Fælles udtalelse fra

Databeskyttelsesrådet og Den Europæiske Tilsynsførende for Databeskyttelse 5/2021

om forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens)

18. juni 2021

Resumé

Den 21. april 2021 forelagde Europa-Kommissionen sit forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (herefter "forslaget"). Databeskyttelsesrådet og EDPS bifalder lovgiverens indsats for at behandle anvendelsen af kunstig intelligens (AI) i Den Europæiske Union (EU) og understreger, at forslaget har fremtrædende **databeskyttelsesmæssige konsekvenser**.

Databeskyttelsesrådet og EDPS noterer sig, at **retsgrundlaget** for forslaget først og fremmest er artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Desuden er forslaget baseret på artikel 16 i TEUF, for så vidt som det indeholder specifikke regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, navnlig begrænsninger i anvendelsen af AI-systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse. Databeskyttelsesrådet og EDPS minder om, at artikel 16 i TEUF i overensstemmelse med praksis ved Den Europæiske Unions Domstol (EU-Domstolen) udgør et passende retsgrundlag, når beskyttelsen af personoplysninger er et af de væsentlige formål med eller led i de af EU-lovgiver vedtagne regler. Anvendelsen af artikel 16 i TEUF indebærer også **et behov for at sikre et uafhængigt tilsyn med overholdelsen** af kravene vedrørende behandling af personoplysninger, således som det også kræves i artikel 8 i EU's charter om grundlæggende rettigheder.

Med hensyn til **forslagets anvendelsesområde** ser Databeskyttelsesrådet og EDPS med stor tilfredshed på, at det også omfatter tilvejebringelsen og anvendelsen af AI-systemer i EU's institutioner, organer eller agenturer **Udelukkelsen af internationalt retshåndhævelsessamarbejde fra forslagets anvendelsesområde** giver imidlertid anledning til alvorlige betænkeligheder for Databeskyttelsesrådet og EDPS, da en sådan udelukkelse skaber en betydelig risiko for omgåelse (f.eks. tredjelande eller internationale organisationer, der gør brug af højrisikoanvendelser, som offentlige myndigheder i EU sætter deres lid til).

Databeskyttelsesrådet og EDPS **bifalder den risikobaserede tilgang,** der ligger til grund for forslaget. Denne tilgang bør imidlertid præciseres, og begrebet "risiko for grundlæggende rettigheder" bør tilpasses GDPR og forordning (EU) 2018/1725 (EUDPR), eftersom det drejer sig om aspekter vedrørende beskyttelse af personoplysninger.

Databeskyttelsesrådet og EDPS er enige i forslaget, når det anføres, at klassificeringen af et **AI-system som et højrisikosystem ikke nødvendigvis betyder, at det er lovligt** i sig selv og kan anvendes af brugeren som sådant. **Yderligere krav, der følger af EU's databeskyttelseslovgivning, skal i givet fald overholdes** af den dataansvarlige. Overholdelsen af de retlige forpligtelser, der følger af EU-lovgivningen (herunder om beskyttelse af personoplysninger), bør endvidere være en forudsætning for at få tilladelse til at komme ind på det europæiske marked som CE-mærket produkt. Med henblik herpå mener Databeskyttelsesrådet og EDPS, at **kravet om at sikre overholdelse af GDPR og EUDPR bør indføjes i afsnit III, kapitel 2**. Desuden finder Databeskyttelsesrådet og EDPS det nødvendigt at tilpasse forslagets overensstemmelsesvurderingsprocedure, således at tredjeparter altid foretager forudgående overensstemmelsesvurderinger af højrisiko-AI-systemer.

I betragtning af den store risiko for forskelsbehandling forbyder forslaget sociale pointsystemer (social scoring), når denne praksis udøves "over en given periode" eller "fra offentlige myndigheders side eller på deres vegne". Private virksomheder, såsom udbydere af sociale medier og cloudtjenester, kan imidlertid også behandle enorme mængder personoplysninger og bruge sociale pointsystemer. Som følge heraf **bør den kommende forordning om kunstig intelligens forbyde enhver form for sociale pointsystemer**.

Biometrisk fjernidentifikation af enkeltpersoner på offentlige steder udgør en høj risiko for krænkelse af enkeltpersoners privatliv med alvorlige følger for befolkningernes forventning om at være anonyme i det offentlige rum. Af disse grunde opfordrer Databeskyttelsesrådet og EDPS **til, at der indføres et generelt forbud mod enhver anvendelse af kunstig intelligens til automatisk genkendelse af menneskelige træk på offentlige steder** – såsom af ansigter, men også af gangart, fingeraftryk, DNA, stemme, tastetryk og andre biometriske eller adfærdsmæssige signaler – i enhver sammenhæng. Der anbefales ligeledes et **forbud mod AI-systemer, der kategoriserer personer på grundlag af biometri i klynger** efter etnicitet, køn samt politisk eller seksuel orientering eller andre grunde til forskelsbehandling i henhold til chartrets artikel 21. Endvidere mener Databeskyttelsesrådet og EDPS, at anvendelsen af kunstig intelligens til at **udlede en fysisk persons følelser er yderst uønsket og bør forbydes.**

Databeskyttelsesrådet og EDPS bifalder **udpegelsen af EDPS som kompetent myndighed og markedsovervågningsmyndighed med ansvar for tilsynet med Unionens institutioner, agenturer og organer**. EDPS' rolle og opgaver bør imidlertid præciseres yderligere, navnlig med hensyn til rollen som markedsovervågningsmyndighed. Endvidere bør den kommende forordning om kunstig intelligens klart fastslå **tilsynsmyndighedernes uafhængighed** i udførelsen af deres tilsyns- og håndhævelsesopgaver.

Udpegelsen af databeskyttelsesmyndigheder som nationale tilsynsmyndigheder ville sikre en mere harmoniseret reguleringsmæssig tilgang og bidrage til en konsekvent fortolkning af bestemmelserne om databehandling og undgå uoverensstemmelser i håndhævelsen heraf blandt medlemsstaterne. Som følge heraf mener Databeskyttelsesrådet og EDPS, at **databeskyttelsesmyndigheder bør udpeges som nationale tilsynsmyndigheder i henhold til forslagets artikel 59.**

Forslaget giver Kommissionen en fremtrædende rolle i Det Europæiske Udvalg for Kunstig Intelligens (EAIB). En sådan rolle er i strid med behovet for, at et europæisk organ for kunstig intelligens er uafhængigt af enhver politisk indflydelse. Med den kommende forordning om kunstig intelligens bør **EAIB sikres mere autonomi,** for at det kan forblive uafhængigt og handle på eget initiativ.

I betragtning af udbredelsen af AI-systemer i det indre marked og sandsynligheden for grænseoverskridende tilfælde er der et afgørende behov for en harmoniseret håndhævelse og en korrekt kompetencefordeling mellem de nationale tilsynsmyndigheder. Databeskyttelsesrådet og EDPS foreslår, at der indføres **en mekanisme, der for hvert AI-system sikrer et enkelt kontaktpunkt for enkeltpersoner, der er berørt af lovgivningen, samt for virksomheder.**

Med hensyn til **sandkasserne anbefaler** Databeskyttelsesrådet og EDPS **en præcisering af deres anvendelsesområde og mål**. Det bør også klart fremgå af forslaget, at retsgrundlaget for sådanne sandkasser bør opfylde de krav, der er fastsat i den eksisterende databeskyttelsesramme.

Det **certificeringssystem,** der fremgår af forslaget, **mangler en klar forbindelse til EU's databeskyttelseslovgivning** og til anden EU-ret og medlemsstatslovgivning, der finder anvendelse på hvert "område" af højrisiko-AI-systemer, og tager ikke hensyn til **principperne om dataminimering og databeskyttelse gennem design** som ét af de aspekter, der skal tages i betragtning, **inden der opnås CE-mærkning**. Databeskyttelsesrådet og EDPS anbefaler derfor, at forslaget ændres for at præcisere forholdet

mellem certifikater udstedt i henhold til den nævnte forordning og databeskyttelsescertifikater, -mærkninger og -mærker. Endelig bør databeskyttelsesmyndighederne inddrages i udarbejdelsen og fastlæggelsen af harmoniserede standarder og fælles specifikationer.

Med hensyn til **adfærdskodekserne** finder Databeskyttelsesrådet og EDPS det **nødvendigt at præcisere,** om beskyttelsen af personoplysninger skal betragtes som "yderligere krav", der kan opfyldes af disse adfærdskodekser, og at sikre, at de "tekniske specifikationer og løsninger" ikke er i strid med reglerne og principperne i EU's eksisterende databeskyttelsesramme.

