsmyndigheterna enligt AI-förordningen måste vara fullständigt oberoende i utförandet av sina uppgifter, då detta skulle vara en avgörande garanti för korrekt övervakning och verkställande av den framtida förordningen.

47. EDPB och EDPS vill även påminna om att dataskyddsmyndigheterna redan tillser verkställandet av den allmänna dataskyddsförordningen, förordning (EU) 2018/1725 och direktivet om dataskydd vid brottsbekämpning vad gäller AI-system som involverar personuppgifter, för att skydda de grundläggande rättigheterna och mer specifikt rätten till dataskydd. Dataskyddsmyndigheterna är därför, såsom krävs i förslaget om nationella tillsynsmyndigheter, redan något insatta i AI-teknik, data och databehandling, grundläggande rättigheter, samt har expertis inom bedömning av de risker för grundläggande rättigheter som nya tekniker medför. När AI-system bygger på behandling av personuppgifter eller behandlar personuppgifter är bestämmelserna i förslaget direkt sammanflätade med den rättsliga ramen för dataskydd, vilket kommer att vara fallet för de flesta AI-system inom förordningens tillämpningsområde. Det kommer därför att finnas gränsöverskridande befogenheter mellan tillsynsmyndigheter enligt förslaget och dataskyddsmyndigheter.

48. Av detta följer att utnämningen av dataskyddsmyndigheter till nationella tillsynsmyndigheter skulle säkerställa en mer harmoniserad regleringsmetod, och bidra till en konsekvent tolkning av bestämmelserna om databehandling och undvika motsägelsefullt verkställande i de olika medlemsstaterna. Det skulle även gynna alla intressenter i AI-värdekedjan att ha en enda kontaktpunkt för alla behandlingar av personuppgifter som ingår i förslagets tillämpningsområde och begränsa samspelet mellan två olika tillsynsorgan för behandling som berörs av förslaget och den allmänna dataskyddsförordningen. EDPB och EDPS finner

följaktligen att **dataskyddsmyndigheter bör utses till nationella tillsynsmyndigheter i enlighet med artikel 59 i förslaget**.

49. I den mån förslaget innehåller särskilda regler om skydd för enskilda vid behandling av personuppgifter som antas på grundval av artikel 16 i fördraget om Europeiska unionens funktionssätt, måste efterlevnaden av dessa regler, särskilt begränsningar av användningen av AI-system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser i brottsbekämpande syfte, under alla omständigheter **kontrolleras av oberoende myndigheter**.

50. Det finns dock ingen uttrycklig bestämmelse i förslaget som skulle tilldela befogenhet att säkerställa efterlevnaden av dessa regler till oberoende myndigheters kontroll. Den enda hänvisningen till behöriga tillsynsmyndigheter för dataskydd enligt den allmänna dataskyddsförordningen eller direktivet om dataskydd vid brottsbekämpning finns i artikel 63.5 i förslaget, men bara som marknadskontrollmyndigheter och alternativt med vissa andra myndigheter. EDPB och EDPS finner att detta inte säkerställer efterlevnaden av kravet för oberoende kontroll som fastställs i artikel 16.2 i fördraget om Europeiska unionens funktionssätt och artikel 8 i stadgan.

2.5.2 Den europeiska AI-nämnden

51. Enligt förslaget inrättas en europeisk nämnd för artificiell intelligens. EDPB och EDPS förstår behovet av en konsekvent och harmoniserad tillämpning av den föreslagna ramen, liksom medverkan av oberoende experter i framtagningen av EU:s politik för AI. Samtidigt innebär förslaget att kommissionen ges en tongivande roll. Kommissionen skulle inte bara delta i den europeiska nämnden för artificiell intelligens utan också leda den och ha vetorätt vad gäller antagandet av nämndens arbetsordning. Detta skiljer sig från behovet av ett europeiskt AI-organ som är oberoende av allt politiskt inflytande. Därför finner EDPB och EDPS att den framtida AI-förordningen bör ge **den europeiska nämnden för artificiell intelligens större autonomi**, så att nämnden verkligen kan säkerställa att förordningen tillämpas konsekvent på hela den inre marknaden

52. EDPB och EDPS noterar även att den europeiska nämnden för artificiell intelligens inte ges någon befogenhet att tillse verkställandet av den föreslagna förordningen. Med tanke på AI-systemens spridning över den inre marknaden och sannolikheten för gränsöverskridande fall finns det ändå ett stort behov av ett harmoniserat verkställande och vederbörlig tilldelning av befogenheter mellan nationella tillsynsmyndigheter. EDPB och EDPS rekommenderar därför att samarbetsmekanismerna mellan nationella tillsynsmyndigheter specificeras i den framtida AI-förordningen. EDPB och EDPS föreslår att en mekanism införs som för varje AI-system garanterar en enda kontaktpunkt för enskilda personer som berörs av lagstiftningen, såväl som för företag, och att den europeiska nämnden för artificiell intelligens till förmån för organisationer vars verksamhet täcker över hälften av EU:s medlemsstater får utse den nationella myndighet som ska ansvara för verkställandet av AI-förordningen för detta AI-system.

53. Vidare, och med tanke på oberoendet av de myndigheter som nämnden ska bestå av, ska den senare ha befogenhet att agera på eget initiativ och inte bara för att ge kommissionen råd och assistans. EDPB och EDPS understryker därför att det är nödvändigt att utvidga det uppdrag som nämnden tilldelas, som dessutom inte motsvarar de uppgifter som förtecknas i förslaget.

54. För att tillmötesgå dessa syften **ska den europeiska nämnden för artificiell intelligens ha tillräckliga och lämpliga befogenheter**, och dess rättsliga status ska förtydligas. För att det relevanta tillämpningsområdet för den framtida förordningen ska fortsätta vara relevant verkar det nödvändigt att de myndigheter som ansvarar för dess tillämpning måste involveras i dess utveckling. EDPB och EDPS rekommenderar därför att den europeiska nämnden för artificiell intelligens bör ha rätt att föreslå ändringar av bilaga I till kommissionen, i vilken AI-teknikerna och AI-metoderna fastställs, och av bilaga III som innehåller förteckningen över AI-system med hög risk som avses i artikel 6.2. Den europeiska nämnden för artificiell intelligens ska även höras av kommissionen före alla ändringar av dessa bilagor.

55. I artikel 57.4 i förslaget föreskrivs utbyten mellan nämnden och andra unionsorgan, unionskontor, unionsbyråer och rådgivande grupper. Med tanke på dess tidigare arbete på AI-området och dess expertis på området mänskliga rättigheter rekommenderar EDPB och EDPS att nämnden bör överväga FRA som en av observatörerna i nämnden.

3 SAMSPEL MED RAMEN FÖR DATASKYDD

3.1 Förslagets förhållande till EU:s befintliga dataskyddslagstiftning

56. Ett tydligt fastställt förhållande mellan förslaget och EU:s befintliga dataskyddslagstiftning är en nödvändig förutsättning för att säkerställa och upprätthålla respekten för och tillämpningen av EU:s regelverk inom området skydd av personuppgifter. Sådan EU-lagstiftning, särskilt den allmänna dataskyddsförordningen, förordning (EU) 2018/1725 och direktivet om dataskydd vid brottsbekämpning, måste betraktas som en förutsättning som ytterligare lagförslag kan bygga på utan att påverka eller hindra de befintliga bestämmelserna, inräknat vad gäller befogenheten för tillsynsmyndigheter och styrning.

57. EDPB och EDPS anser därför att det är viktigt att förslaget tydligt undviker alla bristande överensstämmelser och möjliga konflikter med den allmänna dataskyddsförordningen, förordning (EU) 2018/1725 och direktivet om dataskydd vid brottsbekämpning. Detta är inte bara en fråga om rättssäkerhet, utan syftar också till att förslaget inte direkt eller indirekt ska äventyra den grundläggande rättigheten till skydd av personuppgifter, i enlighet med artikel 16 i fördraget om Europeiska unionens funktionssätt och artikel 8 i stadgan.

58. I synnerhet kan självlärande maskiner skydda enskilda personers personuppgifter endast om detta byggs in i själva designfasen. Den direkta möjligheten att utöva rättigheterna för enskilda personer enligt artikel 22 (automatiserat individuellt beslutsfattande, inbegripet profilering) i den allmänna dataskyddsförordningen eller artikel 23 i förordning (EU) 2018/1725, oavsett behandlingens syfte, är också avgörande. I detta hänseende måste de registrerades övriga rättigheter gällande rätten att få sina uppgifter borttagna och rätten att få sina uppgifter

korrigerade i enlighet med dataskyddslagstiftningen vara inlagda i AI-systemen redan från början, oavsett den valda AI-metoden eller tekniska arkitekturen.

59. Användning av personuppgifter för AI-systeminlärning kan leda till skapandet av snedvridna beslutsmönster i AI-systemets kärna. Vid sådana processer bör det därför krävas olika skyddsåtgärder och i synnerhet kvalificerad mänsklig tillsyn, för att de registrerades rättigheter ska respekteras och garanteras, och för att undvika eventuella negativa effekter för enskilda personer. Behöriga myndigheter bör även kunna föreslå riktlinjer för att bedöma snedvridning i AI-system och assistera vid utövandet av mänsklig tillsyn.

60. När de registrerades data används för AI-utbildning och/eller AI-prognos ska de alltid informeras om den rättsliga grunden för sådan behandling och få en allmän förklaring av AI-systemets logik (förfarande) och tillämpningsområde. Enskilda personers rättighet till begränsning av behandlingen (artikel 18 i den allmänna dataskyddsförordningen och artikel 20 i förordning (EU) 2018/1725) samt borttagning/radering av data (artikel 16 i den allmänna dataskyddsförordningen och artikel 19 i förordning (EU) 2018/1725) ska alltid garanteras i dessa fall. Vidare ska den personuppgiftsansvarige vara uttryckligen skyldig att informera den registrerade om de gällande tidsperioderna för invändning, begränsning, radering av data osv. AI-systemet måste kunna uppfylla alla dataskyddskrav genom tillräckliga tekniska och organisatoriska åtgärder. Rätten till förklaring bör bidra till ytterligare transparens.

3.2 Sandlåda och ytterligare behandling (artiklarna 53 och 54 i förslaget)

61. Inom de befintliga rättsliga och moraliska gränserna är det viktigt att främja europeisk innovation med hjälp av verktyg såsom en sandlåda. En sandlåda gör det möjligt att tillhandahålla de skyddsåtgärder som krävs för att bygga upp tillit till och förtroende för AI-systemen. I komplexa miljöer kan det vara svårt för AI-utövare att på ett lämpligt sätt väga in alla intressen. Särskilt för små och medelstora företag med begränsade resurser kan verksamheten i en regulatorisk sandlåda ge snabbare insikter som främjar innovationer.

62. I artikel 53.3 i förslaget anges att sandlådan inte påverkar tillsynsbefogenheter eller korrigerande befogenheter. Om detta förtydligande är till nytta finns det även ett behov av vägledning eller riktlinje för hur man uppnår en bra balans mellan att å ena sidan vara en tillsynsmyndighet och å andra sidan ge utförliga riktlinjer genom en sandlåda.

63. I artikel 53.6 anges att formerna och villkoren för sandlådornas drift ska fastställas i genomförandeakter. Det är viktigt att specifika riktlinjer tas fram för att säkerställa enhetlighet och stöd i upprättandet och driften av sandlådor. Bindande genomförandeakter kan dock inskränka medlemsstaternas förmåga att anpassa sandlådan efter sina behov och lokal praxis. EDPB och EDPS rekommenderar därför i stället att den europeiska nämnden för artificiell intelligens tillhandahåller riktlinjer för sandlådor.

64. Artikel 54 i förslaget försöker ge en rättslig grund för ytterligare behandling av personuppgifter för att utveckla vissa AI-system i allmänhetens intresse i den regulatoriska AI-sandlådan. Förhållandet mellan artikel 54.1 i förslaget och artikel 54.2 och skäl 41 i förslaget, och därigenom även EU:s befintliga dataskyddslagstiftning, förblir oklart. I den allmänna

dataskyddsförordningen och förordning (EU) 2018/1725 har dock redan en grund lagts för ”ytterligare behandling”. Särskilt när det är i allmänhetens intresse att tillåta ytterligare behandling måste inte balansering mellan den personuppgiftsansvariges intressen och den registrerades intressen vara ett hinder för innovation. Artikel 54 i förslaget tar för närvarande inte upp två viktiga frågor: i) under vilka omständigheter och med hjälp av vilka (ytterligare) kriterier som de registrerades intressen vägs, och ii) huruvida dessa AI-system bara kommer att användas inuti sandlådan. EDPB och EDPS välkomnar kravet på en EU- eller medlemsstatslagstiftning vid behandling av personuppgifter som insamlats enligt direktivet om dataskydd vid brottsbekämpning i en sandlåda, men rekommenderar att det närmare anges vad som planeras här, på ett sätt som överensstämmer med den allmänna dataskyddsförordningen och förordning (EU) 2018/1725, främst genom att förtydliga att den rättsliga grunden för sådana sandlådor bör uppfylla kraven i artikel 23.2 i den allmänna dataskyddsförordningen och artikel 25 i förordning (EU) 2018/1725, och precisera att alla användningar av sandlådan måste genomgå grundlig utvärdering. Detta gäller också den fullständiga förteckningen över villkor i artikel 54.1 led b–j.

65. Vissa ytterligare överväganden avseende återanvändningen av data i artikel 54 i förslaget visar att driften av en sandlåda är resursintensiv och att det därför är realistiskt att anta att endast ett litet antal företag skulle få möjlighet att delta. Deltagande i sandlådan kan vara en konkurrensfördel. För att kunna återanvända data skulle man noga behöva överväga valet av deltagare för att säkerställa att de omfattas av tillämpningsområdet och undgår ojämlik behandling. EDPS och EDPB befarar att möjliggörandet av återanvändning av data inom ramen för sandlådan avviker från ansvarsprincipen i den allmänna dataskyddsförordningen, där ansvarsskyldighet läggs på den personuppgiftsansvarige och inte på den behöriga myndigheten.

66. Med tanke på målsättningarna med sandlådan, som är att utveckla, testa och validera AI-systemen, finner EDPB och EDPS dessutom att sandlådorna inte kan omfattas av tillämpningsområdet för direktivet om dataskydd vid brottsbekämpning. Eftersom direktivet om dataskydd vid brottsbekämpning föreskriver återanvändning av data för vetenskaplig forskning kommer de data som behandlas för detta andrahandssyfte att omfattas av den allmänna dataskyddsförordningen eller förordning (EU) 2018/1725 och inte längre av direktivet om dataskydd vid brottsbekämpning.

67. Det är inte klart vad en regulatorisk sandlåda kommer att omfatta. Frågan är om den föreslagna regulatoriska sandlådan innefattar en it-infrastruktur i varje medlemsstat med vissa ytterligare rättsliga grunder för ytterligare behandling, eller om den bara organiserar tillgång till regulatoriska expertkunskaper och riktlinjer. EDPB och EDPS manar lagstiftaren att förtydliga detta begrepp i förslaget och att i förslaget tydligt ange att den regulatoriska sandlådan inte innebär att behöriga myndigheter är skyldiga att tillhandahålla dess tekniska infrastruktur. I många fall måste finansiella medel och mänskligt kapital följaktligen tillhandahållas till de behöriga myndigheterna för ett sådant förtydligande.

68. Slutligen vill EDPB och EDPS lyfta fram utvecklingen av gränsöverskridande AI-system som kommer att finnas tillgängliga för den europeiska digitala inre marknaden i sin helhet. För sådana AI-system bör inte den regulatoriska sandlådan i sin funktion som innovationsverktyg bli ett hinder för gränsöverskridande utveckling. EDPB och EDPS rekommenderar därför en samordnad gränsöverskridande strategi som fortfarande är tillräckligt tillgänglig på nationell nivå för små och medelstora företag och erbjuder en gemensam ram för hela Europa utan att vara för begränsande. En balans mellan europeisk samordning och nationella förfaranden måste uppnås för att undvika oförenligt genomförande av den framtida AI-förordningen som skulle hindra EU-övergripande innovation.

3.3 Transparens

69. EDPB och EDPS välkomnar att AI-system med hög risk ska registreras i en offentlig databas (som avses i artiklarna 51 och 60 i förslaget). Denna databas bör ses som en möjlighet att ge allmänheten information om AI-systemens tillämpningsområde och om kända brister och händelser som kan äventyra deras funktion och de korrigerande åtgärder som leverantörerna har vidtagit för att hantera och reparera dem.

70. En central demokratisk princip är användningen av kontroller och motvikter. Det faktum att transparenskravet inte gäller för AI-system som används för att upptäcka, förebygga, utreda och lagföra brott utgör därför ett alltför brett undantag. Man måste skilja mellan AI-system som används för att upptäcka eller förebygga och AI-system som är avsedda att utreda och hjälpa till att lagföra brott. Skyddsåtgärder för förebyggande och avslöjande måste vara starkare på grund av presumtionen för oskuld. Vidare beklagar EDPB och EDPS avsaknaden av varningar i förslaget, vilket kan tolkas som ett grönt ljus för att till och med använda ostyrkta AI-system eller AI-tillämpningar med hög risk.

71. I de fall där sekretessen medför att liten eller ingen transparens kan erbjudas allmänheten ska skyddsåtgärder finnas på plats också i en välfungerande demokrati och dessa AI-system bör registreras och vara transparenta för den behöriga tillsynsmyndigheten.

72. Att säkerställa transparens i AI-system är ett mål med högt ställda krav. Det fullständigt kvantitativa beslutsförfarandet för många AI-system, vilket i sig är annorlunda från ett mänskligt förfarande som främst förlitar sig på kausala och teoretiska resonemang, kan stå i konflikt med behovet av en föregående begriplig förklaring av maskinresultaten. Förordningen bör främja nya och mer proaktiva sätt att tidigt och när som helst informera användare av AI-system om systemets (beslutsfattande) status, och ge tidig varning om potentiellt skadliga resultat så att enskilda personer vars rättigheter och friheter kan vara menligt påverkade av maskinens självständiga beslut kan reagera eller söka prövning av beslutet.

3.4 Behandling av särskilda datakategorier och data beträffande brott

73. Behandlingen av särskilda datakategorier inom brottsbekämpning styrs av bestämmelserna i EU:s ram för dataskydd, inräknat direktivet om dataskydd vid brottsbekämpning samt dess nationella genomförande. Förslaget gör inga anspråk på att tillhandahålla en allmän rättslig grund för behandling av personuppgifter, inräknat särskilda kategorier av personuppgifter, jämför

skäl 41. Samtidigt står det i artikel 10.5 i förslaget att ”leverantörer av sådana system [får] behandla särskilda kategorier av personuppgifter”. Vidare krävs ytterligare skyddsåtgärder i samma bestämmelse, som även ger exempel. På så vis verkar förslaget hindra tillämpningen av den allmänna dataskyddsförordningen, direktivet om dataskydd vid brottsbekämpning och förordning (EU) 2018/1725. EDPB och EDPS välkomnar försöket att anordna adekvata skyddsåtgärder men finner att en enhetligare regleringsmetod är nödvändig, då de aktuella bestämmelserna inte förefaller tillräckligt tydliga för att skapa en rättslig grund för behandling av särskilda datakategorier och måste kompletteras med ytterligare skyddsåtgärder som fortfarande behöver bedömas. När personuppgifter dessutom har insamlats genom behandling inom tillämpningsområdet för direktivet om dataskydd vid brottsbekämpning kommer de möjliga ytterligare skyddsåtgärderna och begränsningarna till följd av det nationella införlivandet av direktivet om dataskydd vid brottsbekämpning att behöva beaktas.

3.5 Efterlevnadsmekanismer

3.5.1 Certifiering

74. En av de främsta pelarna i förslaget är certifiering. Det certifieringssystem som beskrivs i förslaget bygger på en struktur av enheter (anmälande myndigheter/anmälda organ/kommissionen) och en mekanism för bedömning av överensstämmelse/certifiering som täcker de obligatoriska kraven för AI-system med hög risk, och bygger på europeiska harmoniserade standarder enligt förordning (EU) nr 1025/2012 samt gemensamma specifikationer som ska fastställas av kommissionen. Denna mekanism skiljer sig från certifieringssystemet som är avsett att säkerställa efterlevnad av regler och principer för dataskydd, vilket beskrivs i artiklarna 42 och 43 i den allmänna dataskyddsförordningen. Det är dock inte klart hur intyg som utfärdas av anmälda organ i enlighet med förslaget kan samordnas med certifieringar, förseglingar och märkningar för dataskydd enligt den allmänna dataskyddsförordningen, till skillnad från vad som föreskrivs för andra typer av certifieringar (se artikel 42.2 vad gäller certifieringar som utfärdats enligt förordning (EU) 2019/881).

75. I den mån AI-system med hög risk bygger på behandling av personuppgifter eller behandlar personuppgifter för att fullgöra sin uppgift kan dessa avvikelser ge upphov till rättsosäkerhet för alla berörda organ, eftersom de kan leda till situationer i vilka AI-system som certifieras enligt förslaget och märks med en CE-märkning om överensstämmelse, efter att de släpps ut på marknaden eller tas i bruk, kan användas på ett sätt som inte uppfyller reglerna och principerna för dataskydd.

76. Förslaget saknar en klar koppling till dataskyddslagstiftningen liksom till EU:s och medlemsstaternas övriga lagstiftning för varje ”område” av AI-system med hög risk som förtecknas i bilaga III. Förslaget ska i synnerhet innefatta principerna om uppgiftsminimering och inbyggt dataskydd som en av de aspekter som bör övervägas före erhållandet av CE-märkning, på grund av den höga nivå av störning som AI-systemet med hög risk innebär för den grundläggande rätten till integritet och skyddet av personuppgifter, samt behovet av en säkerställd hög nivå av tillit till AI-systemet. EDPB och EDPS rekommenderar därför att förslaget ändras för att förtydliga sambandet mellan intyg som utfärdas enligt den nämnda

förordningen och certifieringar, förseglingar och märkningar för dataskydd. Slutligen bör dataskyddsmyndigheterna involveras för att utarbeta och införa harmoniserade standarder och gemensamma specifikationer.

77. I samband med artikel 43 i förslaget, gällande bedömningen av överensstämmelse, verkar undantaget från förfarandena för bedömning av överensstämmelse som fastställs i artikel 47 utgöra ett alltför brett och omfattande undantag, genom att inbegripa exceptionella skäl som rör allmän säkerhet eller skydd av människors liv och hälsa, miljöskydd och skydd av viktiga industriella och infrastrukturella tillgångar. Vi vill föreslå att lagstiftarna begränsar detta.

3.5.2 Uppförandekoder

78. I enlighet med artikel 69 i förslaget ska kommissionen och medlemsstaterna uppmuntra och underlätta utarbetandet av uppförandekoder som syftar till att främja frivillig tillämpning, bland leverantörer av AI-system som inte utgör hög risk, av kraven för AI-system med hög risk, liksom ytterligare krav. I linje med skäl 78 i den allmänna dataskyddsförordningen rekommenderar EDPB och EDPS att synergier identifieras och fastställs mellan dessa instrument och de uppförandekoder som föreskrivs i den allmänna dataskyddsförordningen som stöder efterlevnad av dataskyddet. I detta sammanhang är det relevant att förtydliga att skyddet av personuppgifter ska övervägas bland ”ytterligare krav” som kan hanteras genom de uppförandekoder som avses i artikel 69.2. Det är också relevant att säkerställa att de ”tekniska specifikationerna och lösningarna”, som hanteras genom de uppförandekoder som avses i artikel 69.1, som tagits fram för att främja efterlevnad av kraven i utkastet till förordning om AI, inte strider mot reglerna och principerna i den allmänna dataskyddsförordningen och förordning (EU) 2018/1725. Efterlevnaden av dessa verktyg bland leverantörer av AI-system som inte utgör hög risk – i den mån sådana system bygger på behandling av personuppgifter eller behandlar personuppgifter för att fullgöra sin uppgift – skulle på så vis ge ett mervärde, eftersom det säkerställer att den personuppgiftsansvarige och personuppgiftsbiträdena kommer att kunna fullgöra sina skyldigheter för dataskyddet inom användningen av dessa system.

79. Samtidigt skulle den rättsliga ramen för tillförlitlig AI kompletteras av integreringen av uppförandekoder, för att skapa förtroende för att denna teknik används på ett sätt som är säkert och förenligt med lagstiftningen, inbegripet respekten för de grundläggande rättigheterna. Formgivningen av dessa instrument bör dock förstärkas genom att inplanera mekanismer som ska kontrollera att sådana koder tillhandahåller effektiva ”tekniska specifikationer och lösningar” och fastställer ”tydliga mål och centrala resultatindikatorer för att mäta uppnåendet av dessa mål” som integrerade delar av koderna i fråga. Vidare kan avsaknaden av all hänvisning till (obligatoriska) övervakningsmekanismer för uppförandekoder som utformats för att kontrollera att leverantörer av AI-system som inte utgör hög risk efterlever bestämmelserna, liksom möjligheten att enskilda leverantörer utarbetar (och själva genomför) dessa koder (se avsnitt 5.2.7 i motiveringen) ytterligare försvaga dessa instruments effekt och verkställighet.

80. Slutligen efterfrågar EDPB och EDPS förtydliganden vad gäller vilka typer av initiativ som kommissionen kan ta fram, i enlighet med skäl 81 i förslaget, ”för att minska de tekniska hindren för gränsöverskridande utbyte av data för AI-utveckling”.

4 SLUTSATS

81. Även om EDPB och EDPS välkomnar kommissionens förslag och finner att en sådan förordning är nödvändig för att garantera de grundläggande rättigheterna för medborgare och bosatta inom EU, finner de att förslaget behöver anpassas i flera frågor för att säkerställa dess tillämplighet och effektivitet.

82. Förslagets komplexitet samt de frågor det avser besvara gör att mycket arbete återstår innan förslaget kan utgöra en välfungerande rättslig ram, som effektivt kompletterar den allmänna dataskyddsförordningen i skyddet av grundläggande mänskliga rättigheter och samtidigt främjar innovationer. EDPB och EDPS kommer även fortsättningsvis finnas till förfogande och erbjuda sitt stöd i denna strävan.

Bryssel den 18 juni 2021

För Europeiska dataskyddsstyrelsen	För Europeiska datatillsynsmannen
Ordförande	Tillsynsmannen
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI