

Advies van de EDPB (artikel 64)



Advies 28/2024 over bepaalde aspecten van gegevensbescherming in verband met de verwerking van persoonsgegevens in het kader van AI-modellen

Vastgesteld op 17 december 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Samenvatting

AI-technologie biedt vele kansen en voordelen in een breed scala van sectoren en maatschappelijke activiteiten.

Door het grondrecht op gegevensbescherming te waarborgen ondersteunt de AVG deze kansen en beschermt de verordening ook andere grondrechten van de EU, waaronder het recht op vrijheid van gedachte, van meningsuiting en van informatie, het recht op onderwijs of de vrijheid van ondernemerschap. Op die manier is de AVG een rechtskader dat verantwoorde innovatie stimuleert.

Gezien de vragen die deze technologieën op het gebied van gegevensbescherming oproepen, heeft de Ierse toezichthoudende autoriteit het EDPB op grond van artikel 64, lid 2, AVG gevraagd een advies uit te brengen over aangelegenheden van algemene strekking. Het verzoek heeft betrekking op de verwerking van persoonsgegevens bij de ontwikkeling en de inzet van modellen voor artificiële intelligentie ("AI"). Meer in het bijzonder werd in het verzoek gevraagd: 1) wanneer en op welke wijze een AI-model als "anoniem" kan worden beschouwd; 2) op welke wijze verwerkingsverantwoordelijken kunnen aantonen dat een gerechtvaardigd belang een passende rechtsgrondslag vormt voor de ontwikkelingsfase; en 3) de inzetfase; en 4) welke gevolgen de onrechtmatige verwerking van persoonsgegevens in de ontwikkelingsfase van een AI-model heeft voor de latere verwerking of het latere gebruik van het AI-model.

Ten aanzien van de eerste vraag wordt in het advies aangegeven dat de geclaimde anonimiteit van een AI-model door de bevoegde toezichthoudende autoriteiten per geval moet worden beoordeeld omdat met persoonsgegevens getrainde AI-modellen volgens het EDPB niet in alle gevallen als anoniem kunnen worden beschouwd. Een AI-model kan pas als anoniem worden beschouwd als zowel 1) de kans op rechtstreekse (ook waarschijnlijke) extractie van persoonsgegevens over personen van wie persoonsgegevens zijn gebruikt om het model te ontwikkelen; als 2) de kans dat die persoonsgegevens al dan niet opzettelijk bij zoekopdrachten worden verkregen niet significant is, gelet op *"alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt"* door de verwerkingsverantwoordelijke of door een andere persoon.

Bij hun beoordeling moeten de toezichthoudende autoriteiten de documenten beoordelen die door de verwerkingsverantwoordelijke worden verstrekt om de anonimiteit van het model aan te tonen. In dat verband is in het advies een niet-bindende en niet-uitputtende lijst opgenomen van methoden die verwerkingsverantwoordelijken kunnen gebruiken om anonimiteit aan te tonen en dus door de toezichthoudende autoriteiten moeten worden onderzocht wanneer zij een anonimiteitsclaim van een verwerkingsverantwoordelijke onderzoeken. Hieronder vallen bijvoorbeeld de benaderingen die verwerkingsverantwoordelijken in de ontwikkelingsfase hebben toegepast om het verzamelen van persoonsgegevens voor trainingsdoeleinden te voorkomen of te beperken, om hun identificeerbaarheid te beperken, om hun extractie te voorkomen of om er zeker van te zijn dat hun model volgens de laatste stand van de techniek tegen aanvallen is beschermd.

Ten aanzien van de tweede en de derde vraag zijn in het advies algemene overwegingen opgenomen waarmee toezichthoudende autoriteiten rekening kunnen houden wanneer zij beoordelen of verwerkingsverantwoordelijken een gerechtvaardigd belang mogen gebruiken als rechtsgrondslag voor verwerking in het kader van de ontwikkeling en de inzet van AI-modellen.

In het advies wordt erop gewezen dat de rechtsgronden in de AVG niet hiërarchisch zijn ingedeeld en dat de verwerkingsverantwoordelijken moeten bepalen welke rechtsgrond passend is voor hun

verwerkingsactiviteiten. Vervolgens wordt in het advies gewezen op de driestappentoets die moet worden uitgevoerd wanneer het gebruik van een gerechtvaardigd belang als rechtsgrond wordt beoordeeld: 1) vaststellen welk gerechtvaardigd belang door de verwerkingsverantwoordelijke of een derde wordt nagestreefd; 2) onderzoeken in hoeverre de verwerking noodzakelijk is voor de doeleinden van het (de) nagestreefde gerechtvaardigde belang(en) (ook wel de “noodzakelijkheidstoets” genoemd); en 3) beoordelen of de belangen of grondrechten en fundamentele vrijheden van de betrokkenen niet zwaarder wegen dan het (de) gerechtvaardigde belang(en) (ook wel de “afwegingstoets” genoemd).

Ten aanzien van de eerste stap wordt er in het advies op gewezen dat een belang als gerechtvaardigd kan worden beschouwd als aan alle drie de navolgende criteria wordt voldaan: het belang is 1) rechtmatig; 2) duidelijk en nauwkeurig omschreven; en 3) reëel en concreet (d.w.z. niet hypothetisch). Onder een dergelijk belang kan bij de ontwikkeling van een AI-model bijvoorbeeld de ontwikkeling worden verstaan van een chatfunctie om gebruikers te ondersteunen, of bij de inzet van het model de verbetering van de opsporing van dreigingen in een informatiesysteem.

Met betrekking tot de tweede stap wordt er in het advies op gewezen dat bij een beoordeling van de noodzakelijkheid moet worden onderzocht: 1) of de verwerkingsactiviteit het nastreven van het gerechtvaardigde belang mogelijk zal maken; en 2) of er geen minder indringende manier is om dit belang na te streven. Wanneer zij beoordelen of aan de voorwaarde van noodzakelijkheid wordt voldaan, moeten toezichthoudende autoriteiten bijzondere aandacht schenken aan de hoeveelheid persoonsgegevens die wordt verwerkt en aan de vraag of het evenredig is om het desbetreffende gerechtvaardigde belang na te streven, ook gezien het beginsel van minimale gegevensverwerking.

Met betrekking tot de derde stap wordt er in het advies op gewezen dat bij de afwegingstoets rekening moet worden gehouden met de specifieke omstandigheden van elk geval. Vervolgens wordt in het advies een overzicht gegeven van de aspecten waarmee toezichthoudende autoriteiten rekening kunnen houden als zij beoordelen of de belangen, grondrechten en fundamentele vrijheden van betrokkenen zwaarder wegen dan het belang van een verwerkingsverantwoordelijke of een derde.

In het kader van de derde stap wordt in het advies met name gewezen op specifieke risico's voor de grondrechten die bij de ontwikkeling of de inzet van AI-modellen kunnen ontstaan. Ook wordt verduidelijkt dat de verwerking van persoonsgegevens bij de ontwikkeling of de inzet van AI-modellen verschillende soorten (gunstige of ongunstige) gevolgen voor betrokkenen kan hebben. Om die gevolgen te beoordelen, kunnen de toezichthoudende autoriteiten kijken naar de aard van de gegevens die door de modellen worden verwerkt, naar het kader waarin de verwerking plaatsvindt en naar de mogelijke verdere gevolgen van de verwerking.

Daarnaast wordt in het advies gewezen op de rol van redelijke verwachtingen van betrokkenen in de afwegingstoets. Dit kan van belang zijn vanwege de complexiteit van de technologie die in AI-modellen wordt gebruikt, vanwege het feit dat het voor betrokkenen lastig kan zijn om uiteenlopende toepassingen van die modellen te overzien, en vanwege de uiteenlopende verwerkingsactiviteiten waarom het gaat. In dit verband kan zowel de informatie die aan betrokkenen wordt verstrekt als het kader waarin de verwerking plaatsvindt, behoren tot de aspecten die moeten worden onderzocht om te beoordelen of betrokkenen redelijkerwijs kunnen verwachten dat hun persoonsgegevens worden verwerkt. Ten aanzien van het kader waarin de verwerking plaatsvindt kan het hierbij gaan om: de vraag of de persoonsgegevens al dan niet openbaar waren, de aard van de relatie tussen de betrokkene en de verwerkingsverantwoordelijke (en de vraag of er tussen hen een band bestaat), de aard van de dienst, de situatie waarin de persoonsgegevens werden verzameld, de bron waaruit de gegevens werden verzameld (d.w.z. de website of de dienst waar de persoonsgegevens werden verzameld en

de privacy-instellingen die er worden aangeboden), de mogelijke verdere toepassingen van het model en de vraag of betrokkenen überhaupt weten dat hun persoonsgegevens online staan.

Voor het geval dat de belangen, rechten en vrijheden van betrokkenen zwaarder lijken te wegen dan het (de) door de verwerkingsverantwoordelijke of een derde nagestreefde gerechtvaardigde belang(en), wordt in het advies ook aangegeven dat de verwerkingsverantwoordelijke kan overwegen om door middel van verzachtende maatregelen de gevolgen van de verwerking voor deze betrokkenen te beperken. Onder die verzachtende maatregelen mogen niet de maatregelen worden verstaan die de verwerkingsverantwoordelijke hoe dan ook wettelijk moet nemen om de naleving van de AVG te waarborgen. Daarnaast moeten de maatregelen worden afgestemd op de omstandigheden van het geval en op de eigenschappen van het AI-model, waaronder ook het beoogde gebruik ervan wordt verstaan. In dit verband is in het advies een niet-uitputtende lijst opgenomen met voorbeelden van verzachtende maatregelen voor de ontwikkelingsfase (ook ten aanzien van webscraping) en de inzetfase. Verzachtende maatregelen kunnen aan snelle veranderingen onderhevig zijn en moeten worden afgestemd op de omstandigheden van het geval. Daarom moeten de toezichthoudende autoriteiten per geval blijven beoordelen of de verzachtende maatregelen passend zijn.

Ten aanzien van de vierde vraag wordt in het advies in algemene zin opgemerkt dat de toezichthoudende autoriteiten over discretionaire bevoegdheden beschikken om mogelijke inbreuken te beoordelen en passende, noodzakelijke en evenredige maatregelen te kiezen, rekening houdend met de omstandigheden van elk individueel geval. Vervolgens worden in het advies drie scenario's besproken.

In het eerste scenario worden persoonsgegevens in het AI-model bewaard (en kan dat model dus niet als anoniem worden beschouwd, zoals uiteengezet bij de eerste vraag) en vervolgens door dezelfde verwerkingsverantwoordelijke verwerkt (bijvoorbeeld bij de inzet van het model). Of bij de ontwikkeling en de inzet sprake is van aparte doeleinden (en dus van aparte verwerkingsactiviteiten) en in hoeverre het ontbreken van een rechtsgrondslag voor de eerste verwerkingsactiviteit gevolgen heeft voor de rechtmatigheid van de latere verwerking moet volgens het advies per geval op basis van de omstandigheden worden beoordeeld.

In scenario 2 worden persoonsgegevens in het model bewaard en worden zij door een andere verwerkingsverantwoordelijke verwerkt in het kader van de inzet van het model. In dit verband moeten de toezichthoudende autoriteiten volgens het advies rekening houden met de vraag of de verwerkingsverantwoordelijke die het model inzet in het kader van zijn verantwoordingsplicht om de naleving van artikel 5, lid 1, punt a), en artikel 6 AVG aan te tonen een passende beoordeling heeft uitgevoerd om na te gaan of bij de ontwikkeling van het AI-model geen sprake is geweest van onrechtmatige verwerking van persoonsgegevens. Bij deze beoordeling moet bijvoorbeeld rekening worden gehouden met de bron van de persoonsgegevens en de vraag of bij de verwerking in de ontwikkelingsfase inbreuken zijn vastgesteld, met name als dat door een toezichthoudende autoriteit of een rechtbank is gedaan, waarbij de uitvoerigheid van de beoordeling afhangt van de risico's die aan de verwerking in de inzetfase zijn verbonden.

In scenario 3 verwerkt een verwerkingsverantwoordelijke op onrechtmatige wijze persoonsgegevens voor de ontwikkeling van het AI-model, om vervolgens te waarborgen dat die gegevens worden geanonimiseerd voordat dezelfde of een andere verwerkingsverantwoordelijke in het kader van de inzet een andere verwerking van persoonsgegevens begint. Als kan worden aangetoond dat bij het latere gebruik van het AI-model geen persoonsgegevens worden verwerkt, is het EDPB volgens het advies in dit verband van mening dat de AVG niet van toepassing is. De onrechtmatigheid van de eerste verwerking mag dus geen gevolgen hebben voor het latere gebruik van het model. Voor het geval dat

verwerkingsverantwoordelijken op een later tijdstip persoonsgegevens verwerken die tijdens de inzetfase zijn verzameld nadat het model is geanonimiseerd, is het EDPB daarnaast van mening dat de AVG van toepassing is op deze verwerkingsactiviteiten. In deze gevallen mag met betrekking tot de AVG de onrechtmatigheid van de eerste verwerking volgens het advies geen gevolgen hebben voor de rechtmatigheid van de verwerking tijdens de inzetfase.

Inhoudsopgave

1	Inleiding.....	7
1.1	Overzicht van de feiten	7
1.2	Ontvankelijkheid van het verzoek om een advies op grond van artikel 64, lid 2, AVG	9
2	Reikwijdte en belangrijkste begrippen	10
2.1	Reikwijdte van het advies	10
2.2	Kernbegrippen.....	12
2.3	AI-modellen in het kader van het advies	13
3	Gegrondeerdheid van het verzoek	14
3.1	Aard van AI-modellen in verband met de definitie van persoonsgegevens.....	14
3.2	Omstandigheden waaronder AI-modellen als anoniem kunnen worden beschouwd en de wijze waarop dit moet worden aangetoond	16
3.2.1	Algemene overwegingen ten aanzien van anonimisering in dit verband	16
3.2.2	Punten voor de beoordeling van de resterende kans op identificatie	19
3.3	Geschiktheid van een gerechtvaardigd belang als rechtsgrond voor de verwerking van persoonsgegevens bij de ontwikkeling en de inzet van AI-modellen.....	22
3.3.1	Algemene opmerkingen	22
3.3.2	Overwegingen ten aanzien van de drie stappen in de beoordeling van het gerechtvaardigde belang bij de ontwikkeling en de inzet van AI-modellen.....	24
3.4	Mogelijke gevolgen van onrechtmatige verwerking bij de ontwikkeling van een AI-model voor de rechtmatigheid van de latere verwerking of het latere gebruik van het AI-model	35
3.4.1	Scenario 1. Een verwerkingsverantwoordelijke verwerkt op onrechtmatige wijze persoonsgegevens om het model te ontwikkelen, de persoonsgegevens worden in het model bewaard en worden vervolgens door dezelfde verwerkingsverantwoordelijke verwerkt (bijvoorbeeld in het kader van de inzet van het model).....	37
3.4.2	Scenario 2. Een verwerkingsverantwoordelijke verwerkt op onrechtmatige wijze persoonsgegevens om het model te ontwikkelen, de persoonsgegevens worden in het model bewaard en worden door een andere verwerkingsverantwoordelijke verwerkt in het kader van de inzet van het model.....	38
3.4.3	Scenario 3. Een verwerkingsverantwoordelijke verwerkt op onrechtmatige wijze persoonsgegevens bij de ontwikkeling van het AI-model en waarborgt vervolgens dat het model wordt geanonimiseerd, voordat dezelfde of een andere verwerkingsverantwoordelijke in het kader van de inzet een andere verwerking van persoonsgegevens begint.....	40
4	Slotopmerkingen	40

Het Europees Comité voor gegevensbescherming,

Gezien artikel 63 en artikel 64, lid 2, van 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 (hierna de “AVG” genoemd),

Gezien de EER-overeenkomst en met name bijlage XI en protocol 37 daarbij, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018¹,

Gezien de artikelen 10 en 22 van zijn reglement van orde,

Overwegende hetgeen volgt:

1) De voornaamste taak van het Europees Comité voor gegevensbescherming (hierna het “**Comité**” of het “**EDPB**” genoemd) is het waarborgen van de consistente toepassing van de AVG in de gehele Europese Economische Ruimte (“**EER**”). Op grond van artikel 64, lid 2, AVG kunnen een toezichthoudende autoriteit, de voorzitter van het Comité of de Commissie elk verzoeken dat aangelegenheden van algemene strekking of met rechtsgevolgen in meer dan één lidstaat van de EER worden onderzocht door het Comité teneinde een advies te verkrijgen. Dit advies heeft als doel een aangelegenheid van algemene strekking of met rechtsgevolgen in meer dan één lidstaat van de EER te onderzoeken.

2) Het advies van het Comité wordt overeenkomstig artikel 64, lid 3, AVG, in samenhang met artikel 10, lid 2, van het reglement van orde van het Comité, vastgesteld binnen acht weken nadat de voorzitter en de bevoegde toezichthoudende autoriteit hebben vastgesteld dat het dossier volledig is. De voorzitter kan besluiten deze termijn met zes weken te verlengen, rekening houdend met de complexiteit van de aangelegenheid,

BRENGT HET VOLGENDE ADVIES UIT:

1 Inleiding

1.1 Overzicht van de feiten

1. Op 4 september 2024 heeft de Ierse toezichthoudende autoriteit (de “**Ierse toezichthoudende autoriteit**” of de “**verzoekende toezichthoudende autoriteit**”) het EDPB op grond van artikel 64, lid 2, AVG verzocht om een advies uit te brengen over AI-modellen en de verwerking van persoonsgegevens (“**het verzoek**”).
2. De voorzitter van het Comité en de Ierse toezichthoudende autoriteit hebben op 13 september 2024 vastgesteld dat het dossier volledig was. Op de volgende werkdag, 16 september 2024, werd het dossier verspreid door het secretariaat van het EDPB. Gezien de complexiteit van de aangelegenheid heeft de voorzitter van het Comité besloten de wettelijke termijn te verlengen, overeenkomstig artikel 64, lid 3, AVG en artikel 10, lid 4, van het reglement van orde van het EDPB.

¹ Alle verwijzingen in dit advies naar “lidstaten” moeten worden gelezen als verwijzingen naar “EER-lidstaten”. Alle verwijzingen in dit advies naar de “Unie” moeten worden gelezen als verwijzingen naar de “EER”.

3. Het verzoek heeft betrekking op bepaalde aspecten van het trainen, bijwerken, ontwikkelen en gebruiken van AI-modellen waarin persoonsgegevens deel uitmaken van de desbetreffende gegevensverzameling. De Ierse toezichhoudende autoriteit wijst erop dat het verzoek betrekking heeft op belangrijke vraagstukken die grote gevolgen hebben voor betrokkenen en verwerkingsverantwoordelijken in de EER, en dat een gezamenlijk standpunt van de nationale toezichhoudende autoriteiten op dit moment ontbreekt². Voor de in dit advies gebruikte terminologie wordt verwezen naar de punten 2.2 en 2.3.

4. De Ierse toezichhoudende autoriteit heeft de volgende vragen gesteld:

Vraag 1: Moet in alle gevallen worden aangenomen dat een uiteindelijk AI-model, dat met persoonsgegevens is getraind, niet voldoet aan de definitie van persoonsgegevens (in de zin van artikel 4, punt 1, AVG)?

Als de eerste vraag bevestigend wordt beantwoord:

- i. In welk stadium van de verwerkingsactiviteiten die tot een AI-model leiden, worden niet langer persoonsgegevens verwerkt?
 - a) Hoe kan worden aangetoond dat het AI-model geen persoonsgegevens verwerkt?
- ii. Zijn er factoren waardoor het gebruik van het uiteindelijke AI-model niet langer als anoniem wordt beschouwd?
 - a) Zo ja, hoe kan dan worden aangetoond welke maatregelen er zijn genomen om deze factoren te verzachten, te voorkomen of er bescherming tegen te bieden (om te zorgen dat het AI-model geen persoonsgegevens verwerkt)?

Als de eerste vraag ontkennend wordt beantwoord:

- i. Onder welke omstandigheden kan dit het geval zijn?
 - a) Zo ja, hoe kan dan worden aangetoond welke stappen zijn ondernomen om te zorgen dat het AI-model geen persoonsgegevens verwerkt?

Vraag 2: Wanneer een verwerkingsverantwoordelijke gerechtvaardigde belangen als rechtsgrondslag voor de verwerking van persoonsgegevens gebruikt om een AI-model aan te maken, bij te werken en/of te ontwikkelen, hoe moet die verwerkingsverantwoordelijke dan aantonen dat gerechtvaardigde belangen een passende rechtsgrondslag vormen, voor de verwerking van zowel gegevens van derden als firstpartygegevens?

- i. Met welke overwegingen moet die verwerkingsverantwoordelijke rekening houden om een passend evenwicht te waarborgen tussen enerzijds de belangen van de betrokkenen, van wie persoonsgegevens worden verwerkt, en anderzijds de belangen van die verwerkingsverantwoordelijke in het kader van:
 - a) gegevens van derden;
 - b) firstpartygegevens?

Vraag 3: Wanneer een verwerkingsverantwoordelijke gerechtvaardigde belangen als rechtsgrondslag gebruikt voor de verwerking van persoonsgegevens in een AI-model of een AI-systeem waarvan een

² Verzoek, blz. 1.

AI-model deel uitmaakt, hoe moet die verwerkingsverantwoordelijke dan na het trainen aantonen dat gerechtvaardigde belangen een passende rechtsgrondslag vormen?

Vraag 4: Als blijkt dat een AI-model is gemaakt, bijgewerkt of ontwikkeld met behulp van onrechtmatig verwerkte persoonsgegevens, wat zijn dan eventueel de gevolgen hiervan voor de rechtmatigheid van de (het) verder(e) of later(e) verwerking of gebruik van het AI-model, in zelfstandige vorm of als onderdeel van een AI-systeem, wanneer:

- i. persoonsgegevens worden verwerkt door het AI-model in zelfstandige vorm of als onderdeel van een AI-systeem?
- ii. geen persoonsgegevens worden verwerkt door het AI-model noch door het AI-model dat deel van een AI-systeem uitmaakt?

1.2 Ontvankelijkheid van het verzoek om een advies op grond van artikel 64, lid 2, AVG

5. Op grond van artikel 64, lid 2, AVG kan, in het bijzonder, een toezichthoudende autoriteit verzoeken dat aangelegenheden van algemene strekking of met rechtsgevolgen in meer dan één lidstaat worden onderzocht door het Comité teneinde advies te verkrijgen.
6. De verzoekende toezichthoudende autoriteit heeft het EDPB vragen gesteld over aspecten van gegevensverwerking in het kader van AI-modellen. In het verzoek gaf deze toezichthoudende autoriteit aan dat veel organisaties tegenwoordig weliswaar AI-modellen gebruiken, waaronder grote taalmodellen (Large Language Models, “LLM”), maar dat het toepassen, trainen en gebruiken van deze modellen *“in veel opzichten tot bezorgdheid op het gebied van gegevensbescherming”*³ leidt bij *“betrokkenen in de gehele EU/EER”*⁴.
7. Centraal in het verzoek staan vragen over i) de toepassing van het begrip “persoonsgegevens”; ii) het beginsel van rechtmatigheid, specifiek als het gaat om het gebruik van een gerechtvaardigd belang als rechtsgrondslag in het kader van AI-modellen; en iii) de gevolgen van onrechtmatige verwerking van persoonsgegevens in de ontwikkelingsfase van AI-modellen voor de latere verwerking of het latere gebruik van het model.
8. Het Comité is van mening dat het verzoek een *“aangelegenheid van algemene strekking”* in de zin van artikel 64, lid 2, AVG betreft. Meer in het bijzonder gaat het in dit geval om de interpretatie en de toepassing van artikel 4, punt 1, artikel 5, lid 1, punt a), en artikel 6 AVG voor de verwerking van persoonsgegevens bij de ontwikkeling en de inzet van AI-modellen. Zoals door de verzoekende toezichthoudende autoriteit werd benadrukt, ontstaan bij de toepassing van deze bepalingen op AI-modellen systemische, abstracte en nieuwe vraagstukken⁵. Als gevolg van de snelle ontwikkeling en inzet van AI-modellen door steeds meer organisaties ontstaan specifieke vraagstukken en, zoals ook in het verzoek werd aangegeven, *“zal het EDPB er veel baat bij hebben als een gemeenschappelijk standpunt wordt gevonden over de in dit verzoek aan de orde gestelde aangelegenheden, aangezien deze een centrale rol vervullen in de voorgenomen werkzaamheden van het EDPB op de korte en*

³ Verzoek, blz. 1.

⁴ Ibid.

⁵ Verzoek, blz. 2.

*middellange termijn*⁶. Daarnaast biedt AI-technologie vele kansen en voordelen in een breed scala van sectoren en maatschappelijke activiteiten. Bovendien is de AVG een rechtskader dat verantwoorde innovatie stimuleert. Derhalve wordt een algemeen belang gediend wanneer deze beoordeling plaatsvindt in de vorm van een advies van het EDPB, om een consistente toepassing van een aantal bepalingen uit de AVG in het kader van AI-modellen te waarborgen.

9. De alternatieve voorwaarde uit artikel 64, lid 2, AVG verwijst naar aangelegenheden “*met rechtsgevolgen in meer dan één lidstaat*”. Het EDPB wijst erop dat het begrip “rechtsgevolgen” ruim moet worden geïnterpreteerd en zich dus niet eenvoudigweg beperkt tot juridische gevolgen⁷. Nu er steeds meer AI-modellen worden getraind en gebruikt door steeds meer organisaties in de EER, hebben zij gevolgen voor een groot aantal betrokkenen in de gehele EER, waarvan sommigen reeds hun zorgen kenbaar hebben gemaakt aan een bevoegde toezichthoudende autoriteit⁸. Derhalve is het EDPB van mening dat de door de verzoekende toezichthoudende autoriteit aan de orde gestelde aangelegenheid ook aan deze voorwaarde voldoet.
10. In het verzoek is een schriftelijke motivering opgenomen van de achtergronden en de redenen ervoor, naast een verwijzing naar het toepasselijke rechtskader voor het indienen van de vragen bij het Comité. Derhalve is het Comité van mening dat het verzoek met redenen is omkleed overeenkomstig artikel 10, lid 3, van het reglement van orde van het EDPB.
11. Overeenkomstig artikel 64, lid 3, AVG⁹ brengt het Comité geen advies uit indien het over de aangelegenheid reeds een advies heeft uitgebracht. Het EDPB heeft over dezelfde aangelegenheid niet eerder een advies uitgebracht en de in het verzoek gestelde vragen nog niet eerder beantwoord.
12. Om deze redenen is het Comité van mening dat het verzoek ontvankelijk is en dat de in het verzoek gestelde vragen moeten worden behandeld in dit advies (hierna het “**advies**” genoemd), dat is vastgesteld overeenkomstig artikel 64, lid 2, AVG.

2 Reikwijdte en belangrijkste begrippen

2.1 Reikwijdte van het advies

13. Het Comité is het met de verzoekende toezichthoudende autoriteit eens dat de ontwikkeling en de inzet van AI-modellen vanuit het oogpunt van gegevensbescherming fundamentele vragen doen rijzen. Daarbij gaat het met name over de vraag: i) wanneer en op welke wijze een AI-model als “anoniem” kan worden beschouwd (vraag 1 uit het verzoek); ii) op welke wijze verwerkingsverantwoordelijken kunnen aantonen dat een gerechtvaardigd belang een passende rechtsgrond is tijdens de ontwikkelingsfase (vraag 2 uit het verzoek) en de inzetfase (vraag 3 uit het verzoek); en iii) of de onrechtmatige verwerking van persoonsgegevens tijdens de ontwikkelingsfase gevolgen heeft voor de

⁶ Verzoek, blz. 1. Zoals aangegeven in het op 8 oktober 2024 vastgestelde werkprogramma van het EDPB voor 2024-2025, dat beschikbaar is op https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf, is het EDPB voornemens om onder andere richtsnoeren uit te brengen over anonimisering, pseudonimisering en datascraping in het kader van generatieve AI.

⁷ Intern document 3/2019 van het EDPB over Interne richtsnoeren met betrekking tot artikel 64, lid 2, AVG, vastgesteld op 8 oktober 2019, punt 15, beschikbaar op https://www.edpb.europa.eu/system/files/2022-07/internaledpb_document_201903_art64.2_en.pdf.

⁸ Verzoek, blz. 1-2.

⁹ Artikel 64, lid 3, AVG en artikel 10, lid 4, van het reglement van orde van het Comité.

rechtmatigheid van de latere verwerking of het latere gebruik van het AI-model (vraag 4 uit het verzoek).

14. Het EDPB wijst erop dat de toezichthoudende autoriteiten verantwoordelijk zijn voor het toezicht op de toepassing van de AVG en moeten bijdragen tot een consequente toepassing daarvan in de gehele Unie¹⁰. De toezichthoudende autoriteiten zijn derhalve bevoegd om onderzoek naar specifieke AI-modellen te doen en daarbij individuele gevallen te beoordelen.
15. Dit advies vormt voor de bevoegde toezichthoudende autoriteiten een kader voor de beoordeling van specifieke gevallen waarin (een aantal van) de in het verzoek geformuleerde vragen zich voordoen. Dit advies beoogt niet uitputtend te zijn, maar bevat algemene overwegingen over de interpretatie van de toepasselijke bepalingen, waarmee de bevoegde toezichthoudende autoriteiten zoveel mogelijk rekening moeten houden wanneer zij van hun onderzoeksbevoegdheden gebruikmaken. Hoewel dit advies is gericht tot de bevoegde toezichthoudende autoriteiten en verband houdt met hun werkzaamheden en bevoegdheden, laat het de verplichtingen van verwerkingsverantwoordelijken en verwerkers uit hoofde van de AVG onverlet. Meer in het bijzonder zijn de verwerkingsverantwoordelijken op grond van het verantwoordingsbeginsel uit artikel 5, lid 2, AVG verantwoordelijk voor de naleving van alle beginselen die gelden voor hun verwerking van persoonsgegevens en moeten zij deze naleving kunnen aantonen.
16. In enkele gevallen kan in het advies een aantal voorbeelden worden gegeven, maar gezien de brede aard van de vragen uit het verzoek en de uiteenlopende soorten AI-modellen die eronder vallen, zullen in dit advies niet alle mogelijke scenario's worden behandeld. De technologieën die met AI-modellen verband houden ontwikkelen zich snel en de overwegingen van het EDPB in dit advies moeten dan ook in dat licht worden gezien.
17. **Dit advies gaat niet in op de onderstaande bepalingen, die nog altijd een belangrijke rol kunnen vervullen bij de beoordeling van de vereisten op het gebied van gegevensbescherming die voor AI-modellen gelden:**
 - **verwerking van bijzondere categorieën persoonsgegevens:** het EDPB wijst op het verbod uit artikel 9, lid 1, AVG op de verwerking van bijzondere categorieën gegevens en de beperkte uitzonderingen uit artikel 9, lid 2, AVG¹¹. In dit opzicht heeft het Hof van Justitie van de Europese Unie (hierna het "**Hof**" genoemd) verder verduidelijkt dat *"wanneer [...] een gegevensverzameling [bestaat] uit zowel gevoelige als niet-gevoelige gegevens en al deze gegevens met name als één geheel bijeen worden gebracht zonder dat zij op het moment waarop dat gebeurt van elkaar kunnen worden gescheiden, de verwerking van de hele gegevensverzameling moet worden geacht verboden te zijn in de zin van artikel 9, lid 1, AVG, aangezien al die gegevens bij elkaar ten minste één gevoelig gegeven bevatten en geen van de in artikel 9, lid 2, van deze verordening bedoelde uitzonderingen van toepassing is"*¹². Voorts benadrukte het Hof dat *"ter toepassing van de uitzondering van artikel 9, lid 2, onder e), AVG [...] daarom [moet] worden nagegaan of de betrokkene de aan de orde zijnde persoonsgegevens*

¹⁰ Artikel 51, leden 1 en 2, AVG.

¹¹ Zie ook punt 18 van het op 23 mei 2024 vastgestelde verslag van het EDPB over de Taskforce ChatGPT: "Met betrekking tot de verwerking van bijzondere categorieën van persoonsgegevens kan de verwerking uitsluitend rechtmatig zijn wanneer daarnaast een van de uitzonderingen van artikel 9, lid 2, van toepassing is. *In beginsel kan een van deze uitzonderingen artikel 9, lid 2, punt e), AVG zijn. Het enkele feit dat persoonsgegevens voor het publiek toegankelijk zijn, impliceert echter niet dat "de betrokkene die gegevens klaarblijkelijk openbaar heeft gemaakt" [...].*"

¹² Arrest van het Hof van 4 juli 2023, *Meta/Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, punt 89.

*uitdrukkelijk en door middel van een ondubbelzinnige actieve handeling voor een breed publiek toegankelijk heeft willen maken”*¹³. Deze overwegingen moeten in aanmerking worden genomen wanneer bij de verwerking van persoonsgegevens in het kader van AI-modellen ook bijzondere categorieën gegevens worden verwerkt.

- **Geautomatiseerde besluitvorming, met inbegrip van profilering:** de verwerkingsactiviteiten die in het kader van AI-modellen plaatsvinden, kunnen onder het toepassingsgebied van artikel 22 AVG vallen, waarin aanvullende verplichtingen aan verwerkingsverantwoordelijken worden opgelegd en wordt voorzien in aanvullende bescherming voor betrokkenen. Het EDPB wijst in dit verband op de richtsnoeren van het Comité over geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening 2016/679¹⁴.
- **Verenigbaarheid van doeleinden:** in artikel 6, lid 4, AVG worden voor bepaalde rechtsgrondslagen criteria vastgesteld waarmee een verwerkingsverantwoordelijke rekening moet houden bij de beoordeling van de vraag of de verwerking voor een ander doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld. Deze bepaling kan toepasselijk zijn in het kader van de ontwikkeling en de inzet van AI-modellen, en de toepasselijkheid ervan moet door de toezichthoudende autoriteiten worden beoordeeld.
- **Gegevensbeschermingseffectbeoordelingen** (data protection impact assessment, “**DPIA**”) (artikel 35 AVG): DPIA’s zijn een belangrijk onderdeel van de verantwoording wanneer bij verwerking in het kader van AI-modellen waarschijnlijk een hoog risico ontstaat voor de rechten en vrijheden van natuurlijke personen¹⁵.
- **Beginsel van gegevensbescherming door ontwerp** (artikel 25, lid 1, AVG): gegevensbescherming door ontwerp is een belangrijke waarborg, die door de toezichthoudende autoriteiten moet worden beoordeeld in het kader van de ontwikkeling en de inzet van een AI-model.

2.2 Kernbegrippen

18. Vooraf wil het EDPB uitsluitend voor de toepassing van dit advies een aantal termen en begrippen toelichten die in dit advies worden gebruikt:
- **“Firstpartygegevens”:** persoonsgegevens die de verwerkingsverantwoordelijke bij de betrokkenen heeft verzameld.
 - **“Gegevens van derden”:** persoonsgegevens die verwerkingsverantwoordelijken niet van de betrokkenen hebben verkregen, maar die zij bij, of van een derde hebben verzameld of ontvangen, bijvoorbeeld van een datahandelaar, of gegevens die via webscraping zijn verzameld.
 - **“Webscraping”:** een veel gebruikte techniek voor het verzamelen van informatie uit openbare onlinebronnen. Informatie die door middel van deze techniek in bijvoorbeeld de media, sociale

¹³ Arrest van het Hof van 4 juli 2023, *Meta/Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, punt 77.

¹⁴ Groep gegevensbescherming artikel 29 (“**WP29**”) Richtsnoeren inzake geautomatiseerde besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, zoals laatstelijk gewijzigd en vastgesteld op 6 februari 2018, door het EDPB bekrachtigd op 25 mei 2018. Zie ook het arrest van het Hof van 7 december 2023, *SCHUFA Holding e.a.*, C-634/21, ECLI:EU:C:2023:957.

¹⁵ WP29, Richtsnoeren voor gegevensbeschermingseffectbeoordelingen (DPIA) en bepaling of de verwerking “waarschijnlijk een hoog risico inhoudt” in de zin van Verordening 2016/679, zoals laatstelijk gewijzigd en vastgesteld op 4 april 2017, bekrachtigd door het EDPB op 25 mei 2018.

media, forumdiscussies en persoonlijke websites wordt verzameld, kan persoonsgegevens bevatten.

- In het verzoek wordt gesproken over de **“levenscyclus” van AI-modellen**, maar ook over verschillende stadia, waaronder het “aanmaken”, “ontwikkelen”, “trainen”, “bijwerken”, “verfijnen”, “gebruiken” en “natraineren” van AI-modellen. Het EDPB erkent dat deze stadia, afhankelijk van de omstandigheden, kunnen plaatsvinden tijdens de ontwikkeling en de inzet van AI-modellen en dat zij de verwerking van persoonsgegevens voor diverse verwerkingsdoeleinden kunnen omvatten. Niettemin acht het EDPB het voor dit advies van belang om de categorisering van de stadia die zich waarschijnlijk zullen voordoen te stroomlijnen. Daarom spreekt het EDPB in dit advies over de **“ontwikkelingsfase”** en de **“inzetfase”**. De ontwikkeling van een AI-model omvat alle stadia die aan de inzet van het AI-model voorafgaan, waaronder het ontwikkelen van code, het verzamelen van persoonsgegevens voor trainingsdoeleinden, het voorbereiden van persoonsgegevens voor trainingsdoeleinden en het eigenlijke trainen. De inzet van een AI-model omvat alle stadia die verband houden met het gebruik van een AI-model en kan alle activiteiten omvatten die na afloop van de ontwikkelingsfase plaatsvinden. Het EDPB blijft zich bewust van de verschillen die in de praktijk te zien zijn en van de mogelijke gevolgen ervan als het gaat om de verwerking van persoonsgegevens, en de toezichthoudende autoriteiten moeten dus overwegen of de opmerkingen in dit advies relevant zijn voor de verwerking die zij beoordelen.
- Verder benadrukt het EDPB dat, indien nodig, onder **“training”** het deel van de ontwikkelingsfase wordt verstaan waarin AI-modellen op basis van gegevens leren om hun beoogde taak uit te voeren (zoals toegelicht in het volgende deel van dit advies).
- Het begrip **“AI-modellen”** en de reikwijdte ervan in de opvatting van het EDPB voor dit advies, wordt nader toegelicht in het volgende deel, dat hier specifiek aan is gewijd.

2.3 AI-modellen in het kader van het advies

19. In de verordening artificiële intelligentie van de EU (hierna de **“AI-verordening”** genoemd)¹⁶ wordt een “AI-systeem” gedefinieerd als *“een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen”*¹⁷. In overweging 12 van de AI-verordening wordt het begrip “AI-systeem” nader toegelicht. Een belangrijk kenmerk van AI-systemen is derhalve hun inferentievermogen. Tot de technieken die bij de opbouw van een AI-systeem inferentie mogelijk maken, behoren machinaal leren, alsook op logica en kennis gebaseerde benaderingen.
20. “AI-modellen” worden in de AI-verordening echter alleen indirect gedefinieerd: *“AI-modellen zijn weliswaar een essentieel onderdeel van AI-systemen, maar vormen geen AI-systemen op zich. Om een AI-systeem te worden, moeten er aan AI-modellen nog andere componenten worden toegevoegd, bijvoorbeeld een gebruikersinterface. AI-modellen worden doorgaans geïntegreerd in, en vormen een onderdeel van AI-systemen”*¹⁸.

¹⁶ Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie).

¹⁷ Artikel 3, punt 1, van de AI-verordening.

¹⁸ Overweging 97 van de AI-verordening.

21. Het EDPB onderkent dat de in het verzoek voorgestelde definitie van een AI-model minder ruim is dan die in de AI-verordening, omdat volgens die eerste definitie een “AI-model” *“het product omvat dat voortvloeit uit de trainingsmechanismen die worden toegepast op een verzameling trainingsgegevens, in het kader van artificiële intelligentie, machinaal leren, “deep learning” of andere verwante verwerkingsomgevingen”* en daarin verder wordt aangegeven dat *“de term van toepassing is op AI-modellen die nog nader zullen worden getraind, verfijnd en/of ontwikkeld, alsmede op AI-modellen waarbij dat niet het geval is.”*¹⁹
22. Bij de vaststelling van dit advies is het EDPB er daarom vanuit gegaan dat een AI-systeem een AI-model nodig heeft om zijn beoogde doelstelling te bereiken en met het oog daarop het model integreert in een ruimer kader (zo kan een AI-systeem voor een klantenservice een AI-model gebruiken dat met historische gespreksgegevens is getraind om vragen van gebruikers te beantwoorden).
23. Daarnaast worden onder voor dit advies relevante AI-modellen (of “**modellen**”) de modellen verstaan die zijn ontwikkeld door middel van een trainingsproces. Een dergelijk trainingsproces is onderdeel van de ontwikkelingsfase, waarin modellen op basis van gegevens leren om hun beoogde taak uit te voeren. Voor het trainingsproces is daarom een dataset nodig, waarin het model patronen opspoorde en “aanleert”. In deze gevallen zal het model verschillende technieken gebruiken om een afspiegeling op te bouwen van de kennis die uit de trainingsdataset wordt geëxtraheerd. Dit is met name het geval bij machinaal leren.
24. In de praktijk is elk AI-model een algoritme, waarvan de werking wordt bepaald door een reeks elementen. Zo zijn modellen voor deep learning vaak neurale netwerken met meerdere lagen, die bestaan uit door edge-intelligentie verbonden knooppunten met een bepaald gewicht, die bij het trainen worden bijgesteld om te leren welke relaties er bestaan tussen input en output. Een eenvoudig deep learning model heeft dan de volgende eigenschappen: i) het type en de vorm van elke laag; ii) het aan elke edge toegekende gewicht (soms ook “parameters” genoemd); iii) de activeringsfuncties²⁰ tussen lagen; en mogelijk iv) andere bewerkingen die eventueel tussen lagen plaatsvinden. Wanneer bijvoorbeeld een eenvoudig deep learning model wordt getraind om afbeeldingen in categorieën in te delen, wordt input (de “**afbeeldingspixels**”) gekoppeld aan output, en kunnen gewichten zodanig worden bijgesteld dat meestal de juiste output wordt verkregen.
25. Andere voorbeelden van deep learning modellen zijn grote taalmodellen en generatieve AI, die bijvoorbeeld worden gebruikt voor het genereren van menselijke inhoud en het aanmaken van nieuwe gegevens.
26. **Gelet op het bovenstaande en in overeenstemming met het verzoek gaat dit advies alleen over de groep AI-modellen die voortkomen uit het trainen van dergelijke modellen met persoonsgegevens.**

3 Gegrondheid van het verzoek

3.1 Aard van AI-modellen in verband met de definitie van persoonsgegevens

27. In artikel 4, punt 1, AVG worden persoonsgegevens gedefinieerd als *“alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon”* (d.w.z. de betrokkene). Daarnaast dienen volgens overweging 26 AVG gegevensbeschermingsbeginselen niet van toepassing te zijn op anonieme

¹⁹ Verzoek, blz. 3.

²⁰ D.w.z. functies die op basis van input en gewichten de output van een neurale knooppunt berekenen, die dan naar de volgende laag van het neurale netwerk wordt gestuurd.

gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon, rekening houdend met *“alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt”* door de verwerkingsverantwoordelijke of door een andere persoon. Hieronder vallen: i) gegevens die nooit betrekking hebben gehad op een geïdentificeerde of identificeerbare persoon; en ii) persoonsgegevens die op zodanige wijze anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.

28. Vraag 1²¹ uit het verzoek kan derhalve worden beantwoord door te onderzoeken of een AI-model dat het resultaat is van training waarbij persoonsgegevens zijn verwerkt in alle gevallen als anoniem moet worden beschouwd. Uitgaand van de formulering van de vraag zal het EDPB in dit punt ingaan op het “trainen” van een AI-model.
29. Allereerst overweegt het EDPB in algemene zin het volgende: los van de vraag of zij al dan niet met persoonsgegevens zijn getraind, zijn AI-modellen doorgaans ontworpen om voorspellingen te maken of conclusies te trekken, dus om afleidingen (inferenties) te maken. Daarnaast zijn met persoonsgegevens getrainde AI-modellen vaak ontworpen om afleidingen te maken over andere personen dan degenen van wie persoonsgegevens zijn gebruikt bij het trainen van het AI-model. Sommige AI-modellen zijn echter specifiek ontworpen om persoonsgegevens te leveren over mensen van wie gegevens zijn gebruikt om het model te trainen, of om die gegevens op enigerlei wijze beschikbaar te maken. In die gevallen zal in deze AI-modellen altijd (en meestal kan dat ook niet anders) informatie zijn opgenomen over een geïdentificeerde of identificeerbare natuurlijke persoon, en zullen die modellen dus persoonsgegevens verwerken. Deze soorten AI-modellen kunnen dus niet als anoniem worden beschouwd. Dit zou bijvoorbeeld het geval zijn bij i) een generatief model dat met spraakopnames van een persoon wordt verfijnd om diens stem na te bootsen; of ii) een model dat is ontworpen om te antwoorden met persoonsgegevens uit de training wanneer het wordt gevraagd om informatie over een specifieke persoon.
30. Daarom richt het EDPB zich bij de beantwoording van vraag 1 uit het verzoek met name op AI-modellen die niet zijn ontworpen om aan de trainingsgegevens gerelateerde persoonsgegevens te leveren.
31. Ook wanneer een AI-model niet opzettelijk is ontworpen om op basis van de trainingsgegevens informatie over een geïdentificeerde of identificeerbare natuurlijke persoon te leveren, kunnen gegevens uit de trainingsdataset, waaronder persoonsgegevens, naar de mening van het EDPB nog steeds in de parameters van het model “verwerkt” zijn, en met name worden weergegeven door middel van mathematische objecten. Zij kunnen van de oorspronkelijke punten uit de trainingsgegevens verschillen, maar nog steeds de oorspronkelijke informatie uit die gegevens bevatten, die uiteindelijk extraheerbaar is of op andere wijze rechtstreeks of indirect uit het model kan worden verkregen. In alle gevallen waarin informatie over geïdentificeerde of identificeerbare personen van wie persoonsgegevens zijn gebruikt om het model te trainen uit een AI-model kunnen worden gehaald met behulp van middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt, kan worden geconcludeerd dat een dergelijk model niet anoniem is.
32. In dit verband wordt volgens het verzoek *“in bestaande onderzoekspublicaties gewezen op potentiële kwetsbaarheden in AI-modellen, die ertoe kunnen leiden dat persoonsgegevens worden verwerkt²², en op de verwerking van persoonsgegevens die mogelijk ook nog plaatsvindt wanneer modellen worden*

²¹ “Wordt het uiteindelijke AI-model, dat met persoonsgegevens getraind is, in alle gevallen geacht niet te voldoen aan de definitie van persoonsgegevens (uit artikel 4, punt 1, AVG)?”

²² Waaronder aanvallen met membershipinference ([OWASP](#)) en modelinversie ([OWASP](#) & [Veale et al](#), 2018).

ingezet voor gebruik met andere gegevens, door middel van applicatieprogramma-interfaces (“API’s”) of “prompt“-interfaces”²³.

33. Ook het onderzoek naar extractie van trainingsgegevens is bijzonder dynamisch²⁴. In sommige gevallen blijken middelen te kunnen worden gebruikt waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om persoonsgegevens uit bepaalde AI-modellen te extraheren, of om gewoon toevallig persoonsgegevens te verkrijgen bij interactie met een AI-model (bijvoorbeeld als onderdeel van een AI-systeem). Aanhoudende onderzoeksinspanningen op dit gebied zullen bijdragen aan een beoordeling van de verder resterende risico’s van teruglekken²⁵ en extractie van persoonsgegevens in specifieke gevallen.
34. **Gelet op bovenstaande overwegingen is het EDPB van mening dat met persoonsgegevens getrainde AI-modellen niet in alle gevallen als anoniem kunnen worden beschouwd. De vraag of een AI-model anoniem is, moet daarentegen op basis van specifieke criteria per geval worden beantwoord.**

3.2 Omstandigheden waaronder AI-modellen als anoniem kunnen worden beschouwd en de wijze waarop dit moet worden aangetoond

35. Ten aanzien van vraag 1 uit het verzoek²⁶ wordt het EDPB gevraagd om te verduidelijken onder welke omstandigheden een met persoonsgegevens getraind AI-model als anoniem kan worden beschouwd. Ten aanzien van vraag 1, i), punt a), van het verzoek²⁷ wordt het EDPB gevraagd om te verduidelijken welke bewijsstukken en/of documenten toezichthoudende autoriteiten in aanmerking moeten nemen wanneer zij beoordelen of een AI-model anoniem is.

3.2.1 Algemene overwegingen ten aanzien van anonimisering in dit verband

36. Uit het gebruik van de uitdrukking “alle informatie” in de definitie van “persoonsgegevens” uit artikel 4, punt 1, AVG valt af te leiden dat het de bedoeling was om dit begrip breed te definiëren en er alle soorten informatie onder te laten vallen voor zover dit informatie is “over” de betrokkene en deze betrokkene direct of indirect kan worden geïdentificeerd.

²³ Verzoek, blz. 1-2.

²⁴ Zie in dit opzicht bijvoorbeeld: i) Veale, M., Binns, R., Edwards, L., 2018, *Algorithms that remember: model inversion attacks and data protection law*. Phil. Trans. R. Soc. A 376: 20180083, beschikbaar op <http://dx.doi.org/10.1098/rsta.2018.0083>; ii) Brown, H., Lee, K., Mireshghallah, F., Shokri, R., en Tramèr, F., *What Does it Mean for a Language Model to Preserve Privacy?*, 2022, ACM Digital Library, FAccT '22, 20 juni 2022, Seoul, Republic of Korea, beschikbaar op <https://dl.acm.org/doi/abs/10.1145/3531146.3534642>; iii) Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., *Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations*, januari 2024, National Institute of Standards and Technology, beschikbaar op <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf>; iv) Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T., Song, D., Erlingsson, U., Oprea, A., Raffel, C., *Extracting Training Data from Large Language Models*, arXiv:2012.07805v2 [cs.CR] 15 juni 2021, beschikbaar op <https://arxiv.org/pdf/2012.07805>; v) Fredrikson, M., Jha, S., Ristenpart, T., *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures*, ACM Digital Library, 12 oktober 2015, beschikbaar op <https://dl.acm.org/doi/abs/10.1145/2810103.2813677>; vi) Zhang, Y., Jia, R., Pei, H., Wang, W., Li, B., Song, D., *The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks*, arXiv:1911.07135v2 [cs.LG] 18 april 2020, beschikbaar op <https://arxiv.org/pdf/1911.07135>.

²⁵ In het geval van een op generatieve AI gebaseerd AI-systeem is van teruglekken (“regurgitation”) sprake wanneer output rechtstreeks verband houdt met trainingsgegevens.

²⁶ “Onder welke omstandigheden kan dit het geval zijn?”

²⁷ “Zo ja, hoe kan dan worden aangetoond welke stappen zijn ondernomen om te zorgen dat het AI-model geen persoonsgegevens verwerkt?”

37. Informatie kan ook “over” een natuurlijke persoon gaan wanneer die informatie op zodanige wijze technisch georganiseerd of gecodeerd is (bijvoorbeeld in een open of door eigendomsrechten beschermd formaat dat alleen door machines kan worden gelezen) dat het verband met die natuurlijke persoon niet onmiddellijk zichtbaar is. In dergelijke gevallen kunnen softwareapplicaties worden gebruikt om specifieke gegevens gemakkelijk te identificeren, herkennen en extraheren. Dit geldt met name voor AI-modellen waarin parameters statistische verbanden tussen de trainingsgegevens weergeven, en waarin het mogelijk kan zijn om correcte of niet correcte (want statistisch afgeleide) persoonsgegevens te extraheren, rechtstreeks uit de relatie tussen de in het model opgenomen gegevens, of door het doorzoeken van dat model.
38. Aangezien AI-modellen doorgaans geen records bevatten die rechtstreeks geïsoleerd of gekoppeld kunnen worden, maar veeleer parameters die waarschijnlijke relaties tussen de gegevens in het model weergeven, kan het mogelijk zijn om in realistische scenario’s informatie uit het model af te leiden²⁸, onder meer door membershipinference. Het standpunt van een verwerkingsverantwoordelijke dat een bepaald AI-model als anoniem kan worden beschouwd, kan dus door een toezichthoudende autoriteit alleen worden onderschreven wanneer het volgende redelijkerwijs voldoende is aangetoond: i) persoonsgegevens die met de trainingsgegevens verband houden, kunnen niet uit het model worden geëxtraheerd²⁹; en ii) output die wordt voortgebracht bij het doorzoeken van het model is niet gerelateerd aan de betrokkenen van wie persoonsgegevens zijn gebruikt om het model te trainen.
39. Wanneer toezichthoudende autoriteiten beoordelen of aan deze voorwaarden wordt voldaan, moeten zij drie aspecten onderzoeken.

²⁸ (i) Carlini, N., Chien, S., Nasr, M., Song, S., Terzis, A., Tramer, F., *Membership Inference Attacks From First Principles*, arXiv:2112.03570, beschikbaar op <https://arxiv.org/abs/2112.03570>.

(ii) Crețu, A.M., Guépin, F., en De Montjoye, Y.A., *Correlation inference attacks against machine learning models*. Sci. Adv.10, eadj9260(2024). DOI:10.1126/sciadv.adj9260 beschikbaar op <https://www.science.org/doi/10.1126/sciadv.adj9260>.

(iii) Dana, L., Pydi, M. S., Chevalyre, Y., *Memorization in Attention-only Transformers* arXiv:2411.10115v1 [cs.AI] 15 november 2024, beschikbaar op <https://arxiv.org/abs/2411.10115>.

(iv) Gehrke, M., Liebenow, J., Mohammadi, E., Braun, T., et al. *Lifting in Support of Privacy-Preserving Probabilistic Inference*. Künstl Intell, 13 juni 2024, beschikbaar op <https://doi.org/10.1007/s13218-024-00851-y>.

(v) Hu, H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature*, beschikbaar op <https://github.com/HongshengHu/membership-inference-machine-learning-literature>.

(vi) Nasr, M., Carlini, N., Hayase, J., Jagielski, M., Cooper, A. F., Ippolito, D., Choquette-Choo, C. A., Wallace, E., Tramèr, F., en Lee, K., *Scalable Extraction of Training Data from (Production) Language Models*, arXiv:2311.17035 28 november 2023, beschikbaar op <https://arxiv.org/abs/2311.17035>.

(vii) Shokri, R., Stronati, M., Song, C., Shmatikov, V., *Membership Inference Attacks against Machine Learning Models* arXiv:1610.05820v2 [cs.CR], 31 maart 2017, beschikbaar op <https://arxiv.org/abs/1610.05820>.

(viii) Staab, R., Vero, M., Balunović, M., Vechev, M., 2024, *Beyond Memorization: Violating Privacy Via Inference with Large Language Models*, arXiv:2310.07298v2, 6 mei 2024, beschikbaar op <https://arxiv.org/abs/2310.07298>.

(ix) Wu, F., Cui, L., Yao, S., Yu, S., *Inference Attacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Directions* arXiv:2406.02027v1 [cs.LG], 27 juni 2024, beschikbaar op <https://arxiv.org/abs/2406.02027v1>.

(x) Zhang, J., Das, D., Kamath, G., Tramèr, F., *Membership Inference Attacks Cannot Prove that a Model Was Trained On Your Data* arXiv:2409.19798v1, [cs.LG], 29 september 2024, beschikbaar op <https://arxiv.org/abs/2409.19798>.

(xi) Zhou, Z., Xiang, J., Chen, C., en Su, S., *Quantifying and Analyzing Entity-Level Memorization in Large Language Models*, arXiv:2308.15727v2 [cs.CL] 5 november 2023, beschikbaar op <https://arxiv.org/abs/2308.15727>.

²⁹ Onder extractie wordt met name het geval verstaan waarin persoonsgegevens uit het AI-model zelf worden geëxtraheerd en de zoekinterfaces weinig of niet worden gebruikt.

40. In de eerste plaats moeten toezichthoudende autoriteiten kijken naar de punten die worden genoemd in de recentste adviezen van de WP29-groep en/of richtsnoeren van het EDPB op dit gebied. Met betrekking tot anonimisering gold op het moment van vaststelling van dit advies dat toezichthoudende autoriteiten moeten kijken naar de punten uit WP29-advies 5/2014 over anonimiseringstechnieken (hierna **“WP29-advies 5/2014”** genoemd), waarin wordt aangegeven dat de gegevens als anoniem mogen worden beschouwd als het niet mogelijk is om informatie uit de vermeend anonieme dataset te herleiden, te koppelen en te deduceren³⁰. Ook wordt in het advies aangegeven dat, *“wanneer een voorstel niet aan een van deze drie criteria voldoet, [...] de risico’s van identificatie zorgvuldig [moeten] worden geëvalueerd”*³¹. **Gezien de bovengenoemde kans op extractie en deductie acht het EDPB het zeer waarschijnlijk dat de risico’s van identificatie in het geval van AI-modellen aldus grondig moeten worden geëvalueerd.**
41. In de tweede plaats moet bij deze beoordeling rekening worden gehouden met *“alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt”* door de verwerkingsverantwoordelijke of door een ander om personen te identificeren³², en de bepaling van die middelen moet op objectieve factoren worden gebaseerd, zoals uiteengezet in overweging 26 AVG, waaronder kunnen worden verstaan:
- a. de eigenschappen van de trainingsgegevens zelf, het AI-model en de trainingsprocedure³³;
 - b. het kader waarbinnen het AI-model wordt vrijgegeven en/of verwerkt³⁴;
 - c. de aanvullende informatie die de identificatie mogelijk maakt en beschikbaar is voor de gegeven persoon;
 - d. de kosten en tijd die de persoon nodig zou hebben om die aanvullende informatie te verkrijgen (wanneer deze niet reeds voor die persoon beschikbaar is)³⁵; en
 - e. de beschikbare technologie op het moment van verwerking, alsmede technologische ontwikkelingen³⁶.
42. Ten derde moeten de toezichthoudende autoriteiten onderzoeken of verwerkingsverantwoordelijken het risico hebben beoordeeld van identificatie door de verwerkingsverantwoordelijke en door verschillende soorten *“andere personen”*, waaronder onbedoelde derden met toegang tot het AI-model, en daarbij ook onderzoeken of redelijkerwijs kan worden gemeend dat zij toegang tot de desbetreffende gegevens kunnen krijgen of deze kunnen verwerken.
43. **Concluderend is het EDPB van mening dat een AI-model alleen als anoniem kan worden beschouwd als, met gebruikmaking van redelijke middelen, zowel i) de kans op rechtstreekse (ook waarschijnlijke) extractie van persoonsgegevens over personen van wie persoonsgegevens zijn gebruikt om het model te trainen; als ii) de kans dat dergelijke persoonsgegevens al dan niet**

³⁰ WP29-advies 5/2014, blz. 24.

³¹ WP29-advies 5/2014, blz. 24.

³² Arrest van het Hof van 19 oktober 2016, *Breyer/Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779, punt 43.

³³ Hieronder vallen onder meer de uniekheid van de records in de trainingsgegevens, de nauwkeurigheid van de informatie, aggregatie, randomisering, en met name de vraag hoe deze van invloed zijn op de kwetsbaarheid voor identificatie.

³⁴ Hieronder vallen aspecten die met dat kader verband houden, waaronder de beperking van de toegang tot slechts enkele personen en juridische waarborgen.

³⁵ Arrest van het Hof van 7 maart 2024, *OC/Europese Commissie*, C-479/22 P, ECLI:EU:C:2024:215, punt 50.

³⁶ Arrest van het Hof van 7 maart 2024, *OC/Europese Commissie*, C-479/22 P, ECLI:EU:C:2024:215, punt 50.

opzettelijk bij zoekopdrachten worden verkregen voor een betrokkene niet significant groot³⁷ is. De toezichthoudende autoriteiten moeten er standaard van uitgaan dat de kans op identificatie in AI-modellen grondig moet worden onderzocht voordat een conclusie over hun mogelijke anonimiteit kan worden getrokken. Bij het beoordelen van deze kans moet rekening worden gehouden met “*alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt*” door de verwerkingsverantwoordelijke of door een andere persoon en moet ook aandacht worden geschonken aan onbedoeld(e) (her)gebruik of openbaarmaking van het model.

3.2.2 Punten voor de beoordeling van de resterende kans op identificatie

44. Hoewel zowel in de ontwikkelings- als de inzetfase maatregelen kunnen worden genomen om de kans te verkleinen dat persoonsgegevens uit een AI-model worden verkregen, moet bij de beoordeling van de anonimiteit van een AI-model ook worden gekeken naar de rechtstreekse toegang tot het model.
45. Daarnaast moeten de toezichthoudende autoriteiten per geval beoordelen of de verwerkingsverantwoordelijke passende en doeltreffende maatregelen heeft genomen om de anonimiteit van een AI-model te waarborgen en aan te tonen.
46. Met name kan een toezichthoudende autoriteit bij de beoordeling van een openbaar AI-model dat voor een onbekend aantal mensen toegankelijk is met een onbekende verscheidenheid aan methodes om persoonsgegevens te testen en te extraheren tot een andere conclusie komen dan bij de beoordeling van een intern AI-model dat uitsluitend voor werknemers toegankelijk is. Hoewel de toezichthoudende autoriteiten in beide gevallen moeten controleren of de verwerkingsverantwoordelijken hebben voldaan aan hun verantwoordingsplicht uit hoofde van artikel 5, lid 2, AVG en artikel 24, AVG, kunnen de “*middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt*” door andere personen gevolgen hebben voor het bereik en de aard van de mogelijk te onderzoeken scenario’s. Afhankelijk van het kader waarin het model wordt ontwikkeld en ingezet, kunnen de toezichthoudende autoriteiten daarom verschillende niveaus van beproeving en aanvalsbestendigheid in hun onderzoek betrekken.
47. In dat verband geeft het EDPB hieronder een niet-bindende en niet-uitputtende lijst van mogelijke aspecten die de toezichthoudende autoriteiten kunnen onderzoeken wanneer zij de door een verwerkingsverantwoordelijke geclaimde anonimiteit beoordelen. Andere benaderingen kunnen ook mogelijk zijn als zij een gelijkwaardig niveau van bescherming bieden, met name gelet op de stand van de techniek.
48. De aanwezigheid of het ontbreken van onderstaande aspecten is geen doorslaggevend criterium voor de beoordeling van de anonimiteit van een AI-model.

3.2.2.1 Ontwerp van AI-modellen

49. Met betrekking tot het ontwerp van een AI-model moeten de toezichthoudende autoriteiten de benaderingen beoordelen die verwerkingsverantwoordelijken tijdens de ontwikkelingsfase hebben gevolgd. De toepassing en de doeltreffendheid van vier belangrijke gebieden (zie onder) moeten in dit verband worden onderzocht.

Selectie van bronnen

50. Voor het eerste beoordelingsterrein wordt onderzoek gedaan naar de selectie van de bronnen die worden gebruikt om het AI-model te trainen. In dit kader beoordelen de toezichthoudende

³⁷ Arrest van het Hof van 19 oktober 2016, *Breyer/Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779, punt 46, en arrest van het Hof van 7 maart 2024, *OC/Europese Commissie*, C-479/22 P, ECLI:EU:C:2024:215, punt 51.

autoriteiten of maatregelen die zijn genomen om het verzamelen van persoonsgegevens te voorkomen of te beperken, en daarbij wordt onder meer gekeken naar i) de geschiktheid van de selectiecriteria; ii) de relevantie en de adequaatheid van de gekozen bronnen, gelet op de voorgenomen doelen; en iii) de vraag of ongeschikte bronnen zijn uitgesloten.

Gegevensvoorbereiding en minimale gegevensverwerking

51. Het tweede beoordelingsterrein heeft betrekking op het voorbereiden van gegevens voor de trainingsfase. De toezichthoudende autoriteiten moeten met name het volgende onderzoeken: i) de vraag of het gebruik van anonieme en/of gepseudonimiseerde persoonsgegevens is overwogen; en ii) indien is besloten om dergelijke maatregelen niet te nemen: de redenen voor dit besluit, rekening houdend met het voorgenomen doel; iii) de strategieën en technieken voor minimale gegevensverwerking die zijn gebruikt om de hoeveelheid persoonsgegevens tijdens het trainingsproces te beperken; en iv) procedures voor het filteren van gegevens die voorafgaand aan het trainen van het model zijn uitgevoerd om niet-relevante persoonsgegevens te verwijderen.

Methodologische keuzes voor het trainen

52. Het derde beoordelingsterrein heeft betrekking op de selectie van robuuste methoden voor de ontwikkeling van een AI-model. De toezichthoudende autoriteiten moeten de methodologische keuzes beoordelen die identificeerbaarheid significant kunnen verminderen of wegnemen, waaronder: i) de vraag of die methodiek gebruikmaakt van regularisatiemethoden om de modelgeneralisatie te verbeteren en overfitting te verminderen; en, wat vooral van belang is, ii) de vraag of de verwerkingsverantwoordelijke passende en doeltreffende technieken heeft toegepast om de persoonlijke levenssfeer te beschermen (bv. differentiële privacy).

Maatregelen voor output van het model

53. Het laatste beoordelingsterrein heeft betrekking op aan het AI-model zelf toegevoegde methoden of maatregelen die wellicht niet van invloed zijn op het risico van rechtstreekse extractie van persoonsgegevens voor het model door iedereen die er rechtstreeks toegang toe heeft, maar wel de kans zouden kunnen verkleinen dat bij zoekopdrachten persoonsgegevens worden verkregen die gerelateerd zijn aan trainingsgegevens.

3.2.2.2 Analyse van het AI-model

54. De toezichthoudende autoriteiten kunnen alleen beoordelen of een AI-model met betrekking tot anonimisering robuust is ontworpen als zij eerst nagaan of het ontwerp volgens plan is ontwikkeld en doeltreffend wordt beheerd en geoptimaliseerd. De toezichthoudende autoriteiten moeten beoordelen of de verwerkingsverantwoordelijken op basis van documenten (interne of externe) controles hebben verricht, waaronder een beoordeling van de gekozen maatregelen en van de effecten daarvan om de kans op identificatie te beperken. Hiertoe kan onderzoek behoren van verslagen van codereviews, evenals een theoretische analyse waarin de geschiktheid wordt gedocumenteerd van de maatregelen die zijn gekozen om de kans op heridentificatie van het desbetreffende model te verkleinen.

3.2.2.3 Beproeving en aanvalsbestendigheid van AI-modellen

55. Tot slot moeten de toezichthoudende autoriteiten onderzoek doen naar de reikwijdte, de frequentie, het aantal en de kwaliteit van de testen die de verwerkingsverantwoordelijke op het model heeft uitgevoerd. Met name moeten zij er rekening mee houden dat geslaagde testen voor gangbare en technologisch hoogwaardige aanvallen alleen aantonen dat het model tegen die specifieke aanvallen bestand is. Op het moment van vaststelling van dit advies kan het daarbij onder meer gaan om gestructureerd testen op: i) attribute- en membershipinference; ii) exfiltratie; iii) teruglekken van trainingsgegevens; iv) modelinversie; of v) reconstructieaanvallen.

3.2.2.4 Documentatie

56. In de artikelen 5, 24, 25 en 30 AVG en, in gevallen met waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkenen, artikel 35 AVG, worden verwerkingsverantwoordelijken verplicht om hun verwerkingsactiviteiten naar behoren te documenteren. Dit geldt ook voor verwerking waarbij een AI-model wordt getraind, ook als anonimisering het doel van de verwerking is. De toezichthoudende autoriteiten moeten onderzoek doen naar die documentatie en naar reguliere beoordelingen van de risico's die uit de verwerking door verwerkingsverantwoordelijken voortvloeien, omdat dit fundamentele stappen zijn wanneer moet worden aangetoond dat er geen persoonsgegevens worden verwerkt.
57. **Het EDPB is van mening dat toezichthoudende autoriteiten altijd de documentatie in aanmerking moeten nemen wanneer een anonimiteitsclaim over een bepaald AI-model moet worden onderzocht. Als een toezichthoudende autoriteit na beoordeling van een anonimiteitsclaim en ook gezien de documentatie niet kan bevestigen dat er doeltreffende maatregelen zijn genomen om het AI-model te anonimiseren, dan kan de toezichthoudende autoriteit naar de mening van het EDPB oordelen dat de verwerkingsverantwoordelijke niet heeft voldaan aan zijn verantwoordingsplicht uit hoofde van artikel 5, lid 2, AVG. Derhalve moet ook de naleving van andere bepalingen uit de AVG worden onderzocht.**
58. Idealiter controleren toezichthoudende autoriteiten of in de documentatie van de verwerkingsverantwoordelijke het volgende is opgenomen:
- informatie over DPIA's, waaronder beoordelingen en besluiten waarin wordt vastgesteld dat een DPIA niet nodig was;
 - adviezen of feedback van de functionaris voor gegevensbescherming (Data Protection Officer, "DPO") (wanneer een DPO was aangesteld of had moeten worden aangesteld);
 - informatie over de technische en organisatorische maatregelen die bij het ontwerpen van het AI-model zijn genomen om de kans op identificatie te verkleinen, waaronder het dreigingsmodel en de risicobeoordelingen waarop deze maatregelen zijn gebaseerd. Daartoe moeten de specifieke maatregelen voor elke bron van trainingsdatasets behoren, met inbegrip van relevante bron-URL's en beschrijvingen van maatregelen die zijn genomen (of reeds zijn genomen door derden die datasets leveren);
 - de technische en organisatorische maatregelen die in alle stadia van de levenscyclus van het model zijn genomen en hebben bijgedragen aan de afwezigheid van persoonsgegevens in het model of deze afwezigheid hebben geverifieerd;
 - de documentatie waaruit blijkt dat het AI-model in theorie bestand is tegen technieken voor heridentificatie, evenals de voorzieningen die zijn bedoeld om het slagen en de gevolgen van de belangrijkste aanvallen te beperken of te beoordelen (teruglekken, aanvallen met membershipinference, exfiltratie enz.). Dit kan met name het volgende omvatten: i) de verhouding tussen de hoeveelheid trainingsgegevens en het aantal parameters in het model, waaronder de analyse van het effect ervan op het model³⁸; ii) cijfers over de kans op

³⁸ Ricciato, F., *A Cautionary Reflection on (Pseudo-)Synthetic Data from Deep Learning on Personal Data*, Privacy in Statistical Databases conference (PSD 2024), Antibes, Frankrijk, september 2024, slides beschikbaar op https://cros.ec.europa.eu/system/files/2024-10/20240926_PSD2024_Ricciato_v6_1.pdf en Belkin, M., Hsu, D., Ma, S., en Mandal, S. (2019), *Reconciling modern machine-learning practice and the classical bias–variance trade-off*. Proceedings of the National Academy of Sciences, 24 juli 2019, 116(32) 15849-15854, beschikbaar op <https://www.pnas.org/doi/10.1073/pnas.1903070116>.

heridentificatie uitgaand van de actuele stand van de techniek; iii) rapporten over de wijze waarop het model is getest (door wie, wanneer, hoe, en in hoeverre); en iv) de testresultaten;

- f. de documentatie die is verstrekt aan de verwerkingsverantwoordelijke(n) die het model inzet(ten) en/of aan betrokkenen, waaronder met name de documentatie over de maatregelen die zijn genomen om de kans op identificatie te verkleinen en over de mogelijk resterende risico's.

3.3 Geschiktheid van een gerechtvaardigd belang als rechtsgrond voor de verwerking van persoonsgegevens bij de ontwikkeling en de inzet van AI-modellen

- 59. Bij de beantwoording van de vragen 2 en 3 uit het verzoek maakt het EDPB eerst een aantal algemene opmerkingen over enkele belangrijke aspecten waarmee toezichthoudende autoriteiten ongeacht de rechtsgrondslag voor een verwerking rekening moeten houden bij hun beoordeling van de wijze waarop verwerkingsverantwoordelijken in het kader van AI-modellen de naleving van de AVG kunnen aantonen. Uitgaand van de Richtsnoeren 1/2024 voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG³⁹ zal het EDPB vervolgens ingaan op de drie stappen die bij een beoordeling van het gerechtvaardigde belang moeten worden doorlopen met betrekking tot de ontwikkeling en de inzet van AI-modellen.

3.3.1 Algemene opmerkingen

- 60. Het EDPB wijst erop dat de AVG niet voorziet in een rangorde tussen de verschillende rechtsgrondslagen uit artikel 6, lid 1, AVG⁴⁰.
- 61. In artikel 5 AVG worden de beginselen voor de verwerking van persoonsgegevens vastgesteld. Het EDPB wijst met name op de beginselen die voor dit advies van belang zijn en in ieder geval door de toezichthoudende autoriteiten moeten worden getoetst wanneer zij specifieke AI-modellen beoordelen, en wijst daarnaast op de meest toepasselijke vereisten uit andere bepalingen van de AVG, rekening houdend met de reikwijdte van dit advies.
- 62. **Verantwoordingsbeginsel** (artikel 5, lid 2, AVG) – Dit beginsel houdt in dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de AVG en deze kan aantonen. In dit verband moeten de rollen en verantwoordelijkheden van de partijen die persoonsgegevens verwerken in het kader van de ontwikkeling of de inzet van een AI-model worden beoordeeld voordat de verwerking plaatsvindt, om de verplichtingen van de verwerkingsverantwoordelijken of gezamenlijke verwerkingsverantwoordelijken en van de (eventuele) verwerkers vanaf het begin vast te stellen.
- 63. **Beginselen van rechtmatigheid, behoorlijkheid en transparantie** (artikel 5, lid 1, punt a), AVG) – Het EDPB acht het zinvol om bij de beoordeling van de rechtmatigheid van de verwerking in het kader van AI-modellen, gezien artikel 6, lid 1, AVG een onderscheid te maken tussen de verschillende stadia van de verwerking van persoonsgegevens⁴¹. Het beginsel van behoorlijkheid, dat nauw verband houdt met het beginsel van transparantie, houdt in dat persoonsgegevens niet worden verwerkt met oneerlijke methoden of door middel van bedrog, of op een wijze die “ongerechtvaardigd schadelijk, onrechtmatig

³⁹ Zie de Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024.

⁴⁰ Ibid., punt 1.

⁴¹ Verslag van het EDPB over de werkzaamheden van de ChatGPT Taskforce, vastgesteld op 23 mei 2024, punt 14.

*discriminerend, onverwacht of misleidend voor de betrokkene is*⁴². Gezien de complexiteit van de toegepaste technologieën moet informatie over de verwerking van persoonsgegevens in AI-modellen daarom op een toegankelijke, begrijpelijke en gebruikersvriendelijke manier worden verstrekt⁴³. Transparantie over de verwerking van persoonsgegevens omvat met name de naleving van de informatieverplichtingen uit de artikelen 12, 13 en 14 AVG⁴⁴, waarin voor geautomatiseerde besluitvorming (waaronder profilering) ook wordt voorgeschreven dat nuttige informatie over de onderliggende logica wordt verstrekt, alsmede over het belang en de verwachte gevolgen van die verwerking voor de betrokkene⁴⁵. Aangezien er in de ontwikkelingsfasen van AI-modellen mogelijk grote hoeveelheden gegevens uit openbare bronnen worden verzameld (bijvoorbeeld door middel van webscrapingstechnieken), mag de uitzondering uit artikel 14, lid 5, punt b), AVG uitsluitend worden gebruikt wanneer volledig wordt voldaan aan de vereisten van deze bepaling⁴⁶.

64. **Beginnelsen van doelbinding en minimale gegevensverwerking** (artikel 5, lid 1, punten b) en c), AVG)
- Volgens het beginsel van minimale gegevensverwerking moeten persoonsgegevens bij de ontwikkeling en de inzet van AI-modellen toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor het doel. Dit kan inhouden dat persoonsgegevens worden verwerkt om de risico's van mogelijke vertekeningen en fouten te voorkomen wanneer dit bij het doel duidelijk en specifiek wordt aangegeven, en de persoonsgegevens voor dat doel benodigd zijn (bv. wanneer zij niet doeltreffend kunnen worden verkregen door de verwerking van andere gegevens, waaronder synthetische of geanonimiseerde gegevens)⁴⁷. De WP29-groep heeft al benadrukt dat *“duidelijk en specifiek moet worden aangegeven met welk doel het verzamelen plaatsvindt [...]”*⁴⁸. Wanneer wordt beoordeeld of het nagestreefde doel gerechtvaardigd, specifiek en expliciet is en of de verwerking in overeenstemming is met het beginsel van minimale gegevensverwerking, moet allereerst worden vastgesteld om welke verwerkingsactiviteit het gaat. De verschillende stadia binnen de ontwikkelings- of inzetfasen kunnen namelijk dezelfde of verschillende verwerkingsactiviteiten vormen, waarbij opeenvolgende of gezamenlijke verwerkingsverantwoordelijken betrokken kunnen zijn. In sommige gevallen kan in een vroeg stadium van de ontwikkeling worden bepaald welk doel zal worden nagestreefd bij de inzet van het AI-model. Ook wanneer dit niet het geval is, moet de situatie waarin het model zal worden ingezet al enigszins duidelijk zijn, en moet dus worden onderzocht op welke wijze deze situatie in overeenstemming is met het doel van de ontwikkeling. Bij hun beoordeling van het doel van de verwerking in een bepaald stadium van de ontwikkeling mogen de toezichthoudende autoriteiten een zekere mate van uitvoerigheid van de verwerkingsverantwoordelijke(n) verwachten,

⁴² Verslag van het EDPB over de werkzaamheden van de ChatGPT Taskforce, vastgesteld op 23 mei 2024, punt 23, Richtsnoeren 4/2019 van het EDPB inzake artikel 25 Gegevensbescherming door ontwerp en door standaardinstellingen, versie 2.0, vastgesteld op 20 oktober 2020, punt 69, Groep gegevensbescherming artikel 29 – Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, herzien en goedgekeurd op 11 april 2018, door het EDPB bekrachtigd op 25 mei 2018, punt 2.

⁴³ Groep gegevensbescherming artikel 29 – Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, herzien en goedgekeurd op 11 april 2018, door het EDPB bekrachtigd op 25 mei 2018, punt 5.

⁴⁴ Zie ook overweging 39 AVG, waarin wordt bepaald dat het *“voor natuurlijke personen [...] transparant [dient] te zijn dat hen betreffende persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt en in hoeverre de persoonsgegevens worden verwerkt of zullen worden verwerkt [...]”*.

⁴⁵ Artikel 13, lid 2, punt f), AVG en artikel 14, lid 2, punt g), AVG.

⁴⁶ Verslag van het EDPB over de werkzaamheden van de ChatGPT Taskforce, goedgekeurd op 23 mei 2024, punt 27.

⁴⁷ Verder voorziet artikel 10, lid 5, van de AI-verordening in specifieke regels voor de verwerking van bijzondere categorieën van persoonsgegevens in verband met AI-systemen met een hoog risico, om de opsporing en correctie van vertekeningen te waarborgen.

⁴⁸ Advies 03/2013 van de Groep gegevensbescherming artikel 29 over doelbinding (WP203), blz. 15-16.

evenals een toelichting op de wijze waarop deze details terug te vinden zijn in het doel van de verwerking. Daartoe kan bijvoorbeeld informatie behoren over het type AI-model dat wordt ontwikkeld, de verwachte functionaliteit ervan, en alle overige achtergrondinformatie die in dat stadium reeds bekend is. Tot de context van de inzet kan bijvoorbeeld ook de vraag behoren of een model wordt ontwikkeld voor interne inzet, of de verwerkingsverantwoordelijke voornemens is om het model na afloop van de ontwikkeling aan derden te verkopen of te distribueren, en of het model primair is bedoeld om te worden ingezet voor commerciële of onderzoeksdoeleinden.

65. **Rechten van betrokkenen** (hoofdstuk III, AVG) – Hoewel de toezichthoudende autoriteiten moeten waarborgen dat alle rechten van betrokkenen worden geëerbiedigd bij de ontwikkeling en de inzet van AI-modellen door verwerkingsverantwoordelijken, wijst het EDPB erop dat het recht van bezwaar uit hoofde van artikel 21 AVG van toepassing is en in alle gevallen moet worden gewaarborgd wanneer een verwerkingsverantwoordelijke een gerechtvaardigd belang als rechtsgrondslag gebruikt⁴⁹.

3.3.2 Overwegingen ten aanzien van de drie stappen in de beoordeling van het gerechtvaardigde belang bij de ontwikkeling en de inzet van AI-modellen

66. Om te bepalen of een bepaalde verwerking van persoonsgegevens kan plaatsvinden op grond van artikel 6, lid 1, punt f), AVG, moeten de toezichthoudende autoriteiten verifiëren of de verwerkingsverantwoordelijken zorgvuldig hebben beoordeeld en gedocumenteerd of aan de drie onderstaande cumulatieve voorwaarden is voldaan: i) de verwerkingsverantwoordelijke of een derde streeft een gerechtvaardigd belang na; ii) de verwerking is noodzakelijk voor het nastreven van het gerechtvaardigde belang; en iii) de belangen of grondrechten en vrijheden van de betrokkenen wegen niet zwaarder dan het gerechtvaardigde belang⁵⁰.

3.3.2.1 Eerste stap – Nastreven van een gerechtvaardigd belang door de verwerkingsverantwoordelijke of een derde

67. Een belang is in bredere zin het resultaat of het voordeel dat een verwerkingsverantwoordelijke of derde kan behalen door een specifieke verwerkingsactiviteit⁵¹. Hoewel in de AVG en door het Hof

⁴⁹ Als betrokkenen om met hun specifieke situatie verband houdende redenen bezwaar maken tegen de verwerking van hen betreffende persoonsgegevens, moet de verwerkingsverantwoordelijke volgens artikel 21 AVG de verwerking van de persoonsgegevens staken tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering. De twee aspecten die de toezichthoudende autoriteiten dus in aanmerking moeten nemen, zijn de vraag of de verwerkingsverantwoordelijke die dringende gerechtvaardigde gronden kan aantonen en of het recht van bezwaar kan worden uitgeoefend.

⁵⁰ Arrest van het Hof van 4 juli 2023, *Meta/Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, punt 106, arrest van het Hof van 11 december 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, punt 40. Zie ook de Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 12 e.v. Zoals in deze richtsnoeren wordt aangegeven, moet deze “beoordeling bij aanvang van de verwerking plaatsvinden, moet daarbij de (eventueel aangestelde) functionaris voor gegevensbescherming (DPO) zijn betrokken en moet de beoordeling door de verwerkingsverantwoordelijke worden gedocumenteerd overeenkomstig het verantwoordingsbeginsel van artikel 5, lid 2, AVG”.

⁵¹ Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 14.

verschillende belangen als gerechtvaardigd worden aangemerkt⁵², moet de gerechtvaardigheid van een bepaald belang per geval worden beoordeeld.

68. Zoals door het EDPB aangegeven in haar richtsnoeren over het gerechtvaardigd belang⁵³, kan een belang als gerechtvaardigd worden beschouwd als aan alle drie onderstaande voorwaarden wordt voldaan:
- a. het belang is rechtmatig⁵⁴;
 - b. het is duidelijk en nauwkeurig geformuleerd; en
 - c. het belang is reëel en concreet, niet hypothetisch.
69. Met inachtneming van de twee andere stappen die bij de beoordeling van het gerechtvaardigde belang moeten worden doorlopen, kunnen de volgende voorbeelden een gerechtvaardigd belang vormen in het kader van AI-modellen: i) de ontwikkeling van een chatfunctie om gebruikers te ondersteunen; ii) de ontwikkeling van een AI-systeem om frauduleuze inhoud of gedrag op te sporen; en iii) verbetering van de opsporing van dreigingen in een informatiesysteem.

3.3.2.2 *Tweede stap – Onderzoek van de noodzaak van de verwerking voor het nastreven van het gerechtvaardigde belang.*

70. Bij de tweede stap van de beoordeling wordt bepaald of de verwerking van persoonsgegevens noodzakelijk is voor het nagestreefde gerechtvaardigde belang of de nagestreefde gerechtvaardigde belangen⁵⁵ (“noodzakelijkheidstoets”).
71. Volgens overweging 39 AVG mogen persoonsgegevens alleen worden verwerkt “*indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt*”. Volgens het Hof en eerdere richtsnoeren van het EDPB moet de noodzaak van de verwerking worden getoetst aan de grondrechten en vrijheden van de betrokkenen en worden gezien in combinatie met het beginsel van minimale gegevensverwerking uit artikel 5, lid 1, punt c), AVG⁵⁶.

⁵² Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 16.

⁵³ Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 17.

⁵⁴ Arrest van het Hof van 4 oktober 2024, *Koninklijke Nederlandse Lawn Tennisbond*, C-621/22, ECLI:EU:C:2024:857, punt 49, waarin het Hof benadrukte dat een gerechtvaardigd belang niet in strijd met de wet kan zijn. In dit verband benadrukt het EDPB dat bij de beoordeling van de rechtmatigheid van een bepaald belang naargelang van het geval rekening moet worden gehouden met wetgevingskaders. Zie bijvoorbeeld artikel 26, lid 3, en artikel 28 van Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaaldienstenverordening) over verboden gerichte reclame voor minderjarigen, artikel 5, leden 1 en 2, van de AI-verordening over verboden AI-praktijken (manipulatieve praktijken en technieken waarvan personen zich niet bewust zijn); verwerking in strijd met intellectuele-eigendomsrechten en de bepalingen uit Richtlijn (EU) 2019/790 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt.

⁵⁵ Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punten 28, 29 en 30.

⁵⁶ Arrest van het Hof van 4 juli 2023, *Meta/Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, punten 108 en 109, waarin ook wordt verwezen naar het arrest van het Hof van 11 december 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, punt 48, arrest van het Hof van 9 november 2010, *Volker und Markus Schecke*, gevoegde zaken C-92/09 en C-93/09, ECLI:EU:C:2010:662, punten 85 en 86 en arrest van het Hof van 22 juni 2021, *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504, punten 98, 109, 110 en 113. Zie bijvoorbeeld ook Richtsnoeren 3/2019 van het EDPB inzake de verwerking van persoonsgegevens door middel

72. Bij de door het Hof bedoelde methodiek wordt rekening gehouden met de context van de verwerking en met de gevolgen voor de verwerkingsverantwoordelijke en de betrokkenen. De noodzakelijkheidstoets omvat dus twee aspecten: i) de vraag of de verwerkingsactiviteit het nastreven van het doel mogelijk zal maken⁵⁷; en ii) de vraag of er geen minder indringende manier is om dit doel na te streven⁵⁸.
73. Zo moet bijvoorbeeld, naargelang van het geval, het beoogde volume aan persoonsgegevens in het AI-model worden afgewogen tegen minder indringende alternatieven die redelijkerwijs beschikbaar kunnen zijn om het doel van het nagestreefde gerechtvaardigde belang even doeltreffend te verwezenlijken. Als het doel ook kan worden nagestreefd met een AI-model waarin geen persoonsgegevens worden verwerkt, dan moet de verwerking van persoonsgegevens als niet-noodzakelijk worden beschouwd. Dit is vooral relevant voor de ontwikkeling van AI-modellen. Wanneer zij beoordelen of aan de voorwaarde van noodzakelijkheid wordt voldaan, moeten toezichthoudende autoriteiten bijzondere aandacht schenken aan de hoeveelheid persoonsgegevens die wordt verwerkt en aan de vraag of het evenredig is om het desbetreffende gerechtvaardigde belang na te streven, ook gezien het beginsel van minimale gegevensverwerking.
74. Bij de beoordeling van de noodzaak moet ook rekening worden gehouden met de bredere context van de beoogde verwerking van persoonsgegevens. Het bestaan van middelen die minder indringend zijn voor de grondrechten en fundamentele vrijheden van de betrokkenen kan verschillen en afhangen van de vraag of de verwerkingsverantwoordelijke een rechtstreekse relatie met de betrokkenen heeft (firstpartygegevens) of niet (gegevens van derden). Het Hof heeft enkele overwegingen gegeven waarmee rekening moet worden gehouden bij het onderzoeken van de noodzaak van de verwerking van firstpartygegevens ten behoeve van het gerechtvaardigde belang of de gerechtvaardigde belangen

van videoapparatuur, versie 2.0, vastgesteld op 29 januari 2020, punten 24, 25, 26 en 73, Richtsnoeren 2/2019 van het EDPB betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), AVG in het kader van de verlening van onlinediensten aan betrokkenen, versie 2.0, vastgesteld op 8 oktober 2019, punten 23, 24 en 25, Advies 11/2024 van het EDPB over het gebruik van gezichtsherkenning om de passagiersstroom op luchthavens te stroomlijnen, versie 1.1, vastgesteld op 23 mei 2024, punt 27.

⁵⁷ Zie arrest van het Hof van 16 december 2008, *Heinz Huber/Bundesrepublik Deutschland*, C-524/06, ECLI:EU:C:2008:724, punt 66. Zie in dezelfde zaak ook de conclusie van advocaat-generaal Poiares Maduro in zaak C-524/06, *Heinz Huber/Bundesrepublik Deutschland*, ECLI:EU:C:2008:194, punt 16, waarin staat: “[D]e juiste maatstaf [is hier] de doeltreffendheid en [...] het [is] aan de nationale rechter om deze toe te passen. Hij dient zich de vraag te stellen of er andere manieren van gegevensverwerking zijn waarmee de immigratiediensten de verblijfsrechtelijke regels kunnen handhaven. Beantwoordt hij die vraag bevestigend, moet de centrale opslag en verwerking van gegevens van burgers van de Unie onwettig worden verklaard. Het is niet nodig dat het alternatieve systeem het meest doeltreffend of geschikt is; voldoende is, dat het behoorlijk functioneert. Met andere woorden: ook al is het centraal register doeltreffender, gemakkelijker of gebruiksvriendelijker dan de alternatieven hiervoor (zoals gedecentraliseerde, plaatselijke registers), verdienen deze alternatieven duidelijk de voorkeur wanneer zij gebruikt kunnen worden voor het verkrijgen van inlichtingen over de verblijfsstatus van burgers van de Unie.”

⁵⁸ Zie arrest van het Hof van 27 september 2017, *Peter Puškár*, C-73/16, ECLI:EU:C:2017:725, punt 113: “Het is dan ook aan de verwijzende rechterlijke instantie om na te gaan of met de vaststelling van de litigieuze lijst en de inschrijving daarop van de namen van de betrokken personen de daarmee nagestreefde doelstellingen worden bereikt en of voor de bereiking van die doelstellingen geen andere, minder vergaande middelen kunnen worden aangewend”, zie bijvoorbeeld ook conclusie van advocaat-generaal A. Rantos in *Meta/Bundeskartellamt*, C-252/21, ECLI:EU:C:2022:704, punt 61, waarin staat: “[...] Derhalve moet er een nauw verband bestaan tussen de verwerking en het nagestreefde belang, bij gebreke van alternatieven die de bescherming van persoonsgegevens beter in acht nemen, aangezien het niet volstaat dat de verwerking louter nuttig is voor de verwerkingsverantwoordelijke.”

dat (die) wordt (worden) nagestreefd (zij het in het kader van de verstrekking van die gegevens aan derden)⁵⁹.

75. De invoering van technische waarborgen om persoonsgegevens te beschermen kan ook bijdragen aan een gunstige uitkomst van de noodzakelijkheidstoets. Daartoe kan bijvoorbeeld de zodanige invoering behoren van de in punt 3.2.2 genoemde maatregelen dat geen anonimisering wordt bewerkstelligd, maar de betrokkenen toch minder gemakkelijk kunnen worden geïdentificeerd. Het EDPB merkt op dat enkele van deze maatregelen, wanneer zij niet verplicht zijn om aan de voorschriften van de AVG te voldoen, wel aanvullende waarborgen kunnen vormen, zoals nader wordt uiteengezet in de paragraaf “Verzachtende maatregelen” in punt 3.3.2.3⁶⁰.

3.3.2.3 Derde stap – Afwegingstoets

76. De derde stap bij de beoordeling van het gerechtvaardigde belang is de “**afweging**” (in dit document ook de “**afwegingstoets**” genoemd)⁶¹. In deze stap worden de verschillende strijdige rechten en belangen geïnventariseerd en beschreven⁶², d.w.z. enerzijds de belangen, grondrechten en fundamentele vrijheden van de betrokkenen en anderzijds de belangen van de verwerkingsverantwoordelijke of een derde. Vervolgens moeten de specifieke omstandigheden van het geval worden onderzocht om aan te tonen dat een gerechtvaardigd belang een passende rechtsgrondslag voor de desbetreffende verwerkingsactiviteiten is⁶³.

Belangen, grondrechten en fundamentele vrijheden van betrokkenen

77. In artikel 6, lid 1, punt f), AVG wordt bepaald dat de verwerkingsverantwoordelijke bij de beoordeling van de verschillende aspecten in het kader van de afwegingstoets rekening moet houden met de belangen, grondrechten en fundamentele vrijheden van de betrokkenen. Onder de belangen van betrokkenen worden de belangen verstaan die mogelijk worden geschaad door de desbetreffende verwerking. In het kader van de ontwikkelingsfase van een AI-model kan daartoe onder meer, maar niet uitsluitend, het belang van zelfbeschikking en zeggenschap over de eigen persoonsgegevens behoren (bv. de gegevens die voor de ontwikkeling van het model worden verzameld). In het kader van de inzet van een AI-model kunnen onder de belangen van betrokkenen onder meer, maar niet uitsluitend, worden verstaan het belang van zeggenschap over de eigen persoonsgegevens (bv. de gegevens die worden verwerkt wanneer het model wordt ingezet), financiële belangen (bv. wanneer een AI-model door de betrokkene wordt gebruikt om inkomsten te genereren of door een persoon wordt gebruikt in het kader van zijn of haar beroepsmatige activiteiten), persoonlijke voordelen (bv. wanneer een AI-model wordt gebruikt om de toegang tot bepaalde diensten te verbeteren) of sociaaleconomische belangen (bv. wanneer een AI-model de toegang tot betere gezondheidszorg mogelijk maakt of de uitoefening van een grondrecht bevordert, waaronder de toegang tot onderwijs)⁶⁴.

⁵⁹ Arrest van het Hof van 4 oktober 2024, *Koninklijke Nederlandse Lawn Tennisbond*, C-621/22, ECLI:EU:C:2024:857, punten 51, 52 en 53.

⁶⁰ Zie Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 57.

⁶¹ Zie Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punten 31 tot en met 60.

⁶² Zie Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 32.

⁶³ Zie Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 32, waarin ook wordt verwezen naar het arrest van het Hof van 4 juli 2023, *Meta/Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, punt 110.

⁶⁴ Zie Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 38.

78. Naarmate een belang nauwkeuriger wordt gedefinieerd in het licht van het voorgenomen doel van de verwerking zal het een beter beeld mogelijk maken van de reële voordelen en risico's waarmee rekening moet worden gehouden in de afwegingstoets.
79. Ten aanzien van de grondrechten en fundamentele vrijheden van betrokkenen kunnen de ontwikkeling en de inzet van AI-modellen ernstige risico's doen ontstaan voor rechten die worden beschermd door het Handvest van de grondrechten van de Europese Unie (het "**EU-handvest**"), waaronder onder meer, maar niet uitsluitend, het recht op eerbiediging van het privéleven en het familie- en gezinsleven (artikel 7 EU-handvest) en het recht op bescherming van persoonsgegevens (artikel 8 EU-handvest). Deze risico's kunnen ontstaan tijdens de ontwikkelingsfase, bijvoorbeeld bij "scraping" van persoonsgegevens in strijd met de wens, of zonder medeweten van de betrokkenen. Deze risico's kunnen ook in de inzetfase ontstaan, bijvoorbeeld wanneer persoonsgegevens door (of als onderdeel van) het model worden verwerkt op een manier die strijdig is met de rechten van de betrokkenen, of wanneer het onbedoeld of door middel van aanvallen mogelijk is om af te leiden (bv. membershipinference, extractie of modelinversie) welke persoonsgegevens in de trainingsdatabase aanwezig zijn. Dergelijke situaties vormen een risico voor de privacy van betrokkenen van wie gegevens mogelijk opduiken tijdens de inzetfase van het AI-systeem (bv. reputatierisico's, identiteitsdiefstal of -fraude, veiligheidsrisico's afhankelijk van de aard van de gegevens).
80. Afhankelijk van het geval kunnen er ook risico's voor andere grondrechten zijn. Zo kunnen betrokkenen bij het grootschalig en willekeurig verzamelen van gegevens door AI-modellen in de ontwikkelingsfase het gevoel krijgen dat zij in de gaten worden gehouden, vooral vanwege de moeite die het kost om "scraping" van openbare gegevens te voorkomen. Hierdoor kunnen mensen zelfcensuur gaan toepassen en ontstaan er risico's voor ondermijning van hun vrijheid van meningsuiting (artikel 11 EU-handvest). Tijdens de inzetfase bestaan er ook risico's voor de vrijheid van meningsuiting wanneer AI-modellen worden gebruikt om te voorkomen dat inhoud van betrokkenen wordt gepubliceerd. Ook kan een AI-model dat ongepaste inhoud aan kwetsbare personen aanbeveelt risico's voor hun geestelijke gezondheid inhouden (artikel 3, lid 1, EU-handvest). In andere gevallen kan de inzet van AI-modellen ook nadelige gevolgen hebben voor het recht van een persoon om te werken (artikel 15 EU-handvest), bijvoorbeeld wanneer met behulp van een AI-model een voorselectie uit sollicitaties wordt gemaakt. Ook kan een AI-model risico's inhouden voor het recht op non-discriminatie (artikel 21 EU-handvest) als het mensen discrimineert op grond van bepaalde persoonskenmerken (waaronder nationaliteit of geslacht). Bovendien kan de inzet van AI-modellen ook risico's inhouden voor iemands veiligheid (bv. wanneer het AI-model kwaadwillig wordt gebruikt), alsmede risico's voor de lichamelijke en geestelijke integriteit van personen⁶⁵.
81. De inzet van AI-modellen kan ook gunstige gevolgen hebben voor bepaalde grondrechten en bv. het recht op geestelijke integriteit van een persoon (artikel 3 van het handvest) ondersteunen, bijvoorbeeld wanneer een AI-model wordt gebruikt om schadelijke inhoud online op te sporen, of wanneer het model de toegang tot bepaalde essentiële diensten vergemakkelijkt of de uitoefening van grondrechten vergemakkelijkt, bijvoorbeeld de toegang tot informatie (artikel 11 EU-handvest) of de toegang tot onderwijs (artikel 14 EU-handvest).

⁶⁵ Richtsnoeren 1/2024 voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 46.

Gevolgen van de verwerking voor betrokkenen

82. De verwerking van persoonsgegevens tijdens de ontwikkeling en de inzet van AI-modellen kan voor betrokkenen op verschillende manieren gevolgen hebben, die gunstig of ongunstig kunnen zijn⁶⁶. Als een verwerkingsactiviteit bijvoorbeeld voordelen voor de betrokkene heeft, dan kan daar rekening mee worden gehouden in de afwegingstoets. Hoewel het bestaan van dergelijke voordelen ertoe kan leiden dat een toezichthoudende autoriteit concludeert dat de belangen, grondrechten en fundamentele vrijheden van de betrokkenen niet zwaarder wegen dan de belangen van de verwerkingsverantwoordelijke of een derde, kan die conclusie pas worden getrokken na een onderzoek dat per geval wordt verricht en waarbij alle relevante factoren in aanmerking worden genomen.
83. De gevolgen van de verwerking voor de betrokkenen kunnen worden beïnvloed door i) de aard van de gegevens die door de modellen worden verwerkt; ii) het kader waarin de verwerking plaatsvindt; en iii) de eventuele verdere gevolgen van de verwerking⁶⁷.
84. Ten aanzien van de **aard van de verwerkte gegevens** moet erop worden gewezen dat de verwerking van bepaalde andere categorieën van persoonsgegevens aanzienlijke gevolgen voor betrokkenen kan hebben, met uitzondering van bijzondere categorieën van persoonsgegevens en gegevens over strafrechtelijke veroordelingen en strafbare feiten die respectievelijk aanvullende bescherming genieten op grond van de artikelen 9 en 10 AVG. In dit verband moet er vanuit worden gegaan dat de verwerking van bepaalde soorten persoonsgegevens met zeer persoonlijke informatie (bv. financiële gegevens of locatiegegevens) voor de ontwikkeling en de inzet van een AI-model mogelijk ernstige gevolgen voor betrokkenen kan hebben. Tijdens de inzetfase kunnen de gevolgen van die verwerking voor betrokkenen bijvoorbeeld economisch van aard zijn (bv. discriminatie in de werkomgeving) en/of gevolgen hebben voor een reputatie (bv. laster).
85. Met betrekking tot het **kader waarin de verwerking plaatsvindt** moet eerst worden geïnventariseerd welke aspecten risico's voor de betrokkenen kunnen vormen (bv. de manier waarop het model is ontwikkeld, de manier waarop het model kan worden ingezet, en/of de vraag of passende beveiligingsmaatregelen worden genomen om de persoonsgegevens te beschermen). De aard van het model en het beoogde operationele gebruik spelen een belangrijke rol bij de inventarisatie van deze mogelijke oorzaken.
86. Ook moet de ernst van deze risico's voor de betrokkenen worden beoordeeld. Zo kan onder meer worden onderzocht op welke wijze de persoonsgegevens worden verwerkt (bv. of zij met andere datasets worden gecombineerd), op welke schaal de verwerking plaatsvindt en hoeveel persoonsgegevens worden verwerkt⁶⁸ (bv. het totale volume aan gegevens per betrokkene, het aantal betrokkenen)⁶⁹, de status van de betrokkene (bv. kinderen of andere kwetsbare betrokkenen) en hun relatie met de verwerkingsverantwoordelijke (bv. of de betrokkene een klant is). Zo kan het gebruik van webscraping in de ontwikkelingsfase – als voldoende waarborgen ontbreken – aanzienlijke gevolgen voor mensen hebben vanwege de grote hoeveelheid gegevens die wordt verzameld, het grote aantal betrokkenen, en de willekeur bij het verzamelen van persoonsgegevens.

⁶⁶ Zie Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 39.

⁶⁷ Zie Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 32.

⁶⁸ Zie Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 43.

⁶⁹ Arrest van het Hof van 4 juli 2023, *Meta/Bundeskartellamt*, C252/21, ECLI:EU:C:2023:537, punt 116.

87. De eventuele **verdere gevolgen** van de verwerking moeten ook worden onderzocht bij de beoordeling van de gevolgen van de verwerking voor de betrokkenen. Zij moeten door de toezichthoudende autoriteiten per geval worden beoordeeld op basis van de beschikbare specifieke feiten.
88. Tot die gevolgen kunnen (onder meer, maar niet uitsluitend) de risico's van schending van de grondrechten van de betrokkenen behoren, zoals in de vorige paragraaf is uiteengezet⁷⁰. De kans hierop, en de ernst ervan kunnen verschillen, en deze risico's kunnen ontstaan bij de verwerking van persoonsgegevens die mogelijk fysieke, materiële of immateriële schade tot gevolg heeft, met name wanneer de verwerking aanleiding tot discriminatie kan geven⁷¹.
89. Wanneer bij de inzet van een AI-model persoonsgegevens worden verwerkt van zowel i) betrokkenen van wie de persoonsgegevens aanwezig zijn in de dataset die in de ontwikkelingsfase is gebruikt; en ii) betrokkenen van wie persoonsgegevens in de inzetfase worden verwerkt, moeten de toezichthoudende autoriteiten apart onderzoek doen naar de risico's voor de belangen, rechten en vrijheden van elk van deze categorieën betrokkenen wanneer zij de door een verwerkingsverantwoordelijke verrichte afwegingstoets verifiëren.
90. **Tot slot moet bij het onderzoek van de mogelijke verdere gevolgen van de verwerking ook worden gekeken naar de kans dat deze verdere gevolgen zich daadwerkelijk voordoen.** Bij de beoordeling van die kans moeten de getroffen technische en organisatorische maatregelen en de specifieke omstandigheden van het geval in aanmerking worden genomen. De toezichthoudende autoriteiten kunnen bijvoorbeeld onderzoeken of maatregelen zijn uitgevoerd om potentieel misbruik van het AI-model te voorkomen. Voor AI-modellen die voor uiteenlopende doeleinden kunnen worden ingezet, waaronder generatieve AI, kunnen hiertoe ook voorzieningen behoren die zoveel mogelijk voorkomen dat zij worden gebruikt voor schadelijke praktijken, waaronder deepfakes, chatbots voor desinformatie, phishing en andere vormen van fraude; en manipulatieve AI/AI-agents (met name wanneer zij op mensen lijken of misleidende informatie verstrekken).

Redelijke verwachtingen van betrokkenen

91. Volgens overweging 47 AVG *"[is] in elk geval [...] een zorgvuldige beoordeling geboden om te bepalen of sprake is van een gerechtvaardigd belang, alsook om te bepalen of een betrokkene op het tijdstip en in het kader van de verzameling van de persoonsgegevens redelijkerwijs mag verwachten dat verwerking met dat doel kan plaatsvinden. De belangen en de grondrechten van de betrokkene kunnen met name zwaarder wegen dan het belang van de verwerkingsverantwoordelijke wanneer persoonsgegevens worden verwerkt in omstandigheden waarin de betrokkenen redelijkerwijs geen verdere verwerking verwachten"*⁷².
92. Redelijke verwachtingen vervullen een belangrijke rol in de afwegingstoets, niet in de laatste plaats vanwege de complexiteit van de technologie die in AI-modellen wordt gebruikt en het feit dat het voor betrokkenen lastig kan zijn om inzicht te krijgen in de verscheidenheid aan gebruiksmogelijkheden van

⁷⁰ Zie bovenstaande paragraaf "Belangen, grondrechten en fundamentele vrijheden van betrokkenen".

⁷¹ Zie punt 2.3 van de Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024. Zie voor meer voorbeelden ook overweging 75 AVG.

⁷² Zie ook het arrest van het Hof van 4 juli 2023, *Meta/Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, punt 112, het arrest van het Hof van 11 december 2019, *Asociația de Proprietari bloc M5A-Scara A*, C-708/18, ECLI:EU:C:2019:1064, punt 58 en het arrest van het Hof van 4 oktober 2024, *Koninklijke Nederlandse Lawn Tennisbond*, C-621/22, ECLI:EU:C:2024:857, punt 55.

een AI-model en de bijbehorende gegevensverwerking⁷³. Met het oog daarop kan de informatie die aan de betrokkenen wordt verstrekt worden onderzocht om te beoordelen of zij redelijkerwijs kunnen verwachten dat hun persoonsgegevens worden verwerkt. Hoewel het ontbreken van informatie ertoe kan bijdragen dat de betrokkenen een bepaalde verwerking niet verwachten, volstaat echter het enkele feit dat aan de transparantievereisten uit de AVG wordt voldaan niet om te menen dat de betrokkenen een bepaalde verwerking redelijkerwijs kunnen verwachten⁷⁴. Dat informatie over de ontwikkelingsfase van een AI-model is opgenomen in de privacyverklaring van de verwerkingsverantwoordelijke wil bovendien nog niet automatisch zeggen dat de betrokkenen redelijkerwijs kunnen verwachten dat dit ook gebeurt. Dit moet door de toezichthoudende autoriteiten worden onderzocht op basis van de specifieke omstandigheden van het geval en met inachtneming van alle relevante factoren.

93. Bij het beoordelen van de redelijke verwachtingen van betrokkenen ten aanzien van de verwerking tijdens de ontwikkelingsfase is het van belang om de aspecten te noemen die worden aangegeven in de richtsnoeren van het EDPB over het gerechtvaardigd belang⁷⁵. Daarnaast is het in het kader van dit advies van belang om het bredere kader van de verwerking te bezien. Daarbij kan het onder meer, maar niet uitsluitend, gaan om de vraag of de persoonsgegevens openbaar waren, om de aard van de relatie tussen de betrokkene en de verwerkingsverantwoordelijke (en de vraag of er tussen hen een band bestaat), om de aard van de dienst, het kader waarin de persoonsgegevens werden verzameld, de bron waaruit de gegevens werden verzameld (bv. de website of de dienst waar de persoonsgegevens werden verzameld en de privacy-instellingen die zij bieden), om de mogelijke verdere toepassingen van het model, en om de vraag of de betrokkenen feitelijk weten dat hun persoonsgegevens überhaupt online staan.
94. Tijdens de ontwikkelingsfase van het model kunnen de redelijke verwachtingen van de betrokkenen verschillen naargelang van de vraag of de gegevens die worden verwerkt om het model te ontwikkelen door de betrokkenen al dan niet openbaar worden gemaakt. Daarnaast kunnen de redelijke verwachtingen ook verschillen naargelang van de vraag of zij de gegevens rechtstreeks aan de verwerkingsverantwoordelijke hebben verstrekt (bv. in het kader van hun gebruik van de dienst), of dat de verwerkingsverantwoordelijke ze uit een andere bron heeft verkregen (bv. via een derde of door middel van scraping). In beide gevallen moeten bij het beoordelen van de redelijke verwachtingen de stappen worden onderzocht die zijn ondernomen om de betrokkenen over de verwerkingsactiviteiten te informeren.
95. In de inzetfase van het AI-model is het ook van belang om de redelijke verwachtingen van de betrokkenen te onderzoeken in het kader van de specifieke mogelijkheden van het model. Voor AI-modellen die zich kunnen aanpassen op basis van de verstrekte input kan het bijvoorbeeld relevant zijn om te onderzoeken of de betrokkenen wisten dat zij persoonsgegevens hadden verstrekt om de antwoorden van het AI-model te kunnen laten afstemmen op hun behoeften en om diensten op maat geleverd te kunnen krijgen. Daarnaast kan het ook relevant zijn om te onderzoeken of deze

⁷³ Zo meende het Hof in het arrest van 4 juli 2023, *Meta/Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, punt 123, weliswaar dat “productverbetering” in beginsel niet als gerechtvaardigd belang kan worden uitgesloten, maar oordeelde het ook dat het “*twijfelachtig [is] of het doel van productverbetering, gelet op de omvang van de verwerking en de ingrijpende gevolgen ervan voor de gebruiker, alsook op de omstandigheid dat deze laatste er redelijkerwijs geen rekening mee hoeft te houden dat die gegevens [...] worden verwerkt, zwaarder kan wegen dan de belangen en grondrechten van die gebruiker, vooral wanneer het daarbij om een kind gaat*”.

⁷⁴ Richtsnoeren 1/2024 voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 53.

⁷⁵ Richtsnoeren 1/2024 voor de verwerking van persoonsgegevens op grond van artikel 6, lid 54, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punten 50 tot en met 54.

verwerkingsactiviteit alleen van invloed is op de dienst die voor de betrokkenen wordt verricht (bv. het personaliseren van inhoud voor een specifieke gebruiker) of ook wordt gebruikt voor aanpassingen aan de dienst die aan alle klanten wordt aangeboden (bv. om het model in algemene zin te verbeteren). Net als in de ontwikkelingsfase kan het ook hier bijzonder relevant zijn om te onderzoeken of er een rechtstreekse relatie is tussen de betrokkenen en de verwerkingsverantwoordelijke. Als zo'n rechtstreekse relatie bestaat, dan kan de verwerkingsverantwoordelijke de betrokkenen gemakkelijk informatie verstrekken over de verwerkingsactiviteit en het model, hetgeen vervolgens van invloed kan zijn op de redelijke verwachtingen van die betrokkenen.

Verzachtende maatregelen

96. Wanneer de belangen, rechten en vrijheden van betrokkenen zwaarder lijken te wegen dan het (de) door de verwerkingsverantwoordelijke of een derde nagestreefde gerechtvaardigde belang(en), dan kan de verwerkingsverantwoordelijke overwegen om verzachtende maatregelen te nemen om de gevolgen van de verwerking voor deze betrokkenen te beperken. Verzachtende maatregelen zijn waarborgen die moeten worden afgestemd op de omstandigheden van het geval en die van verschillende factoren afhangen, waaronder het beoogde gebruik van het AI-model. Deze verzachtende maatregelen moeten waarborgen dat er geen andere zaken zwaarder wegen dan de belangen van de verwerkingsverantwoordelijke of de derde, zodat de verwerkingsverantwoordelijke deze rechtsgrondslag kan gebruiken.
97. Zoals aangegeven in de richtsnoeren van het EDPB over het gerechtvaardigd belang, mogen verzachtende maatregelen niet worden verward met de maatregelen die de verwerkingsverantwoordelijke hoe dan ook wettelijk verplicht is te nemen om de naleving van de AVG te waarborgen, ongeacht of de verwerking plaatsvindt op grond van artikel 6, lid 1, punt f), AVG⁷⁶. Dit is met name van belang voor maatregelen die bijvoorbeeld verplicht zijn om aan de beginselen van de AVG te voldoen, waaronder het beginsel van minimale gegevensverwerking.
98. Onderstaande lijst van maatregelen is niet-uitputtend en niet-bindend, en de uitvoering van de maatregelen moet per geval worden beoordeeld. Hoewel, afhankelijk van de omstandigheden, enkele van de hierna genoemde maatregelen verplicht kunnen zijn om aan specifieke verplichtingen uit de AVG te voldoen, kunnen zij wanneer dit niet het geval is in aanmerking worden genomen als aanvullende waarborgen. Daarnaast hebben enkele van de hierna genoemde maatregelen betrekking op gebieden die aan snelle veranderingen onderhevig zijn en waarin veel nieuwe ontwikkelingen plaatsvinden, en moeten zij door de toezichthoudende autoriteiten in aanmerking worden genomen wanneer zij een specifiek geval behandelen.
99. **Met betrekking tot de ontwikkelingsfase van AI-modellen** kunnen verschillende maatregelen worden genomen om de risico's te beperken die zich voordoen bij de verwerking van zowel firstpartygegevens als gegevens van derden (ook om de risico's van webscraping te beperken). Op grond van het bovenstaande geeft het EDPB enkele voorbeelden van maatregelen die kunnen worden uitgevoerd om de in de afwegingstoets aangegeven risico's te beperken en die door de toezichthoudende autoriteiten in aanmerking moeten worden genomen wanneer zij specifieke AI-modellen per geval beoordelen.
100. **Technische maatregelen**
 - a. In punt 3.2.2 genoemde maatregelen die geschikt zijn om de desbetreffende risico's te beperken, wanneer zij niet leiden tot anonimisering van het model en niet vereist zijn om aan

⁷⁶ Richtsnoeren 1/2024 voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 57.

andere verplichtingen uit de AVG of de noodzakelijkheidstoets te voldoen (tweede stap van de beoordeling van het gerechtvaardigd belang).

101. Mogelijke andere relevante maatregelen:

- b. Pseudonimiseringsmaatregelen: hiertoe kunnen bijvoorbeeld maatregelen behoren om combinaties van gegevens op basis van individuele identificatoren te voorkomen. Deze maatregelen zijn wellicht niet passend wanneer de toezichthoudende autoriteit van mening is dat de verwerkingsverantwoordelijke heeft aangetoond dat het redelijkerwijs noodzakelijk is om verschillende gegevens over een bepaalde persoon te verzamelen voor de ontwikkeling van het desbetreffende AI-systeem of-model.
- c. Maatregelen om persoonsgegevens in de trainingsset te maskeren of te vervangen door fictieve persoonsgegevens (bv. de vervanging van namen en e-mailadressen door fictieve namen en fictieve e-mailadressen). Deze maatregel kan met name passend zijn wanneer de daadwerkelijke wezenlijke inhoud van de gegevens niet relevant is voor de algehele verwerking (bv. bij het trainen van LLM).

102. **Maatregelen die het personen gemakkelijker maken om hun rechten uit te oefenen**

- a. Aanhouden van een redelijke termijn tussen het verzamelen van een trainingsdataset en het gebruik ervan. Door deze aanvullende waarborg kunnen betrokkenen hun rechten gedurende deze termijn uitoefenen, waarbij de lengte van de redelijke termijn wordt getoetst aan de omstandigheden van elk geval.
- b. Vanaf het begin aanbieden van een onvoorwaardelijk “opt-out”, bijvoorbeeld door betrokkenen nog voor de verwerking plaatsvindt een discretionair recht te geven om bezwaar te maken, teneinde de zeggenschap van personen over hun gegevens te vergroten en daarbij verder te gaan dan hetgeen is bepaald in artikel 21 AVG⁷⁷.
- c. De betrokkenen toestaan om hun recht op gegevenswissing ook uit te oefenen wanneer de specifieke gronden van artikel 17, lid 1, AVG niet van toepassing zijn⁷⁸.
- d. De betrokkenen toestaan om claims in te dienen over het teruglekken of memoriseren van persoonsgegevens en de omstandigheden en middelen waarmee de claims kunnen worden gereproduceerd, zodat de verwerkingsverantwoordelijken relevante afleertechnieken kunnen reproduceren en beoordelen om de claims op te lossen.

103. **Transparantiemaatregelen:** in sommige gevallen kunnen verzachtende maatregelen ook maatregelen omvatten die tot meer transparantie over de ontwikkeling van het AI-model leiden. Sommige maatregelen kunnen niet alleen zinvol zijn met het oog op de naleving van de verplichtingen uit de AVG, maar ook om de informatieasymmetrie te ondervangen en de betrokkenen beter inzicht te geven in de verwerking in de ontwikkelingsfase:

- a. Uitbrengen van openbare en toegankelijke berichten die verder gaan dan de informatie die op grond van artikel 13 of artikel 14 AVG verplicht is, bijvoorbeeld met meer informatie over de criteria voor het verzamelen en alle gebruikte datasets, rekening houdend met de speciale bescherming voor kinderen en kwetsbare personen.
- b. Andere manieren om de betrokkenen te informeren, bijvoorbeeld mediacampagnes in verschillende media om betrokkenen te informeren, informatiecampagnes per e-mail, het

⁷⁷ Ibid.

⁷⁸ Ibid.

gebruik van infographics, rubrieken met veel gestelde vragen, transparantiekeurmerken en kaarten van het model die zodanig zijn opgezet dat zij de presentatie van informatie over AI-modellen kunnen structureren, naast vrijwillige jaarlijkse transparantierapporten.

104. **Specifieke verzachtende maatregelen bij webscraping:** omdat, zoals reeds aangegeven, bij webscraping specifieke risico's ontstaan ⁷⁹, kunnen in dit verband specifieke risicobeperkende maatregelen worden omschreven. Indien relevant kunnen zij door de toezichthoudende autoriteiten in aanvulling op bovengenoemde verzachtende maatregelen worden beoordeeld bij het onderzoek van verwerkingsverantwoordelijken die webscraping toepassen.
105. Wanneer geen specifieke maatregelen noodzakelijk zijn in het kader van de tweede stap van de beoordeling van het gerechtvaardigd belang, kunnen dergelijke maatregelen nuttig blijken om het risico bij webscraping te beperken. Daarbij kan het bijvoorbeeld gaan om de volgende **technische maatregelen**:
- a. Geen gegevensinhoud in publicaties opnemen als zich daarin mogelijk persoonsgegevens bevinden die risico's vormen voor specifieke personen of groepen personen (bv. mensen die de kans lopen op misbruik, schade of zelfs letsel als de informatie openbaar zou worden).
 - b. Waarborgen dat bepaalde categorieën gegevens niet worden verzameld of dat bepaalde bronnen bij het verzamelen van gegevens worden uitgesloten, bijvoorbeeld door het uitsluiten van bepaalde websites die bijzonder indringend zijn door de gevoeligheid van hun onderwerpen.
 - c. Geen gegevens verzamelen op websites (of delen van websites) die duidelijk bezwaar maken tegen webscraping en hergebruik van hun inhoud voor het opbouwen van AI-trainingsdatabases (bijvoorbeeld door rekening te houden met robots.txt- of ai.txt-bestanden of andere erkende methodes om aan te geven dat geen automatische crawling of scraping mag plaatsvinden).
 - d. Voorschrijven van andere relevante beperkingen aan het verzamelen van gegevens, mogelijk met periodegebonden criteria.
106. Bij webscraping kunnen onder meer de volgende specifieke maatregelen worden genomen **om transparantie en de uitoefening van rechten door personen te vergemakkelijken**: het aanleggen van een door de verwerkingsverantwoordelijke beheerde opt-outlijst die betrokkenen de mogelijkheid biedt om bezwaar te maken tegen het verzamelen van hun gegevens op bepaalde websites of onlineplatforms, door informatie te verstrekken waarmee zij op die websites kunnen worden geïdentificeerd, ook voordat er gegevens worden verzameld⁸⁰.
107. **Specifieke overwegingen met betrekking tot verzachtende maatregelen in de inzetfase:** Hoewel sommige van de bovengenoemde maatregelen afhankelijk van de omstandigheden ook relevant kunnen zijn voor de inzetfase, geeft het EDPB hierna een niet-uitputtende lijst met aanvullende

⁷⁹ Bij deze praktijken kunnen ook andere vraagstukken ontstaan die buiten het bestek van dit advies vallen; zie bijvoorbeeld Pagallo, U., Ciani Sciolla, J., *Anatomy of web data scraping: ethics, standards, and the troubles of the law*. European Journal of Privacy Law & Technologies, (2023) 2 blz. 1-19, beschikbaar op <https://doi.org/10.57230/EJPLT232PS>.

⁸⁰ Tenzij de verwerkingsverantwoordelijke dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsovereenkomst.

ondersteunende maatregelen die kunnen worden genomen en door de toezichthoudende autoriteiten per geval moeten worden beoordeeld.

- a. **Technische maatregelen** kunnen bijvoorbeeld worden genomen om het opslaan, terugleken of genereren van persoonsgegevens te voorkomen, met name in het kader van generatieve AI-modellen (waaronder outputfilters) en/of om het risico van onrechtmatig hergebruik door AI-modellen voor algemeen gebruik te beperken (bv. digitale watermerken in door AI gegenereerde output).
 - b. **Maatregelen die de uitoefening van de rechten van personen vergemakkelijken of versnellen** in de inzetfase en verder gaan dan wat wettelijk vereist is, met name ten aanzien van onder meer, maar niet uitsluitend, de uitoefening van het recht op wissing van persoonsgegevens uit outputgegevens van modellen of ontduubeling, in combinatie met natraintechieken die worden toegepast om te trachten persoonsgegevens te verwijderen of te onderdrukken.
108. Bij onderzoek naar de inzet van een specifiek AI-model moeten de toezichthoudende autoriteiten nagaan of de verwerkingsverantwoordelijke de door hem uitgevoerde afwegingstoets heeft gepubliceerd, omdat daarmee transparantie en behoorlijkheid kunnen worden vergroot. Zoals aangegeven in de richtsnoeren van het EDPB over het gerechtvaardigd belang, kunnen andere maatregelen worden overwogen om betrokkenen nog voordat persoonsgegevens worden verzameld te voorzien van informatie uit de afwegingstoets⁸¹. Daarnaast herhaalt het EDPB⁸² dat onderzocht moet worden of de verwerkingsverantwoordelijke in voorkomend geval de functionaris voor gegevensbescherming heeft ingeschakeld.

3.4 Mogelijke gevolgen van onrechtmatige verwerking bij de ontwikkeling van een AI-model voor de rechtmatigheid van de latere verwerking of het latere gebruik van het AI-model

109. In dit onderdeel van het advies wordt ingegaan op vraag 4 uit het verzoek. Hierbij gaat het om verduidelijking van de mogelijke gevolgen van onrechtmatige verwerking in de ontwikkelingsfase voor de latere verwerking (bijvoorbeeld tijdens de inzetfase van het AI-model) of voor het gebruik van het model. De vraag heeft betrekking op zowel de situatie waarin een dergelijk AI-model persoonsgegevens verwerkt die in het model zijn opgenomen (vraag 4, i), uit het verzoek) als op de situatie waarin bij de inzet van het AI-model geen sprake meer is van verwerking van persoonsgegevens (en het model dus anoniem is) (vraag 4, ii), uit het verzoek).
110. Voordat het op enkele specifieke scenario's ingaat, maakt het EDPB de volgende algemene opmerkingen.
111. Ten eerste zullen de verduidelijkingen in dit deel betrekking hebben op de verwerking van persoonsgegevens tijdens de ontwikkelingsfase terwijl niet wordt voldaan aan het beginsel van rechtmatigheid zoals specifiek uiteengezet in artikel 5, lid 1, punt a), AVG en artikel 6 AVG (hierna "**onrechtmatigheid**" genoemd)⁸³. In dezelfde zin zullen de overwegingen van het EDPB zich richten op

⁸¹ Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 68.

⁸² Richtsnoeren 1/2024 van het EDPB voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt f), AVG, versie 1.0, vastgesteld op 8 oktober 2024, punt 12.

⁸³ Arrest van het Hof van 4 mei 2023, *Bundesrepublik Deutschland*, C-60/22, ECLI:EU:C:2023:373, punten 55, 56 en 57.

de gevolgen van de onrechtmatigheid van de verwerking tijdens de ontwikkelingsfase voor de rechtmatigheid (d.w.z. de naleving van artikel 5, lid 1, punt a), AVG en artikel 6 AVG) van de latere verwerking of het latere gebruik van het model. Het EDPB wijst er echter op dat er bij verwerking in de ontwikkelingsfase ook inbreuk kan worden gemaakt op andere bepalingen uit de AVG, waaronder het gebrek aan transparantie jegens betrokkenen, of gegevensbescherming door ontwerp en/of door standaardinstellingen, die buiten het bestek van dit advies vallen.

112. Ten tweede is in de beantwoording van deze vraag een belangrijke rol weggelegd voor het verantwoordingsbeginsel, dat inhoudt dat verwerkingsverantwoordelijken verantwoordelijk zijn voor, en de naleving moeten aantonen van onder andere artikel 5, lid 1, AVG en artikel 6 AVG⁸⁴. Dat geldt ook voor de noodzaak om te beoordelen welke organisatie een verwerkingsverantwoordelijke is voor de desbetreffende verwerkingsactiviteit en de vraag of er situaties ontstaan met een gezamenlijke verwerkingsverantwoordelijkheid (omdat zij onlosmakelijk verbonden zijn)⁸⁵. Gezien het belang van de feitelijke omstandigheden van elk geval, onder meer als het gaat om de rol van elke betrokken partij bij de verwerking, moeten de overwegingen van het EDPB worden opgevat als algemene opmerkingen die per geval door de toezichthoudende autoriteiten moeten worden getoetst.
113. In de derde plaats wijst het EDPB erop dat de toezichthoudende autoriteiten, overeenkomstig artikel 51, lid 1, AVG *“verantwoordelijk zijn voor het toezicht op de toepassing van [de AVG], teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de verwerking van hun persoonsgegevens te beschermen en het vrije verkeer van persoonsgegevens binnen de Unie te vergemakkelijken”*. Derhalve zijn de toezichthoudende autoriteiten bevoegd om de rechtmatigheid van de verwerking te beoordelen en om hun bevoegdheden uit hoofde van de AVG uit te oefenen overeenkomstig het kader van hun interne recht⁸⁶. In die gevallen beschikken de toezichthoudende autoriteiten over discretionaire bevoegdheden om de mogelijke inbreuk(en) te beoordelen en passende, noodzakelijke en evenredige maatregelen te kiezen uit de in artikel 58 AVG genoemde maatregelen, rekening houdend met de omstandigheden van elk individueel geval⁸⁷.
114. **Wanneer een inbreuk wordt vastgesteld, kunnen de toezichthoudende autoriteiten corrigerende maatregelen opleggen en bijvoorbeeld de verwerkingsverantwoordelijken, rekening houdend met de omstandigheden van elk geval, opdragen om maatregelen te nemen om de onrechtmatigheid van de aanvankelijke verwerking weg te nemen.** Voorbeelden van dergelijke maatregelen zijn het opleggen van een boete, het voorschrijven van een tijdelijke beperking van de verwerking, het wissen van een deel van de onrechtmatig verwerkte dataset of, indien dat niet mogelijk is, afhankelijk van de feiten, gelet op de evenredigheid van de maatregel, de opdracht om de gehele dataset die is gebruikt om het AI-model te ontwikkelen en/of het AI-model zelf te wissen. Bij hun beoordeling van de evenredigheid van de beoogde maatregelen kunnen de toezichthoudende autoriteiten rekening

⁸⁴ Arrest van het Hof van 4 mei 2023, *Bundesrepublik Deutschland*, C-60/22, ECLI:EU:C:2023:373, punt 53.

⁸⁵ Richtsnoeren 7/2020 van het EDPB over de begrippen “verwerkingsverantwoordelijke” en “verwerker” in de AVG, versie 2.1, vastgesteld op 7 juli 2021, punt 55.

⁸⁶ Mogelijk moet rekening worden gehouden met specifieke nationale regels. Zie bijvoorbeeld artikel 2 decies van de Italiaanse wet Gegevensbescherming (wetsbesluit 196/2003), waarin wordt bepaald dat geen gebruik mag worden gemaakt van de gegevens die in strijd met de voorschriften voor gegevensbescherming zijn verwerkt. Dit laat andere interne rechtskaders, waaronder het strafrecht, onverlet.

⁸⁷ Zie in dit verband overweging 129 AVG en het arrest van het Hof van 26 september 2024, *TR/Land Hessen*, C-768-21, ECLI:EU:C:2024:785, punt 37, het arrest van het Hof van 7 december 2023, *SCHUFA Holding* (Kwijtschelding van restschulden), in de gevoegde zaken C-26/22 en C-64/22, ECLI:EU:C:2023:958, punt 57 en het arrest van het Hof van 14 maart 2024, *Újpesti Polgármesteri Hivatal*, C-46/23, ECLI:EU:C:2024:239, punt 34.

houden met maatregelen die door de verwerkingsverantwoordelijke kunnen worden toegepast om de onrechtmatigheid van de eerste verwerking te herstellen (bv. hertraining).

115. Voor het geval persoonsgegevens onrechtmatig worden verwerkt, wijst het EDPB er ook op dat betrokkenen met inachtneming van de voorwaarden uit artikel 17 AVG om wissing van hun persoonsgegevens kunnen vragen, en dat de toezichthoudende autoriteiten kunnen bevelen dat de persoonsgegevens ambtshalve worden gewist⁸⁸.
116. Wanneer zij beoordelen of een maatregel passend, noodzakelijk en evenredig is, kunnen de toezichthoudende autoriteiten onder meer kijken naar de risico's die voor de betrokkenen ontstaan, de ernst van de inbreuk, de technische en financiële haalbaarheid van de maatregel en naar het desbetreffende volume aan persoonsgegevens.
117. Tot slot wijst het EDPB erop dat de maatregelen die door de toezichthoudende autoriteiten krachtens de AVG worden genomen de maatregelen van de bevoegde autoriteiten krachtens de AI-verordening en/of andere toepasselijke rechtskaders onverlet laten (bv. wetgeving over civielrechtelijke aansprakelijkheid).
118. In de navolgende paragrafen gaat het EDPB in op drie scenario's waarop vraag 4 uit het verzoek van toepassing is, waarbij de verschillen zijn gelegen in de vraag of de persoonsgegevens die worden verwerkt om het model te ontwikkelen in het model worden bewaard, en/of de latere verwerking plaatsvindt door dezelfde of door een andere verwerkingsverantwoordelijke.

3.4.1 Scenario 1. Een verwerkingsverantwoordelijke verwerkt op onrechtmatige wijze persoonsgegevens om het model te ontwikkelen, de persoonsgegevens worden in het model bewaard en worden vervolgens door dezelfde verwerkingsverantwoordelijke verwerkt (bijvoorbeeld in het kader van de inzet van het model)

119. Dit scenario houdt verband met vraag 4, i), van het verzoek, wanneer een verwerkingsverantwoordelijke op onrechtmatige wijze persoonsgegevens verwerkt (d.w.z. zonder te voldoen aan de vereisten van artikel 5, lid 1, punt a), AVG en artikel 6 AVG) om een AI-model te ontwikkelen en in het AI-model informatie aanwezig is over een geïdentificeerde of identificeerbare natuurlijke persoon, waardoor het model niet anoniem is. Vervolgens worden de persoonsgegevens verwerkt door dezelfde verwerkingsverantwoordelijke (bijvoorbeeld in het kader van de inzet van het model). Ten aanzien van dit scenario overweegt het EDPB het volgende.
120. De bevoegdheid van de toezichthoudende autoriteit om corrigerende maatregelen op te leggen ten aanzien van de eerste verwerking (zoals hiervoor uiteengezet in de punten 113, 114, en 115) heeft in beginsel gevolgen voor de latere verwerking (als de toezichthoudende autoriteit de verwerkingsverantwoordelijke bijvoorbeeld beveelt om de onrechtmatig verwerkte persoonsgegevens te wissen, zou deze laatste de persoonsgegevens waarvoor de maatregel geldt als gevolg van die maatregel later niet meer kunnen verwerken).
121. Specifiek ten aanzien van de gevolgen van de onrechtmatige verwerking in de ontwikkelingsfase voor de latere verwerking (bijvoorbeeld tijdens de inzetfase) wijst het EDPB erop dat de toezichthoudende

⁸⁸ Zie in dit verband Advies 39/2021 van het EDPB over de vraag of artikel 58, lid 2, punt g), AVG voor een toezichthoudende autoriteit als rechtsgrondslag kan dienen om ambtshalve te bevelen dat persoonsgegevens worden gewist wanneer een dergelijk verzoek niet door de betrokkene is ingediend, punt 28. Zie in dit verband ook het arrest van het Hof van 14 maart 2024, *Újpesti Polgármesteri Hivatal*, C-46/23, ECLI:EU:C:2024:239, punt 42.

autoriteiten elk geval afzonderlijk moeten onderzoeken en daarbij rekening moeten houden met de specifieke omstandigheden van elk geval.

122. **Of bij de ontwikkeling en de inzet sprake is van aparte doeleinden (en dus van aparte verwerkingsactiviteiten) en in hoeverre het ontbreken van een rechtsgrondslag voor de eerste verwerkingsactiviteit gevolgen heeft voor de rechtmatigheid van de latere verwerking moet per geval op basis van de omstandigheden worden beoordeeld.**
123. Wanneer de latere verwerking plaatsvindt op grond van een gerechtvaardigd belang, moet bijvoorbeeld specifiek met betrekking tot de rechtsgrondslag van artikel 6, lid 1, punt f), AVG het feit dat de eerste verwerking onrechtmatig was in aanmerking worden genomen bij de beoordeling van het gerechtvaardigde belang (bv. als het gaat om de risico's voor betrokkenen of het feit dat betrokkenen die latere verwerking wellicht niet verwachten). In die gevallen kan de onrechtmatigheid van de verwerking tijdens de ontwikkelingsfase gevolgen hebben voor de rechtmatigheid van de latere verwerking.

3.4.2 Scenario 2. Een verwerkingsverantwoordelijke verwerkt op onrechtmatige wijze persoonsgegevens om het model te ontwikkelen, de persoonsgegevens worden in het model bewaard en worden door een andere verwerkingsverantwoordelijke verwerkt in het kader van de inzet van het model.

124. Dit scenario houdt verband met vraag 4, i), van het verzoek. Het verschilt van scenario 1 (in punt 3.4.1 van dit advies) omdat de persoonsgegevens later door een andere verwerkingsverantwoordelijke worden verwerkt in het kader van de inzet van het AI-model.
125. Het EDPB wijst erop dat de vaststelling van de in het kader van gegevensbescherming aan deze verschillende partijen toegewezen rollen een wezenlijke stap is bij de inventarisatie van de verplichtingen die krachtens de AVG van toepassing zijn en de identificatie van degene die voor die verplichtingen verantwoordelijk is, en dat situaties met gezamenlijke verwerkingsverantwoordelijken ook moeten worden onderzocht bij de beoordeling van de verantwoordelijkheden die elke partij uit hoofde van de AVG heeft. De navolgende opmerkingen moeten daarom worden beschouwd als algemene aspecten waarmee in voorkomend geval door de toezichthoudende autoriteiten rekening moet worden gehouden. Ten aanzien van dit scenario 2 overweegt het EDPB het volgende.
126. Ten eerste moet worden opgemerkt dat volgens artikel 5, lid 1, punt a), AVG, gezien in het licht van artikel 5, lid 2, AVG elke verwerkingsverantwoordelijke de rechtmatigheid moet waarborgen van de verwerking die hij uitvoert en dat hij deze moet kunnen aantonen. Derhalve moeten de toezichthoudende autoriteiten de rechtmatigheid beoordelen van de verwerking door i) de verwerkingsverantwoordelijke die het AI-model oorspronkelijk heeft ontwikkeld; en ii) de verwerkingsverantwoordelijke die het AI-model heeft gekocht en zelf de persoonsgegevens verwerkt.
127. In de tweede plaats zijn de overwegingen uit de bovenstaande punten 113, 114 en 115 in dit geval relevant, gelet op de bevoegdheid van de toezichthoudende autoriteiten om op te treden in verband met de eerste verwerking. Artikel 17, lid 1, punt d), AVG (wissing van onrechtmatig verwerkte gegevens) en artikel 19 AVG (kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking) kunnen, afhankelijk van de omstandigheden van het geval, in dit verband ook van toepassing zijn, bijvoorbeeld met betrekking tot de verplichte kennisgeving door de verwerkingsverantwoordelijke die het model ontwikkelt aan de verwerkingsverantwoordelijke die het model inzet.

128. In de derde plaats moet met betrekking tot de mogelijke gevolgen van de onrechtmatigheid van de eerste verwerking voor de latere verwerking door een andere verwerkingsverantwoordelijke die beoordeling per geval door de toezichthoudende autoriteiten worden gemaakt.
129. **De toezichthoudende autoriteiten moeten in aanmerking nemen of de verwerkingsverantwoordelijke die het model inzet in het kader van zijn verantwoordingsplicht⁸⁹ om de naleving van artikel 5, lid 1, punt a), en artikel 6 AVG aan te tonen een passende beoordeling heeft uitgevoerd om vast te stellen of het AI-model niet is ontwikkeld door onrechtmatige verwerking van persoonsgegevens.** Bij die beoordeling moeten de toezichthoudende autoriteiten rekening houden met de vraag of de verwerkingsverantwoordelijke een aantal niet-uitputtende criteria heeft getoetst, waaronder de bron van de gegevens en de vraag of het AI-model voortkomt uit een inbreuk op de AVG, met name wanneer een toezichthoudende autoriteit of een rechtbank die inbreuk heeft vastgesteld, zodat de verwerkingsverantwoordelijke die het model inzet wel moest weten dat de eerste verwerking onrechtmatig is geweest.
130. De verwerkingsverantwoordelijke moet bijvoorbeeld onderzoeken of de gegevens afkomstig zijn van een inbreuk in verband met persoonsgegevens of dat door een toezichthoudende autoriteit of een rechtbank is vastgesteld dat bij de verwerking sprake is geweest van een inbreuk. **De kwaliteit van de beoordeling die de verwerkingsverantwoordelijke verricht en de door de toezichthoudende autoriteiten verwachte uitvoerigheid kunnen van diverse factoren afhangen, waaronder het type en de ernst van de risico's die ontstaan door de verwerking in het AI-model tijdens de inzet ervan voor de betrokkenen van wie gegevens zijn gebruikt om het model te ontwikkelen.**
131. Het EDPB merkt op dat aanbieders van AI-systemen met een hoog risico in de AI-verordening worden verplicht om een EU-conformiteitsverklaring op te stellen⁹⁰, en dat in die verklaring moet worden aangegeven dat het desbetreffende AI-systeem voldoet aan het gegevensbeschermingsrecht van de EU⁹¹. Het EDPB merkt op dat de naleving van de AVG met een dergelijke eigen verklaring niet op overtuigende wijze kan worden vastgesteld. De toezichthoudende autoriteiten kunnen er echter wel rekening mee houden wanneer zij een specifiek AI-model onderzoeken.
132. De overwegingen uit bovenstaand punt 123 zijn ook in dit geval van toepassing. Wanneer de toezichthoudende autoriteiten nagaan of, en op welke wijze de verwerkingsverantwoordelijke heeft geverifieerd in hoeverre een gerechtvaardigd belang passend is als rechtsgrondslag voor de door hem uitgevoerde verwerking, moet de onrechtmatigheid van de eerste verwerking in aanmerking worden genomen bij de beoordeling van het gerechtvaardigde belang, bijvoorbeeld door de risico's te beoordelen die kunnen ontstaan voor de betrokkenen van wie persoonsgegevens onrechtmatig zijn verwerkt bij de ontwikkeling van het model. Verschillende aspecten van technische aard (bv. het bestaan van tijdens de ontwikkeling van het model aangebrachte filters of toegangsbeperkingen die de latere verwerkingsverantwoordelijke niet kan omzeilen of beïnvloeden, en die de toegang tot, of de verstrekking van persoonsgegevens kunnen voorkomen) of van juridische aard (bv. de aard en de ernst van de onrechtmatigheid van de eerste verwerking) moeten in het kader van de afwegingstoets naar behoren worden onderzocht.

⁸⁹ Artikel 5, lid 2, AVG en artikel 24 AVG.

⁹⁰ Artikel 16, punt g), en artikel 47 van de AI-verordening.

⁹¹ Bijlage V, punt 5, bij de AI-verordening.

3.4.3 Scenario 3. Een verwerkingsverantwoordelijke verwerkt op onrechtmatige wijze persoonsgegevens bij de ontwikkeling van het AI-model en waarborgt vervolgens dat het model wordt geanonimiseerd, voordat dezelfde of een andere verwerkingsverantwoordelijke in het kader van de inzet een andere verwerking van persoonsgegevens begint

133. Dit scenario houdt verband met vraag 4, ii), van het verzoek en gaat over een geval waarin een verwerkingsverantwoordelijke op onrechtmatige wijze persoonsgegevens verwerkt voor de ontwikkeling van het AI-model, maar daarbij waarborgt dat de persoonsgegevens worden geanonimiseerd voordat dezelfde of een andere verwerkingsverantwoordelijke een andere verwerking van de persoonsgegevens in het kader van de inzet begint. Ten eerste wijst het EDPB erop dat de toezichthoudende autoriteiten bevoegd zijn en mogen optreden ten aanzien van de verwerking in verband met de anonimisering van het model, en ten aanzien van de verwerking die plaatsvindt tijdens de ontwikkelingsfase. Afhankelijk van de specifieke omstandigheden van het geval mogen de toezichthoudende autoriteiten dus corrigerende maatregelen opleggen wegens deze eerste verwerking (zoals uiteengezet in de bovenstaande punten 113, 114 en 115).
134. Als kan worden aangetoond dat bij het latere gebruik van het AI-model geen persoonsgegevens worden verwerkt, is het EDPB van mening dat de AVG niet van toepassing is⁹². De onrechtmatigheid van de eerste verwerking heeft dan dus geen gevolgen voor het latere gebruik van het model. Het EDPB benadrukt echter dat de enkele verklaring dat het model anoniem is niet volstaat om het aan de toepassing van de AVG te onttrekken, en merkt op dat de toezichthoudende autoriteiten bij hun beoordeling per geval rekening moeten houden met de overwegingen van het EDPB ten aanzien van vraag 1 uit het verzoek.
135. **Wanneer de verwerkingsverantwoordelijken vervolgens persoonsgegevens verwerken die gedurende de inzetfase zijn verzameld, nadat het model is geanonimiseerd, is voor deze verwerkingsactiviteiten de AVG van toepassing. Voor deze gevallen mag met betrekking tot de AVG de rechtmatigheid van de verwerking tijdens de inzetfase geen gevolgen ondervinden van de onrechtmatigheid van de eerste verwerking.**

4 Slotopmerkingen

136. Dit advies is gericht tot alle toezichthoudende autoriteiten en wordt bekendgemaakt op grond van artikel 64, lid 5, punt b), AVG.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

Anu Talus

⁹² Overweging 26 AVG.