INDHOLDSFORTEGNELSE

Det Europæiske Databeskyttelsesråd og Den Europæiske Tilsynsførende for Databeskyttelse har –

under henvisning til artikel 42, stk. 2, i forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF[1],

under henvisning til EØS-aftalen, særlig bilag XI og protokol 37, som ændret ved afgørelse nr. 154/2018 truffet af Det Blandede EØS-Udvalg den 6. juli 2018[2],

under henvisning til anmodningen om en fælles udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse og Det Europæiske Databeskyttelsesråd af 22. april 2021 vedrørende forslaget om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) –

VEDTAGET FØLGENDE FÆLLES UDTALELSE

1 INDLEDNING

1. Fremkomsten af systemer for kunstig intelligens ("AI") er et meget vigtigt skridt med hensyn til udviklingen af teknologier og den måde, hvorpå mennesker interagerer med dem. Kunstig intelligens er et sæt centrale teknologier, der i væsentlig grad vil ændre vores dagligdag, hvad enten det er ud fra et samfundsmæssigt eller økonomisk synspunkt. I de næste par år forventes der afgørende beslutninger om kunstig intelligens, da det hjælper os med at overvinde nogle af de største udfordringer, vi står over for på mange områder i dag, lige fra sundhed til mobilitet eller fra offentlig forvaltning til uddannelse.

2. Disse lovede fremskridt er imidlertid ikke uden risici. Risiciene er således meget relevante i betragtning af, at de individuelle og samfundsmæssige virkninger af AI-systemer i vid udstrækning ikke opleves. Generering af indhold, udarbejdelse af forudsigelser eller automatisk beslutningstagning, som AI-systemer gør, ved hjælp af maskinlæringsteknikker eller logik og regler om probabilistisk inferens er ikke det samme som mennesker, der udfører disse aktiviteter ved hjælp af kreativ eller teoretisk ræsonnement, og som er fuldt ansvarlige for konsekvenserne.

3. Kunstig intelligens vil øge mængden af forudsigelser, der kan foretages på mange områder, med udgangspunkt i målbare korrelationer mellem data, som er usynlige for det menneskelige øje, men synlige for maskiner, hvilket vil gøre vores liv lettere og løse en lang række problemer, men samtidig svække vores evne til at foretage en kausal fortolkning af resultaterne på en sådan måde, at begreberne gennemsigtighed, menneskelig kontrol, ansvarlighed og ansvar i forhold til resultaterne vil blive alvorligt udfordret.

[1] EUT L 295 af 21.11.2018, s. 39-98.
[2] Henvisninger til "medlemsstater" i dette dokument skal forstås som henvisninger til "EØS-medlemsstater".

4. Data (personoplysninger og andre data end personoplysninger) inden for kunstig intelligens er i mange tilfælde den vigtigste forudsætning for selvstændige beslutninger, som uundgåeligt vil påvirke den enkeltes liv på forskellige niveauer. Dette er grunden til, at Databeskyttelsesrådet og EDPS allerede på nuværende tidspunkt gør kraftigt gældende, at forslaget til forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) ("forslaget")[3] har **vigtige databeskyttelsesmæssige konsekvenser**.

5. Hvis man overlader opgaven med at træffe beslutninger til maskiner på grundlag af data, vil det skabe risici for enkeltpersoners rettigheder og frihedsrettigheder, påvirke deres privatliv og kan skade grupper eller endog samfund som helhed. Databeskyttelsesrådet og EDPS understreger, at retten til privatlivets fred og til beskyttelse af personoplysninger, som er i modstrid med den antagelse om maskiners beslutningsautonomi, der ligger til grund for begrebet kunstig intelligens, er en grundpille i EU's værdier som anerkendt i verdenserklæringen om menneskerettigheder (artikel 12), den europæiske menneskerettighedskonvention (artikel 8) og EU's charter om grundlæggende rettigheder (herefter "chartret") (artikel 7 og 8). Det er et meget ambitiøst, men nødvendigt mål at forene vækstperspektivet i forbindelse med AI-anvendelser og menneskers centrale rolle og forrang i forhold til maskiner.

6. Databeskyttelsesrådet og EDPS bifalder, at alle interessenter i AI-værdikæden inddrages i reguleringen, og at der indføres specifikke krav til udbydere af løsninger, da de spiller en væsentlig rolle i forbindelse med de produkter, der gør brug af deres systemer. De forskellige parters ansvar – bruger, udbyder, importør eller distributør af et AI-system – skal dog klart afgrænses og fordeles. Navnlig i forbindelse med behandling af personoplysninger bør der lægges særlig vægt på, at disse roller og ansvarsområder er i overensstemmelse med begreberne dataansvarlig og databehandler i databeskyttelsesrammen, da de to begreber ikke er overensstemmende.

7. Forslaget giver begrebet menneskeligt tilsyn (artikel 14) en central plads, hvilket Databeskyttelsesrådet og EDPS hilser velkomment. På grund af visse AI-systemers store potentielle indvirkning på enkeltpersoner eller grupper af enkeltpersoner bør imidlertid som nævnt menneskers reelt centrale rolle udnytte et højt kvalificeret menneskeligt tilsyn og en lovlig behandling, for så vidt som sådanne systemer er baseret på behandling af personoplysninger eller behandler personoplysninger for at udføre deres opgaver, så det sikres, at retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, respekteres.

8. På grund af mange AI-anvendelsers dataintensive karakter bør forslaget endvidere fremme indførelsen af en tilgang med databeskyttelse gennem design og gennem standardindstillinger på alle niveauer og tilskynde til en effektiv gennemførelse af databeskyttelsesprincipper (som fastsat i artikel 25 i GDPR og artikel 27 i EUDPR) ved hjælp af de mest avancerede teknologier.

9. Endelig understreger Databeskyttelsesrådet og EDPS, at denne fælles udtalelse kun afgives som en foreløbig analyse af forslaget, uden at dette berører eventuelle yderligere vurderinger

[3] COM(2021) 206 final.

og udtalelser om forslagets virkninger og dets forenelighed med EU's databeskyttelseslovgivning.

2 ANALYSE AF HOVEDPRINCIPPERNE I FORSLAGET

2.1 Forslagets anvendelsesområde og forholdet til den eksisterende retlige ramme

10. Ifølge begrundelsen er **retsgrundlaget** for forslaget først og fremmest artikel 114 i TEUF, som indeholder bestemmelser om vedtagelse af foranstaltninger, der skal sikre det indre markeds oprettelse og funktion[4]. Desuden er forslaget baseret på artikel 16 i TEUF, *for så vidt som det indeholder specifikke regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger*, navnlig begrænsninger i anvendelsen af AI-systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse[5].

11. Databeskyttelsesrådet og EDPS minder om, at artikel 16 i TEUF i overensstemmelse med EU-Domstolens praksis udgør et passende retsgrundlag, når beskyttelsen af personoplysninger er et af de væsentlige formål med eller led i de af EU-lovgiver vedtagne regler[6]. Anvendelsen af artikel 16 i TEUF indebærer også et behov for at sikre et uafhængigt tilsyn med overholdelsen af kravene vedrørende behandling af personoplysninger, således som det også kræves i chartrets artikel 8.

12. EDPS og Databeskyttelsesrådet minder om, at der allerede findes en omfattende databeskyttelsesramme, der er vedtaget på grundlag af artikel 16 i TEUF, bestående af den generelle forordning om databeskyttelse (GDPR)[7], databeskyttelsesforordningen for Den Europæiske Unions institutioner, kontorer, organer og agenturer (EUDPR)[8] og direktivet om databeskyttelse på retshåndhævelsesområdet (retshåndhævelsesdirektivet)[9]. Ifølge forslaget er det kun de yderligere begrænsninger for behandling af biometriske data, der er indeholdt i forslaget, som kan anses for at være baseret på artikel 16 i TEUF og derfor have samme retsgrundlag som GDPR, EUDPR eller retshåndhævelsesdirektivet. Dette har betydelige konsekvenser for forholdet mellem forslaget og GDPR, EUDPR og retshåndhævelsesdirektivet mere generelt som anført nedenfor.

---

[4] Begrundelsen, s. 5.
[5] Begrundelsen, s. 6. Se også forslagets betragtning 2.
[6] Udtalelse af 26. juli 2017, *PNR Canada*, udtalelsessag 1/15, ECLI:EU:C:2017:592, præmis 96.
[7] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), EUT L 119 af 4.5.2016, s. 1-88.
[8] Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF, EUT L 295 af 21.11.2018, s. 39-98.
[9] Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA, EUT L 119 af 4.5.2016, s. 89-131.

13. Med hensyn til **forslagets anvendelsesområde** ser Databeskyttelsesrådet og EDPS med stor tilfredshed på, at forslaget også omfatter anvendelsen af AI-systemer i EU's institutioner, organer eller agenturer. Eftersom disse enheders anvendelse af AI-systemer også kan have en betydelig indvirkning på enkeltpersoners grundlæggende rettigheder i lighed med anvendelsen i EU-medlemsstaterne, er det absolut nødvendigt, at den nye lovramme for kunstig intelligens finder anvendelse på både EU-medlemsstaterne og EU's institutioner, kontorer, organer og agenturer for at sikre en sammenhængende tilgang i hele Unionen. Da EU's institutioner, kontorer, organer og agenturer kan fungere både som udbydere og brugere af AI-systemer, finder EDPS og Databeskyttelsesrådet det fuldt ud hensigtsmæssigt at lade disse enheder være omfattet af forslagets anvendelsesområde på grundlag af artikel 114 i TEUF.

14. Databeskyttelsesrådet og EDPS har imidlertid alvorlige betænkeligheder med hensyn til udelukkelsen af internationalt retshåndhævelsessamarbejde fra det anvendelsesområde, der er fastsat i forslagets artikel 2, stk. 4. Denne udelukkelse skaber en betydelig risiko for omgåelse (f.eks. tredjelande eller internationale organisationer, der gør brug af højrisikoanvendelser, som offentlige myndigheder i EU sætter deres lid til).

15. Udviklingen og anvendelsen af AI-systemer vil i mange tilfælde omfatte behandling af personoplysninger. Det er yderst vigtigt at sikre klarhed i forholdet mellem dette forslag og den eksisterende EU-lovgivning om databeskyttelse. Forslaget berører ikke, men supplerer GDPR, EUDPR og retshåndhævelsesdirektivet. Selv om betragtningerne til forslaget præciserer, at anvendelsen af AI-systemer stadig bør være i overensstemmelse med databeskyttelseslovgivningen, **anbefaler Databeskyttelsesrådet og EDPS kraftigt, at det præciseres i forslagets artikel 1, at Unionens lovgivning om beskyttelse af personoplysninger**, navnlig GDPR, EUDPR, e-databeskyttelsesdirektivet[10] og retshåndhævelsesdirektivet, finder anvendelse på enhver behandling af personoplysninger, der er omfattet af forslagets anvendelsesområde. I en tilhørende betragtning bør det ligeledes præciseres, at forslaget ikke har til formål at påvirke anvendelsen af eksisterende EU-lovgivning om behandling af personoplysninger, herunder de opgaver og beføjelser, der påhviler de uafhængige tilsynsmyndigheder med kompetence til at overvåge, at disse instrumenter overholdes.

2.2 Risikobaseret tilgang

16. Databeskyttelsesrådet og EDPS **bifalder den risikobaserede tilgang,** der ligger til grund for forslaget. Forslaget vil finde anvendelse på alle AI-systemer, herunder systemer, der ikke omfatter behandling af personoplysninger, men som stadig kan have indvirkning på interesser eller grundlæggende rettigheder og frihedsrettigheder.

17. Databeskyttelsesrådet og EDPS bemærker, at nogle af bestemmelserne i forslaget udelader risiciene for grupper af enkeltpersoner eller samfundet som helhed (f.eks. samlede virkninger med særlig relevans, såsom gruppediskrimination eller politiske meningstilkendegivelser i det

[10] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) som ændret ved direktiv 2006/24/EF og direktiv 2009/136/EF.

offentlige rum). Databeskyttelsesrådet og EDPS anbefaler, at risici for grupper/samfundet, der er forbundet med AI-systemer, ligeledes bør vurderes og afbødes.

18. Databeskyttelsesrådet og EDPS er af den opfattelse, at forslagets risikobaserede tilgang bør præciseres, og at begrebet "risiko for grundlæggende rettigheder" bør **tilpasses GDPR**, for så vidt som det drejer sig om aspekter vedrørende beskyttelse af personoplysninger. Hvad enten der er tale om slutbrugere, blot registrerede eller andre personer, der er omfattet af AI-systemet, forekommer den manglende henvisning i teksten til den person, der er berørt af AI-systemet, at være et blindt punkt i forslaget. De forpligtelser, der pålægges aktører over for de berørte personer, bør således mere konkret komme fra beskyttelsen af den enkelte og dennes rettigheder. Databeskyttelsesrådet og EDPS opfordrer derfor lovgiverne til i forslaget udtrykkeligt at behandle de **rettigheder og retsmidler, der er til rådighed for enkeltpersoner,** der er omfattet af AI-systemer.

19. Databeskyttelsesrådet og EDPS noterer sig valget med hensyn til at tilvejebringe en udtømmende liste over **højrisiko-AI-systemer**. Dette valg kan skabe en sort-hvid effekt med ringe tiltrækningsevne i meget risikobetonede situationer og underminere den overordnede risikobaserede tilgang, der ligger til grund for forslaget. Denne liste over højrisiko-AI-systemer, der er nærmere anført i bilag II og III til forslaget, mangler ligeledes visse typer anvendelsestilfælde, der indebærer betydelige risici, såsom anvendelsen af kunstig intelligens til fastsættelse af forsikringspræmien eller til vurdering af lægebehandlinger eller til sundhedsforskningsformål. Databeskyttelsesrådet og EDPS understreger også, at disse bilag vil skulle ajourføres regelmæssigt for at sikre, at deres anvendelsesområde er passende.

20. Ifølge forslaget skal **udbyderne** af AI-systemet foretage en risikovurdering, men i de fleste tilfælde vil de dataansvarlige være **brugerne** og ikke udbyderne af AI-systemerne (f.eks. er en bruger af et ansigtsgenkendelsessystem en "dataansvarlig" og er derfor ikke bundet af kravene til udbydere af højrisiko-AI-systemer i henhold til forslaget).

21. Desuden vil det **ikke altid være muligt for en udbyder at vurdere alle anvendelser** i forbindelse med AI-systemet. Den indledende risikovurdering vil således have en mere generel karakter end den, der foretages af brugeren af AI-systemet. Selv om udbyderens indledende risikovurdering ikke viser, at AI-systemet udgør en "høj risiko" i henhold til forslaget, bør dette ikke udelukke **en efterfølgende (mere detaljeret) vurdering** (konsekvensanalyse vedrørende databeskyttelse ("DPIA") i henhold til artikel 35 i GDPR, artikel 39 i EUDPR eller artikel 27 i retshåndhævelsesdirektivet), **som bør foretages af brugeren af systemet**, under hensyntagen til anvendelsessammenhængen og de specifikke anvendelsestilfælde. Fortolkningen af, om en type behandling i henhold til GDPR, EUDPR og retshåndhævelsesdirektivet sandsynligvis vil indebære en høj risiko, skal foretages uafhængigt af forslaget. Klassificeringen af et AI-system som et system, der udgør en "høj risiko" på grund af dets indvirkning på de grundlæggende rettigheder[11], **udløser imidlertid en formodning om "høj risiko" i henhold til GDPR, EUDPR og retshåndhævelsesdirektivet, for så vidt som der behandles personoplysninger.**

[11] Den Europæiske Unions Agentur for Grundlæggende Rettigheder (FRA) har allerede behandlet nødvendigheden af at foretage konsekvensanalyser vedrørende grundlæggende rettigheder, når der anvendes kunstig intelligens eller relaterede teknologier. I sin rapport fra 2020, "Rettidig omhu for fremtiden – Kunstig

22. **Databeskyttelsesrådet og EDPS er enige i forslaget, når det præciseres, at klassificeringen af et AI-system som højrisikosystem ikke nødvendigvis betyder, at det er lovligt i sig selv og kan anvendes af brugeren som sådant. Yderligere krav, der følger af EU's databeskyttelseslovgivning, skal i givet fald overholdes af den dataansvarlige.** Desuden skal den underliggende begrundelse for forslagets artikel 5, hvorefter højrisikosystemerne i modsætning til forbudte systemer i princippet kan være tilladt, behandles og fjernes i forslaget, navnlig da den foreslåede CE-mærkning ikke indebærer, at den dermed forbundne behandling af personoplysninger er lovlig.

23. Overholdelsen af de retlige forpligtelser, der følger af EU-lovgivningen (herunder om beskyttelse af personoplysninger), bør imidlertid være en forudsætning for at få tilladelse til at komme ind på det europæiske marked som CE-mærket produkt. Med henblik herpå anbefaler Databeskyttelsesrådet og EDPS, **at der i forslagets afsnit III, kapitel 2, indføjes et krav om at sikre overholdelse af GDPR og EUDPR**. Disse krav skal auditeres (ved tredjepartsaudit) før CE-mærkningen i overensstemmelse med ansvarlighedsprincippet. I forbindelse med denne tredjepartsvurdering vil den indledende konsekvensanalyse, som skal foretages af udbyderen, være særlig relevant.

24. I betragtning af kompleksiteten som følge af udviklingen af AI-systemer bør det påpeges, at AI-systemers tekniske karakteristika (f.eks. typen af AI-tilgang) kan medføre større risici. Derfor bør enhver risikovurdering af et AI-system tage hensyn til **de tekniske karakteristika** sammen **med dets specifikke anvendelsestilfælde og den sammenhæng**, som systemet indgår i.

25. I lyset af ovenstående anbefaler Databeskyttelsesrådet og EDPS, at det præciseres i forslaget, at **udbyderen** skal foretage en indledende risikovurdering af det pågældende AI-system **under hensyntagen til anvendelsestilfældene** (som skal angives i forslaget – som supplement til f.eks. bilag III, punkt 1, litra a), hvor anvendelsestilfældene af biometriske AI-systemer ikke er nævnt), og at **brugeren** af AI-systemet i sin egenskab af dataansvarlig i henhold til EU's databeskyttelseslovgivning (hvis det er relevant) skal foretage konsekvensanalysen vedrørende databeskyttelse, jf. artikel 35 i GDPR, artikel 39 i EUDPR og artikel 27 i retshåndhævelsesdirektivet, under hensyntagen ikke blot til de tekniske karakteristika og **anvendelsestilfældet**, men **også den specifikke sammenhæng**, som den kunstige intelligens vil indgå i.

26. Desuden bør nogle af de udtryk, der er nævnt i bilag III til forslaget, f.eks. udtrykket "væsentlige private tjenester" eller mindre udbydere, der anvender kunstig intelligens i forbindelse med vurdering af kreditværdighed til eget brug, præciseres.

---

intelligens og grundlæggende rettigheder", identificerede FRA "faldgruber i brugen af AI, f.eks. i forbindelse med forudsigende politiarbejde, medicinske diagnoser, sociale tjenester og målrettet reklame" og understregede, at "private og offentlige organisationer bør foretage vurderinger af, hvordan AI kan skade de grundlæggende rettigheder" for at mindske negative følgevirkninger for enkeltpersoner.

2.3 Forbudte anvendelser af kunstig intelligens

27. Databeskyttelsesrådet og EDPS mener, at **indgribende former for kunstig intelligens** – navnlig dem, der kan påvirke den menneskelige værdighed – skal betragtes som forbudte AI-systemer i henhold til forslagets artikel 5 i stedet for blot at blive klassificeret som "højrisiko" i bilag III til forslaget, f.eks. systemerne under punkt 6. Dette gælder navnlig for datasammenligning, der i stor skala også berører personer, der ikke eller kun i ringe omfang har givet anledning til politiovervågning, eller behandling, der svækker princippet om formålsbegrænsning i henhold til databeskyttelseslovgivningen. Anvendelsen af kunstig intelligens inden for politi og retshåndhævelse kræver områdespecifikke, præcise, forudsigelige og forholdsmæssige regler, der skal tage hensyn til de berørte personers interesser og indvirkningen på et demokratisk samfunds funktion.

28. Forslagets artikel 5 risikerer at blive tomme floskler om "værdierne" og forbuddet mod AI-systemer i modsætning til sådanne værdier. Kriterierne i artikel 5 om at "klassificere" AI-systemerne som forbudte **begrænser forbuddets anvendelsesområde** i et sådant omfang, at det kan vise sig at være meningsløst i praksis (f.eks. "påfører eller sandsynligvis vil påføre [...] fysisk eller psykisk skade" i artikel 5, stk. 1, litra a) og b), begrænsning til offentlige myndigheder i artikel 5, stk. 1, litra c), vag formulering i litra c), nr. i) og ii), begrænsning til kun biometrisk fjernidentifikation i realtid uden nogen klar definition osv.).

29. Navnlig kan anvendelsen af kunstig intelligens til sociale pointsystemer (social scoring), jf. forslagets artikel 5, stk. 1, litra c), føre til forskelsbehandling og er i strid med EU's grundlæggende værdier. Forslaget forbyder kun disse former for praksis, når de udøves "over en given periode" eller "fra offentlige myndigheders side eller på deres vegne". Private virksomheder, navnlig udbydere af sociale medier og cloudtjenester, kan behandle enorme mængder personoplysninger og bruge sociale pointsystemer. Som følge heraf **bør forslaget forbyde enhver form for sociale pointsystemer**. Det skal bemærkes, at artikel 4 i retshåndhævelsesdirektivet i forbindelse med retshåndhævelse allerede i betydelig grad begrænser – hvis ikke i praksis forbyder – denne type aktiviteter.

30. **Biometrisk fjernidentifikation** af enkeltpersoner på offentlige steder udgør en høj risiko for krænkelse af enkeltpersoners privatliv. Databeskyttelsesrådet og EDPS mener derfor, **at der er behov for en strengere tilgang**. Anvendelsen af AI-systemer kan give alvorlige problemer med proportionaliteten, da det kan indebære behandling af oplysninger om et vilkårligt og uforholdsmæssigt stort antal registrerede med henblik på identifikation af kun få personer (f.eks. passagerer i lufthavne og på togstationer). Den **gnidningsløse** karakter af systemer til biometrisk fjernidentifikation giver også anledning til problemer med gennemsigtighed og problemstillinger i forbindelse med retsgrundlaget for behandlingen i henhold til EU-retten (retshåndhævelsesdirektivet, GDPR, EUDPR og anden gældende ret). Problemet med hensyn til, hvordan enkeltpersoner kan underrettes behørigt om denne behandling, er stadig ikke løst, og det samme er tilfældet med hensyn til enkeltpersoners effektive og rettidige udøvelse af deres rettigheder. Det samme gælder **dens uoprettelige og alvorlige følge for befolkningernes** (rimelige) **forventning om at være anonyme i det offentlige rum**, hvilket

har en direkte negativ indvirkning på udøvelsen af ytrings-, forsamlings-, forenings- og bevægelsesfriheden.

31. Forslagets artikel 5, stk. 1, litra d), indeholder en omfattende **liste over ekstraordinære tilfælde**, hvor biometrisk fjernidentifikation i realtid på offentlige steder er tilladt med henblik på retshåndhævelse. Databeskyttelsesrådet og EDPS finder **denne tilgang mangelfuld** i flere henseender: For det første er det uklart, hvad der skal forstås ved "væsentlig forsinkelse", og hvordan det kan anses som en formildende omstændighed i betragtning af, at et system til masseidentifikation er i stand til at identificere tusindvis af personer på nogle få timer. Desuden afhænger behandlingens indgribende karakter ikke altid af, om identifikationen sker i realtid eller ej. Efterfølgende biometrisk fjernidentifikation i forbindelse med en politisk protest vil sandsynligvis have en betydelig afdæmpende virkning på udøvelsen af de grundlæggende rettigheder og frihedsrettigheder, såsom forsamlings- og foreningsfriheden og mere generelt de grundlæggende demokratiske principper. For det andet afhænger behandlingens indgribende karakter ikke nødvendigvis af dens formål. Anvendelsen af dette system til andre formål, f.eks. privat sikkerhed, udgør de samme trusler mod de grundlæggende rettigheder om respekt for privatliv og familieliv og beskyttelse af personoplysninger. Endelig vil det potentielle antal mistænkte eller gerningsmænd til kriminalitet – selv med de planlagte begrænsninger – næsten altid være "højt nok" til at retfærdiggøre en fortsat anvendelse af AI-systemer til afsløring af mistænkte, trods de yderligere betingelser i forslagets artikel 5, stk. 2-4. Begrundelsen for forslaget synes at udelade, at forpligtelserne i henhold til EU's databeskyttelseslovgivning ved overvågning af åbne områder skal opfyldes ikke blot for mistænkte, men for alle, der i praksis overvåges.

32. Af alle disse grunde opfordrer Databeskyttelsesrådet og EDPS **til, at der indføres et generelt forbud mod enhver anvendelse af kunstig intelligens til automatisk genkendelse af menneskelige træk på offentlige steder – såsom af ansigter, men også af gangart, fingeraftryk, DNA, stemme, tastetryk og andre biometriske eller adfærdsmæssige signaler – i enhver sammenhæng**. Den nuværende tilgang i forslaget er at identificere og opregne alle AI-systemer, der bør forbydes. Af konsekvenshensyn bør **AI-systemer til fjernidentifikation i stor skala på online steder** således forbydes i henhold til forslagets artikel 5. Under hensyntagen til retshåndhævelsesdirektivet, EUDPR og GDPR kan EDPS og Databeskyttelsesrådet ikke se, hvordan denne form for praksis vil kunne opfylde kravene om nødvendighed og proportionalitet, og dette følger i sidste ende af, hvad EU-Domstolen og Menneskerettighedsdomstolen anser for acceptable indgreb i grundlæggende rettigheder.

33. Desuden **anbefaler** Databeskyttelsesrådet og EDPS **et forbud**, for både offentlige myndigheder og private enheder, mod **AI-systemer, der kategoriserer personer på grundlag af biometri (f.eks. ansigtsgenkendelse) i klynger efter etnicitet, køn samt politisk eller seksuel orientering eller andre grunde til forskelsbehandling, der er forbudt i henhold til chartrets artikel 21, eller** AI-systemer, hvis videnskabelige gyldighed ikke er dokumenteret, eller som er i direkte modstrid med EU's væsentlige værdier (f.eks. polygrafer, bilag III, punkt 6, litra b), og punkt 7, litra a)). "**Biometrisk kategorisering**" bør derfor **forbydes i henhold til artikel 5**.

34. Det påvirker også **den menneskelige værdighed, at en persons fremtidige adfærd fastlægges eller klassificeres af en computer uafhængigt af den pågældendes egen frie vilje**. AI-systemer, der er beregnet til at blive anvendt af retshåndhævende myndigheder til at foretage individuelle risikovurderinger af fysiske personer for at vurdere risikoen for, at en fysisk person begår eller genbegår lovovertrædelser, jf. bilag III, punkt 6, litra a), eller til at forudsige forekomsten eller gentagelsen af en faktisk eller potentiel strafbar handling ud fra profilering af fysiske personer eller til at vurdere personlighedstræk og personlige egenskaber eller tidligere kriminel adfærd, jf. bilag III, punkt 6, litra e), og som anvendes i overensstemmelse med deres tilsigtede formål, vil føre til, at politiets og retsinstansernes beslutninger bliver afgørende, hvorved det berørte menneske objektiveres. Sådanne AI-systemer, der berører det væsentligste indhold af retten til menneskelig værdighed, bør forbydes i henhold til artikel 5.

35. Endvidere mener Databeskyttelsesrådet og EDPS, at anvendelsen af kunstig intelligens til at **udlede en fysisk persons følelser er yderst uønsket og bør forbydes,** undtagen i visse veldefinerede anvendelsestilfælde, nemlig til sundheds- eller forskningsformål (f.eks. patienter, hvor følelsesgenkendelse er vigtig), altid med passende garantier på plads og naturligvis med forbehold af alle andre databeskyttelsesbetingelser og -begrænsninger, herunder formålsbegrænsning.

2.4 Højrisiko-AI-systemer

2.4.1 Behov for en forudgående overensstemmelsesvurdering foretaget af eksterne tredjeparter

36. Databeskyttelsesrådet og EDPS glæder sig over, at AI-systemer, der udgør en høj risiko, skal underkastes en forudgående overensstemmelsesvurdering, inden de bringes i omsætning eller på anden måde tages i brug i EU. I princippet hilses denne reguleringsmodel velkommen, da den sikrer en passende balance mellem innovationsvenlighed og et højt niveau af proaktiv beskyttelse af de grundlæggende rettigheder. For at kunne anvendes i særlige miljøer, såsom beslutningsprocesser i offentlige institutioner eller kritisk infrastruktur, skal der fastlægges metoder til at undersøge den fuldstændige kildekode.

37. Databeskyttelsesrådet og EDPS går dog ind for at tilpasse overensstemmelsesvurderingsproceduren i henhold til forslagets artikel 43, således at **der generelt af tredjeparter skal foretages en forudgående overensstemmelsesvurdering af højrisiko-AI-systemer**. Selv om en af tredjepart foretaget overensstemmelsesvurdering af højrisikobehandling af personoplysninger ikke er et krav i GDPR eller EUDPR, er de risici, der er forbundet med AI-systemer, endnu ikke fuldt ud forstået. En generel indføjelse af en forpligtelse til overensstemmelsesvurderinger foretaget af tredjeparter vil derfor yderligere styrke retssikkerheden og tilliden til alle højrisiko-AI-systemer.

2.4.2 Forordningens anvendelsesområde skal også omfatte AI-systemer, der allerede er i brug

38. I henhold til forslagets artikel 43, stk. 4, bør højrisiko-AI-systemer underkastes en ny overensstemmelsesvurderingsprocedure, hvis der foretages en væsentlig ændring. Det er det

rigtige at sikre, at AI-systemer opfylder kravene i forordningen om kunstig intelligens gennem hele deres livscyklus. AI-systemer, der er bragt i omsætning eller taget i brug inden anvendelsen af den foreslåede forordning (eller 12 måneder derefter for store IT-systemer, der er opført i bilag IX), er udelukket fra deres anvendelsesområde, medmindre disse systemer er genstand for "betydelige ændringer" af design eller tilsigtet formål (artikel 83).

39. Tærsklen for "betydelige ændringer" er dog uklar. I forslagets betragtning 66 fastsættes en lavere tærskel for ny overensstemmelsesvurdering, "når der sker en ændring, som kan have indflydelse på systemets overensstemmelse". En tilsvarende tærskel ville være hensigtsmæssig i artikel 83, i det mindste for højrisiko-AI-systemer. For at lukke eventuelle huller i beskyttelsen er det desuden nødvendigt, at AI-systemer, der allerede er indført og anvendes – efter en vis gennemførelsesfase – også opfylder alle kravene i forordningen om kunstig intelligens.

40. De mange muligheder for behandling af personoplysninger og eksterne risici påvirker ligeledes AI-systemers sikkerhed. Fokus i artikel 83 på "betydelige ændringer af design eller tilsigtet formål" omfatter ikke en henvisning til ændringer i eksterne risici. En henvisning til ændringer i trusselsscenariet, der følger af eksterne risici, f.eks. cyberangreb, fjendtlige angreb og begrundede klager fra forbrugere, bør derfor indføjes i forslagets artikel 83.

41. Da datoen for anvendelse er planlagt til 24 måneder efter den kommende forordnings ikrafttræden, finder EDPS og Databeskyttelsesrådet det endvidere ikke hensigtsmæssigt at undtage AI-systemer, der allerede er bragt i omsætning i en endnu længere periode. Selv om forslaget også fastsætter, at kravene i forordningen skal tages i betragtning ved evalueringen af hvert af de store IT-systemer, jf. de retsakter, der er opført i bilag IX, mener Databeskyttelsesrådet og EDPS, at kravene vedrørende ibrugtagning af AI-systemer bør finde anvendelse fra datoen for den kommende forordnings anvendelse.

2.5 Forvaltning og Det Europæiske Udvalg for Kunstig Intelligens

2.5.1 Forvaltning

42. Databeskyttelsesrådet og EDPS bifalder udpegelsen af EDPS som kompetent myndighed og markedsovervågningsmyndighed med ansvar for tilsynet med Unionens institutioner, agenturer og organer, når de er omfattet af dette forslags anvendelsesområde. EDPS er rede til at udfylde sin nye rolle som AI-reguleringsmyndighed for EU's offentlige forvaltning. Endvidere er EDPS' rolle og opgaver ikke tilstrækkeligt detaljerede og bør præciseres yderligere i forslaget, navnlig med hensyn til rollen som markedsovervågningsmyndighed.

43. Databeskyttelsesrådet og EDPS anerkender den tildeling af finansielle ressourcer, der er fastsat i forslaget til udvalget og EDPS' funktion som et bemyndigende organ. Udførelsen af EDPS' nye opgaver – uanset om det er i funktionen som bemyndiget organ – vil imidlertid kræve betydeligt større finansielle og menneskelige ressourcer.

44. For det første fordi det af ordlyden af artikel 63, stk. 6, fremgår, at EDPS "fungerer [...] som [...] markedsovervågningsmyndighed" for Unionens institutioner, agenturer og organer, der er omfattet af forslagets anvendelsesområde, hvilket ikke præciserer, om EDPS skal betragtes

som en fuldgyldig "markedsovervågningsmyndighed" som fastsat i forordning (EU) 2019/1020. Dette rejser spørgsmål om EDPS' opgaver og beføjelser i praksis. For det andet – og forudsat at det foregående spørgsmål besvares bekræftende – er det uklart, hvordan EDPS' rolle i henhold til EUDPR kan dække den opgave, der er fastsat i artikel 11 i forordning (EU) 2019/1020, som omfatter "effektiv markedsovervågning på deres område af produkter, som er gjort tilgængelige online" eller "fysisk kontrol og laboratorieundersøgelser baseret på et passende antal prøver". Der er risiko for, at det nye sæt opgaver uden yderligere præciseringer i forslaget kan bringe opfyldelsen af EDPS' forpligtelser som tilsynsførende for databeskyttelse i fare.

45. Databeskyttelsesrådet og EDPS understreger imidlertid, at nogle bestemmelser i forslaget, der definerer de forskellige kompetente myndigheders opgaver og beføjelser i henhold til forordningen om kunstig intelligens, deres forbindelser, deres art og garantien for deres uafhængighed, synes uklare på nuværende tidspunkt. Mens markedsovervågningsmyndigheden i henhold til forordning 2019/1020 skal være uafhængig, kræves det ikke i udkastet til forordning, at tilsynsmyndigheder er uafhængige, og det er endda fastsat, at de skal aflægge rapport til Kommissionen om visse opgaver, der udføres af markedsovervågningsmyndigheder, som kan være forskellige institutioner. Da det ligeledes fremgår af forslaget, at databeskyttelsesmyndigheder vil være markedsovervågningsmyndigheder for AI-systemer, der anvendes til retshåndhævelsesformål (artikel 63, stk. 5), betyder det også, at de, eventuelt via deres nationale tilsynsmyndighed, vil være omfattet af rapporteringsforpligtelser over for Kommissionen (artikel 63, stk. 2), hvilket synes at være uforeneligt med deres uafhængighed.

46. Databeskyttelsesrådet og EDPS mener derfor, at disse bestemmelser bør præciseres for at være i overensstemmelse med forordning 2019/1020, EUDPR og GDPR, og forslaget bør klart fastslå, at tilsynsmyndigheder i henhold til forordningen om kunstig intelligens skal være fuldstændig uafhængige i udførelsen af deres opgaver, da dette vil være en væsentlig garanti for korrekt tilsyn med og håndhævelse af den kommende forordning.

47. Databeskyttelsesrådet og EDPS vil også gerne minde om, at databeskyttelsesmyndigheder allerede håndhæver GDPR, EUDPR og retshåndhævelsesdirektivet i forhold til AI-systemer, hvor personoplysninger er involveret, for at sikre beskyttelsen af de grundlæggende rettigheder og, mere specifikt, retten til databeskyttelse. Derfor har databeskyttelsesmyndighederne allerede i et vist omfang, – som det kræves i forslaget med hensyn til de nationale tilsynsmyndigheder – en forståelse af AI-teknologier, data og databehandling, grundlæggende rettigheder samt ekspertise i at vurdere de risici for de grundlæggende rettigheder, der er forbundet med nye teknologier. Når AI-systemer er baseret på behandling af personoplysninger eller behandler personoplysninger, er forslagets bestemmelser desuden direkte forbundet med den retlige ramme for databeskyttelse, hvilket vil være tilfældet for de fleste AI-systemer inden for forordningens anvendelsesområde. Som følge heraf vil der være indbyrdes forbindelser af kompetencer mellem tilsynsmyndigheder i henhold til forslaget og databeskyttelsesmyndigheder.

48. Udpegelsen af databeskyttelsesmyndigheder som nationale tilsynsmyndigheder ville derfor sikre en mere harmoniseret reguleringsmæssig tilgang og bidrage til en konsekvent fortolkning

af bestemmelserne om databehandling og undgå uoverensstemmelser i håndhævelsen heraf blandt medlemsstaterne. Det vil også være til gavn for alle interessenter i AI-værdikæden at have et enkelt kontaktpunkt for alle behandlingsaktiviteter vedrørende personoplysninger, der er omfattet af forslagets anvendelsesområde, og begrænse interaktionerne mellem to forskellige reguleringsorganer for behandling, der er berørt af forslaget og GDPR. Som følge heraf mener Databeskyttelsesrådet og EDPS, at **databeskyttelsesmyndigheder bør udpeges som nationale tilsynsmyndigheder i henhold til forslagets artikel 59**.

49. For så vidt som forslaget indeholder specifikke regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, der er vedtaget på grundlag af artikel 16 i TEUF, skal overholdelsen af disse regler, navnlig begrænsninger i anvendelsen af AI-systemer til biometrisk fjernidentifikation i realtid på offentlig steder med henblik på retshåndhævelse, under alle omstændigheder **være underlagt uafhængige myndigheders kontrol**.

50. Der er imidlertid ingen udtrykkelig bestemmelse i forslaget, hvorefter kompetencen til at sikre overholdelsen af disse regler overlades til uafhængige myndigheders kontrol. Den eneste henvisning til kompetente databeskyttelsesmyndigheder i henhold til GDPR eller retshåndhævelsesdirektivet findes i forslagets artikel 63, stk. 5, men kun som "markedsovervågningsmyndigheder" og alternativt sammen med andre myndigheder. Databeskyttelsesrådet og EDPS mener, at denne opbygning ikke sikrer overholdelse af kravet om uafhængig kontrol i artikel 16, stk. 2, i TEUF og chartrets artikel 8.

2.5.2 Det Europæiske Udvalg for Kunstig Intelligens

51. Med forslaget oprettes Det Europæiske Udvalg for Kunstig Intelligens (EAIB). Databeskyttelsesrådet og EDPS anerkender behovet for en konsekvent og harmoniseret anvendelse af den foreslåede ramme samt uafhængige eksperters inddragelse i udviklingen af EU's politik for kunstig intelligens. Samtidig lægges der i forslaget op til at give Kommissionen en fremtrædende rolle. Således vil sidstnævnte ikke alene være en del af EAIB, men også varetage udvalgets formandskab og have vetoret i forbindelse med vedtagelsen af EAIB's forretningsorden. Dette står i modsætning til behovet for et europæisk organ for kunstig intelligens, der er uafhængigt af enhver politisk indflydelse. Databeskyttelsesrådet og EDPS mener derfor, at den kommende forordning om kunstig intelligens bør give **EAIB mere autonomi**, således at det virkelig kan sikre en konsekvent anvendelse af forordningen i hele det indre marked.

52. Databeskyttelsesrådet og EDPS bemærker også, at EAIB ikke er tillagt nogen beføjelse vedrørende håndhævelsen af den foreslåede forordning. I betragtning af udbredelsen af AI-systemer i det indre marked og sandsynligheden for grænseoverskridende tilfælde er der dog et afgørende behov for en harmoniseret håndhævelse og en korrekt kompetencefordeling mellem de nationale tilsynsmyndigheder. Databeskyttelsesrådet og EDPS anbefaler derfor, at samarbejdsmekanismerne mellem de nationale tilsynsmyndigheder præciseres i den kommende forordning om kunstig intelligens. Databeskyttelsesrådet og EDPS foreslår, at der indføres en mekanisme, der for hvert AI-system sikrer et enkelt kontaktpunkt for enkeltpersoner, der er berørt af lovgivningen, samt for virksomheder, og at EAIB for organisationer, hvis aktiviteter dækker mere end halvdelen af EU's medlemsstater, kan udpege

den nationale myndighed, der vil være ansvarlig for at håndhæve forordningen om kunstig intelligens for dette AI-system.

53. I betragtning af den uafhængige karakter af de myndigheder, som udvalget skal være sammensat af, har sidstnævnte endvidere ret til at handle på eget initiativ og ikke kun til at yde rådgivning og bistand til Kommissionen. Databeskyttelsesrådet og EDPS understreger derfor behovet for en udvidelse af den mission, der er tildelt udvalget, som endvidere ikke svarer til de opgaver, der er anført i forslaget.

54. For at opfylde disse formål skal **EAIB have tilstrækkelige og passende beføjelser**, og udvalgets retlige status bør præciseres. For at den kommende forordnings materielle anvendelsesområde fortsat er relevant, synes det navnlig nødvendigt at inddrage de myndigheder, der er ansvarlige for dens anvendelse, i dens udvikling. Databeskyttelsesrådet og EDPS anbefaler derfor, at EAIB får beføjelse til at foreslå Kommissionen ændringer af bilag I, der definerer teknikker og tilgange til kunstig intelligens, og af bilag III, der indeholder en liste over de højrisiko-AI-systemer, der er omhandlet i artikel 6, stk. 2. EAIB bør også høres af Kommissionen forud for enhver ændring af disse bilag.

55. Forslagets artikel 57, stk. 4, indeholder bestemmelser om udveksling mellem udvalget og andre af Unionens organer, kontorer, agenturer og rådgivende grupper. Under hensyntagen til dets tidligere arbejde inden for kunstig intelligens og dets ekspertise på menneskerettighedsområdet anbefaler Databeskyttelsesrådet og EDPS at overveje at lade Agenturet for Grundlæggende Rettigheder indgå som en af observatørerne i udvalget.

3 INTERAKTION MED DATABESKYTTELSESRAMMEN

3.1 Forholdet mellem forslaget og EU's eksisterende databeskyttelseslovgivning

56. Et klart defineret forhold mellem forslaget og den eksisterende databeskyttelseslovgivning er en afgørende forudsætning for at sikre og opretholde respekten for og anvendelsen af gældende EU-ret på området for beskyttelse af personoplysninger. En sådan EU-lovgivning, navnlig GDPR, EUDPR og retshåndhævelsesdirektivet, skal betragtes som en forudsætning, som yderligere lovgivningsforslag kan bygge videre på uden at påvirke eller gribe ind i de eksisterende bestemmelser, herunder med hensyn til tilsynsmyndighedernes kompetence og forvaltning.

57. Efter Databeskyttelsesrådets og EDPS' opfattelse er det derfor vigtigt i forslaget klart at undgå enhver uoverensstemmelse og mulig konflikt med GDPR, EUDPR og retshåndhævelsesdirektivet. Dette er ikke kun af hensyn til retssikkerheden, men også for at undgå, at forslaget direkte eller indirekte bringer den grundlæggende ret til beskyttelse af personoplysninger, jf. artikel 16 i TEUF og chartrets artikel 8, i fare.

58. Navnlig kan selvlærende maskiner kun beskytte enkeltpersoners personoplysninger, hvis dette inkorporeres i idéfasen. Den umiddelbare mulighed for at udøve enkeltpersoners rettigheder i henhold til artikel 22 (automatiske individuelle afgørelser, herunder profilering) i GDPR eller artikel 23 i EUDPR, uanset formålene med behandlingen, er ligeledes afgørende. I denne

henseende skal de registreredes andre rettigheder i forbindelse med retten til sletning og retten til berigtigelse i henhold til databeskyttelseslovgivningen sikres i AI-systemerne helt fra begyndelsen, uanset hvilken AI-tilgang eller teknisk arkitektur der vælges.

59. Anvendelse af personoplysninger til træning af AI-systemer kan føre til, at der skabes partiske beslutningsmønstre i kernen i AI-systemet. Der bør derfor stilles krav om forskellige garantier og navnlig et kvalificeret menneskeligt tilsyn i sådanne processer for at sikre, at de registreredes rettigheder respekteres og garanteres, og for at undgå enhver negativ virkning for fysiske personer. De kompetente myndigheder bør også kunne foreslå retningslinjer for at vurdere skævheder i AI-systemer og bistå med udøvelsen af menneskeligt tilsyn.

60. Registrerede bør altid, når deres data anvendes til AI-træning og/eller -forudsigelse, underrettes om retsgrundlaget for en sådan behandling med en generel forklaring af AI-systemets logik (procedure) og anvendelsesområde. I den henseende bør fysiske personers ret til begrænsning af behandling (artikel 18 i GDPR og artikel 20 i EUDPR) samt sletning af oplysninger (artikel 16 i GDPR og artikel 19 i EUDPR) altid sikres i disse tilfælde. Endvidere bør den dataansvarlige have en udtrykkelig forpligtelse til at informere den registrerede om de gældende frister for indsigelse, begrænsning, sletning af oplysninger osv. AI-systemet skal kunne opfylde alle databeskyttelseskrav gennem passende tekniske og organisatoriske foranstaltninger. En ret til forklaring bør sikre yderligere gennemsigtighed.

3.2 Sandkasse og viderebehandling (forslagets artikel 53 og 54)

61. Inden for de eksisterende juridiske og moralske grænser er det vigtigt at fremme europæisk innovation ved hjælp af værktøjer som f.eks. en sandkasse. En sandkasse giver mulighed for at tilvejebringe de sikkerhedsforanstaltninger, der er nødvendige for at opbygge tillid og tiltro til AI-systemer. I komplekse miljøer kan det være vanskeligt for aktører inden for kunstig intelligens at foretage en korrekt afvejning af alle interesser. Især for små og mellemstore virksomheder med begrænsede ressourcer kan det give hurtigere indsigt og dermed fremme innovation at operere i en reguleringsmæssig sandkasse.

62. I forslagets artikel 53, stk. 3, hedder det, at sandkassen ikke berører tilsynsbeføjelser eller korrigerende beføjelser. Hvis denne præcisering er nyttig, er der også behov for at udarbejde retningslinjer for eller vejledning om, hvordan der kan sikres en passende balance mellem på den ene side at være tilsynsmyndighed og på den anden side at give detaljeret vejledning gennem en sandkasse.

63. Det fremgår af artikel 53, stk. 6, at de nærmere bestemmelser og betingelserne for driften af sandkasserne fastsættes i gennemførelsesretsakter. Det er vigtigt, at der udarbejdes specifikke retningslinjer for at sikre sammenhæng og støtte i forbindelse med etableringen og driften af sandkasser. Bindende gennemførelsesretsakter kan imidlertid begrænse den enkelte medlemsstats mulighed for at skræddersy sandkassen efter dens behov og lokal praksis. Databeskyttelsesrådet og EDPS anbefaler derfor, at EAIB i stedet fastsætter retningslinjer for sandkasser.

64. Forslagets artikel 54 har til formål at sikre et retsgrundlag for viderebehandling af personoplysninger med henblik på udvikling af visse AI-systemer i offentlighedens interesse i den reguleringsmæssige sandkasse for kunstig intelligens. Forholdet mellem forslagets artikel 54, stk. 1, og forslagets artikel 54, stk. 2, og betragtning 41 og dermed også EU's eksisterende databeskyttelseslovgivning er fortsat uklart. GDPR og EUDPR har imidlertid allerede et etableret grundlag for "viderebehandling". Navnlig med hensyn til tilfælde, hvor det er i offentlighedens interesse at tillade viderebehandling, behøver en afvejning mellem den dataansvarliges interesser og den registreredes interesser ikke at hindre innovation. Forslagets artikel 54 omhandler på nuværende tidspunkt ikke to vigtige spørgsmål: i) under hvilke omstændigheder ved anvendelse af hvilke (yderligere) kriterier afvejes de registreredes interesser, og ii) om disse AI-systemer kun vil blive anvendt i sandkassen. Databeskyttelsesrådet og EDPS glæder sig over kravet om EU-lovgivning eller national lovgivning ved behandling af personoplysninger indsamlet i henhold til retshåndhævelsesdirektivet i en sandkasse, men anbefaler, at det yderligere angives, hvad der er planlagt i denne forbindelse, på en måde, der er i overensstemmelse med GDPR og EUDPR, hovedsagelig ved at præcisere, at retsgrundlaget for sådanne sandkasser bør opfylde kravene i artikel 23, stk. 2, i GDPR og artikel 25 i EUDPR, og præcisere, at enhver anvendelse af sandkassen skal gennemgå en grundig evaluering. Dette gælder også for den fuldstændige liste over betingelser i artikel 54, stk. 1, litra b)-j).

65. Nogle yderligere betragtninger vedrørende videreanvendelsen af data i forslagets artikel 54 viser, at driften af en sandkasse er ressourcekrævende, og at det derfor er realistisk at vurdere, at kun et lille antal virksomheder vil få mulighed for at deltage. Deltagelse i sandkassen kan være en konkurrencemæssig fordel. For at muliggøre videreanvendelse af data skal det nøje overvejes, hvordan deltagerne udvælges, for at sikre, at de er omfattet af anvendelsesområdet, og for at undgå urimelig behandling. Databeskyttelsesrådet og EDPS er betænkelige ved, at muligheden for videreanvendelse af data inden for rammerne af sandkassen afviger fra ansvarlighedstilgangen i GDPR, hvor ansvarligheden påhviler den dataansvarlige og ikke den kompetente myndighed.

66. Endvidere mener Databeskyttelsesrådet og EDPS, at i betragtning af formålene med sandkassen, som er at udvikle, teste og validere AI-systemer, kan sandkasserne ikke være omfattet af retshåndhævelsesdirektivets anvendelsesområde. Mens retshåndhævelsesdirektivet indeholder bestemmelser om videreanvendelse af data til videnskabelig forskning, vil de data, der behandles til dette sekundære formål, være omfattet af GDPR eller EUDPR og ikke længere af retshåndhævelsesdirektivet.

67. Det er ikke klart, hvad en reguleringsmæssig sandkasse vil omfatte. Der rejser sig det spørgsmål, om den foreslåede reguleringsmæssige sandkasse omfatter en IT-infrastruktur i hver medlemsstat med yderligere retlige grunde til viderebehandling, eller om den blot organiserer adgang til reguleringsmæssig ekspertise og vejledning. Databeskyttelsesrådet og EDPS opfordrer lovgiveren til at præcisere dette begreb i forslaget og til i forslaget klart at anføre, at den reguleringsmæssige sandkasse ikke indebærer en forpligtelse for de kompetente myndigheder til at stille deres tekniske infrastruktur til rådighed. Under alle omstændigheder

skal der stilles finansielle og menneskelige ressourcer til rådighed for de kompetente myndigheder i overensstemmelse med en sådan præcisering.

68. Endelig vil Databeskyttelsesrådet og EDPS gerne understrege udviklingen af grænseoverskridende AI-systemer, som vil være tilgængelige for det europæiske digitale indre marked som helhed. I forbindelse med sådanne AI-systemer bør den reguleringsmæssige sandkasse som et innovationsværktøj ikke blive en hindring for grænseoverskridende udvikling. Databeskyttelsesrådet og EDPS anbefaler derfor en koordineret grænseoverskridende tilgang, der stadig er tilstrækkelig tilgængelig på nationalt plan for alle SMV'er, og som tilbyder en fælles ramme i hele Europa uden at være for restriktiv. Der skal findes en balance mellem europæisk koordinering og nationale procedurer for at undgå en modstridende gennemførelse af den kommende forordning om kunstig intelligens, som ville hindre innovation i hele EU.

3.3 Gennemsigtighed

69. Databeskyttelsesrådet og EDPS bifalder, at højrisiko-AI-systemer skal registreres i en offentlig database (jf. forslagets artikel 51 og 60). Denne database bør udnyttes som en mulighed for at give den brede offentlighed oplysninger om AI-systemers anvendelsesområde og om kendte mangler og hændelser, der kan gribe ind i deres funktion, og de foranstaltninger, som udbyderne har truffet for at håndtere og afhjælpe dem.

70. Et centralt demokratisk princip er anvendelsen af kontrolforanstaltninger. Derfor er den omstændighed, at gennemsigtighedsforpligtelsen ikke finder anvendelse på AI-systemer, der anvendes til at afsløre, forebygge, efterforske eller retsforfølge strafbare handlinger, en for bred undtagelse. Der skal sondres mellem AI-systemer, der anvendes til at afsløre eller forebygge, og AI-systemer, der har til formål at efterforske eller bistå ved retsforfølgning af strafbare handlinger. Sikkerhedsforanstaltningerne til forebyggelse og afsløring skal være stærkere på grund af uskyldsformodningen. Desuden beklager Databeskyttelsesrådet og EDPS manglen på forsigtighedsadvarsler i forslaget, som kan fortolkes som et grønt lys for anvendelsen af endog uprøvede højrisiko-AI-systemer eller -anvendelser.

71. I de tilfælde, hvor der på grund af tavshedspligt kun kan sikres en ringe eller ingen gennemsigtighed for offentligheden – selv i et velfungerende demokrati – bør der være truffet sikkerhedsforanstaltninger, og disse AI-systemer bør registreres hos og skabe gennemsigtighed for den kompetente tilsynsmyndighed.

72. Det er et meget udfordrende mål at sikre gennemsigtighed i AI-systemer. Den fuldt kvantitative beslutningstilgang i mange AI-systemer, som i sagens natur adskiller sig fra den menneskelige tilgang, der hovedsagelig er baseret på årsagsforbindelse og teoretisk ræsonnement, kan være i strid med behovet for at få en forudgående forståelig forklaring af maskinernes resultater. Forordningen bør fremme nye, mere proaktive og rettidige måder til at informere brugere af AI-systemer om den (beslutningsmæssige) status for, hvor systemet på et hvilket som helst tidspunkt befinder sig, og give mulighed for tidlig varsling af mulige skadelige resultater, således at enkeltpersoner, hvis rettigheder og frihedsrettigheder kan blive krænket af maskinens selvstændige beslutninger, kan reagere eller rette op på beslutningen.

3.4 Behandling af særlige kategorier af oplysninger og oplysninger vedrørende strafbare handlinger

73. Behandlingen af særlige kategorier af oplysninger på retshåndhævelsesområdet reguleres af bestemmelserne i EU's databeskyttelsesramme, herunder retshåndhævelsesdirektivet samt den nationale gennemførelse heraf. Forslaget hævder ikke at udgøre et generelt retsgrundlag for behandling af personoplysninger, herunder særlige kategorier af personoplysninger, jf. betragtning 41. Samtidig hedder det i forslagets artikel 10, stk. 5, at "udbydere af sådanne systemer [kan] behandle særlige kategorier af personoplysninger". Endvidere kræver samme bestemmelse yderligere sikkerhedsforanstaltninger, og der gives også eksempler. Forslaget synes derved at gribe ind i anvendelsen af GDPR, retshåndhævelsesdirektivet og EUDPR. Selv om Databeskyttelsesrådet og EDPS bifalder forsøget på at sørge for passende sikkerhedsforanstaltninger, er der behov for en mere sammenhængende reguleringsmæssig tilgang, da de nuværende bestemmelser ikke synes at være tilstrækkeligt klare til at skabe et retsgrundlag for behandling af særlige kategorier af oplysninger og skal suppleres med yderligere beskyttelsesforanstaltninger, der stadig skal vurderes. Når personoplysninger er blevet indsamlet ved behandling inden for retshåndhævelsesdirektivets anvendelsesområde, skal der desuden tages hensyn til mulige yderligere garantier og begrænsninger som følge af den nationale gennemførelse af retshåndhævelsesdirektivet.

3.5 Overholdelsesmekanismer

3.5.1 Certificering

74. Én af forslagets hovedsøjler er certificering. Det certificeringssystem, der fremgår af forslaget, er baseret på en struktur af enheder (bemyndigende myndigheder/bemyndigede organer/Kommissionen) og en overensstemmelsesvurderings-/certificeringsmekanisme, som omfatter de obligatoriske krav, der gælder for højrisiko-AI-systemer, og er baseret på europæiske harmoniserede standarder i henhold til forordning (EU) nr. 1025/2012 og fælles specifikationer, der skal fastlægges af Kommissionen. Denne mekanisme adskiller sig fra det certificeringssystem, der har til formål at sikre overholdelse af databeskyttelsesregler og -principper og er fastsat i artikel 42 og 43 i GDPR. Det er imidlertid ikke klart, hvordan certifikater, der udstedes af bemyndigede organer i overensstemmelse med forslaget, kan danne grænseflade med databeskyttelsescertifikater, -mærkninger og -mærker, der er fastsat i GDPR, i modsætning til det, der er fastsat for andre certificeringstyper (jf. artikel 42, stk. 2, med hensyn til certificeringer udstedt i henhold til forordning (EU) 2019/881).

75. For så vidt som højrisiko-AI-systemer er baseret på behandling af personoplysninger eller behandler personoplysninger for at udføre deres opgaver, kan disse manglende overensstemmelser skabe retlig usikkerhed for alle berørte organer, da de kan føre til situationer, hvor AI-systemer, der er certificeret i henhold til forslaget og mærket med CE-overensstemmelsesmærkning, når de er bragt i omsætning eller taget i brug, kan blive anvendt på en måde, der ikke er i overensstemmelse med databeskyttelsesreglerne og -principperne.

76. Forslaget mangler en klar forbindelse til databeskyttelseslovgivningen og anden EU-ret og medlemsstatslovgivning, der finder anvendelse på hvert "område" af højrisiko-AI-systemer, der er opført i bilag III. Forslaget bør navnlig omfatte principperne om dataminimering og databeskyttelse gennem design som ét af de aspekter, der skal tages i betragtning, inden der opnås CE-mærkning, i betragtning af højrisiko-AI-systemernes mulige høje grad af indgriben i de grundlæggende rettigheder til privatlivets fred og beskyttelse af personoplysninger og behovet for at sikre en høj grad af tillid til AI-systemet. Databeskyttelsesrådet og EDPS anbefaler derfor, at forslaget ændres for at præcisere forholdet mellem certifikater udstedt i henhold til den nævnte forordning og databeskyttelsescertifikater, -mærkninger og -mærker. Endelig bør databeskyttelsesmyndighederne inddrages i udarbejdelsen og fastlæggelsen af harmoniserede standarder og fælles specifikationer.

77. I forbindelse med forslagets artikel 43 vedrørende overensstemmelsesvurdering synes undtagelsen fra overensstemmelsesvurderingsproceduren i artikel 47 at være meget bred og omfatter for mange undtagelser, såsom ekstraordinære hensyn til den offentlige sikkerhed eller beskyttelse af menneskers liv og sundhed, miljøbeskyttelse eller beskyttelse af centrale industrielle og infrastrukturmæssige aktiver. Vi vil foreslå lovgiverne at indsnævre dem.

3.5.2 Adfærdskodekser

78. I henhold til forslagets artikel 69 tilskynder Kommissionen og medlemsstaterne til og letter udarbejdelsen af adfærdskodekser, der har til formål at fremme, at udbydere af AI-systemer, der ikke er højrisikosystemer, frivilligt anvender de krav, der gælder for højrisiko-AI-systemer, samt yderligere krav. I overensstemmelse med betragtning 78 til GDPR anbefaler Databeskyttelsesrådet og EDPS at identificere og definere synergier mellem disse instrumenter og adfærdskodekserne i GDPR, som understøtter overholdelsen af databeskyttelsesreglerne. I denne forbindelse er det relevant at præcisere, om beskyttelsen af personoplysninger skal betragtes som "yderligere krav", der kan opfyldes af de i artikel 69, stk. 2, omhandlede adfærdskodekser. Det er ligeledes relevant at sikre, at de "tekniske specifikationer og løsninger", jf. de i artikel 69, stk. 1, omhandlede adfærdskodekser, som er udformet med henblik på at fremme overholdelse af kravene i udkastet til forordning om kunstig intelligens, ikke er i strid med reglerne og principperne i GDPR og EUDPR. Ved at gøre dette vil det være en merværdi, hvis udbydere af AI-systemer, der ikke er højrisikosystemer, overholder disse værktøjer – for så vidt som sådanne systemer er baseret på behandling af personoplysninger eller behandler personoplysninger for at udføre deres opgaver – da dette vil sikre, at dataansvarlige og databehandlere vil være i stand til at opfylde deres databeskyttelsesforpligtelser i forbindelse med anvendelsen af disse systemer.

79. Samtidig vil der fremkomme en retlig ramme for pålidelig kunstig intelligens, som suppleres med integrationen af adfærdskodekser, for at fremme tilliden til anvendelsen af denne teknologi på en måde, der er sikker og i overensstemmelse med lovgivningen, herunder respekten for de grundlæggende rettigheder. Udformningen af disse instrumenter bør imidlertid styrkes ved at indføre mekanismer, der har til formål at kontrollere, at sådanne kodekser indeholder effektive "tekniske specifikationer og løsninger" og fastsætter "klare mål og centrale resultatindikatorer til måling af realiseringen af disse mål" som en integreret del af de pågældende kodekser. Endvidere

kan den manglende henvisning til (obligatoriske) overvågningsmekanismer for adfærdskodekser, der har til formål at kontrollere, at udbydere af AI-systemer, der ikke er højrisikosystemer, overholder deres bestemmelser, samt muligheden for, at de enkelte udbydere selv kan udarbejde (og gennemføre) de nævnte kodekser (jf. afsnit 5.2.7 i begrundelsen), yderligere svække effektiviteten og håndhævelsen af disse instrumenter.

80. Endelig anmoder Databeskyttelsesrådet og EDPS om præciseringer med hensyn til de typer af initiativer, som Kommissionen i henhold til forslagets betragtning 81 kan udvikle "[f]or at fremme mindskelsen af tekniske hindringer for grænseoverskridende udveksling af data til udvikling af kunstig intelligens".

4 KONKLUSION

81. Selv om Databeskyttelsesrådet og EDPS hilser Kommissionens forslag velkommen og mener, at en sådan forordning er nødvendig for at sikre de grundlæggende rettigheder for EU-borgere og personer med bopæl i EU, mener de, at forslaget bør tilpasses i flere henseender for at sikre dets anvendelighed og effektivitet.

82. I betragtning af forslagets kompleksitet og de problemstillinger, det har til formål at løse, er der stadig meget arbejde, der skal gøres, inden forslaget kan skabe en velfungerende retlig ramme, der effektivt supplerer GDPR med hensyn til at beskytte grundlæggende menneskerettigheder og samtidig fremme innovation. Databeskyttelsesrådet og EDPS vil fortsat stå til rådighed og tilbyde deres støtte på denne rejse.

Bruxelles, den 18. juni 2021

På vegne af Det Europæiske Databeskyttelsesråd	På vegne af Den Europæiske Tilsynsførende for Databeskyttelse
Formand	Tilsynsførende
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI