



EDPB-EDPS

**Gezamenlijk advies 5/2021
over het voorstel voor een
verordening van het Europees
Parlement en de Raad tot
vaststelling van
geharmoniseerde regels
betreffende artificiële
intelligentie (wet inzake
artificiële intelligentie)**

18 juni 2021

Samenvatting

De Europese Commissie heeft op 21 april 2021 haar voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (hierna “het voorstel” genoemd) ingediend. Het EDPB en de EDPS vinden de bezorgdheid van de wetgever over het gebruik van artificiële intelligentie (AI) in de Europese Unie (EU) een goede zaak en benadrukken dat het voorstel zeer belangrijke **gevolgen voor de bescherming van gegevens** heeft.

Het EDPB en de EDPS merken op dat de **rechtsgrondslag** voor het voorstel in de eerste plaats artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU) is. Daarnaast is het voorstel ook gebaseerd op artikel 16 van het VWEU voor zover het specifieke regels bevat inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens, met name beperkingen op het gebruik van AI-systemen voor “realtime” biometrische identificatie op afstand in openbare ruimten met het oog op rechtshandhaving. Het EDPB en de EDPS herinneren eraan dat, in overeenstemming met de jurisprudentie van het Hof van Justitie van de EU (HvJ-EU), artikel 16 van het VWEU een passende rechtsgrondslag biedt in gevallen waarin de bescherming van persoonsgegevens een van de wezenlijke doelstellingen of onderdelen van de door de EU-wetgever vastgestelde regels is. De toepassing van artikel 16 van het VWEU houdt ook in dat **onafhankelijk toezicht moet worden uitgeoefend op de naleving** van de vereisten inzake de verwerking van persoonsgegevens, zoals ook vereist is op grond van artikel 8 van het Handvest van de grondrechten van de EU.

Wat het **toepassingsgebied van het voorstel** betreft, zijn het EDPB en de EDPS zeer ingenomen met het feit dat het zich uitstrekt tot het verstrekken en het gebruik van AI-systemen door EU-instellingen, -organen of -instanties. **De uitsluiting van internationale samenwerking op het gebied van rechtshandhaving uit het vastgestelde toepassingsgebied** van het voorstel geeft echter aanleiding tot ernstige bezorgdheid voor het EDPB en de EDPS, aangezien een dergelijke uitsluiting een aanzienlijk risico op het omzeilen van de regels inhoudt (bv. derde landen of internationale organisaties die toepassingen met een hoog risico uitvoeren waarop overheidsinstanties in de EU in een beroep doen).

Het EDPB en de EDPS **zijn ingenomen met de risicogebaseerde aanpak** die aan het voorstel ten grondslag ligt.. Deze aanpak moet echter worden verduidelijkt en het begrip “risico voor de grondrechten” moet worden afgestemd op de AVG en Verordening (EU) 2018/1725 (EUDPR), aangezien aspecten in verband met de bescherming van persoonsgegevens meespelen.

Het EDPB en de EDPS onderschrijven het uitgangspunt van het voorstel dat als een AI-systeem als **stelsel met een hoog risico** wordt geclassificeerd, **dit niet noodzakelijkerwijs betekent dat het** als zodanig **rechtmatig is** en door de gebruiker kan worden ingezet. **Het is mogelijk dat de verwerkingsverantwoordelijke moet voldoen aan verdere vereisten die voortvloeien uit de EU-wetgeving inzake gegevensbescherming.** Bovendien moet de naleving van wettelijke verplichtingen die voortvloeien uit de wetgeving van de Unie (met inbegrip van de bescherming van persoonsgegevens) een basisvoorwaarde zijn om als product met CE-markering op de Europese markt te mogen komen. Daartoe zijn het EDPB en de EDPS van mening dat het **vereiste om de naleving van de AVG en de EUDPR te waarborgen, moet worden opgenomen in hoofdstuk 2 van titel III.** Daarnaast achten het EDPB en de

EDPS het noodzakelijk de conformiteitsbeoordelingsprocedure in het voorstel aan te passen zodat derden altijd een conformiteitsbeoordeling vooraf van een AI-systeem met een hoog risico uitvoeren.

Gezien het grote risico op discriminatie wordt in het voorstel “sociale scoring” verboden wanneer deze “gedurende een bepaalde periode” of “door of namens overheidsinstanties” wordt uitgevoerd. Particuliere ondernemingen, zoals sociale media en aanbieders van clouddiensten, kunnen echter ook grote hoeveelheden persoonsgegevens verwerken en sociale scoring uitvoeren. Bijgevolg **moet in de toekomstige AI-verordening elke vorm van sociale scoring verboden worden.**

Biometrische identificatie op afstand van individuen in openbare ruimten houdt een hoog risico in van inmenging in hun privéleven, met ernstige gevolgen voor de verwachting van de bevolking dat zij anoniem zullen zijn in openbare ruimten. Om deze redenen **dringen** het EDPB en de EDPS **aan op een algemeen verbod op het gebruik van AI voor de geautomatiseerde herkenning van menselijke kenmerken in openbare ruimten** – zoals van gezicht, maar ook van bewegingspatroon, vingerafdrukken, DNA, spraak, toetsaanslagen en andere biometrische of gedragsignalen – in elke context. Ook wordt ook een **verbod** aanbevolen op **AI-systemen waarbij personen op basis van biometrische gegevens worden ingedeeld in clusters** volgens etnische afkomst, geslacht, politieke of seksuele gerichtheid of andere gronden voor discriminatie op grond van artikel 21 van het Handvest. Voorts zijn het EDPB en de EDPS van mening dat het gebruik van AI om **emoties van een natuurlijke persoon af te leiden uiterst onwenselijk is en moet worden verboden.**

Verder zijn het EDPB en de EDPS ingenomen met **het feit dat de EDPS in het voorstel wordt aangewezen als de bevoegde autoriteit en als de markttoezichtautoriteit voor het toezicht op de instellingen, instanties en organen van de Unie.** De rol en de taken van de EDPS moeten echter verder worden verduidelijkt, met name voor wat betreft zijn rol als markttoezichtautoriteit. Voorts moet in toekomstige AI-verordening de **onafhankelijkheid van de toezichthoudende autoriteiten** bij de uitvoering van hun toezicht- en handhavingstaken duidelijk worden vastgelegd.

De aanwijzing van de gegevensbeschermingsautoriteiten als de nationale toezichthoudende autoriteiten zou zorgen voor een meer geharmoniseerde regelgevingsaanpak, bijdragen tot een consistente interpretatie van de bepalingen inzake gegevensverwerking en tegenstrijdigheden in de handhaving ervan tussen de lidstaten vermijden. Bijgevolg zijn het EDPB en de EDPS van mening dat de **gegevensbeschermingsautoriteiten moeten worden aangewezen als de nationale toezichthoudende autoriteiten overeenkomstig artikel 59 van het voorstel.**

In het voorstel wordt een doorslaggevende rol toegekend aan de Commissie in het “Europees Comité voor artificiële intelligentie” (EAIB). Een dergelijke rol staat haaks op de noodzaak dat een Europees AI-orgaan onafhankelijk is van politieke beïnvloeding. Om zijn onafhankelijkheid te garanderen, moet in de toekomstige AI-verordening worden voorzien in **meer autonomie voor het EAIB** en in de nodige mogelijkheden om op eigen initiatief op te treden.

Gezien de verspreiding van AI-systemen in de eengemaakte markt en de waarschijnlijkheid van grensoverschrijdende gevallen is er een cruciale behoefte aan een geharmoniseerde handhaving en een behoorlijke verdeling van bevoegdheden tussen de nationale toezichthoudende autoriteiten. Het EDPB en de EDPS stellen voor te voorzien in **een mechanisme dat voor elk AI-systeem een centraal contactpunt waarborgt voor personen die onder de wetgeving vallen en voor bedrijven.**

Wat de **testomgevingen** betreft, **bevelen** het EDPB en de EDPS **aan het toepassingsgebied en de doelstellingen ervan te verduidelijken.** In het voorstel moet ook duidelijk worden gesteld dat de

rechtsgrondslag van dergelijke testomgevingen moet voldoen aan de in het bestaande gegevensbeschermingskader vastgestelde vereisten.

In het **certificeringssysteem** dat in het voorstel wordt geschetst, ontbreekt **een duidelijk verband met de EU-wetgeving inzake gegevensbescherming** en met andere wetgeving van de EU en de lidstaten die van toepassing is op elk “gebied” van een AI-systeem met hoog risico en wordt er geen rekening gehouden met de **beginselen van minimale gegevensverwerking en gegevensbescherming door ontwerp** als een van de aspecten waarmee rekening moet worden gehouden **voordat de CE-markering wordt verkregen**. Het EDPB en de EDPS bevelen dan ook aan het voorstel te wijzigen om het verband tussen certificaten die op grond van de genoemde verordening zijn afgegeven en certificaten, zegels en merktekens op het gebied van gegevensbescherming te verduidelijken. Ten slotte moeten de gegevensbeschermingsautoriteiten worden betrokken bij de voorbereiding en vaststelling van geharmoniseerde normen en gemeenschappelijke specificaties.

Wat de **gedragscodes** betreft, achten het EDPB en de EDPS het **noodzakelijk te verduidelijken** of de bescherming van persoonsgegevens valt onder de “aanvullende voorschriften” die in deze gedragscodes kunnen worden behandeld, en om ervoor te zorgen dat de “technische specificaties en oplossingen” niet in strijd zijn met de regels en beginselen van het bestaande EU-kader voor gegevensbescherming.

INHOUDSOPGAVE

1	INLEIDING.....	6
2	ANALYSE VAN DE BELANGRIJKSTE BEGINSELEN VAN HET VOORSTEL.....	8
2.1	Toepassingsgebied van het voorstel en verhouding tot het bestaande rechtskader.....	8
2.2	Risicogebaseerde aanpak.....	10
2.3	Verboden gevallen van gebruik van AI.....	12
2.4	AI-systemen met een hoog risico	15
2.4.1	Noodzaak van een conformiteitsbeoordeling vooraf door externe derden	15
2.4.2	Het toepassingsgebied van de regelgeving moet ook AI-systemen omvatten die reeds in gebruik zijn	15
2.5	Governance en Europees AI-comité	16
2.5.1	Governance	16
2.5.2	Europees AI-comité	18
3	INTERACTIE MET HET gegevensbeschermingskader.....	19
3.1	Verhouding van het voorstel tot de bestaande EU-wetgeving inzake gegevensbescherming.....	19
3.2	Testomgeving & verdere verwerking (artikelen 53 en 54 van het voorstel).....	20
3.3	Transparantie	22
3.4	Verwerking van bijzondere categorieën gegevens & gegevens betreffende strafbare feiten	23
3.5	Nalevingsmechanismen.....	23
3.5.1	Certificering	23
3.5.2	Gedragcodes	24
4	CONCLUSIE.....	26

Het Europees Comité voor gegevensbescherming en de Europese Toezichthouder voor gegevensbescherming

Gezien artikel 42, lid 2, van Verordening (EU) 2018/1725 van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG¹,

Gezien de EER-overeenkomst en met name bijlage XI en Protocol 37 daarvan, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018²,

Gezien het verzoek om een gezamenlijk advies van de Europese Toezichthouder voor gegevensbescherming en het Europees Comité voor gegevensbescherming van 22 april 2021 over het voorstel voor een verordening tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie),

HEBBEN HET VOLGENDE GEZAMENLIJK ADVIES VASTGESTELD

1 INLEIDING

1. De opkomst van systemen voor artificiële intelligentie (“AI”) is een zeer belangrijke stap in de ontwikkeling van technologieën en in de manier waarop mensen met deze systemen omgaan. AI is een reeks belangrijke technologieën die ons dagelijks leven ingrijpend zullen veranderen, zowel vanuit een maatschappelijk als vanuit economisch oogpunt. De komende jaren worden definitieve beslissingen verwacht voor AI, aangezien dit ons helpt een aantal van de grootste uitdagingen waar we vandaag voor staan, in een groot aantal domeinen gaande van gezondheid tot mobiliteit, of van openbaar bestuur tot onderwijs, het hoofd te bieden.
2. Deze beloofde vooruitgang brengt echter risico’s met zich mee. De risico’s zijn inderdaad zeer relevant, aangezien de individuele en maatschappelijke effecten van AI-systemen grotendeels onbekend zijn. Het genereren van inhoud, het maken van voorspellingen of het op geautomatiseerde wijze nemen van een besluit, zoals AI-systemen doen, door middel van technieken voor machinaal leren of logische en probabilistische inferentieregels, is niet hetzelfde als mensen die deze activiteiten uitvoeren door middel van creatief of theoretisch redeneren en de volledige verantwoordelijkheid voor de gevolgen dragen.
3. AI zal de hoeveelheid voorspellingen uitbreiden die op veel gebieden kunnen worden gedaan, te beginnen met meetbare correlaties tussen gegevens, onzichtbaar voor het menselijke oog maar zichtbaar voor machines, waardoor ons leven gemakkelijker wordt en een groot aantal problemen wordt opgelost. Tegelijkertijd zal ons vermogen om resultaten causaal te interpreteren echter op zodanige wijze worden uitgehold dat de begrippen transparantie,

¹ PB L 295 van 21.11.2018, blz. 39.

² Alle verwijzingen in dit document naar “lidstaten” moeten worden gelezen als verwijzingen naar “EER-lidstaten”.

menselijke controle, verantwoordingsplicht en aansprakelijkheid ten aanzien van de resultaten ernstig in het gedrang komen.

4. Gegevens (persoonsgegevens en niet-persoonsgebonden gegevens) in AI zijn in veel gevallen het belangrijkste uitgangspunt voor autonome beslissingen, die onvermijdelijk van invloed zullen zijn op het leven van individuen op verschillende niveaus. Daarom stellen het EDPB en de EDPS reeds in dit stadium met klem dat het voorstel voor een verordening tot vaststelling van geharmoniseerde regels inzake artificiële intelligentie (wet inzake artificiële intelligentie) (“het voorstel”)³ **belangrijke gevolgen heeft voor de gegevensbescherming.**
5. De toewijzing van de beslissingsbevoegdheid aan machines, op basis van gegevens, brengt risico’s met zich mee voor de rechten en vrijheden van individuen, heeft gevolgen voor hun privéleven en kan schade toebrengen aan groepen of zelfs aan samenlevingen in hun geheel. Het EDPB en de EDPS benadrukken dat het recht op eerbiediging van het privéleven en op bescherming van persoonsgegevens, hetgeen in strijd is met de aanname van beslissingsautonomie van machines die aan het concept van AI ten grondslag ligt, een pijler is van de EU-waarden zoals erkend in de Universele Verklaring van de rechten van de mens (artikel 12), het Europees Verdrag tot bescherming van de rechten van de mens (artikel 8) en het Handvest van de grondrechten van de EU (hierna “het Handvest”) (artikelen 7 en 8). Het verzoenen van het door AI-toepassingen geboden groeiperspectief met de centrale rol en de voorrang van mensen ten opzichte van machines is een zeer ambitieus, maar noodzakelijk doel.
6. Het EDPB en de EDPS zijn ingenomen met de betrokkenheid bij de regulering van alle belanghebbenden in de AI-waardeketen en de invoering van specifieke vereisten voor aanbieders van oplossingen, aangezien zij een belangrijke rol spelen bij de producten die gebruikmaken van hun systemen. De verantwoordelijkheden van de verschillende partijen – gebruiker, aanbieder, importeur of distributeur van een AI-systeem – moeten echter duidelijk worden afgebakend en toegewezen. In het bijzonder moet bij de verwerking van persoonsgegevens bijzondere aandacht worden besteed aan de consistentie van deze rollen en verantwoordelijkheden met de begrippen “verwerkingsverantwoordelijke” en “verwerker” in het kader voor gegevensbescherming, aangezien beide normen niet in overeenstemming zijn.
7. In het voorstel wordt een belangrijke plaats gegeven aan het begrip menselijk toezicht (artikel 14), wat door het EDPB en de EDPS wordt toegejuicht. Vanwege het grote potentiële effect van bepaalde AI-systemen voor personen of groepen personen moet de reële centrale rol van de mens zoals eerder vermeld echter een hefboomeffect hebben op zeer deskundig menselijk toezicht en een rechtmatige verwerking, voor zover dergelijke systemen gebaseerd zijn op de verwerking van persoonsgegevens of persoonsgegevens verwerken om hun taak te vervullen, zodat het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit wordt geëerbiedigd.
8. Bovendien moet in het voorstel, gezien de data-intensieve aard van veel AI-toepassingen, de vaststelling van een benadering van gegevensbescherming door ontwerp en door standaardinstellingen op elk niveau worden gestimuleerd, waardoor de doeltreffende

³ COM(2021) 206 final.

toepassing van de gegevensbeschermingsbeginselen (zoals bedoeld in artikel 25 van de AVG en artikel 27 van de EUDPR) wordt aangemoedigd door middel van geavanceerde technologieën.

9. Tot slot benadrukken het EDPB en de EDPS dat dit gezamenlijk advies slechts wordt verstrekt als een voorlopige analyse van het voorstel, zonder vooruit te lopen op eventuele verdere beoordelingen en adviezen over de gevolgen van het voorstel en de verenigbaarheid ervan met de EU-wetgeving inzake gegevensbescherming.

2 ANALYSE VAN DE BELANGRIJKSTE BEGINSELEN VAN HET VOORSTEL

2.1 Toepassingsgebied van het voorstel en verhouding tot het bestaande rechtskader

10. Volgens de toelichting is de **rechtsgrondslag** van het voorstel in de eerste plaats artikel 114 van het VWEU, dat voorziet in de vaststelling van maatregelen om de instelling en de werking van de interne markt te waarborgen.⁴ Daarnaast is het voorstel gebaseerd op artikel 16 van het VWEU *voor zover het specifieke regels bevat inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens*, met name beperkingen op het gebruik van AI-systemen voor “realtime” biometrische identificatie op afstand in openbare ruimten met het oog op rechtshandhaving⁵.
11. Het EDPB en de EDPS herinneren eraan dat artikel 16 van het VWEU, in overeenstemming met de jurisprudentie van het HvJ-EU, een passende rechtsgrondslag biedt in gevallen waarin de bescherming van persoonsgegevens een van de essentiële doelstellingen of onderdelen van de door de EU-wetgever vastgestelde regels is⁶. De toepassing van artikel 16 van het VWEU houdt ook in dat onafhankelijk toezicht moet worden uitgeoefend op de naleving van de vereisten inzake de verwerking van persoonsgegevens, zoals ook vereist is in artikel 8 van het Handvest.
12. De EDPS en het EDPB herinneren eraan dat er reeds een alomvattend gegevensbeschermingskader bestaat dat is vastgesteld op basis van artikel 16 van het VWEU, bestaande uit de algemene verordening gegevensbescherming (AVG)⁷, de verordening gegevensbescherming voor de instellingen, organen en instanties van de Europese Unie

⁴ Toelichting, blz. 5.

⁵ Toelichting, blz. 6. Zie ook overweging (2) van het voorstel.

⁶ Advies van 26 juli 2017, *PNR Canada*, adviesprocedure 1/15, ECLI:EU:C:2017:592, punt 96.

⁷ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), PB L 119 van 4.5.2016, blz. 1.

(EUDPR)⁸ en de richtlijn gegevensbescherming bij rechtshandhaving (LED)⁹. Volgens het voorstel kunnen alleen de aanvullende beperkingen met betrekking tot de verwerking van biometrische gegevens in het voorstel worden beschouwd als gebaseerd op artikel 16 van het VWEU en dus dezelfde rechtsgrondslag hebben als de AVG, EUDPR of LED. Dit heeft belangrijke gevolgen voor het verband tussen het voorstel en de AVG, EUDPR en LED in het algemeen, zoals hieronder uiteengezet.

13. Wat het **toepassingsgebied van het voorstel** betreft, zijn het EDPB en de EDPS zeer ingenomen met het feit dat het voorstel zich uitstrekt tot het gebruik van AI-systemen door EU-instellingen, -organen of -instanties. Aangezien het gebruik van AI-systemen door deze entiteiten ook aanzienlijke gevolgen kan hebben voor de grondrechten van individuen, vergelijkbaar met het gebruik in de EU-lidstaten, is het absoluut noodzakelijk dat het nieuwe regelgevingskader voor AI van toepassing is op zowel EU-lidstaten als EU-instellingen, -bureaus, -organen en -instanties om een coherente aanpak in de hele Unie te waarborgen. Aangezien EU-instellingen, -bureaus, -organen en -instanties zowel aanbieders als gebruikers van AI-systemen kunnen zijn, achten de EDPS en het EDPB het ten volle passend deze entiteiten op te nemen in het toepassingsgebied van het voorstel op grond van artikel 114 van het VWEU.
14. Het EDPB en de EDPS hebben echter ernstige bedenkingen bij de uitsluiting van internationale samenwerking op het gebied van rechtshandhaving van het toepassingsgebied van artikel 2, lid 4, van het voorstel. Deze uitsluiting brengt een aanzienlijk risico met zich mee dat de regels worden omzeild (bv. derde landen of internationale organisaties die toepassingen met een hoog risico uitvoeren waarop overheidsinstanties in de EU een beroep doen).
15. Bij de ontwikkeling en het gebruik van AI-systemen zullen in veel gevallen persoonsgegevens worden verwerkt. Het is van het grootste belang dat het verband tussen dit voorstel en de bestaande EU-wetgeving inzake gegevensbescherming duidelijk wordt. Het voorstel doet geen afbreuk aan de AVG, de EUDPR en de LED en vormt er een aanvulling op. Hoewel in de overwegingen van het voorstel wordt verduidelijkt dat het gebruik van AI-systemen nog steeds in overeenstemming moet zijn met de gegevensbeschermingswetgeving, **bevelen het EDPB en de EDPS ten zeerste aan in artikel 1 van het voorstel te verduidelijken dat de Uniewetgeving inzake de bescherming van persoonsgegevens**, met name de algemene verordening gegevensbescherming, de EUDPR, de e-privacyrichtlijn¹⁰ en de LED, van

⁸ Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG, PB L 295 van 21.11.2018, blz. 39.

⁹ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, PB L 119 van 4.5.2016, blz. 89.

¹⁰ Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) zoals gewijzigd bij Richtlijn 2006/24/EG en Richtlijn 2009/136/EG.

toepassing zou zijn op elke verwerking van persoonsgegevens die binnen het toepassingsgebied van het voorstel valt. In een overeenkomstige overweging moet tevens worden verduidelijkt dat met het voorstel niet wordt beoogd afbreuk te doen aan de toepassing van de bestaande EU-wetgeving betreffende de verwerking van persoonsgegevens, met inbegrip van de taken en bevoegdheden van de onafhankelijke toezichhoudende autoriteiten die bevoegd zijn om toezicht te houden op de naleving van die instrumenten.

2.2 Risicogebaseerde aanpak

16. Het EDPB en de EDPS **zijn ingenomen met de risicogebaseerde aanpak** die aan het voorstel ten grondslag ligt.. Het voorstel zou van toepassing zijn op alle AI-systemen, met inbegrip van systemen die geen betrekking hebben op de verwerking van persoonsgegevens, maar toch van invloed kunnen zijn op belangen of grondrechten en fundamentele vrijheden.
17. Het EDPB en de EDPS merken op dat in sommige bepalingen van het voorstel de risico's voor groepen individuen of voor de samenleving in haar geheel worden uitgesloten (bv. gezamenlijke effecten met een bijzonder belang, zoals groepsdiscriminatie of het uiten van politieke opvattingen in openbare ruimten). Het EDPB en de EDPS raden aan om maatschappelijke risico's/risico's voor groepen eveneens te beoordelen en beperken.
18. Het EDPB en de EDPS zijn van mening dat de risicogebaseerde benadering van het voorstel moet worden verduidelijkt en dat het begrip "risico voor de grondrechten", voor zover aspecten in verband met de bescherming van persoonsgegevens meespelen, **moet worden afgestemd op de AVG**. Of het nu gaat om eindgebruikers, simpelweg betrokkenen of andere personen die bij het AI-systeem betrokken zijn, het ontbreken van enige verwijzing in de tekst naar de persoon die door het AI-systeem wordt getroffen, lijkt in het voorstel een dode hoek te zijn. De verplichtingen die aan actoren ten aanzien van de betrokken personen worden opgelegd, moeten immers concreter voortvloeien uit de bescherming van het individu en zijn of haar rechten. Daarom dringen het EDPB en de EDPS er bij de wetgevers op aan in het voorstel expliciet aandacht te besteden aan de **rechten en rechtsmiddelen die beschikbaar zijn voor personen** die aan AI-systemen onderworpen zijn.
19. Het EDPB en de EDPS nemen nota van de keuze om een uitputtende lijst van **AI-systemen met een hoog risico te verstrekken**. Deze keuze kan een zwart-wit-effect hebben, en zeer riskante situaties enigszins aantrekkelijk maken, waardoor de algemene risicogebaseerde aanpak die aan het voorstel ten grondslag ligt, wordt ondermijnd. In deze lijst van AI-systemen met een hoog risico die in de bijlagen II en III bij het voorstel zijn opgenomen, ontbreekt het ook aan bepaalde soorten praktijkvoorbeelden die aanzienlijke risico's met zich meebrengen, zoals het gebruik van AI voor het bepalen van de verzekeringspremie, voor de beoordeling van medische behandelingen of voor gezondheidsonderzoekdoeleinden. Het EDPB en de EDPS benadrukken ook dat deze bijlagen regelmatig moeten worden bijgewerkt om ervoor te zorgen dat het toepassingsgebied ervan passend is.
20. In het voorstel staat dat de **aanbieders** van het AI-systeem een risicobeoordeling moeten uitvoeren, maar in de meeste gevallen zijn de (gegevens)verwerkingsverantwoordelijken de **gebruikers** en niet de aanbieders van de AI-systemen (een gebruiker van een

gezichtsherkenningssysteem is bv. een “verwerkingsverantwoordelijke” en is daarom niet gebonden aan de vereisten voor aanbieders van AI met een hoog risico in het kader van het voorstel).

21. Bovendien zal het **voor een aanbieder niet altijd mogelijk zijn om alle toepassingen** voor het AI-systeem **te beoordelen**. De initiële risicobeoordeling zal dus algemener zijn dan die welke door de gebruiker van het AI-systeem wordt uitgevoerd. Zelfs als uit de initiële risicobeoordeling door de aanbieder niet blijkt dat het AI-systeem op grond van het voorstel een “hoog risico” is, mag dit niet uitsluiten dat **de gebruiker van het systeem een latere (meer gedetailleerde) beoordeling** (gegevensbeschermingseffectbeoordeling) op grond van artikel 35 van de AVG, artikel 39 van de EUDPR of op grond van artikel 27 van de LED) **moet uitvoeren**, rekening houdend met de context van het gebruik en de specifieke praktijkvoorbeelden. De interpretatie van de vraag of een soort verwerking op grond van de AVG, de EUDPR en de LED waarschijnlijk tot een hoog risico zal leiden, moet onafhankelijk van het voorstel worden gemaakt. De classificatie van een AI-systeem als “hoog risico” vanwege de gevolgen ervan voor de grondrechten¹¹ **leidt echter tot een vermoeden van “hoog risico” in het kader van de AVG, de EUDPR en de LED voor zover persoonsgegevens worden verwerkt**.
22. **Het EDPB en de EDPS onderschrijven het uitgangspunt van het voorstel dat als een AI-systeem als systeem met een hoog risico wordt geclassificeerd, dit niet noodzakelijkerwijs betekent dat het als zodanig rechtmatig is en door de gebruiker kan worden ingezet. Het is mogelijk dat de verwerkingsverantwoordelijke moet voldoen aan verdere vereisten die voortvloeien uit de EU-wetgeving inzake gegevensbescherming.** Bovendien moet de redenering die ten grondslag ligt aan artikel 5 van het voorstel, namelijk dat, in tegenstelling tot de verboden systemen, de systemen met een hoog risico in beginsel toelaatbaar kunnen zijn, in het voorstel wordt aangepakt en geschrapt, temeer daar de voorgestelde CE-markering niet impliceert dat de daarmee gepaard gaande verwerking van persoonsgegevens rechtmatig is.
23. De naleving van de wettelijke verplichtingen die voortvloeien uit de wetgeving van de Unie (met inbegrip van de bescherming van persoonsgegevens) moet echter een basisvoorwaarde zijn om als product met CE-markering op de Europese markt te mogen komen. Daartoe bevelen het EDPB en de EDPS aan om het **vereiste om de naleving van de AVG en de EUDPR te waarborgen, op te nemen in hoofdstuk 2 van titel III**. Deze vereisten moeten worden gecontroleerd (door middel van een audit door een derde) vóór de CE-markering overeenkomstig het verantwoordingsbeginsel. In het kader van deze beoordeling door derden zal de initiële effectbeoordeling die door de aanbieder moet worden uitgevoerd, bijzonder relevant zijn.

¹¹Het Bureau van de Europese Unie voor de grondrechten (FRA) heeft al aandacht besteed aan de noodzaak om effectbeoordelingen met betrekking tot de grondrechten uit te voeren bij het gebruik van AI of aanverwante technologieën. In zijn verslag uit 2020, “[Op het juiste pad voor de toekomst – Artificiële intelligentie en de grondrechten](#)”, wees het FRA op (vrije vertaling) “valkuilen in het gebruik van AI, bijvoorbeeld bij voorspellend politiewerk, medische diagnoses, sociale diensten en gerichte reclame” en benadrukte het dat “particuliere en publieke organisaties moeten beoordelen hoe AI de grondrechten kan schaden” om de negatieve gevolgen voor individuen te beperken.

24. Gezien de complexiteit die de ontwikkeling van AI-systemen met zich meebrengt, moet erop worden gewezen dat de technische kenmerken van AI-systemen (bv. het soort AI-benadering) tot grotere risico's kunnen leiden. Daarom moet bij elke risicobeoordeling van AI-systemen rekening worden gehouden **met de technische kenmerken, samen met specifieke praktijkvoorbeelden en de context** waarin het systeem werkt.
25. In het licht van het bovenstaande bevelen het EDPB en de EDPS aan in het voorstel te specificeren dat **de aanbieder** een eerste risicobeoordeling van het betrokken AI-systeem moet uitvoeren, **rekening houdend met de praktijkvoorbeelden** (te specificeren in het voorstel – ter aanvulling bijvoorbeeld van bijlage III, punt 1, onder a), waar de praktijkvoorbeelden van AI-biometrische systemen niet worden genoemd), en dat de **gebruiker** van het AI-systeem, in zijn hoedanigheid van verwerkingsverantwoordelijke in het kader van de EU-gegevensbeschermingswetgeving (indien van toepassing), de gegevensbeschermingseffectbeoordeling moet uitvoeren zoals bepaald in artikel 35 van de AVG, artikel 39 van de EUDPR en artikel 27 van de LED, en niet alleen met de technische kenmerken en het **praktijkvoorbeeld** rekening houdt, maar **ook met de specifieke context** waarin AI werkt.
26. Bovendien moeten sommige van de in bijlage III bij het voorstel vermelde termen, zoals de term “essentiële particuliere diensten” of de kleine aanbieder die voor eigen gebruik een AI-beoordeling van kredietwaardigheid aanwendt, worden verduidelijkt.

2.3 Verboden gevallen van gebruik van AI

27. Het EDPB en de EDPS zijn van mening dat **indringende vormen van AI** – met name die welke de menselijke waardigheid kunnen aantasten – moeten worden beschouwd als verboden AI-systemen uit hoofde van artikel 5 van het voorstel in plaats van eenvoudigweg als “risicovol” te worden geclassificeerd in bijlage III bij het voorstel, zoals die onder nr. 6. Dit geldt met name voor gegevensvergelijkingen die op grote schaal ook betrekking hebben op personen die geen of slechts geringe aanleiding hebben gegeven tot politieobservatie of verwerking die afbreuk doet aan het beginsel van doelbinding in het kader de gegevensbeschermingswetgeving. Het gebruik van AI op het gebied van politie en rechtshandhaving vereist gebiedsspecifieke, nauwkeurige, voorzienbare en evenredige regels waarin rekening moet worden gehouden met de belangen van de betrokken personen en de gevolgen voor de werking van een democratische samenleving.
28. In artikel 5 van het voorstel wordt geriskeerd lippendienst te bewijzen aan de “waarden” en het verbod op AI-systemen, in tegenstelling tot dergelijke waarden. De in artikel 5 bedoelde criteria om de AI-systemen te “kwalificeren” als verboden **beperken het toepassingsgebied van het verbod** in die mate dat het in de praktijk zinloos kan blijken te zijn (bv. “die ertoe leidt of waarschijnlijk toe zal leiden dat [...] fysieke of psychologische schade zullen oplopen” in artikel 5, lid 1, onder a) en b); beperking tot overheidsinstanties in artikel 5, lid 1, onder c); vage formulering in punten i) en ii), onder c); beperking tot “real-time” biometrische identificatie op afstand, zonder duidelijke definitie enz.).

29. Met name het gebruik van AI voor “sociale scoring”, zoals bedoeld in artikel 5, lid 1, onder c), van het voorstel, kan leiden tot discriminatie en druist in tegen de fundamentele waarden van de EU. In het voorstel worden deze praktijken alleen verboden wanneer zij “gedurende een bepaalde periode” of “door of namens overheidsinstanties” worden uitgevoerd. Particuliere ondernemingen, met name sociale media en aanbieders van clouddiensten, kunnen grote hoeveelheden persoonsgegevens verwerken en sociale scoring uitvoeren. Bijgevolg **moet in het voorstel elke vorm van sociale waardering worden verboden**. Er zij op gewezen dat in artikel 4 van de LED in het kader van rechtshandhaving dergelijke activiteiten al aanzienlijk worden beperkt, zo niet in de praktijk zijn verboden.
30. **Biometrische identificatie op afstand** van personen in openbare ruimten houdt een hoog risico in van inmenging in het privéleven van personen. Daarom zijn het EDPB en de EDPS **van mening dat een striktere aanpak noodzakelijk is**. Het gebruik van AI-systemen kan ernstige evenredigheidsproblemen opleveren, aangezien het kan gaan om de verwerking van gegevens van een willekeurig en onevenredig aantal betrokkenen voor de identificatie van slechts enkele personen (bv. passagiers op luchthavens en treinstations). De **vlotte** aard van systemen voor biometrische identificatie op afstand leidt ook tot transparantieproblemen en problemen in verband met de rechtsgrondslag voor de verwerking in het kader van het EU-recht (de LED, de AVG, de EUDPR en andere toepasselijke wetgeving). Het probleem met betrekking tot de manier waarop personen naar behoren over deze verwerking kunnen worden geïnformeerd, blijft overeind, evenals de effectieve en tijdige uitoefening van de rechten van personen. Hetzelfde geldt voor **de onomkeerbare, ernstige gevolgen voor de** (redelijke) **verwachting van de bevolking dat zij anoniem zullen zijn in openbare ruimten**, met als gevolg een rechtstreeks negatief effect op de uitoefening van de vrijheid van meningsuiting, vergadering, vereniging en vrijheid van verkeer.
31. In artikel 5, lid 1, onder d), van het voorstel is voorzien in een uitgebreide **lijst van uitzonderlijke gevallen** waarin “real time” biometrische identificatie op afstand in openbare ruimten is toegestaan met het oog op rechtshandhaving. Het EDPB en de EDPS achten **deze aanpak** op verschillende punten gebrekkig: Ten eerste is het onduidelijk wat moet worden verstaan onder “een aanzienlijke vertraging” en hoe deze als een verzachtende omstandigheid moet worden beschouwd, rekening houdend met het feit dat een massa-identificatiesysteem duizenden personen in slechts enkele uren kan identificeren. Bovendien hangt de indringendheid van de verwerking niet altijd af van de vraag of de identificatie in realtime of niet gebeurt. Biometrische identificatie op afstand die achteraf in het kader van een politiek protest wordt uitgevoerd zal waarschijnlijk een aanzienlijk remmend effect hebben op de uitoefening van de fundamentele rechten en vrijheden, zoals de vrijheid van vergadering en vereniging en meer in het algemeen de grondbeginselen van de democratie. In de tweede plaats hangt de indringendheid van de verwerking niet noodzakelijkerwijs af van het doel ervan. Het gebruik van dit systeem voor andere doeleinden, zoals particuliere beveiliging, vormt dezelfde bedreiging voor de grondrechten van de eerbiediging van het privéleven, het familie- en gezinsleven en de bescherming van persoonsgegevens. Tot slot zal zelfs met de voorziene beperkingen, het potentiële aantal verdachten of daders van misdrijven bijna altijd “hoog genoeg” zijn om het doorlopende gebruik van AI-systemen voor de opsporing van verdachte personen te rechtvaardigen, ondanks de verdere voorwaarden in artikel 5, lid 2 tot en met lid 4

van het voorstel. In de redenering die aan het voorstel ten grondslag ligt, lijkt te worden voorbijgegaan aan het feit dat bij het toezicht op vrij toegankelijke ruimten, niet alleen voor verdachten moeten worden voldaan aan de verplichtingen uit hoofde van de EU-wetgeving inzake gegevensbescherming, maar ook voor al degenen waarop in de praktijk toezicht wordt uitgeoefend.

32. Om al deze redenen **dringen** het EDPB en de EDPS **aan op een algemeen verbod op het gebruik van AI voor de geautomatiseerde herkenning van menselijke kenmerken in openbare ruimten – zoals gezichten, maar ook van bewegingspatroon, vingerafdrukken, DNA, spraak, toetsaanslagen en andere biometrische of gedragssignalen – in elke context.** De huidige aanpak van het voorstel bestaat erin alle AI-systemen die verboden moeten worden, in kaart te brengen en op te sommen. Daarom moeten **AI-systemen voor grootschalige identificatie op afstand in onlineruimten** omwille van de consistentie worden verboden op grond van artikel 5 van het voorstel. Rekening houdend met de LED, de EUDPR en de AVG kunnen de EDPS en het EDPB niet vaststellen hoe dit soort praktijken zou kunnen voldoen aan de vereisten van noodzakelijkheid en evenredigheid, en hoe dit uiteindelijk voortvloeit uit wat door het HvJ-EU en het EHRM aanvaardbaar wordt geacht wat inmenging in de grondrechten aangaat.
33. Bovendien **bevelen** het EDPB en de EDPS voor zowel overheidsinstanties als particuliere entiteiten **een verbod aan op AI-systemen die personen categoriseren op basis van biometrische kenmerken (bijvoorbeeld van gezichtsherkenning) in clusters volgens etnische afkomst, geslacht, politieke of seksuele geaardheid of andere discriminatiegronden die verboden zijn op grond van artikel 21 van het Handvest, of AI-systemen waarvan de wetenschappelijke validiteit niet is aangetoond of die rechtstreeks indruisen tegen de essentiële waarden van de EU (bv. polygraaf, bijlage III, punt 6, onder b), en punt 7, onder a)).** Daarom moet **“biometrische categorisering” op grond van artikel 5 worden verboden.**
34. Het tast ook **de menselijke waardigheid aan om door een computer bepaald of ingedeeld te worden voor toekomstig gedrag, onafhankelijk van iemands eigen vrije wil.** AI-systemen die bedoeld zijn om door rechtshandhavingsautoriteiten te worden gebruikt voor het uitvoeren van individuele risicobeoordelingen van natuurlijke personen om te beoordelen hoe groot het risico is dat een natuurlijke persoon (opnieuw) een strafbaar feit pleegt, zie bijlage III, punt 6, onder a), of voor het voorspellen van een daadwerkelijk of potentieel strafbaar feit dat (opnieuw) zal worden gepleegd, op basis van de profilering van een natuurlijke persoon of de beoordeling van persoonlijkheidskenmerken en kenmerken of eerder crimineel gedrag, zie bijlage III, punt 6, onder e), en worden gebruikt overeenkomstig het beoogde doel, zullen leiden tot een centrale onderwerping van de politieke en justitiële besluitvorming, waardoor de betrokken persoon wordt ontmenselijkt. Dergelijke AI-systemen die de essentie van het recht op menselijke waardigheid raken, moeten op grond van artikel 5 worden verboden.
35. Voorts zijn het EDPB en de EDPS van mening dat het gebruik van AI **om emoties van een natuurlijke persoon af te leiden zeer onwenselijk is en moet worden verboden**, behalve in bepaalde welomschreven gevallen van gebruik, namelijk voor gezondheids- of onderzoeksdoeleinden (bv. patiënten bij wie emotieherkenning belangrijk is), altijd met

passende waarborgen en uiteraard met inachtneming van alle andere gegevensbeschermingsvoorwaarden en -beperkingen, waaronder doelbinding.

2.4 [AI-systemen met een hoog risico](#)

2.4.1 [Noodzaak van een conformiteitsbeoordeling vooraf door externe derden](#)

36. Het EDPB en de EDPS juichen toe dat AI-systemen met een hoog risico vooraf aan een conformiteitsbeoordeling moeten worden onderworpen voordat zij in de EU in de handel kunnen worden gebracht of anderszins in gebruik kunnen worden genomen. Dit regelgevingsmodel wordt in principe toegejuicht, omdat het een goed evenwicht biedt tussen innovatievriendelijkheid en een hoog niveau van proactieve bescherming van de grondrechten. Om in specifieke omgevingen zoals besluitvormingsprocessen van openbare diensten of kritieke infrastructuur te kunnen worden gebruikt, moet worden bepaald hoe de volledige broncode kan worden onderzocht.
37. Het EDPB en de EDPS pleiten er echter voor de conformiteitsbeoordelingsprocedure uit hoofde van artikel 43 van het voorstel zodanig aan te passen dat een **conformiteitsbeoordeling vooraf door derden in het algemeen moet worden uitgevoerd voor AI met een hoog risico**. Hoewel een conformiteitsbeoordeling door derden voor de verwerking van persoonsgegevens met een hoog risico geen vereiste is in de AVG of de EUDPR, begrijpt men de risico's van AI-systemen nog niet helemaal. De algemene opname van een verplichting tot conformiteitsbeoordeling door derden zou derhalve de rechtszekerheid en het vertrouwen in alle AI-systemen met een hoog risico verder versterken.

2.4.2 [Het toepassingsgebied van de regelgeving moet ook AI-systemen omvatten die reeds in gebruik zijn](#)

38. Overeenkomstig artikel 43, lid 4, van het voorstel moeten AI-systemen met een hoog risico aan een nieuwe conformiteitsbeoordelingsprocedure worden onderworpen wanneer een significante wijziging wordt aangebracht. Het is goed ervoor te zorgen dat AI-systemen gedurende hun hele levenscyclus voldoen aan de vereisten van de AI-verordening. AI-systemen die vóór de toepassing van de voorgestelde verordening in de handel zijn gebracht of in gebruik zijn genomen (of 12 maanden daarna voor de in bijlage IX vermelde grootschalige IT-systemen) zijn van het toepassingsgebied ervan uitgesloten, tenzij deze systemen onderhevig zijn aan “significante wijzigingen” in het ontwerp of het beoogde doel (artikel 83).
39. De drempel voor “significante wijzigingen” is echter onduidelijk. In overweging 66 van het voorstel wordt een lagere drempel vermeld voor hernieuwde conformiteitsbeoordeling “wanneer zich een verandering voordoet die gevolgen kan hebben voor de overeenstemming van het systeem met deze verordening”. Een soortgelijke drempel zou passend zijn voor artikel 83, ten minste voor AI-systemen met een hoog risico. Om eventuele lacunes in de bescherming te dichten, is het bovendien noodzakelijk dat AI-systemen die reeds zijn opgezet en in gebruik zijn – na een bepaalde uitvoeringsfase – ook voldoen aan alle vereisten van de AI-verordening.

40. Ook de vele mogelijkheden voor de verwerking van persoonsgegevens en externe risico's zijn van invloed op de veiligheid van AI-systemen. De focus in artikel 83 op "significante wijzigingen in het ontwerp of het beoogde doel" omvat geen verwijzing naar veranderingen in externe risico's. Daarom moet in artikel 83 van het voorstel worden verwezen naar veranderingen in het dreigingsscenario die voortvloeien uit externe risico's, zoals cyberaanvallen, vijandelijke aanvallen en gemotiveerde klachten van consumenten.
41. Aangezien de inwerkingtreding is gepland voor 24 maanden na de inwerkingtreding van de toekomstige verordening, achten de EDPS en het EDPB het bovendien niet passend AI-systemen die reeds voor een nog langere periode in de handel zijn gebracht, vrij te stellen. Hoewel in het voorstel ook is bepaald dat bij de evaluatie van elk grootschalig IT-systeem overeenkomstig de in bijlage IX vermelde rechtshandelingen rekening moet worden gehouden met de vereisten van de verordening, zijn het EDPB en de EDPS van mening dat de vereisten betreffende het gebruik van AI-systemen van toepassing moeten zijn vanaf de datum van inwerkingtreding van de toekomstige verordening.

2.5 Governance en Europees AI-comité

2.5.1 Governance

42. Het EDPB en de EDPS zijn ingenomen met de aanwijzing van de EDPS als bevoegde autoriteit en markttoezichtautoriteit voor het toezicht op de instellingen, instanties en organen van de Unie wanneer deze binnen het toepassingsgebied van dit voorstel vallen. De EDPS is bereid om zijn nieuwe rol als AI-regulator voor het openbaar bestuur van de EU te vervullen. Bovendien zijn de rol en de taken van de EDPS niet nauwkeurig genoeg bepaald en moeten ze in het voorstel verder worden verduidelijkt, met name voor wat betreft zijn rol als markttoezichtautoriteit.
43. Het EDPB en de EDPS erkennen de toewijzing van financiële middelen, die in het voorstel aan het Comité en de EDPS, dat als aanmeldende instantie optreedt, is toegewezen. De vervulling van de nieuwe voorziene taken van de EDPS, ongeacht of hij optreedt als aangemelde instantie, vergt echter aanzienlijk meer financiële en personele middelen.
44. Ten eerste omdat in de formulering van artikel 63, lid 6, is bepaald dat de EDPS "[op]treedt [...] als markttoezichtautoriteit" voor instellingen, instanties en organen van de Unie die onder het toepassingsgebied van het voorstel vallen, hetgeen niet verduidelijkt of de EDPS moet worden beschouwd als een volwaardige "markttoezichtautoriteit" zoals bepaald in Verordening (EU) 2019/1020. Dit roept vragen op over de taken en bevoegdheden van de EDPS in de praktijk. Ten tweede, en op voorwaarde dat de eerste vraag bevestigend wordt beantwoord, is het onduidelijk hoe de rol van de EDPS, zoals voorzien in de EUDPR, kan voldoen aan de taak bepaald in artikel 11 van Verordening (EU) 2019/1020, waartoe "op hun grondgebied doeltreffend markttoezicht [...] op de online [...] aangeboden producten" of "fysieke en laboratoriumcontroles op basis van geschikte monsters" behoort. Het risico bestaat dat het opnemen van de nieuwe reeks taken zonder verdere verduidelijking in het voorstel de vervulling van zijn verplichtingen als toezichthouder voor gegevensbescherming in gevaar zou kunnen brengen.

45. Het EDPB en de EDPS benadrukken echter dat sommige bepalingen van het voorstel waarin de taken en bevoegdheden van de verschillende bevoegde autoriteiten in het kader van de AI-verordening, hun relaties, hun aard en de garantie van hun onafhankelijkheid worden omschreven, in dit stadium onduidelijk lijken. In Verordening (EU) 2019/1020 is bepaald dat de markttoezichtautoriteit onafhankelijk moet zijn, maar in de ontwerpverordening is er geen vereiste opgenomen dat de toezichthoudende autoriteiten onafhankelijk moeten zijn; er is zelfs een verplichting opgenomen voor hen om aan de Commissie verslag uit te brengen over bepaalde taken die worden uitgevoerd door markttoezichtautoriteiten, die verschillende instellingen kunnen zijn. Aangezien in het voorstel ook wordt bepaald dat de gegevensbeschermingsautoriteiten de markttoezichtautoriteiten zullen zijn voor AI-systemen die voor rechtshandavingsdoeleinden worden gebruikt (artikel 63, lid 5), betekent dit ook dat zij, eventueel via hun nationale toezichthoudende autoriteit, onderworpen zullen zijn aan rapportageverplichtingen aan de Commissie (artikel 63, lid 2), hetgeen onverenigbaar lijkt met hun onafhankelijkheid.
46. Daarom zijn het EDPB en de EDPS van mening dat die bepalingen moeten worden verduidelijkt om in overeenstemming te zijn met Verordening (EU) 2019/1020, de EUDPR en de AVG, en dat in het voorstel duidelijk moet worden bepaald dat de toezichthoudende autoriteiten in het kader van de AI-verordening volledig onafhankelijk moeten zijn bij de uitvoering van hun taken, aangezien dit een essentiële garantie zou zijn voor het correcte toezicht op en de handhaving van de toekomstige verordening.
47. Het EDPB en de EDPS willen er ook aan herinneren dat de AVG, de EUDPR en de LED al door gegevensbeschermingsautoriteiten worden gehandhaafd als het gaat om AI-systemen waarbij persoonsgegevens betrokken zijn, teneinde de bescherming van de grondrechten en meer specifiek het recht op gegevensbescherming te garanderen. Daarom beschikken gegevensbeschermingsautoriteiten reeds tot op zekere hoogte, zoals vereist in het voorstel voor de nationale toezichthoudende autoriteiten, over inzicht in AI-technologieën, data en big data, grondrechten, alsook over deskundigheid bij het beoordelen van de risico's die samenhangen met nieuwe technologieën voor de grondrechten. Wanneer AI-systemen gebaseerd zijn op de verwerking van persoonsgegevens of persoonsgegevens verwerken, zijn de bepalingen van het voorstel bovendien rechtstreeks verweven met het rechtskader voor gegevensbescherming, wat het geval zal zijn voor de meeste AI-systemen die onder het toepassingsgebied van de verordening vallen. Als gevolg daarvan zullen er bevoegdheden van de toezichthoudende autoriteiten in het kader van het voorstel en de gegevensbeschermingsautoriteiten met elkaar worden verbonden.
48. Derhalve zou de aanwijzing van de gegevensbeschermingsautoriteiten als de nationale toezichthoudende autoriteiten zorgen voor een meer geharmoniseerde regelgevingsbenadering en bijdragen tot een consistente interpretatie van de bepalingen over gegevensverwerking en tegenstrijdigheden in de handhaving ervan tussen de lidstaten vermijden. Het zou ook ten goede komen aan alle belanghebbenden in de AI-waardeketen als er één contactpunt is voor alle verwerkingen van persoonsgegevens die onder het toepassingsgebied van het voorstel vallen, en het zou de interactie tussen twee verschillende toezichthoudende instanties voor verwerking die onder het voorstel en de AVG vallen, beperken. Bijgevolg zijn het EDPB en de EDPS van

mening dat **gegevensbeschermingsautoriteiten moeten worden aangewezen als nationale toezichthoudende autoriteiten overeenkomstig artikel 59 van het voorstel.**

49. Voor zover in het voorstel specifieke regels zijn opgenomen inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens die zijn vastgesteld op basis van artikel 16 van het VWEU, moet de naleving van deze regels, met name beperkingen op het gebruik van AI-systemen voor “real-time” biometrische identificatie op afstand in openbare ruimten met het oog op rechtshandhaving, **aan de controle van onafhankelijke autoriteiten worden onderworpen.**
50. Het voorstel bevat echter geen expliciete bepaling op grond waarvan de bevoegdheid om ervoor te zorgen dat deze regels worden nageleefd, wordt toegewezen aan de controle van onafhankelijke autoriteiten. De enige verwijzing naar bevoegde toezichthoudende autoriteiten voor gegevensbescherming in het kader van de AVG, of de LED, is te vinden in artikel 63, lid 5, van het voorstel, maar alleen als organen voor “markttoezichtautoriteit” en soms met enkele andere autoriteiten. Het EDPB en de EDPS zijn van mening dat deze oprichting niet waarborgt dat de in artikel 16, lid 2, van het VWEU en artikel 8 van het Handvest neergelegde eis van onafhankelijke controle wordt nageleefd.

2.5.2 Europees AI-comité

51. Het voorstel voorziet in de oprichting van een “Europees comité voor artificiële intelligentie” (EAIB). Het EDPB en de EDPS erkennen de noodzaak van een consistente en geharmoniseerde toepassing van het voorgestelde kader en van de betrokkenheid van onafhankelijke deskundigen bij de ontwikkeling van het EU-beleid inzake AI. Tegelijkertijd voorziet het voorstel in een doorslaggevende rol voor de Commissie, die niet alleen deel zou uitmaken van het EAIB, maar dit ook zou voorzitten en vetorecht zou hebben voor de vaststelling van het reglement van orde van het EAIB. Dit staat in contrast met de behoefte aan een Europees AI-orgaan dat onafhankelijk is van enige politieke invloed. Daarom zijn het EDPB en de EDPS van mening dat de toekomstige AI-verordening **het EAIB meer autonomie moet geven**, zodat het daadwerkelijk kan zorgen voor een consistente toepassing van de verordening in de hele interne markt.
52. Het EDPB en de EDPS merken ook op dat het EAIB geen bevoegdheid krijgt met betrekking tot de handhaving van de voorgestelde verordening. Gezien de verspreiding van AI-systemen over de eengemaakte markt en de waarschijnlijkheid van grensoverschrijdende gevallen is er echter een cruciale behoefte aan een geharmoniseerde handhaving en een behoorlijke verdeling van bevoegdheden tussen de nationale toezichthoudende autoriteiten. Het EDPB en de EDPS bevelen daarom aan dat de samenwerkingsmechanismen tussen de nationale toezichthoudende autoriteiten in de toekomstige AI-verordening nader worden bepaald. Het EDPB en de EDPS stellen voor een mechanisme op te leggen dat een centraal contactpunt garandeert voor personen die onder de wetgeving vallen en voor bedrijven, voor elk AI-systeem, en dat voor organisaties waarvan de activiteiten zich over meer dan de helft van de lidstaten van de EU uitstrekken, het EAIB de nationale autoriteit kan aanwijzen die verantwoordelijk zal zijn voor de handhaving van de AI-verordening voor dit AI-systeem.

53. Gezien het onafhankelijke karakter van de autoriteiten die het comité vormen, heeft deze laatste bovendien het recht om op eigen initiatief op te treden en niet alleen om de Commissie advies en bijstand te verlenen. Het EDPB en de EDPS benadrukken daarom de noodzaak van een uitbreiding van de aan het Comité toegewezen taken, die bovendien niet in overeenstemming zijn met de in het voorstel genoemde taken.
54. Om aan deze doelstellingen te voldoen, **moet het EAIB over voldoende passende bevoegdheden beschikken** en moet de juridische status ervan worden verduidelijkt. Met name om het materiële toepassingsgebied van de toekomstige verordening relevant te houden, lijkt het noodzakelijk de autoriteiten die met de toepassing ervan belast zijn, bij de ontwikkeling ervan te betrekken. Daarom bevelen het EDPB en de EDPS aan dat het EAIB de bevoegdheid krijgt om aan de Commissie wijzigingen voor te stellen van bijlage I waarin de AI-technieken en -benaderingen worden gedefinieerd en van bijlage III waarin de in artikel 6, lid 2, bedoelde AI-systemen met een hoog risico worden opgesomd. Het EAIB moet ook door de Commissie worden geraadpleegd voordat deze bijlagen worden gewijzigd.
55. In artikel 57, lid 4, van het voorstel is voorzien in uitwisseling van informatie tussen het Comité en andere instanties, bureaus, agentschappen en adviesgroepen van de Unie. Rekening houdend met hun eerdere werkzaamheden op het gebied van AI en hun deskundigheid op het gebied van mensenrechten, bevelen het EDPB en de EDPS aan het Bureau voor de grondrechten als een van de waarnemers van het Comité in overweging te nemen.

3 INTERACTIE MET HET GEGEVENSBEWAKINGSKADER

3.1 Verhouding van het voorstel tot de bestaande EU-wetgeving inzake gegevensbescherming

56. Een duidelijk omschreven verband tussen het voorstel en de bestaande gegevensbeschermingswetgeving is een essentiële voorwaarde om de eerbiediging en toepassing van het EU-acquis op het gebied van de bescherming van persoonsgegevens te waarborgen en te handhaven. Dergelijke EU-wetgeving, met name de AVG, de EUDPR en de LED, moet worden beschouwd als een grondvoorwaarde waarop verdere wetgevingsvoorstellen kunnen voortbouwen zonder afbreuk te doen aan of inbreuk te maken op de bestaande bepalingen, ook wat betreft de bevoegdheid van toezichthoudende autoriteiten en governance.
57. Volgens het EDPB en de EDPS is het daarom belangrijk om in het voorstel elke inconsistentie en mogelijke strijdigheid met de AVG, de EUDPR en de LED duidelijk te vermijden. Dit is niet alleen omwille van de rechtszekerheid, maar ook om te voorkomen dat het voorstel tot gevolg heeft dat het grondrecht op bescherming van persoonsgegevens, zoals neergelegd in artikel 16 van het VWEU en artikel 8 van het Handvest, direct of indirect in gevaar wordt gebracht.

58. Met name zelflerende machines zouden de persoonsgegevens van natuurlijke personen alleen kunnen beschermen als dit vanaf het ontwerp ervan wordt vastgelegd. De onmiddellijke mogelijkheid om de rechten van personen uit hoofde van artikel 22 (geautomatiseerde individuele besluitvorming, met inbegrip van profilering) van de AVG of artikel 23 van de EUDPR uit te oefenen, ongeacht de doeleinden van de verwerking, is eveneens van essentieel belang. In dit verband moeten bij de AI-systemen vanaf het prille begin andere rechten van de betrokkenen worden verleend in verband met het recht op wissen, het recht op correctie overeenkomstig de wetgeving inzake gegevensbescherming, ongeacht de gekozen AI-benadering of de technische architectuur.
59. Het gebruik van persoonsgegevens voor het leren met AI-systemen kan leiden tot het ontstaan van vooringenomen besluitvormingspatronen die centraal staan in het AI-systeem. Daarom zijn verschillende waarborgen, en met name deskundig menselijk toezicht op dergelijke processen vereist om ervoor te zorgen dat de rechten van betrokkenen worden geëerbiedigd en gewaarborgd, en om eventuele en alle negatieve gevolgen voor natuurlijke personen te voorkomen. De bevoegde autoriteiten moeten ook richtsnoeren kunnen voorstellen om vertekening in AI-systemen te beoordelen en de uitoefening van menselijk toezicht te ondersteunen.
60. Betrokkenen moeten altijd worden geïnformeerd wanneer hun gegevens worden gebruikt voor AI-training en/of -voorspellingen, over de rechtsgrondslag voor een dergelijke verwerking, een algemene uitleg van de logica (procedure) en het toepassingsgebied van het AI-systeem. In dat verband moet het recht van personen op beperking van de verwerking (artikel 18 van de AVG en artikel 20 van de EUDPR) en op het wissen/wissing van gegevens (artikel 16 van de AVG en artikel 19 van de EUDPR) in die gevallen altijd worden gewaarborgd. Voorts moet de verwerkingsverantwoordelijke de uitdrukkelijke verplichting hebben om de betrokkene in kennis te stellen van de toepasselijke termijnen voor bezwaar, beperking, verwijdering van gegevens enz. Het AI-systeem moet door middel van passende technische en organisatorische maatregelen aan alle gegevensbeschermingsvereisten kunnen voldoen. Recht op uitleg moet zorgen voor meer transparantie.

3.2 Testomgeving & verdere verwerking (artikelen 53 en 54 van het voorstel)

61. Binnen de bestaande juridische en morele grenzen is het belangrijk om Europese innovatie te bevorderen door middel van instrumenten zoals een testomgeving. Een testomgeving biedt de mogelijkheid de nodige waarborgen te bieden voor het opbouwen van geloof en vertrouwen in AI-systemen. In complexe omgevingen kan het voor AI-professionals moeilijk zijn alle belangen op een juiste manier af te wegen. Vooral voor kleine en middelgrote ondernemingen met beperkte middelen kan het werken in een testomgeving voor regelgeving sneller inzicht opleveren en zo innovatie bevorderen.
62. In artikel 53, lid 3, van het voorstel wordt bepaald dat de testomgeving de toezichthoudende en corrigerende bevoegdheden onverlet laat. Indien deze verduidelijking nuttig is, is er ook behoefte aan het aanreiken van richting of sturing voor het vinden van een goed evenwicht

tussen het uitvoeren van de taken van een toezichhoudende autoriteit enerzijds en het verstrekken van gedetailleerde richtsnoeren via een testomgeving anderzijds.

63. In artikel 53, afdeling 6, wordt beschreven dat de modaliteiten en voorwaarden van de werking van de testomgevingen worden uiteengezet in uitvoeringshandelingen. Het is belangrijk dat er specifieke richtsnoeren worden opgesteld om te zorgen voor consistentie en ondersteuning bij de totstandkoming en werking van testomgevingen. Met bindende uitvoeringshandelingen kan het vermogen van elke lidstaat echter worden beperkt om de testomgeving aan te passen aan hun behoeften en lokale praktijken. Daarom bevelen het EDPB en de EDPS aan dat het EAIB in plaats daarvan richtsnoeren voor testomgevingen verstrekt.
64. Met artikel 54 van het voorstel wordt beoogd een rechtsgrondslag te verschaffen voor verdere verwerking van persoonsgegevens met het oog op de ontwikkeling van bepaalde AI-systemen in het algemeen belang in de testomgeving voor AI-regelgeving. De verhouding tussen artikel 54, lid 1, van het voorstel en artikel 54, lid 2, en overweging 41 van het voorstel en dus ook met de bestaande EU-wetgeving inzake gegevensbescherming, blijft onduidelijk. De AVG en de EUDPR hebben echter al een vaste basis voor “verdere verwerking”. Vooral in gevallen waarin het in het algemeen belang is verdere verwerking toe te staan, hoeft de afweging tussen de belangen van de verwerkingsverantwoordelijke en de belangen van de betrokkene innovatie immers niet in de weg te staan. In artikel 54 van het voorstel wordt momenteel niet ingegaan op twee belangrijke kwesties: i) onder welke omstandigheden, met behulp van welke (aanvullende) criteria de belangen van de betrokkenen worden gewogen, en ii) of deze AI-systemen alleen binnen de testomgeving zullen worden gebruikt. Het EDPB en de EDPS zijn ingenomen met het vereiste van wetgeving van de Unie of van de lidstaten bij de verwerking van persoonsgegevens die in het kader van de LED in een testomgeving zijn verzameld, maar bevelen aan om nader te bepalen wat hier wordt beoogd, op een wijze die in overeenstemming is met de AVG en de EUDPR, voornamelijk door te verduidelijken dat de rechtsgrondslag van dergelijke testomgevingen moet voldoen aan de vereisten van artikel 23, lid 2, van de AVG, artikel 25 van de EUDPR, en nauwkeurig aan te geven dat elk gebruik van de testomgeving aan een grondige evaluatie moet worden onderworpen. Dit geldt ook voor de volledige lijst van voorwaarden uit artikel 54, lid 1, onder b) tot en met j).
65. Uit een aantal aanvullende overwegingen met betrekking tot het hergebruik van gegevens in artikel 54 van het voorstel blijkt dat de exploitatie van een testomgeving arbeidsintensief is en dat het daarom realistisch is te veronderstellen dat slechts een klein aantal bedrijven de kans zal krijgen om deel te nemen. Deelname aan de testomgeving zou een concurrentievoordeel kunnen zijn. Om hergebruik van gegevens mogelijk te maken, moet zorgvuldig worden nagegaan hoe deelnemers kunnen worden geselecteerd om ervoor te zorgen dat zij binnen het toepassingsgebied vallen en om oneerlijke behandeling te voorkomen. Het EDPB en de EDPS vrezen dat de mogelijkheid die wordt geboden om gegevens te hergebruiken in het kader van de testomgeving afwijkt van de verantwoordingsbenadering in de AVG, daar waar de verantwoordingsplicht wordt gelegd bij de verwerkingsverantwoordelijke en niet bij de bevoegde autoriteit.

66. Voorts zijn het EDPB en de EDPS van mening dat, gezien de doelstellingen van de testomgeving, namelijk het ontwikkelen, testen en valideren van AI-systemen, de testomgevingen niet onder het toepassingsgebied van de LED kunnen vallen. De LED voorziet weliswaar in het hergebruik van gegevens voor wetenschappelijk onderzoek, maar de voor dat secundaire doel verwerkte gegevens vallen onder de AVG of de EUDPR en niet langer onder de LED.
67. Het is niet duidelijk wat een testomgeving voor regelgeving zal omvatten. De vraag rijst of de voorgestelde testomgeving voor regelgeving een IT-infrastructuur in elke lidstaat omvat met een aantal aanvullende juridische gronden voor verdere verwerking, dan wel of ze alleen toegang verleent tot deskundigheid en richtsnoeren op het gebied van regelgeving. Het EDPB en de EDPS dringen er bij de wetgever op aan dit concept in het voorstel te verduidelijken en in het voorstel duidelijk te vermelden dat een testomgeving voor regelgeving de bevoegde autoriteiten niet verplicht hun technische infrastructuur ter beschikking te stellen. In ieder geval moeten met het oog op deze verduidelijking dienovereenkomstig financiële en personele middelen ter beschikking van de bevoegde autoriteiten worden gesteld.
68. Tot slot willen het EDPB en de EDPS de nadruk leggen op de ontwikkeling van grensoverschrijdende AI-systemen die beschikbaar zullen zijn voor de Europese digitale eengemaakte markt in zijn geheel. In het geval van dergelijke AI-systemen mag de testomgeving voor regelgeving als instrument voor innovatie geen belemmering vormen voor grensoverschrijdende ontwikkeling. Daarom bevelen het EDPB en de EDPS een gecoördineerde grensoverschrijdende aanpak aan die op nationaal niveau nog steeds voldoende beschikbaar is voor alle kmo's, en die een gemeenschappelijk kader in heel Europa biedt zonder al te restrictief te zijn. Er moet een evenwicht worden gevonden tussen Europese coördinatie en nationale procedures om tegenstrijdige tenuitvoerlegging van de toekomstige AI-verordening te voorkomen, wat innovatie in de hele EU zou belemmeren.

3.3 Transparantie

69. Het EDPB en de EDPS juichen toe dat AI-systemen met een hoog risico worden geregistreerd in een openbare databank (als bedoeld in artikel 51 en 60 van het voorstel). Van deze databank moet gebruik worden gemaakt om het grote publiek te informeren over het toepassingsgebied van het AI-systeem en over bekende tekortkomingen en incidenten die de werking ervan in het gedrang kunnen brengen, en over de maatregelen die aanbieders hebben getroffen om deze aan te pakken en te verhelpen.
70. Een essentieel democratisch beginsel is het gebruik van controlemechanismen. Daarom is het feit dat de transparantieverplichting niet van toepassing is op AI-systemen die worden gebruikt om strafbare feiten op te sporen, te voorkomen, te onderzoeken of te vervolgen, een te ruime uitzondering. Er moet een onderscheid worden gemaakt tussen AI-systemen die worden gebruikt om strafbare feiten op te sporen of te voorkomen en AI-systemen die gericht zijn op het onderzoeken of helpen bij de vervolging van strafbare feiten. De waarborgen voor preventie en opsporing moeten strenger zijn vanwege het vermoeden van onschuld. Bovendien betreuren het EDPB en de EDPS het ontbreken van waarschuwingen in het voorstel, wat kan worden

geïnterpreteerd als een groen licht voor het gebruik van AI-systemen met een hoog risico, zelfs als dat niet bewezen is, of -toepassingen.

71. In gevallen waarin om redenen van geheimhouding, zelfs in een goed functionerende democratie, weinig tot geen transparantie kan worden gegeven aan het publiek, moeten er waarborgen zijn en moeten die AI-systemen worden geregistreerd bij en transparantie bieden aan de bevoegde toezichthoudende autoriteit.
72. Het waarborgen van transparantie in AI-systemen is een zeer uitdagende doelstelling. De volledig kwantitatieve besluitvormingsaanpak van veel AI-systemen, die inherent verschilt van de menselijke benadering, die meestal gebaseerd is op causale en theoretische redenering, kan ingaan tegen de noodzaak om vooraf een begrijpelijke uitleg te krijgen over de resultaten van de machine. In de verordening moeten nieuwe, proactievere en tijdige manieren worden bevorderd om gebruikers van AI-systemen te informeren over de (besluitvormings)status waar het systeem zich bevindt, waarbij vroegtijdig wordt gewaarschuwd voor mogelijk schadelijke uitkomsten, zodat personen wier rechten en vrijheden door autonome besluiten van machines in het gedrang kunnen komen, kunnen reageren of het besluit kunnen herroepen.

3.4 Verwerking van bijzondere categorieën gegevens & gegevens betreffende strafbare feiten

73. De verwerking van bijzondere categorieën gegevens op het gebied van rechtshandhaving, valt onder de bepalingen van het EU-kader voor gegevensbescherming, met inbegrip van de LED en de nationale uitvoering ervan. In het voorstel wordt gesteld dat het geen algemene rechtsgrond verstrekt voor de verwerking van persoonsgegevens, met inbegrip van bijzondere categorieën persoonsgegevens (zie overweging 41). Tegelijkertijd luidt artikel 10, lid 5, van het voorstel als volgt: “de aanbieders van dergelijke systemen [mogen] bijzondere categorieën persoonsgegevens verwerken”. Bovendien vereist dezelfde bepaling aanvullende waarborgen, waarbij ook voorbeelden worden gegeven. Daardoor lijkt in het voorstel te worden ingegrepen in de toepassing van de AVG, de LED en de EUDPR. Hoewel het EDPB en de EDPS ingenomen zijn met de poging om passende waarborgen te bieden, is een coherenter regelgevingsaanpak nodig, aangezien de huidige bepalingen niet duidelijk genoeg lijken om een rechtsgrondslag te creëren voor de verwerking van bijzondere categorieën gegevens, en moeten ze worden aangevuld met aanvullende beschermingsmaatregelen die nog moeten worden beoordeeld. Bovendien moet, wanneer persoonsgegevens zijn verzameld door verwerking binnen het toepassingsgebied van de LED, rekening worden gehouden met de mogelijke aanvullende waarborgen en beperkingen die voortvloeien uit de nationale omzetting van de LED.

3.5 Nalevingsmechanismen

3.5.1 Certificering

74. Een van de belangrijkste pijlers van het voorstel is certificering. Het in het voorstel geschetste certificeringssysteem is gebaseerd op een structuur van entiteiten (aanmeldende autoriteiten/aangemelde instanties/Commissie) en een conformiteitsbeoordelings-/certificeringsmechanisme dat betrekking heeft op de verplichte eisen die van toepassing zijn op

AI-systemen met een hoog risico, en is gebaseerd op Europese geharmoniseerde normen uit hoofde van Verordening (EU) nr. 1025/2012 en gemeenschappelijke specificaties die door de Commissie moeten worden vastgesteld. Dit mechanisme verschilt van het certificeringssysteem dat gericht is op het waarborgen van de naleving van de regels en beginselen inzake gegevensbescherming, zoals uiteengezet in de artikelen 42 en 43 van de AVG. Het is echter niet duidelijk hoe certificaten die overeenkomstig het voorstel door aangemelde instanties zijn afgegeven, kunnen worden gekoppeld aan gegevensbeschermingscertificaten, zegels en merktekens waarin de AVG voorziet, in tegenstelling tot wat voor andere soorten certificaten wordt bepaald (zie artikel 42, lid 2, met betrekking tot certificaten die zijn afgegeven op grond van Verordening (EU) 2019/881).

75. Voor zover AI-systemen met een hoog risico gebaseerd zijn op de verwerking van persoonsgegevens of persoonsgegevens verwerken om hun taak te vervullen, kunnen deze discrepanties rechtsonzekerheid veroorzaken voor alle betrokken instanties, aangezien zij kunnen leiden tot situaties waarin AI-systemen die in het kader van het voorstel zijn gecertificeerd en voorzien zijn van een CE-markering van overeenstemming zodra zij in de handel zijn gebracht of in gebruik zijn genomen, kunnen worden gebruikt op een wijze die niet in overeenstemming is met de regels en beginselen inzake gegevensbescherming.
76. In het voorstel ontbreekt een duidelijk verband met de gegevensbeschermingswetgeving en met andere wetgeving van de EU en de lidstaten die van toepassing is op elk “gebied” van een in bijlage III vermeld AI-systeem met een hoog risico. In het voorstel moeten met name de beginselen van minimale gegevensverwerking en gegevensbescherming door ontwerp worden opgenomen als een van de aspecten waarmee rekening moet worden gehouden voordat de CE-markering wordt verkregen, gezien de mogelijke hoge mate van inmenging van de AI-systemen met een hoog risico in de grondrechten op privacy en op de bescherming van persoonsgegevens, en de noodzaak om een hoog vertrouwensniveau in het AI-systeem te waarborgen. Het EDPB en de EDPS bevelen dan ook aan het voorstel te wijzigen om het verband tussen certificaten die op grond van de genoemde verordening zijn afgegeven en certificaten, zegels en merktekens op het gebied van gegevensbescherming te verduidelijken. Ten slotte moeten de gegevensbeschermingsautoriteiten worden betrokken bij de voorbereiding en vaststelling van geharmoniseerde normen en gemeenschappelijke specificaties.
77. In verband met artikel 43 van het voorstel, dat betrekking heeft op de conformiteitsbeoordeling, lijkt de in artikel 47 bedoelde afwijking van de conformiteitsbeoordelingsprocedure zeer ruim te zijn, met inbegrip van te veel uitzonderingen, zoals uitzonderlijke redenen van openbare veiligheid of de bescherming van het leven en de gezondheid van personen, milieubescherming en de bescherming van essentiële industriële en infrastructurele activa. Wij stellen de wetgevers voor om deze te beperken.

3.5.2 Gedragscodes

78. Overeenkomstig artikel 69 van het voorstel stimuleren en faciliteren de Commissie en de lidstaten de opstelling van gedragscodes ter bevordering van de vrijwillige toepassing door aanbieders van AI-systemen zonder een hoog risico van de vereisten die van toepassing zijn op

AI-systemen met een hoog risico, alsmede van aanvullende vereisten. Overeenkomstig overweging 78 van de AVG bevelen het EDPB en de EDPS aan om synergieën vast te stellen en te definiëren tussen deze instrumenten en de gedragscodes waarin de AVG voorziet ter ondersteuning van de naleving van de gegevensbescherming. In dit verband is het van belang te verduidelijken of de bescherming van persoonsgegevens valt onder de “aanvullende voorschriften” waaraan de in artikel 69, lid 2, bedoelde gedragscodes kunnen voldoen. Het is ook van belang ervoor te zorgen dat de “technische specificaties en oplossingen”, waarop de in artikel 69, lid 1, bedoelde gedragscodes betrekking hebben en die bedoeld zijn om de naleving van de vereisten van de AI-ontwerpverordening te bevorderen, niet in strijd zijn met de regels en beginselen van de AVG en de EUDPR. Op die manier zou de naleving van deze instrumenten door aanbieders van AI-systemen zonder een hoog risico – voor zover dergelijke systemen gebaseerd zijn op de verwerking van persoonsgegevens of het verwerken van persoonsgegevens om hun taak te vervullen – een toegevoegde waarde hebben, aangezien dit ervoor zal zorgen dat de verwerkingsverantwoordelijke en de verwerkers hun gegevensbeschermingsverplichtingen bij het gebruik van die systemen kunnen nakomen.

79. Tegelijkertijd zou het rechtskader voor betrouwbare AI worden aangevuld met de integratie van gedragscodes, om het vertrouwen in het gebruik van deze technologie te bevorderen op een manier die veilig is en in overeenstemming is met de wet, met inbegrip van de eerbiediging van de grondrechten. Het ontwerp van deze instrumenten moet echter worden versterkt door mechanismen te overwegen om na te gaan of dergelijke codes doeltreffende “technische specificaties en oplossingen” bieden en “duidelijke doelstellingen en kernprestatie-indicatoren vaststellen om de verwezenlijking van die doelstellingen te meten” als integraal onderdeel van de desbetreffende codes. Bovendien kan de doeltreffendheid en afdwingbaarheid van deze instrumenten verder worden verzwakt door het ontbreken van zowel een verwijzing naar (verplichte) monitoringmechanismen voor gedragscodes die bedoeld zijn om na te gaan of aanbieders van AI-systemen zonder een hoog risico aan de bepalingen ervan voldoen, als de mogelijkheid voor individuele aanbieders om de genoemde codes op te stellen (en zelf ten uitvoer te leggen) (zie punt 5.2.7 van de toelichting).
80. Tot slot vragen het EDPB en de EDPS om opheldering over de soorten initiatieven die de Commissie volgens overweging 81 van het voorstel kan ontwikkelen “om de technische belemmeringen te helpen beperken die de grensoverschrijdende uitwisseling van gegevens voor AI-ontwikkeling belemmeren”.

4 CONCLUSIE

81. Hoewel het EDPB en de EDPS het voorstel van de Commissie toejuichen en van mening zijn dat een dergelijke verordening noodzakelijk is om de grondrechten van EU-burgers en -ingezetenen te waarborgen, zijn zij van mening dat het voorstel op verschillende punten moet worden aangepast om de toepasbaarheid en efficiëntie ervan te waarborgen.
82. Gezien de complexiteit van het voorstel en de problemen die men ermee beoogt aan te pakken, moet er nog veel werk worden verzet totdat het voorstel kan leiden tot een goed functionerend rechtskader dat de AVG op efficiënte wijze aanvult op het gebied van de bescherming van de mensenrechten en tegelijkertijd innovatie bevordert. Het EDPB en de EDPS zullen beschikbaar blijven om hun steun in dit proces te bieden.

Brussel, 18 juni 2021

Voor het Europees Comité voor
gegevensbescherming

De voorzitter

Andrea JELINEK

Voor de Europese Toezichthouder voor
gegevensbescherming

De toezichthouder

Wojciech Rafał WIEWIÓROWSKI