



Groep gegevensbescherming artikel 29
Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679.

Vastgesteld op 28 november 2017.

Laatstelijk herzien en vastgesteld op 10 april 2018.

DE GROEP VOOR BESCHERMING VAN PERSONEN IN VERBAND MET DE
VERWERKING VAN PERSOONS GEGEVENS

Ingesteld bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995,

Gezien artikel 29 en 30 van die richtlijn,

Gezien het reglement van orde van de Groep,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD

De groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Het is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer, waarvan de taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG. Haar taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en artikel 15 van Richtlijn 2002/58/EG.

Het secretariaat wordt verzorgd door Directoraat C (grondrechten en burgerschap van de Unie) van het directoraat-generaal Justitie van de Europese Commissie, 1049 Brussel, België, kamer MO-59 02/013.

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Inhoud

1.	Inleiding	3
2.	Toestemming in artikel 4, lid 11 van de AVG	4
3.	Elementen van geldige toestemming	5
3.1.	Vrij/vrijelijk gegeven	5
3.1.1.	Wanverhouding	6
3.1.2.	Conditionaliteit	8
3.1.3.	Granulariteit	11
3.1.4.	Nadeel	12
3.2.	Specifiek	13
3.3.	Vaste	14
3.3.1.	De minimale inhoudelijke eisen voor het "geïnformeerd" zijn van toestemming	14
3.3.2.	Hoe moet informatie worden verstrekt?	15
3.4.	Ondubbelzinnige wilsuiting	17
4.	Het verkrijgen van de uitdrukkelijke toestemming	20
5.	Aanvullende voorwaarden voor het verkrijgen van geldige toestemming	23
5.1.	Toestemming aantonen	23
5.2.	Intrekken van toestemming	24
6.	Wisselwerking tussen toestemming en andere rechtsgronden in artikel 6 AVG	27
7.	Specifieke aandachtspunten in de AVG	27
7.1.	Kinderen (artikel 8)	27
7.1.1.	Dienst van de informatiemaatschappij	28
7.1.2.	Rechtstreeks aanbod aan een kind	29
7.1.3.	Leeftijd	29
7.1.4.	Toestemming van kinderen en ouderlijke verantwoordelijkheid	30
7.2.	Wetenschappelijk onderzoek	32
7.3.	De rechten van betrokkenen	35
8.	Toestemming verkregen krachtens Richtlijn 95/46/EG	35

1. Inleiding

Deze richtsnoeren verschaffen een gedegen analyse van het begrip 'toestemming' in Verordening 2016/679, de Algemene verordening gegevensbescherming (hierna: AVG). Het begrip 'toestemming' zoals gebruikt in de richtlijn gegevensbescherming (hierna: Richtlijn 95/46/EG) en in de huidige e-Privacy-richtlijn heeft zich ontwikkeld. De AVG geeft een nadere toelichting en specificatie van de vereisten voor het verkrijgen en aantonen van geldige toestemming. Deze richtsnoeren zijn gericht op deze veranderingen. Ze bieden een praktische leidraad om te zorgen voor naleving van de AVG en bouwen voort op Advies 15/2011 over de definitie van 'toestemming'. Verwerkingsverantwoordelijken moeten nieuwe oplossingen vinden die werken binnen het kader van de wetgeving en de bescherming van persoonsgegevens en de belangen van betrokkenen beter ondersteunen.

Toestemming blijft een van de zes rechtsgronden voor de verwerking van persoonsgegevens, zoals beschreven in artikel 6 van de AVG¹. Bij het opzetten van activiteiten die verwerking van persoonsgegevens omvatten, moet een verwerkingsverantwoordelijke altijd de tijd nemen om na te gaan wat een passende rechtsgrond is voor de geplande verwerking.

In het algemeen kan toestemming alleen een passende rechtsgrond zijn als aan een betrokkene controle en een werkelijke keuze worden geboden met betrekking tot het accepteren of afwijzen van de aangeboden voorwaarden of het afwijzen ervan zonder nadeel. Bij het vragen om toestemming heeft de verwerkingsverantwoordelijke de plicht om na te gaan of het verzoek voldoet aan alle vereisten voor het verkrijgen van rechtsgeldige toestemming. Indien de toestemming wordt verkregen met volledige naleving van de AVG, is toestemming een instrument dat betrokkenen controle geeft over het al dan niet verwerken van hun persoonsgegevens. Indien dit echter niet het geval is, dan is deze controle van de betrokkene slechts schijn, en een niet-rechtsgeldige grond voor verwerking, waardoor de verwerkingsactiviteiten onrechtmatig worden².

De bestaande adviezen over toestemming van de Groep gegevensbescherming artikel 29 (WP29)³ blijven relevant, voor zover ze verenigbaar zijn met het nieuwe wetgevingskader, omdat de bestaande richtsnoeren en algemene goede praktijken van WP29 in de AVG zijn vastgelegd, en het merendeel van de kernelementen van toestemming onder de AVG gelijk blijven. Daarom worden door WP29 in dit document eerdere adviezen over specifieke onderwerpen verder ontwikkeld en aangevuld, waaronder verwijzing naar toestemming krachtens Richtlijn 95/46/EG, en vormt dit document geen vervanging voor eerdere adviezen.

Zoals vermeld in Advies 15/2011 over de definitie van 'toestemming' moet het aan personen vragen om in te stemmen met een gegevensverwerking aan strenge eisen zijn onderworpen, omdat het

¹ Artikel 9 AVG verschaft een lijst van mogelijke uitzonderingen op het verbod op de verwerking van bijzondere categorieën gegevens. Een van deze uitzonderingen is de situatie waarin de betrokkene uitdrukkelijke toestemming verleent voor het gebruik van deze gegevens.

² Zie ook Advies 15/2011 over de definitie van 'toestemming' (WP 187), blz. 6-8, en/of Advies 06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG (WP 217), blz. 9, 10, 13 en 14.

³ En dit geldt met name voor Advies 15/2011 over de definitie van 'toestemming' (WP 187).

hierbij gaat om de grondrechten van betrokkenen, en de verwerkingsverantwoordelijke gegevensverwerking wil uitvoeren die zonder de toestemming van de betrokkene onrechtmatig zou zijn⁴. De cruciale rol van toestemming wordt onderstreept door de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie. Daarnaast vormt het verkrijgen van toestemming geen ontkrachting van, en doet geenszins afbreuk aan, de verplichting van de verwerkingsverantwoordelijke om de beginselen van verwerking die zijn vastgelegd in de AVG in acht te nemen, met name artikel 5 van de AVG met betrekking tot behoorlijkheid, noodzaak en evenredigheid, alsmede kwaliteit van gegevens. Zelfs indien de verwerking van persoonsgegevens is gebaseerd op de toestemming van de betrokkene, vormt dit geen legitimering voor het verzamelen van gegevens die niet noodzakelijk zijn in verband met een specifiek doel van verwerking, wat wezenlijk oneerlijk zou zijn⁵.

Ondertussen is WP29 zich bewust van de herziening van de e-Privacy-richtlijn (2002/58/EG). Het begrip toestemming in de ontwerp-verordening e-Privacy blijft gekoppeld aan het begrip 'toestemming' in de AVG⁶. Organisaties zullen op grond van de herziene e-Privacy-verordening waarschijnlijk toestemming nodig hebben voor de meeste online marketingberichten of marketinggesprekken en online traceermethodes, zoals door middel van cookies of apps of andere software. WP29 heeft reeds aanbevelingen en richtsnoeren verstrekt aan de Europese wetgever voor het voorstel voor een verordening inzake e-Privacy⁷.

Met betrekking tot de bestaande e-Privacy-richtlijn, merkt WP29 op dat verwijzingen naar de ingetrokken Richtlijn 95/46/EG moeten worden gelezen als verwijzingen naar de AVG⁸. Dit geldt ook voor verwijzingen naar toestemming in de huidige Richtlijn 2002/58/EG, omdat de e-Privacy-verordening op 25 mei 2018 (nog) niet van kracht is. Volgens artikel 95 AVG worden geen aanvullende verplichtingen opgelegd met betrekking tot verwerking in verband met het verstrekken van openbare elektronische communicatiediensten in openbare communicatienetwerken in de Unie, voor zover zij op grond van de e-Privacy-richtlijn onderworpen zijn aan specifieke verplichtingen met dezelfde doelstelling. WP29 merkt op dat de vereisten voor toestemming krachtens de AVG niet worden beschouwd als een "aanvullende verplichting", maar als randvoorwaarde voor rechtmatige verwerking. Daarom zijn de vereisten van de AVG voor het verkrijgen van geldige toestemming van toepassing in situaties die vallen binnen de werkingssfeer van de e-Privacy-richtlijn.

2. Toestemming in artikel 4, lid 11 van de AVG

Artikel 4, lid 11 van de AVG definieert toestemming als: *"elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een*

⁴ Advies 15/2011, pagina over de definitie van 'toestemming' (WP 187), blz. 8

⁵ Zie ook Advies 15/2011 over de definitie van 'toestemming' (WP 187), en artikel 5 AVG.

⁶ Op grond van artikel 9 van de voorgestelde e-Privacy-verordening, zijn de definitie van en de voorwaarden voor toestemming als bedoeld in artikel 4, punt 11, en artikel 7 van de AVG van toepassing.

⁷ Zie Advies 03/2016 over de beoordeling en toetsing van de e-Privacy-richtlijn (WP 240).

⁸ Zie artikel 94 AVG.

ondubbelzinnige actieve handeling hem of haar betreffende verwerking van persoonsgegevens aanvaardt."

Het basisconcept van toestemming blijft vergelijkbaar met het concept op grond van Richtlijn 95/46/EU, en toestemming is een van de rechtsgronden waarop verwerking van persoonsgegevens, op grond van artikel 6 van de AVG, moet zijn gebaseerd⁹. Naast de gewijzigde definitie in artikel 4, lid 11, verstrekt de AVG aanvullende richtsnoeren in artikel 7 en in de punten 32, 33, 42 en 43 over hoe de verwerkingsverantwoordelijke moet handelen om te voldoen aan de belangrijkste elementen van het vereiste van toestemming.

Ten slotte bevestigt het opnemen van specifieke bepalingen en overwegingen over de intrekking van toestemming dat toestemming een omkeerbaar besluit moet zijn, en dat de betrokkene een zekere mate van controle moet behouden.

3. Elementen van geldige toestemming

Artikel 4, lid 11 van de AVG bepaalt dat toestemming van de betrokkene het volgende betekent:

- vrije
- specifieke
- op informatie berustende en
- ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.

In de onderstaande hoofdstukken wordt geanalyseerd in hoeverre de formulering van artikel 4, lid 11 van verwerkingsverantwoordelijken vereist dat zij hun toestemmingsverzoeken/-formulieren wijzigen zodat naleving van de AVG wordt gewaarborgd¹⁰.

3.1. Vrij/vrijelijk gegeven¹¹

⁹ Toestemming werd in Richtlijn 95/46/EU gedefinieerd als "elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt" die "ondubbelzinnig moet worden gegeven" om ervoor te zorgen dat de verwerking van persoonsgegevens rechtmatig is (artikel 7, onder a van Richtlijn 95/46/EU)). Zie WP29 Advies 15/2011 over de definitie van "toestemming" (WP 187) voor voorbeelden van de toepasselijkheid van toestemming als rechtsgrond. In dit Advies heeft WP29 richtsnoeren verstrekt om onderscheid te maken tussen situaties waarin toestemming een passende rechtsgrond is en situaties waarin vertrouwen op de rechtsgrond van een gerechtvaardigd belang (misschien met een mogelijkheid tot opt-out) voldoende is, of een contractuele relatie zou worden aanbevolen. Zie ook WP29 Advies 06/2014, paragraaf III.1.2, blz. 14 en verder. Uitdrukkelijke toestemming is ook een van de uitzonderingen op het verbod op verwerking van speciale categorieën gegevens: Zie artikel 9 AVG.

¹⁰ Voor richtsnoeren ten aanzien van lopende verwerkingsactiviteiten op basis van toestemming in Richtlijn 95/46, zie hoofdstuk 7 van dit document en overweging 171 van de AVG.

¹¹ In diverse adviezen heeft de Groep gegevensbescherming artikel 29 de grenzen van toestemming in situaties waarin deze niet vrij kan worden gegeven onderzocht. Dit was met name het geval in haar Advies 15/2011 over de definitie van "toestemming" (WP187), het werkdocument inzake de verwerking van persoonsgegevens betreffende gezondheid in elektronische medische dossiers (WP131), Advies 8/2001 inzake de verwerking van persoonsgegevens in het kader van de arbeidsverhouding (WP48), en tweede advies 4/2009 over de Internationale Standaard van het Wereldantidopingagentschap (WADA) voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens,

Het element "vrij" impliceert werkelijke keuze en controle voor betrokkenen. Als algemene regel schrijft de AVG voor dat als een betrokkene geen werkelijke keuze heeft, zich gedwongen voelt om toestemming te geven of het voor hem negatieve gevolgen zal hebben als hij of zij niet toestemt, de toestemming niet geldig is¹². Indien toestemming wordt samengevoegd als een niet-onderhandelbaar onderdeel van voorwaarden, wordt deze verondersteld niet vrij gegeven te zijn. Bijgevolg wordt toestemming niet geacht vrij gegeven te zijn indien de betrokkene zijn of haar toestemming niet zonder nadelige gevolgen kan weigeren of intrekken¹³. De AVG besteedt ook aandacht aan het concept van een wanverhouding tussen de verwerkingsverantwoordelijke en de betrokkene.

Bij het beoordelen of toestemming vrij is gegeven, moet ook rekening worden gehouden met de specifieke situatie van het opnemen van toestemming in contracten of dienstverlening zoals beschreven in artikel 7, lid 4. Artikel 7, lid 4 is opgesteld op een niet-uitputtende wijze, wat blijkt uit de woorden "onder meer", wat betekent dat er wellicht een aantal andere situaties zijn waarop deze bepaling van toepassing is. In het algemeen maakt elk element dat ongepaste druk of invloed op de betrokkene inhoudt (dat op veel verschillende manieren tot uiting kan komen) waardoor een betrokkene zijn of haar vrije wil niet kan uitoefenen, de toestemming ongeldig.

[Voorbeeld 1]

Een mobiele app voor fotobewerking vraagt haar gebruikers om hun GPS-locatie te activeren voor het gebruik van haar diensten. De app deelt haar gebruikers ook mee dat zij de verzamelde gegevens zal gebruiken voor doeleinden van gerichte reclame op basis van surfgedrag (behavioural advertising). Zowel de geolocalisatie als de behavioural advertising zijn niet nodig voor het verstrekken van de fotobewerking-service, en vallen buiten de levering van de aangeboden kerndienst. Omdat gebruikers de app niet kunnen gebruiken zonder met deze doeleinden in te stemmen, kan de toestemming niet worden beschouwd als vrijelijk gegeven.

3.1.1. Wanverhouding

Overweging 43¹⁴ geeft duidelijk aan dat het onwaarschijnlijk is dat **overheidsinstanties** kunnen vertrouwen op toestemming voor verwerkingen, omdat in het geval de verwerkingsverantwoordelijke een overheidsinstantie is, er vaak een wanverhouding bestaat in de relatie tussen de betrokkene en de verwerkingsverantwoordelijke. Het is ook duidelijk dat in de meeste gevallen de betrokkene geen realistische alternatieven heeft voor het aanvaarden van de verwerking (voorwaarden) van deze verwerkingsverantwoordelijke. WP29 is van mening dat er andere rechtsgronden zijn die, in principe, meer geschikt zijn voor de activiteiten van overheidsinstanties¹⁵.

aanverwante bepalingen van de WADA-code en andere privacyvraagstukken in de context van de bestrijding van doping in de sport door het WADA en (nationale) antidopingorganisaties (WP162).

¹² Zie Advies 15/2011, pagina over de definitie van "toestemming" (WP187), blz. 12.

¹³ Zie overwegingen 42, 43 AVG en WP29 Advies 15/2011 over de definitie van "toestemming", vastgesteld op 13 juli 2011, (WP 187), blz. 12.

¹⁴ Overweging 43 van de AVG stelt: "Om ervoor te zorgen dat toestemming vrijelijk wordt verleend, mag toestemming geen geldige rechtsgrond zijn voor de verwerking van persoonsgegevens in een specifiek geval wanneer er sprake is van een duidelijke wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke, met name wanneer de verwerkingsverantwoordelijke een overheidsinstantie is, en dit het onwaarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk is verleend (...)"

¹⁵ Zie artikel 6, AVG, met name lid 1 onder c) en e).

Onverminderd deze algemene beschouwingen wordt het gebruik van toestemming als een rechtsgrond voor gegevensverwerking door overheidsinstanties in het wetgevingskader van de AVG niet volledig uitgesloten. De volgende voorbeelden laten zien dat het gebruik van toestemming onder bepaalde omstandigheden passend kan zijn.

[Voorbeeld 2] Een gemeente is van plan wegwerkzaamheden uit te voeren. Omdat wegwerkzaamheden het verkeer voor lange tijd kunnen verstoren, biedt de gemeente haar inwoners de gelegenheid om zich te abonneren op een mailinglijst om nieuws te ontvangen over de voortgang van de werkzaamheden en verwachte vertragingen. De gemeente maakt duidelijk dat deelname niet verplicht is, en vraagt om toestemming om de e-mailadressen te gebruiken (uitsluitend) voor dit doel. Inwoners die geen toestemming verlenen, lopen geen basisdiensten van de gemeente mis, en er wordt geen afbreuk gedaan aan de uitoefening van hun rechten, en zij zijn dus in staat om voor dit gebruik van gegevens vrijelijk hun toestemming te verlenen of te weigeren. Alle informatie over de wegwerkzaamheden zal ook beschikbaar zijn op de website van de gemeente.

[Voorbeeld 3] Een persoon die eigenaar is van een stuk land heeft bepaalde vergunningen nodig van zowel de gemeente als het provinciaal bestuur waaronder de gemeente valt. Beide overheidsorganen hebben dezelfde informatie nodig voor de afgifte van hun respectieve vergunning, maar ze hebben geen toegang tot elkaars databanken. Daarom vragen beiden om dezelfde informatie, en de landeigenaar stuurt haar gegevens naar beide overheidsorganen. De gemeente en de provinciale overheid vragen om haar toestemming om de dossiers samen te voegen, zodat dubbele procedures en correspondentie worden voorkomen. Beide overheidsinstanties verzekeren dat dit optioneel is, en dat de vergunningsaanvragen nog steeds afzonderlijk zullen worden verwerkt als ze besluit geen toestemming te verlenen met het samenvoegen van haar gegevens. De landeigenaar kan de overheidsinstanties vrijelijk toestemming verlenen voor het doel van het samenvoegen van de dossiers.

[Voorbeeld 4] Een openbare school vraagt leerlingen om toestemming om hun foto's te gebruiken in een gedrukte schoolkrant. Toestemming is in een dergelijke situatie een werkelijke keuze zolang leerlingen niet worden uitgesloten van onderwijs of diensten, en zonder enig nadeel hun toestemming voor het gebruik van deze foto's kunnen onthouden.¹⁶

Wanverhouding doet zich ook voor in het kader van de **arbeidsverhouding**¹⁷. Gezien de afhankelijkheid die het gevolg is van de relatie tussen werkgever en werknemer, is het onwaarschijnlijk dat de betrokkene zijn/haar toestemming voor gegevensverwerking zou kunnen onthouden zonder angst of reële dreiging van nadelige gevolgen als gevolg van een weigering. Het is onwaarschijnlijk dat de werknemer vrijelijk zou kunnen reageren op een verzoek voor toestemming van zijn/haar werkgever voor, bijvoorbeeld, het activeren van toezichtsystemen zoals camera observatie op de werkvloer, of het invullen van beoordelingsformulieren, zonder druk te voelen om toestemming te verlenen¹⁸. Daarom is WP29 van mening dat het voor werknemers

¹⁶ In het kader van dit voorbeeld, wordt onder openbare school verstaan een publiekelijk gefinancierde school of een onderwijsinstelling die op grond van nationaal recht kan worden beschouwd als een overheidsinstantie of overheidsorgaan.

¹⁷ Zie ook artikel 88 AVG, waarin de behoefte aan bescherming voor de specifieke belangen van werknemers wordt benadrukt en dat een mogelijkheid biedt om in het recht van de lidstaten uitzonderingsvoorwaarden op te nemen. Zie ook overweging 155.

¹⁸ Zie Advies 15/2011 over de definitie van "toestemming" (WP 187), blz. 12-14, Advies 8/2001 inzake de verwerking van persoonsgegevens in het kader van de arbeidsverhouding (WP 48), Hoofdstuk 10 10, Werkdocument over de controle op elektronische communicatie op het werk (WP 55), paragraaf 4.2 en Advies 2/2017 over gegevensbescherming op het werk (WP 249), paragraaf 6.2.

problematisch is om persoonsgegevens van huidige of toekomstige werknemers te verwerken op basis van toestemming, omdat het onwaarschijnlijk is dat deze vrijelijk wordt verleend. Voor de merendeel van dergelijke gegevensverwerking op het werk, kan en mag de rechtsgrond geen toestemming van de werknemers zijn (artikel 6, lid 1, onder a) vanwege de aard van de relatie tussen werkgever en werknemer¹⁹.

Dit betekent echter niet dat werkgevers nooit kunnen vertrouwen op toestemming als een rechtsgrond voor verwerking. Er kunnen situaties zijn waarin de werkgever kan aantonen dat toestemming daadwerkelijk vrijelijk wordt verleend. Gezien de wanverhouding tussen een werkgever en zijn personeel, kunnen werknemers alleen in uitzonderlijke omstandigheden vrijelijk toestemming geven, en wel wanneer het geen negatieve gevolgen heeft als zij al dan niet toestemming geven²⁰.

[Voorbeeld 5]

Een cameraploeg wil gaan filmen in een bepaald deel van een kantoor. De werknemer vraagt alle werknemers die op die plek werken om hun toestemming om te worden gefilmd, omdat ze in de opnames op de achtergrond te zien kunnen zijn. De werknemers die niet gefilmd willen worden, worden op geen enkele wijze gestraft, maar krijgen voor de duur van de opnames gelijkwaardige bureaus elders in het kantoor toegewezen.

Wanverhoudingen zijn niet beperkt tot overheidsinstanties en werknemers, ze kunnen zich ook voordoen in andere situaties. Zoals WP29 in verschillende Adviezen heeft benadrukt, kan "toestemming" alleen rechtsgeldig zijn als de betrokkene een werkelijke keuze heeft en er geen sprake is van bedrog, intimidatie of dwang en de betrokkene ook niet het risico van aanzienlijke negatieve gevolgen (bijvoorbeeld op aanzienlijke extra kosten) loopt wanneer hij of zij niet toestemt. Toestemming is niet vrij in gevallen waar sprake is van enig element van dwang, druk of niet kunnen uitoefenen van de vrije wil.

3.1.2. Conditionaliteit

Bij het beoordelen of toestemming vrijelijk is gegeven, speelt artikel 7, lid 4 AVG een belangrijke rol²¹.

Artikel 7, lid 4, AVG geeft aan dat, onder meer, de situatie van het "samenvoegen" van toestemming met de aanvaarding van voorwaarden, of het "koppelen" van het uitvoeren van een overeenkomst, met inbegrip van een dienstenovereenkomst, aan een verzoek om toestemming voor de verwerking van persoonsgegevens die niet nodig zijn voor de uitvoering van de overeenkomst, hoogst ongewenst is. Als in een dergelijke situatie toestemming wordt gegeven, wordt deze verondersteld niet vrijelijk te zijn gegeven (overweging 43). Artikel 7, lid 4, beoogt te waarborgen

¹⁹ Zie Advies 2/2017 over gegevensverwerking op het werk, blz. 6-7.

²⁰ Zie ook Advies 2/2017 over gegevensverwerking op het werk (WP249), paragraaf 6.2.

²¹ Artikel 7, lid 4, AVG: "Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst." Zie ook overweging 43, AVG, die luidt: "[...]De toestemming wordt geacht niet vrijelijk te zijn verleend indien geen afzonderlijke toestemming kan worden gegeven voor verschillende persoonsgegevensverwerkingen ondanks het feit dat dit in het individuele geval passend is, of indien de uitvoering van een overeenkomst, daaronder begrepen het verlenen van een dienst, afhankelijk is van de toestemming ondanks het feit dat dergelijke toestemming niet noodzakelijk is voor die uitvoering."

dat het doel van de verwerking van persoonsgegevens niet verkapt wordt door of samengevoegd met de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, waarvoor deze persoonsgegevens niet noodzakelijk zijn. Hierdoor verzekert de AVG dat de verwerking van persoonsgegevens waarvoor toestemming wordt gevraagd niet direct of indirect de tegenprestatie voor een overeenkomst is. De twee rechtsgronden voor rechtmatige verwerking van persoonsgegevens, namelijk toestemming en overeenkomst, kunnen niet worden samengevoegd wat als gevolg heeft dat de grenzen tussen de twee rechtsgronden vervagen.

Dwang om in te stemmen met het gebruik van persoonsgegevens in aanvulling op hetgeen strikt noodzakelijk is, beperkt de keuze van de betrokkene en staat vrije toestemming in de weg. Omdat wetgeving inzake gegevensbescherming is gericht op de bescherming van grondrechten, is het van essentieel belang dat een persoon de controle heeft over zijn of haar persoonsgegevens, en in er bestaat een sterke veronderstelling dat toestemming voor de onnodige verwerking van persoonsgegevens niet kan worden beschouwd als een verplichte tegenprestatie voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst.

Wanneer een verzoek om toestemming door de verwerkingsverantwoordelijke gekoppeld wordt aan de uitvoering van een overeenkomst, loopt een betrokkene die zijn of haar persoonsgegevens niet beschikbaar wil stellen voor verwerking door de verwerkingsverantwoordelijke dus het risico dat door hem of haar gevraagde diensten niet worden verstrekt.

Om te beoordelen of er sprake is van een dergelijke situatie van samenvoeging of koppeling, is het belangrijk om vast te stellen wat de werkingssfeer van de overeenkomst is, en welke gegevens nodig zijn voor de uitvoering van deze overeenkomst.

Overeenkomstig Advies 06/2014 van WP29 moet de term "noodzakelijk voor de uitvoering van een overeenkomst" strikt worden geïnterpreteerd. De verwerking moet noodzakelijk zijn om de overeenkomst met elke individuele betrokkene na te komen. Dit kan bijvoorbeeld betrekking hebben op de verwerking van het adres van de betrokkene, zodat online gekochte goederen kunnen worden geleverd, of de verwerking van creditcardgegevens om betaling mogelijk te maken. In het kader van de arbeidsverhouding kan deze rechtsgrond, bijvoorbeeld, de verwerking toestaan van salarisgegevens en bankgegevens zodat lonen kunnen worden uitbetaald²². Er moet een direct en objectief verband zijn tussen de verwerking van de gegevens en het doel van de uitvoering van de overeenkomst.

Als een verwerkingsverantwoordelijke persoonsgegevens wil verwerken die in feite noodzakelijk zijn voor de uitvoering van een overeenkomst, dan is toestemming niet de passende rechtsgrond²³.

Artikel 7, lid 4 is slechts relevant indien de gevraagde gegevens **niet** nodig zijn voor de uitvoering van een overeenkomst (met inbegrip van een dienstenovereenkomst), en de uitvoering van die overeenkomst afhankelijk wordt gesteld van het verkrijgen van deze gegevens op basis van

²² Zie voor meer informatie en voorbeelden Advies 06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" op grond van artikel 7 van Richtlijn 95/46/EG, door WP29 aangenomen op 9 april 2014, blz. 16-17. (WP 217).

²³ De passende rechtsgrond zou dan artikel 6, lid 1, onder b), kunnen zijn (overeenkomst).

toestemming. Omgekeerd is in het geval dat de verwerking **wel** noodzakelijk is voor de uitvoering van de overeenkomst (met inbegrip van een dienstenovereenkomst), artikel 7, lid 4, niet van toepassing.

[Voorbeeld 6]

Een bank vraagt klanten voor toestemming om derden toe te staan om hun betalingsgegevens te gebruiken voor direct marketingdoeleinden. Deze verwerkingsactiviteit is niet noodzakelijk voor de uitvoering van de overeenkomst met de klant en de levering van gewone diensten met betrekking tot bankrekeningen. Indien de weigering van de klant om toestemming te verlenen voor dit doel van verwerking zou leiden tot de ontzegging van bankdiensten, sluiten van de bankrekening, of naargelang het geval, een verhoging van de tarieven, kan toestemming niet vrijelijk worden verleend.

De keuze van de wetgever om, onder andere, conditionaliteit te benadrukken als een vermoeden van een gebrek aan vrijheid om toestemming te verlenen, toont aan dat de aanwezigheid van conditionaliteit zorgvuldig moet worden onderzocht. De term "ten sterkste rekening gehouden" in artikel 7, lid 4, suggereert dat de verwerkingsverantwoordelijke extra voorzichtig moet zijn in het geval dat aan een overeenkomst (waaronder een dienstenovereenkomst) een verzoek tot toestemming voor verwerking van persoonsgegevens is gekoppeld.

Omdat de formulering van artikel 7, lid 4 niet op een absolute wijze wordt uitgelegd, is er wellicht een zeer beperkte ruimte voor gevallen waarin deze conditionaliteit de toestemming niet onrechtmatig zou maken. Uit het woord "verondersteld" in overweging 43 blijkt echter duidelijk dat deze gevallen zeer uitzonderlijk zijn.

Hoe dan ook ligt de bewijslast in artikel 7, lid 4 bij de verwerkingsverantwoordelijke²⁴. Deze specifieke regel weerspiegelt het algemene beginsel van verantwoording dat in de hele AVG tot uiting komt. Indien artikel 7, lid 4 echter van toepassing is, is het voor de verwerkingsverantwoordelijke moeilijker om te bewijzen dat de betrokkene vrijelijk toestemming heeft verleend²⁵.

De verwerkingsverantwoordelijke zou kunnen aanvoeren dat zijn organisatie betrokkenen een echte keuze biedt als zij kunnen kiezen tussen een dienst die toestemming omvat voor het gebruik van persoonsgegevens voor aanvullende doeleinden enerzijds, en een gelijkwaardige dienst die aangeboden wordt door dezelfde verwerkingsverantwoordelijke die geen toestemming omvat voor het gebruik van gegevens voor aanvullende doeleinden anderzijds. Zolang als er geen mogelijkheid is om de overeenkomst uit te laten voeren of de dienst geleverd te krijgen door deze verwerkingsverantwoordelijke zonder toestemming te verlenen voor ander of aanvullend gebruik

²⁴ Zie ook artikel 7, lid 1, AVG, waarin staat dat de verwerkingsverantwoordelijke moet aantonen dat de betrokkene vrijelijk toestemming heeft verleend.

²⁵ Tot op zekere hoogte is de invoering van dit lid een codificatie van de bestaande richtsnoeren van WP29. Zoals beschreven in Advies 15/2011, kan er in het geval dat een betrokkene zich in een situatie van afhankelijkheid jegens de verwerkingsverantwoordelijke bevindt, een sterke presumptie zijn dat de vrijheid om toestemming te verlenen in deze omstandigheden beperkt is (bijv. in een arbeidsverhouding of als het verzamelen van gegevens wordt uitgevoerd door een overheidsinstantie). Maar nu artikel 7, lid 4, in werking is getreden, is het voor de verwerkingsverantwoordelijke moeilijker om te bewijzen dat de betrokkene vrijelijk toestemming heeft verleend. Zie: Advies 15/2011 over de definitie van "toestemming" (WP 187), blz. 12-17.

van de betreffende gegevens, betekent dit dat er niet langer sprake is van een conditionele dienst. Beide diensten moeten echter daadwerkelijk gelijkwaardig zijn.

De WP29 is van mening dat toestemming niet kan worden beschouwd als vrijelijk verleend als een verwerkingsverantwoordelijke aanvoert dat er een keuze is tussen zijn dienst die toestemming omvat voor het gebruik van persoonsgegevens voor aanvullende doeleinden enerzijds, en een gelijkwaardige dienst die wordt aangeboden door een andere verwerkingsverantwoordelijke anderzijds. In een dergelijk geval zou de keuzevrijheid afhankelijk worden gemaakt van wat andere spelers in de markt doen, en of een individuele betrokkene de diensten van de andere verwerkingsverantwoordelijke echt gelijkwaardig vindt. Dit zou voorts een verplichting inhouden voor verwerkingsverantwoordelijken om de ontwikkelingen op de markt te volgen, om de blijvende geldigheid van toestemming van hun verwerkingsactiviteiten te waarborgen, omdat een concurrent haar diensten in een later stadium zou kunnen wijzigen. Het gebruik van dit argument betekent dus dat deze toestemming niet voldoet aan de AVG.

3.1.3. Granulariteit

Een dienst kan meerdere verwerkingsactiviteiten voor meerdere doeleinden omvatten. In dergelijke gevallen zouden betrokkenen vrij moeten kunnen kiezen welk doeleinde ze accepteren, in plaats van toestemming te moeten verlenen voor een pakket verwerkingsdoeleinden. In een bepaald geval kan het, volgens de AVG, gerechtvaardigd zijn om meerdere toestemmingen te moeten verkrijgen voor met het aanbieden van een dienst wordt begonnen.

Overweging 43 verduidelijkt dat de toestemming wordt geacht niet vrijelijk te zijn verleend als het proces/de procedure voor het verkrijgen van toestemming niet toestaat dat betrokkenen afzonderlijke toestemming verlenen voor verschillende persoonsgegevensverwerkingen (bijvoorbeeld alleen voor bepaalde verwerkingsactiviteiten en niet voor anderen), ondanks het feit dat dit in het individuele geval passend is. In Overweging 32 staat *"De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doeleinden dienen. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend"*.

Indien de verwerkingsverantwoordelijke verschillende doeleinden voor verwerking heeft samengevoegd, en niet heeft getracht om voor elk doel afzonderlijke toestemming te krijgen, is er sprake van een gebrek aan vrijheid. Deze granulariteit is nauw verwant aan het vereiste dat toestemming specifiek moet zijn, zoals nader beschreven in paragraaf 3.2 hieronder. In het geval gegevensverwerking plaatsvindt ter verwezenlijking van verschillende doeleinden, ligt de oplossing om te voldoen aan de voorwaarden voor geldige toestemming in granulariteit, d.w.z. de scheiding van deze doeleinden en het verkrijgen van toestemming voor elk doel.

[Voorbeeld 7]

In hetzelfde verzoek om toestemming vraagt een detailhandelaar zijn klanten om toestemming om hun gegevens te gebruiken voor marketing via e-mail, en ook om hun gegevens te delen met andere ondernemingen binnen zijn groep. Deze toestemming is niet granulair, omdat er geen afzonderlijke toestemmingen zijn voor deze twee afzonderlijke doeleinden, en daarom is de toestemming niet geldig. In dit geval zou specifieke toestemming moeten worden verkregen om de contactgegevens aan commerciële partners te sturen. Deze specifieke toestemming wordt geacht geldig te zijn voor elke partner (zie ook paragraaf 3.3.1) wiens identiteit

aan de betrokkene is verstrekt ten tijde van het verkrijgen van zijn of haar toestemming, aangezien deze toestemming aan hen verleend is voor hetzelfde doel (in dit voorbeeld: een marketingdoel).

3.1.4. Nadeel

De verwerkingsverantwoordelijke moet aantonen dat het mogelijk is om toestemming te weigeren of in te trekken zonder dat nadeel wordt ondervonden (overweging 42). Zo moet de verwerkingsverantwoordelijke bijvoorbeeld bewijzen dat het intrekken van toestemming niet leidt tot kosten voor de betrokkene, en dus geen duidelijk nadeel heeft voor degene die zijn toestemming intrekt.

Andere voorbeelden van nadeel zijn bedrog, intimidatie of dwang of aanzienlijke negatieve gevolgen als de betrokkene geen toestemming verleent. De verwerkingsverantwoordelijke moet kunnen aantonen dat de betrokkene een vrije of echte keuze had om al dan niet toestemming te verlenen, en dat het mogelijk was om de toestemming in te trekken zonder nadeel.

Indien een verwerkingsverantwoordelijke kan aantonen dat een dienst de mogelijkheid omvat om toestemming in te trekken zonder negatieve gevolgen, bijvoorbeeld zonder dat de uitvoering van de dienst ten nadele van de gebruiker wordt bijgesteld, kan dit dienen om aan te tonen dat de toestemming vrijelijk verleend is. De AVG sluit niet alle initiatieven uit, maar de bewijslast om aan te tonen dat toestemming wel onder alle omstandigheden vrijelijk is verleend, berust bij de verwerkingsverantwoordelijke.

[Voorbeeld 8]

Tijdens het downloaden van een lifestyle-app voor mobiele telefoons, vraagt de app om toestemming tot de accelerometer van de telefoon. Dit is niet noodzakelijk voor de werking van de app, maar is nuttig voor de verwerkingsverantwoordelijke die meer te weten wil komen over het niveau van beweging en activiteit van de gebruikers. Wanneer een gebruiker deze toestemming later intrekt, merkt ze dat de app alleen nog in beperkte mate werkt. Dit is een voorbeeld van nadeel als bedoeld in overweging 42, wat betekent dat de toestemming nooit rechtmatig is verkregen (en dat de verwerkingsverantwoordelijke dus alle op deze wijze verzamelde persoonsgegevens over de beweging van de gebruiker moet verwijderen).

[Voorbeeld 9]

Een betrokkene abonneert zich op de nieuwsbrief met algemene kortingen van een modewinkel. De winkelier vraagt de betrokkene om toestemming voor het verzamelen van meer gegevens over zijn of haar winkelvoorkeuren om de aanbiedingen af te stemmen op zijn of haar voorkeuren op basis van zijn of haar aankoopgeschiedenis of een vragenlijst die vrijwillig kan worden ingevuld. Wanneer de betrokkene later zijn of haar toestemming intrekt, zal hij of zij weer niet-gepersonaliseerde kledingkortingen ontvangen. Dit vormt geen nadeel, omdat alleen het mogelijke extra voordeel verloren wordt.

[Voorbeeld: 10]

Een modetijdschrift biedt zijn lezers de mogelijkheid om nieuwe make-upproducten te kopen voordat deze op de markt worden gebracht.

De producten zullen binnenkort in de verkoop komen, maar aan de lezers van dit tijdschrift wordt een exclusief voorproefje van deze producten aangeboden. Om gebruik te kunnen maken van dit voordeel, moeten mensen hun postadres verstrekken en akkoord gaan met een abonnement op de mailinglijst van het tijdschrift. Het postadres is nodig voor verzending, en de mailinglijst wordt gebruikt om het hele jaar door commerciële aanbiedingen voor producten zoals cosmetica of T-shirts te versturen.

Het bedrijf verklaart dat de gegevens van de mailinglijst alleen zullen worden gebruikt voor het verzenden van goederen en papieren reclame door het tijdschrift zelf, en ze niet zullen worden gedeeld met enige andere organisatie.

In het geval de lezer zijn of haar adres om deze reden niet bekend wil maken, is er geen nadeel, omdat de producten toch voor hem of haar beschikbaar zijn.

3.2. Specifiek

Artikel 6, lid 1, onder a) bevestigt dat de toestemming van de betrokkene verleend moet worden met betrekking tot "een of meer specifieke" doeleinden, en dat een betrokkene een keuze heeft ten aanzien van elk van deze doeleinden²⁶. De eis dat de toestemming "*specifiek*" moet zijn, beoogt te zorgen voor een zekere mate van controle en transparantie voor de betrokkene. Deze eis is door de AVG niet gewijzigd, en blijft nauw verbonden aan de eis van "geïnformeerde" toestemming. Tegelijkertijd moet dit worden geïnterpreteerd in overeenstemming met de eis van "granulariteit" om "vrije" toestemming te verkrijgen²⁷. Kortom, om te voldoen aan het element van "specifiek" moet de verwerkingsverantwoordelijke het volgende toepassen:

- (i) Specificatie van doeleinden als een bescherming tegen 'function creep',
- (ii) Granulariteit in toestemmingsverzoeken, en
- (iii) Een duidelijke scheiding van informatie met betrekking tot het verkrijgen van toestemming voor verwerkingsactiviteiten van informatie over andere zaken.

Ad. (i): Overeenkomstig artikel 5, lid 1, onder b) AVG, wordt het verkrijgen van rechtmatige toestemming altijd voorafgegaan door de vaststelling van een welbepaald, uitdrukkelijk omschreven gerechtvaardigd doel voor de beoogde verwerkingsactiviteit.²⁸ De noodzaak van specifieke toestemming in combinatie met de notie van doelbinding in artikel 5, lid 1, onder b) functioneert als een bescherming tegen de geleidelijke verbreding of vervaging van doeleinden waarvoor gegevens worden verwerkt nadat een betrokkene heeft ingestemd met de oorspronkelijke verzameling van de gegevens. Dit verschijnsel, ook wel 'function creep' genoemd, is een risico voor betrokkenen, omdat het kan leiden tot onvoorzien gebruik van persoonsgegevens door de verwerkingsverantwoordelijke of door derden en verlies van controle door de betrokkene.

Als de verwerkingsverantwoordelijke vertrouwt op artikel 6, lid 1, onder a), moeten betrokkenen altijd toestemming geven voor een bepaald doel van verwerking²⁹. In lijn met het concept van *doelbinding*, kan toestemming op grond van artikel 5, lid 1, onder b) en overweging 32 verschillende werkzaamheden omvatten, zolang deze werkzaamheden maar hetzelfde doel dienen. Het spreekt vanzelf dat specifieke toestemming alleen kan worden verkregen wanneer de betrokkenen specifiek zijn geïnformeerd over de voorgenomen doelen van gebruik van gegevens die op hen betrekking hebben.

²⁶ Nadere richtsnoeren voor het bepalen van "doeleinden" zijn te vinden in Advies 3/2013 over doelbinding (WP 203).

²⁷ Overweging 43 AVG stelt dat afzonderlijke toestemming voor verschillende persoonsgegevensverwerkingen in voorkomende gevallen nodig is. Granulaire toestemming moet worden verleend om betrokkenen in staat te stellen om afzonderlijk in te stemmen met verschillende doeleinden.

²⁸ Zie WP 29 Advies 3/2013 over doelbinding (WP 203), blz. 16: "Om deze redenen voldoet een doel dat vaag of algemeen is, zoals "verbetering van de gebruikerservaring", "marketingdoeleinden", doeleinden met betrekking tot IT-beveiliging, of "toekomstig onderzoek" – zonder meer informatie – meestal niet aan de criteria voor "specifiek"."

²⁹ Dit is in overeenstemming met WP29 Advies 15/2011 over de definitie van "toestemming" (WP 187), bijvoorbeeld op blz. 17.

Onverminderd de bepalingen inzake compatibiliteit van doeleinden moet toestemming specifiek voor het doel zijn. Betrokkenen verlenen hun toestemming met het besef dat zij controle kunnen uitoefenen en dat hun gegevens uitsluitend worden verwerkt voor die vermelde doeleinden. Indien een verwerkingsverantwoordelijke op basis van toestemming gegevens verwerkt, en de gegevens ook wil verwerken voor een ander doel, moet deze verwerkingsverantwoordelijke vragen om aanvullende toestemming voor dit andere doel, tenzij er een andere rechtsgrond is die beter is toegesneden op de situatie.

[Voorbeeld 11] Een kabeltelevisienet verzamelt, op basis van hun toestemming, persoonsgegevens van abonnees om hen op basis van hun kijkgedrag persoonlijke suggesties te kunnen doen voor nieuwe films waarin ze wellicht zijn geïnteresseerd. Na een tijdje besluit het tv-netwerk dat het derden wil inschakelen om gerichte reclame te versturen (of te tonen) op basis van het kijkgedrag van de abonnee. Door dit nieuwe doel is nieuwe toestemming nodig.

Ad. (ii): Mechanismen voor toestemming moeten niet alleen granulair zijn om te voldoen aan de eis van "vrij", maar moeten ook voldoen aan het element van "specifiek". Dit betekent dat een verwerkingsverantwoordelijke die toestemming wil krijgen voor een aantal verschillende doeleinden, voor elk doel een afzonderlijke opt-in moet aanbieden om gebruikers in staat te stellen om specifieke toestemming te verlenen voor specifieke doeleinden.

Ad. (iii): Ten slotte moeten verwerkingsverantwoordelijke bij elk afzonderlijk verzoek om toestemming specifieke informatie verstrekken over de gegevens die voor elk doel worden verwerkt, om de betrokkenen te informeren over de gevolgen van de verschillende keuzes die ze hebben. Op deze manier worden betrokkenen in staat gesteld om specifieke toestemming te verlenen. Dit onderwerp valt gedeeltelijk samen met de eis dat verwerkingsverantwoordelijken duidelijke informatie moeten verstrekken, zoals besproken in paragraaf 3.3 hieronder.

3.3. Vaste

De AVG versterkt de eis dat toestemming geïnformeerd moet zijn. Op basis van artikel 5 van de AVG, is de eis van transparantie een van de fundamentele beginselen, en is nauw verwant aan de beginselen van behoorlijkheid en rechtmatigheid. Het verstrekken van informatie aan betrokkenen voorafgaand aan het verkrijgen van hun toestemming is noodzakelijk om hen in staat te stellen om geïnformeerde beslissingen te nemen, te begrijpen waarmee ze instemmen en bijvoorbeeld hun recht tot intrekking van hun toestemming uit te oefenen. Indien de verwerkingsverantwoordelijke geen begrijpelijke informatie verstrekt, wordt de controle van de betrokkene slechts schijn en is toestemming een onrechtmatige rechtsgrond voor verwerking.

Het gevolg van het niet voldoen aan de eisen voor geïnformeerde toestemming is dat de toestemming onrechtmatig is, en de verwerkingsverantwoordelijke mogelijk artikel 6 van de AVG schendt.

3.3.1. De minimale inhoudelijke eisen voor het "geïnformeerd" zijn van toestemming

Om toestemming met kennis van zaken wordt gegeven, moet de betrokkene geïnformeerd worden over bepaalde elementen die van essentieel belang zijn om een keuze te maken. Daarom is WP29 van mening dat ten minste de volgende informatie nodig is voor het verkrijgen van rechtmatige toestemming:

- (i) De identiteit van de verwerkingsverantwoordelijke;³⁰
- (ii) Het doel van elk van de verwerkingen waarvoor toestemming wordt gevraagd;³¹
- (iii) Welk(e) (soort) gegevens worden verzameld en gebruikt;³²
- (iv) Het bestaan van het recht om toestemming in te trekken;³³
- (v) Informatie over het gebruik van de gegevens voor geautomatiseerde besluitvorming overeenkomstig artikel 22, lid 2, onder c,³⁴ indien van toepassing, en
- (vi) Over de risico's die dergelijke doorgiften bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen, zoals beschreven in artikel 46³⁵.

Ten aanzien van punt i) en iii) merkt WP29 op dat in een geval waarin de gevraagde toestemming wordt ingeroepen door meerdere (gezamenlijke) verwerkingsverantwoordelijken of als de gegevens worden doorgegeven aan of verwerkt door andere verwerkingsverantwoordelijken die een beroep willen doen op de oorspronkelijke toestemming, deze organisaties allen moeten worden genoemd. Verwerkingsverantwoordelijken hoeven niet te worden genoemd als onderdeel van de eisen voor toestemming, hoewel verwerkingsverantwoordelijken om te voldoen aan artikelen 13 en 14 AVG wel een volledige lijst moeten verstrekken van ontvangers of categorieën van ontvangers, waaronder verwerkingsverantwoordelijken. Tot slot merkt WP29 op dat, afhankelijk van de omstandigheden en de context van een geval, meer informatie nodig kan zijn om de betrokkene in staat te stellen om de betreffende verwerkingsactiviteiten te begrijpen.

3.3.2. Hoe moet informatie worden verstrekt?

De AVG bepaalt niet in welke vorm de informatie moet worden verstrekt om te voldoen aan de eis van geïnformeerde toestemming. Dit betekent dat geldige informatie op verschillende manieren kan worden verstrekt, bijvoorbeeld door middel van schriftelijke of mondelinge verklaringen of audio- of video-berichten. De AVG stelt echter wel een aantal eisen voor geïnformeerde toestemming, voornamelijk in artikel 7, lid 2, en overweging 32. Dit leidt tot een hogere standaard voor de duidelijkheid en toegankelijkheid van de informatie.

Bij het vragen om toestemming moeten verwerkingsverantwoordelijken ervoor zorgen dat zij in alle gevallen heldere en duidelijke taal gebruiken. Dit betekent dat een bericht gemakkelijk te begrijpen moet zijn voor de gemiddelde persoon, en niet alleen voor juristen. Verwerkingsverantwoordelijken

³⁰ Zie ook overweging 42, AVG. "[...] Opdat toestemming met kennis van zaken wordt gegeven, moet de betrokkene ten minste bekend zijn met de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking van de persoonsgegevens [...]."

³¹ Zie wederom overweging 42, AVG.

³² Zie ook WP29 Advies 15/2011 over de definitie van 'toestemming' (WP 187), blz. 19-20.

³³ Zie artikel 7, lid 3 AVG.

³⁴ Zie ook WP 29 Richtsnoeren betreffende geautomatiseerde individuele besluitvorming en profilering in de zin van verordening 2016/679 (WP251), paragraaf IV.B, blz. 20 e.v.

³⁵ Overeenkomstig artikel 49, lid 1, onder a), is bij het vragen om uitdrukkelijke toestemming specifieke informatie nodig over het ontbreken van de waarborgen zoals bedoeld in artikel 46. Zie ook WP29 Advies 15/2011 over de definitie van 'toestemming' (WP 187), blz. 19.

mogen geen gebruik maken van uitgebreide privacybepalingen die moeilijk te begrijpen zijn, of van verklaringen vol juridisch jargon. Toestemming moet duidelijk en van andere zaken te onderscheiden zijn, en moet verstrekt worden in een begrijpelijke en gemakkelijk toegankelijke vorm. Deze eis betekent in wezen dat informatie die relevant is voor het nemen van weloverwogen beslissingen over het al dan niet verlenen van toestemming niet mogen worden verborgen in algemene voorwaarden³⁶.

Een verwerkingsverantwoordelijke moet zorgen dat toestemming wordt verleend op basis van informatie die de betrokkene in staat stelt om gemakkelijk vast te stellen wie de verwerkingsverantwoordelijke is, en om te begrijpen waarmee hij instemt. De verwerkingsverantwoordelijke moet een duidelijke beschrijving geven van het doel van de gegevensverwerking waarvoor toestemming wordt gevraagd³⁷.

Andere specifieke richtsnoeren betreffende toegankelijkheid zijn verstrekt in de WP29 richtsnoeren inzake transparantie. Als toestemming wordt gegeven via elektronische middelen, moet het verzoek duidelijk en beknopt zijn. Gelaagde en granulaire informatie kan een passende manier zijn voor het omgaan met de dubbele verplichting om enerzijds nauwkeurig en volledig te zijn, en anderzijds begrijpelijk te zijn.

Een verwerkingsverantwoordelijke moet beoordelen welk soort publiek persoonsgegevens aan zijn organisatie verstrekt. In het geval de beoogde doelgroep bijvoorbeeld minderjarige betrokkenen omvat, wordt van de verwerkingsverantwoordelijke verwacht dat hij ervoor zorgt dat de informatie begrijpelijk is voor minderjarigen³⁸. Nadat een verwerkingsverantwoordelijke het betreffende publiek heeft vastgesteld, moet hij bepalen welke informatie hij moet verstrekken, en vervolgens hoe deze informatie aan de betrokkenen wordt gepresenteerd.

Artikel 7, lid 2, behandelt vooraf geformuleerde schriftelijke verklaringen van toestemming die ook betrekking hebben op andere zaken. Indien toestemming wordt gevraagd als onderdeel van een (papieren) overeenkomst, moet het verzoek om toestemming moeten duidelijk te onderscheiden zijn van de andere zaken. Als de papieren overeenkomst vele aspecten omvat die niets te maken hebben met het verzoek om toestemming of het gebruik van persoonsgegevens, moet het onderwerp toestemming worden behandeld op een manier die duidelijk opvalt, of in een apart document. Evenzo geldt dat als toestemming wordt gevraagd via elektronische middelen, het verzoek om toestemming afzonderlijk en gescheiden moet zijn: het mag, volgens overweging 32, niet eenvoudigweg een paragraaf in de algemene voorwaarden zijn³⁹. Om tegemoet te komen aan kleine schermen of situaties met beperkt ruimte voor informatie, kan, in voorkomende gevallen, een

³⁶ De verklaring van toestemming moet als zodanig worden genoemd. Formuleringen zoals "Ik weet dat..." voldoen niet aan de eis van duidelijke taal.

³⁷ Zie artikel 4, lid 11 en 7, lid 2 AVG.

³⁸ Zie ook overweging 58 betreffende voor kinderen begrijpelijke informatie.

³⁹ Zie ook overweging 42 en Richtlijn 93/13/EG, met name artikel 5 (duidelijke en begrijpelijke taal en, in geval van twijfel, is de interpretatie ten gunste van de consument) en artikel 6 (ongeldigheid van oneerlijke voorwaarden, overeenkomst blijft zonder deze voorwaarden alleen bestaan als deze nog steeds zinnig is, anders is de volledige overeenkomst ongeldig).

gelaagde presentatie van informatie worden overwogen om buitensporige verstoring van de gebruikerservaring of het productontwerp te voorkomen.

Om te voldoen aan de AVG moet een verwerkingsverantwoordelijke die een beroep doet op de toestemming van de betrokkene, moet ook voldoen aan de verplichtingen voor afzonderlijke informatie die omschreven zijn in artikel 13 en 14. In de praktijk kan de naleving van de informatieverplichtingen en voldoen aan de eis van geïnformeerde toestemming in veel gevallen leiden tot een geïntegreerde aanpak. Deze paragraaf is echter geschreven in de veronderstelling dat rechtmatige "geïnformeerde" toestemming ook kan bestaan wanneer niet alle elementen van artikel 13 en/of 14 genoemd worden in het proces van het verkrijgen van toestemming (deze punten moeten dan natuurlijk worden vermeld op andere plaatsen, zoals in het privacybeleid van een onderneming). WP29 heeft afzonderlijke richtsnoeren verstrekt betreffende de eis van transparantie.

[Voorbeeld 12]

Bedrijf X is een verwerkingsverantwoordelijke die klachten heeft ontvangen dat het voor betrokkenen onduidelijk is voor welke doeleinden voor gegevensgebruik zij worden gevraagd om toestemming te verlenen. Het bedrijf is zich bewust van de noodzaak om na te gaan of de informatie in het verzoek om toestemming begrijpelijk is voor betrokkenen. X organiseert vrijwillige testpanels van specifieke categorieën van zijn afnemers en presenteert nieuwe versies van zijn informatie inzake toestemming aan dit testpubliek voordat de informatie naar buiten wordt gebracht. De selectie van het panel eerbiedigt het beginsel van onafhankelijkheid, en wordt uitgevoerd op basis van standaarden die een representatieve, niet-bevooroordeelde uitkomst garanderen. Het panel ontvangt een vragenlijst en geeft aan wat het heeft opgemaakt uit de informatie, en hoe het deze informatie zou beoordelen in termen van begrijpelijkheid en relevante informatie. De verwerkingsverantwoordelijke blijft testen totdat de panels aangeven dat de informatie begrijpelijk is. X stelt een verslag op van de test en houdt dit beschikbaar voor toekomstige raadpleging. Dit voorbeeld toont een mogelijke manier waarop X kan aantonen dat de betrokkenen duidelijke informatie hadden ontvangen voordat ze toestemming verleenden voor verwerking van persoonsgegevens door X.

[Voorbeeld 13]

Een bedrijf voert gegevensverwerking uit op basis van toestemming. Het bedrijf maakt gebruik van een gelaagd privacybeleid dat een verzoek om toestemming omvat. Het bedrijf maakt alle basisgegevens van de verwerkingsverantwoordelijke en de voorgenomen verwerkingsactiviteiten bekend⁴⁰. Het bedrijf geeft in de eerste informatielaag van het beleid echter niet aan hoe contact kan worden opgenomen met zijn functionaris voor gegevensbescherming. Ten behoeve van een rechtmatige rechtsgrond zoals bedoeld in artikel 6 heeft deze verwerkingsverantwoordelijke rechtmatige "geïnformeerde" toestemming verkregen, ondanks dat de contactgegevens van de functionaris voor gegevensbescherming, niet aan de betrokkene zijn doorgegeven (in de eerste informatielaag) zoals verplicht op grond van artikel 13, lid 1, onder b of 14, lid 1, onder van de AVG.

3.4. Ondubbelzinnige wilsuiting

De AVG is duidelijk dat voor toestemming een verklaring van de betrokkene of een ondubbelzinnige actieve handeling van de betrokkene is vereist, wat betekent dat toestemming altijd

⁴⁰ Wij merken op dat wanneer de identiteit van de verwerkingsverantwoordelijke of het doel van de verwerking niet blijkt uit de eerste informatielaag van het gelaagde privacybeleid (en opgenomen is in de volgende lagen), het voor de verwerkingsverantwoordelijke moeilijk zal zijn om aan te tonen dat de betrokkene geïnformeerde toestemming heeft verleend, tenzij de verwerkingsverantwoordelijke kan aantonen dat de betreffende betrokkene deze informatie heeft ingezien alvorens toestemming te verlenen.

moet worden verleend door middel van een actieve handeling of verklaring. Het moet duidelijk zijn dat de betrokkene toestemming heeft verleend voor de specifieke verwerking.

Artikel 2, onder h) van Richtlijn 95/46/EG beschrijft toestemming als "wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt". Artikel 4, lid 11 van de AVG bouwt voort op deze definitie door te verduidelijken dat voor rechtmatige toestemming een *ondubbelzinnige* wilsuiting vereist door middel van een *verklaring of ondubbelzinnige actieve handeling*, in lijn met de eerder door WP29 verstrekte richtsnoeren.

Een "ondubbelzinnige actieve handeling" betekent dat de betrokkene een opzettelijke handeling moet hebben uitgevoerd om toestemming te verlenen voor de specifieke verwerking⁴¹. Overweging 32 bevat aanvullende richtsnoeren met betrekking hiertoe. Toestemming kan worden ingewonnen door middel van een schriftelijke of een (opgenomen) mondelinge verklaring, waaronder via elektronische middelen.

Misschien is de meest letterlijke manier om te voldoen aan het criterium van een "schriftelijke verklaring" ervoor te zorgen dat een betrokkene in een brief of een e-mail aan de verwerkingsverantwoordelijke uitlegt waarmee hij/zij precies instemt. Dit is echter vaak niet realistisch. Schriftelijke verklaringen kunnen in vele soorten en maten aan de AVG voldoen.

Onverminderd het bestaande (nationale) contractenrecht kan toestemming worden verkregen door middel van een geregistreerd mondelinge verklaring, hoewel wel rekening moet worden gehouden met de informatie die voor de betrokkene beschikbaar is vóór de verklaring van toestemming. Het gebruik van vooraf aangevinkte opt-invakjes is krachtens de AVG onrechtmatig. Stilzwijgen of inactiviteit van de betrokkene, evenals enkel doorgaan met het gebruik van een dienst, kan niet worden beschouwd als een actieve indicatie van een keuze.

[Voorbeeld 14]

Bij het installeren van software, vraagt een applicatie de betrokkene om toestemming voor het gebruik van niet-geanonimiseerde crashrapporten om de software te verbeteren. Het verzoek om toestemming gaat vergezeld van een gelaagd privacybeleid waarin de noodzakelijke informatie wordt verstrekt. Door actief het optionele vakje met "Ik ga akkoord" aan te vinken, kan de gebruiker rechtmatig een "ondubbelzinnige actieve handeling" uitvoeren om toestemming te verlenen voor de verwerking.

⁴¹ Zie Werkdocument van de diensten van de Commissie, Effectbeoordeling, Bijlage 2, blz. 20 en ook blz. 105-106: *"Zoals ook aangegeven in het door WP29 vastgestelde advies inzake toestemming, lijkt het absoluut noodzakelijk om te verduidelijken dat rechtmatige toestemming het gebruik vereist van mechanismen die geen twijfel laten bestaan over de intentie van de betrokkene om toestemming te verlenen, waarbij het duidelijk moet worden gemaakt dat – in de context van de online omgeving – het gebruik van standaardopties die de betrokkene moet wijzigen om de verwerking te weigeren ("stilzwijgende toestemming"), op zichzelf geen ondubbelzinnige toestemming vormt. Dit zou personen meer controle over hun eigen gegevens geven in het geval verwerking is gebaseerd op de toestemming van de betrokkene. Wat betreft de effecten voor verwerkingsverantwoordelijken, zou dit geen grote effecten hebben omdat het slechts de gevolgen van de huidige richtlijn met betrekking tot de voorwaarden voor een rechtmatige en betekenisvolle toestemming van de betrokkene verduidelijkt en beter formuleert. Met name in de mate dat "uitdrukkelijke" toestemming – door het vervangen van "ondubbelzinnig" – de modaliteiten en kwaliteit zou verduidelijken van toestemming die niet bedoeld is om de gevallen en situaties waarin (uitdrukkelijke) toestemming moet worden gebruikt als rechtsgrond voor verwerking, zijn de effecten van deze maatregel op verwerkingsverantwoordelijken naar verwachting niet groot."*

Een verwerkingsverantwoordelijke moet zich er ook van bewust zijn dat toestemming niet kan worden verkregen door middel van dezelfde handeling als die voor het instemmen met een overeenkomst of het aanvaarden van algemene voorwaarden van een dienst. Allesomvattende aanvaarding van algemene voorwaarden kan niet worden beschouwd als een ondubbelzinnige actieve handeling voor toestemming voor het gebruik van persoonsgegevens. De AVG staat verwerkingsverantwoordelijken niet toe om vooraf aangevinkte vakjes of opt-outconstructies waarvoor de betrokkene een handeling moet verrichten om instemming te voorkomen (bijvoorbeeld 'opt-outvakjes')⁴².

Wanneer toestemming moet worden gegeven naar aanleiding van een verzoek via elektronische middelen, mag het verzoek om toestemming niet *onnodig* verstorend zijn voor het gebruik van de dienst waarvoor de toestemming wordt verleend⁴³. Een actieve bevestigende handeling waarmee de betrokkene toestemming verleent kan nodig zijn wanneer een minder inbreukmakende of verstorende manier zou leiden tot onduidelijkheid. Het kan dus noodzakelijk zijn dat verzoek om toestemming de gebruikerservaring tot op zekere hoogte verstoort om dit verzoek effectief te maken.

Binnen het kader van de eisen van de AVG hebben verwerkingsverantwoordelijken echter de vrijheid om een toestemmingsprocedure te ontwikkelen die het best aansluit bij hun organisatie. In dit verband kunnen fysieke handelingen worden gekwalificeerd als een ondubbelzinnige actieve handeling in overeenstemming met de AVG.

Verwerkingsverantwoordelijken moeten mechanismen voor toestemming op een dusdanige manier ontwerpen dat ze voor betrokkenen duidelijk zijn. Verwerkingsverantwoordelijken moeten dubbelzinnigheid vermijden en ervoor zorgen dat de handeling waarmee toestemming wordt verleend kan worden onderscheiden van andere handelingen. Daarom is het alleen voortzetten van het gewone gebruik van een website geen gedrag waaruit een wilsuiting kan worden opgemaakt van de betrokkene om zijn of haar instemming te geven voor een voorgenomen gegevensverwerking.

[Voorbeeld 15]

Het over een scherm vegen van een balk, wuiven voor een slimme camera, een smartphone ronddraaien of in een achtje bewegen, kunnen mogelijkheden zijn om toestemming aan te geven, als maar duidelijke informatie wordt verstrekt, en het duidelijk is dat de betreffende beweging betekent dat wordt ingestemd met een specifiek verzoek (bijv.: Als u deze balk naar links veegt, gaat u akkoord met het gebruik van informatie X voor doel X. Herhaal de beweging om te bevestigen). De verwerkingsverantwoordelijke moet kunnen aantonen dat toestemming op deze wijze is verkregen, en betrokkenen moeten hun toestemming even eenvoudig kunnen intrekken als dat deze is verleend.

[Voorbeeld 16]

Omlaag scrollen of vegen door een website voldoet niet aan de eis van een ondubbelzinnige actieve handeling. Dit is omdat de waarschuwing dat doorgaan met scrollen toestemming vormt moeilijk te onderscheiden kan

⁴² Zie artikel 7, lid 2. Zie ook Werkdocument 02/2013 inzake het verkrijgen van toestemming voor cookies (WP 208), blz. 3-6.

⁴³ Zie overweging 32, AVG.

zijn en/of gemist kan worden wanneer een betrokkene snel door grote hoeveelheden tekst scrolt en deze handeling niet voldoende ondubbelzinnig is.

In de digitale context hebben veel diensten persoonsgegevens nodig om te werken, en daarom ontvangen betrokkenen dagelijks meerdere verzoeken om toestemming waarop ze door middel van klikken en vegen moeten antwoorden. Dit kan leiden tot een zekere mate van 'klikmoeheid': het daadwerkelijke waarschuwingseffect van mechanismen voor toestemming wordt minder wanneer men deze waarschuwingen te vaak tegenkomt.

Dit resulteert in een situatie waarin verzoeken om toestemming niet meer worden gelezen. Dit vormt een bijzonder risico voor betrokkenen, omdat meestal om toestemming wordt gevraagd voor handelingen die zonder toestemming van een betrokkene in beginsel onrechtmatig zijn. De AVG legt verwerkingsverantwoordelijken de verplichting op om manieren te ontwikkelen om dit probleem aan te pakken.

Een vaak aangehaald voorbeeld om dit binnen de online context is om toestemming te verkrijgen internetgebruikers via hun browserinstellingen. Deze instellingen moeten worden ontwikkeld in overeenstemming met de voorwaarden voor rechtmatige toestemming van de AVG, zoals de eis dat toestemming granulair moet zijn voor elk van de voorgenomen doeleinden, en dat de te verstrekken informatie de naam van de verwerkingsverantwoordelijken moet omvatten.

In ieder geval moet toestemming altijd worden verkrijgen voordat de verwerkingsverantwoordelijke begint met de verwerking van persoonsgegevens waarvoor toestemming nodig is. WP29 heeft in eerdere adviezen consequent op het standpunt gesteld dat toestemming moet worden verleend voordat wordt begonnen met de verwerking⁴⁴. Hoewel de AVG in artikel 4, lid 11, niet letterlijk voorschrijft dat toestemming moet worden verleend voordat begonnen wordt met de verwerkingsactiviteiten, wordt dit duidelijk verondersteld. De aanhef van artikel 6, lid 1 en de tekst "heeft gegeven" in artikel 6, lid 1 ondersteunt deze interpretatie. Uit artikel 6 en overweging 40 volgt logischerwijs dat een geldige rechtsgrond moet zijn voordat begonnen wordt met gegevensverwerking. Daarom moet toestemming worden gegeven vóór aanvang van de verwerkingsactiviteiten. In beginsel kan het volstaan om eenmaal te vragen om de toestemming van een betrokkene. Verwerkingsverantwoordelijken moeten echter nieuwe en specifieke toestemming verkrijgen wanneer de doeleinden voor gegevensverwerking veranderen nadat toestemming is verkregen, of wanneer een aanvullend doel wordt beoogd.

4. Het verkrijgen van de uitdrukkelijke toestemming

Uitdrukkelijke toestemming is vereist in bepaalde situaties waarin zich een ernstig risico voor gegevensbescherming voordoet, waarbij een hoog niveau van individuele controle over persoonsgegevens passend wordt geacht. Op grond van de AVG speelt uitdrukkelijke toestemming een rol in artikel 9 betreffende de verwerking van bijzondere categorieën van persoonsgegevens, de bepalingen inzake doorgifte van gegevens aan derde landen of internationale organisaties bij het

⁴⁴ WP29 heeft dit standpunt consequent ingenomen vanaf Advies 15/2011 over de definitie van 'toestemming' (WP 187), blz. 30-31.

ontbreken van de passende waarborgen in artikel 49⁴⁵, en in artikel 22 betreffende geautomatiseerde individuele besluitvorming, waaronder profilering⁴⁶.

De AVG bepaalt dat een "verklaring of ondubbelzinnige actieve handeling" een voorwaarde is voor "regelmatige" toestemming. Omdat de eis van "regelmatige" toestemming in de AVG reeds van een hoger niveau is dan de voorwaarde voor toestemming in Richtlijn 95/46/EG, dient te worden verduidelijkt welke extra inspanningen een verwerkingsverantwoordelijke moet verrichten om de *uitdrukkelijke* toestemming van de betrokkene overeenkomstig de AVG te verkrijgen.

De term *uitdrukkelijk* verwijst naar de manier waarop toestemming door de betrokkene tot uitdrukking wordt gebracht. Het betekent dat de betrokkene een uitdrukkelijke verklaring van toestemming moet geven. Een voor de hand liggende manier om ervoor te zorgen dat toestemming uitdrukkelijk is, is het uitdrukkelijk bevestigen van toestemming in een schriftelijke verklaring. In voorkomende gevallen zou de verwerkingsverantwoordelijke ervoor kunnen zorgen dat de schriftelijke verklaring door de betrokkene wordt ondertekend, om elke mogelijke twijfel en mogelijk gebrek aan bewijs in de toekomst te voorkomen⁴⁷.

Een dergelijke ondertekende verklaring is echter niet de enige manier om uitdrukkelijke toestemming te verkrijgen, en het is niet zo dat de AVG in alle omstandigheden waarin geldige uitdrukkelijke toestemming nodig is voorschrijft dat dit op basis van een schriftelijke en ondertekende verklaring moet zijn. In de digitale of online context bijvoorbeeld kan een betrokkene de vereiste verklaring verstrekken door het invullen van een elektronisch formulier, door het versturen van een e-mail, door het uploaden van een gescand document waarop de handtekening van de betrokkene staat, of door middel van een elektronische handtekening. In theorie kan het gebruik van mondelinge verklaring ook voldoende zijn om geldige uitdrukkelijke toestemming te verkrijgen, het kan echter voor de verwerkingsverantwoordelijke moeilijk te bewijzen zijn dat bij het opnemen van de verklaring voldaan is aan alle voorwaarden voor geldige uitdrukkelijke toestemming.

Een organisatie kan ook uitdrukkelijke toestemming verkrijgen door middel van een telefoongesprek, mits de informatie over de keuze, eerlijk, begrijpelijk en duidelijk is, en de organisatie vraagt om een specifieke bevestiging van de betrokkene (bijvoorbeeld door een knop in te drukken of mondeling bevestiging te verschaffen).

⁴⁵ Volgens artikel 49, lid 1, onder a), AVG, kan uitdrukkelijke toestemming het verbod opheffen op doorgiften van gegevens zonder een adequaat beschermingsniveau van wetgeving inzake gegevensbescherming. Zie ook het werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1 van Richtlijn 95/46/EG of 24 oktober 1995 (WP 114), blz. 11, waarin WP29 aangeeft dat toestemming voor gegevensdoorgiften die periodiek of op regelmatige basis plaatsvinden ongepast is.

⁴⁶ Artikel 22 van de AVG bevat bepalingen om betrokkenen te beschermen tegen besluitvorming uitsluitend gebaseerd op geautomatiseerde verwerking, waaronder profilering. Besluiten die op deze basis worden genomen, zijn onder bepaalde wettelijke voorwaarden toegestaan. Toestemming speelt een sleutelrol in dit beschermingsmechanisme, omdat artikel 22, lid 2, onder c) AVG het duidelijk maakt dat een verwerkingsverantwoordelijke geautomatiseerde besluitvorming, waaronder profilering, kan uitvoeren die een aanzienlijke invloed kan hebben op het individu wanneer de betrokkene hiervoor uitdrukkelijk toestemming heeft verleend. WP29 heeft aparte richtsnoeren voor dit onderwerp opgesteld: WP29 Richtsnoeren betreffende geautomatiseerde besluitvorming en profilering in de zin van verordening 2016/679 van 3 oktober 2017 (WP251).

⁴⁷ Zie ook WP29 Advies 15/2011 over de definitie van 'toestemming' (WP 187), blz. 25.

[Voorbeeld 17] Een verwerkingsverantwoordelijke kan ook uitdrukkelijke toestemming verkrijgen van een bezoeker aan zijn website door een scherm voor het verlenen van uitdrukkelijke toestemming aan te bieden waarop selectievakjes "Ja" en "Nee" worden weergegeven, mits de tekst duidelijk de toestemming verwoordt, bijvoorbeeld: "Hierbij verleen ik toestemming voor de verwerking van mijn gegevens", en bijvoorbeeld niet "het is mij duidelijk dat mijn gegevens zullen worden verwerkt". Het spreekt vanzelf dat moet worden voldaan aan de voorwaarden voor geïnformeerde toestemming alsmede de andere voorwaarden voor het verkrijgen van geldige toestemming.

[Voorbeeld 18] Een kliniek voor cosmetische chirurgie vraagt om uitdrukkelijke toestemming van een patiënt om zijn medisch dossier door te geven aan een deskundige aan wie een second opinion wordt gevraagd over de toestand van de patiënt. Het medisch dossier is een digitaal bestand. Gezien het specifieke karakter van de betreffende gegevens vraagt de kliniek om een elektronische handtekening van de betrokkene om geldige uitdrukkelijke toestemming te verkrijgen en om te kunnen aantonen dat uitdrukkelijke toestemming is verkregen⁴⁸.

Tweestapsverificatie van toestemming kan ook een manier zijn om ervoor te zorgen dat uitdrukkelijke toestemming geldig is. Bijvoorbeeld: een betrokkene ontvangt een e-mail waarin hij of zij geïnformeerd wordt dat de verwerkingsverantwoordelijke van plan is om een dossier met medische gegevens te verwerken. De verwerkingsverantwoordelijke verduidelijkt in de e-mail dat hij om toestemming vraagt voor het gebruik van een bepaalde informatie voor een bepaald doel. Als de betrokkene instemt met het gebruik van deze gegevens, vraagt de verwerkingsverantwoordelijke hem of haar om de e-mail te beantwoorden met de mededeling "Ik ga akkoord". Nadat dit antwoord is verzonden, ontvangt de betrokkene een verificatielink waarop moet worden geklikt, of een sms-bericht met een verificatiecode, waarmee hij of zij de toestemming kan bevestigen.

Artikel 9, lid 2, erkent "noodzakelijk voor de uitvoering van een overeenkomst" niet als een uitzondering op het algemene verbod op verwerking van bijzondere categorieën gegevens. Daarom moeten verwerkingsverantwoordelijken en lidstaten die met deze situatie te maken krijgen, bekijken of een van de specifieke uitzonderingen in artikel 9, lid 2, onder b) tot en met j) van toepassing is. Indien geen van de uitzonderingen onder b) tot en met j) van toepassing is, is het verkrijgen van uitdrukkelijke toestemming overeenkomstig de voorwaarden voor geldige toestemming in de AVG de enige mogelijke rechtmatige uitzondering om deze gegevens te verwerken.

[Voorbeeld 19]

Een luchtvaartmaatschappij, Holiday Airways, biedt extra assistentie aan passagiers die, bijvoorbeeld vanwege een beperking, niet zelfstandig kunnen reizen. Een klant boekt een vlucht van Amsterdam naar Boedapest en vraagt om extra assistentie om aan boord van het vliegtuig te kunnen gaan. Holiday Airways vraagt haar om informatie over haar gezondheidstoestand te verstrekken om de juiste assistentie voor haar te kunnen regelen (er zijn namelijk een aantal mogelijkheden, bijvoorbeeld een rolstoel bij de gate bij aankomst, of een medewerker die samen met haar van A naar B reist). Holiday Airways vraagt om uitdrukkelijke toestemming om de medische gegevens van deze klant te verwerken ten behoeve van het regelen van de gevraagde extra assistentie. De gegevens die op basis van toestemming worden verwerkt, moeten noodzakelijk zijn voor de gevraagde dienst. Bovendien blijven er vluchten naar Boedapest zonder extra assistentie beschikbaar. Houd er

⁴⁸ Dit voorbeeld is onverminderd Verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

rekening mee dat omdat er gegevens nodig zijn voor de verlening van de gevraagde dienst, artikel 7, lid 4, niet van toepassing is.

[Voorbeeld 20]

Een succesvolle onderneming is gespecialiseerd in de levering van op maat gemaakte ski- en snowboardbrillen, en andere soorten speciale brillen voor buitensporten. Het idee is dat mensen deze brillen kunnen dragen zonder hun eigen bril. Het bedrijf ontvangt de bestellingen op een centraal punt en levert de producten vanuit één locatie in de gehele EU. Om zijn op maat gemaakte producten te kunnen leveren aan slechtziende klanten, verzoekt de verwerkingsverantwoordelijke om toestemming van het gebruik van de gegevens over de oogafwijking van de klanten. Klanten verstrekken bij het online plaatsten van hun bestelling de benodigde medische gegevens, zoals de strekte van hun bril. Zonder deze gegevens kunnen de gewenste aangepaste brillen niet worden geleverd. Het bedrijf biedt ook een assortiment sneeuwbrillen met gestandaardiseerde correcties aan. Klanten die hun medische gegevens niet willen delen, kunnen kiezen voor de standaarduitvoeringen. Daarom is uitdrukkelijke toestemming overeenkomstig artikel 9 vereist, en kan de toestemming worden beschouwd als vrijelijk verleend.

5. Aanvullende voorwaarden voor het verkrijgen van geldige toestemming

De AVG voert eisen in voor verwerkingsverantwoordelijken om aanvullende maatregelen te nemen om ervoor te zorgen dat zij geldige toestemming verkrijgen en behouden, en dit aan kunnen tonen. Artikel 7 van de AVG omschrijft deze aanvullende voorwaarden voor geldige toestemming, met specifieke bepalingen over het bijhouden van registers inzake toestemming en het recht om toestemming gemakkelijk in te trekken. Artikel 7 geldt ook voor toestemming zoals bedoeld in de andere artikelen van de AVG, bijvoorbeeld artikel 8 en 9. Richtsnoeren voor de aanvullende eis om geldige toestemming aan te tonen en voor het intrekken van toestemming worden hieronder verstrekt.

5.1. Toestemming aantonen

In artikel 7, lid 1, beschrijft de AVG duidelijk de uitdrukkelijke verplichting van de verwerkingsverantwoordelijke om aan te tonen dat de betrokkene toestemming heeft verleend. Overeenkomstig artikel 7, lid 1, rust de bewijslast op de verwerkingsverantwoordelijke.

Overweging 42 stelt: *"Indien de verwerking plaatsvindt op grond van toestemming van de betrokkene, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking."*

Het staat verwerkingsverantwoordelijken vrij om methodes te ontwikkelen om aan deze bepaling te voldoen op een manier die past bij hun dagelijkse bedrijfsvoering. Tegelijkertijd mag de verplichting om aan te tonen dat door een verwerkingsverantwoordelijke geldige toestemming is verkregen op zichzelf niet leiden tot het verwerken van buitensporige hoeveelheden extra gegevens. Dit betekent dat verwerkingsverantwoordelijken genoeg gegevens moeten hebben om een verband met de verwerking aan te tonen (om te laten zien dat toestemming is verkregen), maar dat ze niet meer gegevens mogen verzamelen dan nodig is.

Het is aan de verwerkingsverantwoordelijke om te bewijzen dat geldige toestemming van de betrokkene is verkregen. De AVG schrijft niet precies voor hoe dit moet gebeuren. De verwerkingsverantwoordelijke moet echter wel kunnen aantonen dat een betrokkene in een bepaald

geval heeft ingestemd. De verplichting om aan te tonen dat toestemming bestaat, geldt zolang als een bepaalde verwerkingsactiviteit voortduurt. Nadat de verwerkingsactiviteit wordt beëindigd, mag het bewijs van toestemming niet langer worden bewaard dan strikt noodzakelijk is om te voldoen aan een wettelijke verplichting of voor de instelling, uitoefening of onderbouwing van een rechtsvordering, overeenkomstig artikel 17, lid 3, onder b) en e).

De verwerkingsverantwoordelijke kan bijvoorbeeld een register bijhouden van ontvangen verklaringen van toestemming, zodat hij kan aantonen hoe toestemming is verkregen, wanneer toestemming is verkregen en welke informatie aan de betrokkene is verstrekt. De verwerkingsverantwoordelijke moet ook kunnen aantonen dat de betrokkene geïnformeerd is, en dat de werkstroom van de verwerkingsverantwoordelijke voldeed aan alle relevante criteria voor een geldige toestemming. De ratio achter deze verplichting in de AVG is dat verwerkingsverantwoordelijken verantwoording moeten afleggen met betrekking tot het verkrijgen van geldige toestemming van betrokkenen en de mechanismen voor toestemming die zij hebben ingevoerd. In een online context kan een verwerkingsverantwoordelijke bijvoorbeeld gegevens bewaren over de sessie waarin toestemming tot uitdrukking is gebracht, tezamen met de documentatie over de werkstroom van de toestemming ten tijde van de sessie, en een kopie van de informatie die op dat moment aan de betrokkene is verstrekt. Het is niet voldoende om alleen te verwijzen naar een juiste configuratie van de betreffende website.

[Voorbeeld 21] Een ziekenhuis start een wetenschappelijk onderzoeksprogramma, project X genaamd, waarvoor tandheelkundige dossiers van echte patiënten nodig zijn. Deelnemers worden gerekruteerd door middel van telefoongesprekken met patiënten die vrijwillig hebben ingestemd om te worden opgenomen op een lijst van kandidaten die voor dit doel kunnen worden benaderd. De verwerkingsverantwoordelijke vraagt om uitdrukkelijke toestemming van de betrokkenen voor het gebruik van hun tandheelkundige dossier. Toestemming wordt tijdens een telefoongesprek verkregen door het opnemen van een mondelinge verklaring van de betrokkene waarin de betrokkene bevestigt dat hij of zij instemt met het gebruik van zijn of haar gegevens voor de doeleinden van project X.

De AVG verschaft geen specifieke termijn voor hoe lang toestemming geldig blijft. Hoe lang toestemming geldig blijft, hangt af van de context, de werkingssfeer van de oorspronkelijke toestemming en de verwachtingen van de betrokkene. Wanneer de verwerkingsactiviteiten veranderen of in aanzienlijke mate transformeren, is de oorspronkelijke toestemming niet meer geldig. Indien dit het geval is, moet opnieuw toestemming worden verkregen.

WP29 adviseert als een beste praktijk om toestemming met passende tussenpozen te vernieuwen. Ook hier helpt het verstrekken van alle informatie om ervoor te zorgen dat de betrokkene goed geïnformeerd blijft over hoe zijn of haar gegevens worden gebruikt, en hoe zijn of haar rechten kunnen worden uitgeoefend⁴⁹.

5.2. Intrekken van toestemming

⁴⁹ Zie WP29 richtsnoeren inzake transparantie. [Aanhaling in afwachting van definitieve tekst]

Het intrekken van toestemming heeft een prominente plaats binnen de AVG. De bepalingen en overwegingen inzake het intrekken van toestemming in de AVG kunnen worden beschouwd als een codificatie van de bestaande interpretatie van dit vraagstuk in WP29 adviezen⁵⁰.

Artikel 7, lid 3 van de AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat het intrekken van toestemming door de betrokkene even eenvoudig moet zijn als het geven ervan. De AVG stelt niet dat het geven en intrekken van informatie altijd plaats moet vinden door middel van dezelfde handeling.

Wanneer toestemming echter wordt verkregen via elektronische middelen, door middel van slechts één muisklik, veeg of toetsenaanslag, moet de betrokkene deze toestemming, in de praktijk, ook even eenvoudig kunnen intrekken. Indien toestemming wordt verkregen door het gebruik van een dienstspecifieke gebruikersinterface (bijvoorbeeld via een website, een app, een gebruikersaccount, de interface van een IoT-apparaat of via e-mail), lijdt het geen twijfel dat de betrokkene zijn of haar toestemming moet kunnen intrekken via dezelfde elektronische interface, omdat overschakelen naar een andere interface enkel voor het intrekken van toestemming buitensporige moeite zou kosten. Voorts moet de betrokkene zijn of haar toestemming kunnen intrekken zonder nadeel. Dit betekent onder meer dat een verwerkingsverantwoordelijke het mogelijk moet maken dat toestemming kosteloos of zonder verslechtering van het serviceniveau wordt ingetrokken⁵¹.

[Voorbeeld 22] Een muziekfestival verkoopt kaartjes via een online ticketservice. Bij elke online verkoop van kaartjes wordt toestemming gevraagd om de contactgegevens voor marketingdoeleinden te gebruiken. Om toestemming voor dit doel te geven, kunnen klanten "Nee" of "Ja" selecteren. De verwerkingsverantwoordelijke informeert de klanten dat zij de mogelijkheid hebben om hun toestemming in te trekken. Hiertoe kunnen ze op werkdagen tussen 8.00 uur en 17.00 uur kosteloos contact opnemen met een callcenter. De verwerkingsverantwoordelijke uit dit voorbeeld voldoet niet aan artikel 7, lid 3 van de AVG. Voor het intrekken van toestemming moet in dit geval tijdens kantooruren een telefoongesprek worden gevoerd. Dit is een grotere moeite dan de ene muisklik die nodig is voor het geven van toestemming via de online ticketservice, die dag en nacht open is.

De eis van het eenvoudig kunnen intrekken van toestemming wordt in de AVG beschreven als een noodzakelijk aspect van geldige toestemming. Als het recht op intrekking niet voldoet aan de eisen van de AVG, dan voldoet het mechanisme voor toestemming van de verwerkingsverantwoordelijke niet aan de AVG. Zoals vermeld in paragraaf 3.1 over de voorwaarde van *geïnformeerde* toestemming moet de verwerkingsverantwoordelijke de betrokkene informeren over het recht op intrekking van toestemming voordat daadwerkelijk toestemming wordt verleend, overeenkomstig

⁵⁰ WP29 heeft dit onderwerp besproken in haar Advies 15/2011 over de definitie van 'toestemming' (WP 187), blz. 9, 13, 20, 27 en 32-33), en, onder meer, haar Advies over het gebruik van locatiegegevens. (Zie Advies 5/2005 over het gebruik van locatiegegevens voor het verstrekken van diensten met toegevoegde waarde (WP 115), blz. 7).

⁵¹ Zie ook WP29 Advies 4/2010 over de Europese gedragscode van FEDMA voor het gebruik van persoonsgegevens in het kader van direct marketing (WP174) en het Advies over het gebruik van locatiegegevens voor het verstrekken van diensten met toegevoegde waarde (WP 115).

artikel 7, lid 3 van de AVG. Daarnaast moet de verwerkingsverantwoordelijke als onderdeel van de transparantieplichting de betrokkenen informeren hoe zij hun rechten kunnen uitoefenen⁵².

Als algemene regel geldt dat als toestemming wordt ingetrokken, alle gegevensverwerkingen die overeenkomstig de AVG waren gebaseerd op toestemming en plaatsgevonden hebben voordat de toestemming werd ingetrokken, rechtmatig blijven, maar de verwerkingsverantwoordelijke wel moet stoppen met de desbetreffende verwerkingsactiviteiten. Als er geen andere rechtsgrond is voor de verwerking (bijv. verdere opslag) van de gegevens, moeten deze door de verwerkingsverantwoordelijke worden gewist⁵³.

Zoals reeds vermeld in deze richtsnoeren is het zeer belangrijk dat verwerkingsverantwoordelijken de doeleinden waarvoor de gegevens daadwerkelijk worden verwerkt en de rechtsgronden waarop de gegevensverwerking is gebaseerd beoordelen voordat zij beginnen met het verzamelen van gegevens. Vaak hebben bedrijven persoonsgegevens nodig voor verschillende doeleinden, en is de verwerking gebaseerd op meer dan één rechtsgrond, klantgegevens kunnen bijvoorbeeld gebaseerd zijn op overeenkomst en toestemming. Daarom betekent het intrekken van toestemming niet dat een verwerkingsverantwoordelijke gegevens moet wissen die verwerkt worden voor een doel dat is gebaseerd op de uitvoering van een overeenkomst met de betrokkene. Verwerkingsverantwoordelijken moeten daarom vanaf het begin duidelijk zijn over welk doel geldt voor elk element van de gegevens en welke rechtsgrond wordt ingeroepen.

Verwerkingsverantwoordelijken zijn verplicht om gegevens te wissen die zijn verwerkt op basis van toestemming nadat deze toestemming is ingetrokken, ervan uitgaande dat er geen ander doel is dat het bewaren van deze gegevens rechtvaardigt⁵⁴.

Naast deze situatie, die bestreken wordt door artikel 17, lid 1, onder b), kan een afzonderlijke betrokkene verzoeken om het wissen van andere gegevens die hem betreffen die zijn verwerkt op basis van een andere rechtsgrond, bijvoorbeeld op basis van artikel 6, lid 1, onder b)⁵⁵. Verwerkingsverantwoordelijken zijn verplicht om na te gaan of verdere verwerking van de betreffende gegevens passend is, zelfs zonder een verzoek tot wissen door de betrokkene.⁵⁶

In gevallen waarin de betrokkene zijn of haar toestemming intrekt en de verwerkingsverantwoordelijke op basis van een andere rechtsgrond door wil gaan met de verwerking van de persoonsgegevens, kan een verwerkingsverantwoordelijke niet stilzwijgend overschakelen van toestemming (die ingetrokken is) op deze andere rechtsgrond. Elke wijziging van de rechtsgrond voor verwerking moet aan de betrokkene worden meegedeeld overeenkomstig

⁵² Overweging 39 AVG, die verwijst naar de artikelen 13 en 14 van deze verordening, bepaalt dat *"Natuurlijke personen moeten bewust worden gemaakt van de risico's, regels, waarborgen en rechten in verband met de verwerking van persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot deze verwerking kunnen uitoefenen."*

⁵³ Zie artikel 17, lid 1, onder b) en artikel 3 AVG.

⁵⁴ In dat geval moet het andere doel dat de verwerking rechtvaardigt een eigen, afzonderlijke rechtsgrond hebben. Dit betekent dat de verwerkingsverantwoordelijke van toestemming kan overstappen op een andere rechtsgrond, zie onderstaand punt 6.

⁵⁵ Zie artikel 17, inclusief mogelijke toepasselijke uitzonderingen, en overweging 65 AVG.

⁵⁶ Zie ook artikel 5, lid 1, onder e) AVG.

de informatievereisten in de artikelen 13 en 14 en op grond van het algemene beginsel van transparantie.

6. Wisselwerking tussen toestemming en andere rechtsgronden in artikel 6 AVG

Artikel 6 bevat de voorwaarden voor een rechtmatige verwerking van persoonsgegevens en beschrijft zes rechtsgronden waarop een verwerkingsverantwoordelijke een beroep kan doen. Voordat begonnen wordt met de verwerkingsactiviteiten moet bepaald worden welke rechtsgrondslag van toepassing is, en in verband met welk specifiek doel⁵⁷.

Het is belangrijk om hier op te merken dat als een verwerkingsverantwoordelijke ervoor kiest om een beroep te doen op toestemming voor een deel van de verwerking, hij bereid moet zijn om de keuzen ten aanzien van toestemming te respecteren, en te stoppen met dat deel van de verwerking als een persoon zijn of haar toestemming intrekt. Het verzenden van een bericht waarin vermeld wordt dat gegevens worden verwerkt op basis van toestemming, terwijl in werkelijkheid een beroep wordt gedaan op een andere rechtsgrond, zou wezenlijk oneerlijk zijn ten aanzien van personen.

Met andere woorden, de verwerkingsverantwoordelijke kan niet van toestemming op een andere rechtsgrond overstappen. Het is bijvoorbeeld niet toegestaan om achteraf de rechtsgrond 'rechtmatig belang' te gebruiken ter rechtvaardiging van verwerking wanneer problemen zijn ondervonden met de geldigheid van toestemming. Wegens de verplichting om ten tijde van het verzamelen van persoonsgegevens de rechtsgrond te verstrekken waarop de verwerkingsverantwoordelijke een beroep doet, moeten verwerkingsverantwoordelijken voordat begonnen wordt met verzamelen beslissen wat de rechtsgrond hiervoor is.

7. Specifieke aandachtspunten in de AVG

7.1. Kinderen (artikel 8)

In vergelijking met de huidige richtlijn creëert de AVG een extra beveiligingslaag voor situaties waarin persoonsgegevens van kwetsbare natuurlijke personen, met name kinderen, worden verwerkt. Artikel 8 voert aanvullende verplichtingen in om te zorgen voor een beter niveau van gegevensbescherming voor kinderen in verband met diensten van de informatiemaatschappij. De redenen voor de verbeterde bescherming zijn vermeld in overweging 38: "*[...] aangezien zij zich allicht minder bewust zijn van de betrokken risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van persoonsgegevens [...]*" Overweging 38 stelt ook dat "*Die specifieke bescherming moet met name gelden voor het gebruik van persoonsgegevens van kinderen voor marketingdoeleinden of voor het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten.*" De woorden "met name" geven aan dat de specifieke bescherming niet beperkt is tot marketing of profilering, maar het bredere "verzamelen van persoonsgegevens over kinderen" omvat.

⁵⁷ Overeenkomstig artikel 13, lid 1, onder c), en/of artikel 14, lid 1, onder c), moet de verwerkingsverantwoordelijke de betrokkene hiervan in kennis stellen.

Artikel 8, lid 1, bepaalt dat indien toestemming van toepassing is, in verband met een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, de verwerking van persoonsgegevens van een kind rechtmatig is wanneer het kind ten minste 16 jaar is. Wanneer het kind jonger is dan 16 jaar, is zulke verwerking slechts rechtmatig indien en voor zover de toestemming of machtiging tot toestemming in dit verband wordt verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt⁵⁸. Ten aanzien van de leeftijdsgrens voor geldige toestemming is de AVG flexibel: lidstaten kunnen bij wet een lagere leeftijd instellen, maar deze leeftijd kan niet lager zijn dan 13 jaar.

Zoals vermeld in paragraaf 3.1 over geïnformeerde toestemming moet de informatie begrijpelijk zijn voor de beoogde doelgroep van de verwerkingsverantwoordelijke, met bijzondere aandacht voor de positie van kinderen. Voor het verkrijgen van "geïnformeerde toestemming" van een kind moet de verwerkingsverantwoordelijke in voor kinderen heldere en duidelijke taal uitleggen voornemens is om de door hem verzamelde gegevens te verwerken⁵⁹. Als de ouder toestemming moet geven, dan kan informatie nodig zijn waarmee volwassenen een geïnformeerde beslissing kunnen nemen.

Uit het voorgaande volgt dat artikel 8 alleen van toepassing is wanneer aan de volgende voorwaarden wordt voldaan:

- De verwerking heeft betrekking op een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind.^{60, 61}
- De verwerking is gebaseerd op toestemming.

7.1.1. Dienst van de informatiemaatschappij

Voor het bepalen van de werkingssfeer van de term "dienst van de informatiemaatschappij" in de AVG, wordt in artikel 4, lid 25 AVG verwezen naar Richtlijn 2015/1535.

Voor de beoordeling van de werkingssfeer van deze definitie, verwijst WP29 tevens naar jurisprudentie van het Europees Hof van Justitie.⁶² Het Hof oordeelde dat *diensten van de*

⁵⁸ Onverminderd de mogelijkheid voor lidstaten om bij wet af te wijken van de leeftijdsgrens, zie artikel 8, lid 1.

⁵⁹ Overweging 58 AVG bevestigt deze verplichting, door de bepaling dat een verwerkingsverantwoordelijke er in voorkomende gevallen voor moet zorgen dat de verstrekte informatie begrijpelijk is voor kinderen.

⁶⁰ Volgens artikel 4, lid 25, AVG, betekent een dienst van de informatiemaatschappij een dienst zoals gedefinieerd onder b) van artikel 1, lid 1, van Richtlijn 2015/1535: b) "dienst": *elke dienst van de informatiemaatschappij, dat wil zeggen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht. Voor de toepassing van deze definitie wordt verstaan onder: i) "op afstand": een dienst die wordt geleverd zonder dat de partijen gelijktijdig aanwezig zijn, ii) "langs elektronische weg": een dienst die wordt verzonden en ontvangen via elektronische apparatuur voor de verwerking (met inbegrip van digitale compressie) en de opslag van gegevens, en die geheel via draden, radio, optische middelen of andere elektromagnetische middelen wordt verzonden, doorgelid en ontvangen, iii) "op individueel verzoek van een afnemer van diensten": een dienst die op individueel verzoek via de transmissie van gegevens wordt geleverd.* In Bijlage I van genoemde richtlijn is een indicatieve lijst van niet onder deze definitie vallend diensten opgenomen. Zie ook overweging 18 van Richtlijn 2000/31/EG.

⁶¹ Volgens het VN-Verdrag inzake de bescherming van het kind, artikel 1, "[...] onder een kind wordt verstaan ieder mens jonger dan achttien jaar, tenzij volgens het op het kind van toepassing zijnde recht de meerderjarigheid eerder wordt bereikt", zie de Algemene Vergadering van de Verenigde Naties bij Resolutie 44/25 van 20 november 1989 (Verdrag inzake de bescherming van het kind).

informatiemaatschappij overeenkomst en andere diensten omvatten die online gesloten of verzonden worden. In het geval dat een dienst twee economische zelfstandige onderdelen omvat, namelijk de online component, zoals het aanbod en de aanvaarding van een aanbod in het kader van het sluiten van een overeenkomst of de informatie met betrekking tot producten en diensten, waaronder marketingactiviteiten, wordt deze component gedefinieerd als een dienst van de informatiemaatschappij, en valt de andere component, namelijk de fysieke levering distributie van goederen niet onder het begrip "dienst van de informatiemaatschappij". De online levering van een dienst valt dus binnen de werkingssfeer van het begrip "*dienst van de informatiemaatschappij*" in artikel 8 AVG.

7.1.2. Rechtstreeks aanbod aan een kind

Het opnemen van de formulering "rechtstreeks aanbod aan een kind" geeft aan dat artikel 8 van toepassing is op bepaalde, maar niet alle diensten van de informatiemaatschappij. Als een verlener van diensten van de informatiemaatschappij het in dit verband duidelijk maakt aan potentiële gebruikers dat hij zijn diensten alleen aanbiedt aan personen van 18 jaar of ouder, en dit niet wordt ondermijnd door ander bewijs (zoals de inhoud van de website of marketingplannen), dan wordt de dienst beschouwd als "rechtstreeks aanbod aan een kind", en is artikel 8 niet van toepassing.

7.1.3. Leeftijd

De AVG bepaalt dat "*De lidstaten kunnen bij wet voorzien in een lagere leeftijd, op voorwaarde dat die leeftijd niet onder 13 jaar ligt*". De verwerkingsverantwoordelijke moet zich bewust zijn van deze verschillende nationale wetgevingen, en rekening houden met de doelgroep voor zijn diensten. Er dient in het bijzonder te worden opgemerkt dat een verwerkingsverantwoordelijke die een grensoverschrijdende dienst aanbiedt, er niet altijd vanuit kan gaan dat het voldoende is om te voldoen aan de wetgeving van een lidstaat waarin hij zijn belangrijkste vestiging heeft, maar dat hij mogelijk ook moet voldoen aan de desbetreffende nationale wetgeving van elke lidstaat waar hij de dienst(en) van de informatiemaatschappij aanbiedt. Dit is afhankelijk van de vraag of een lidstaat ervoor kiest om de plaats van de belangrijkste vestiging van de verwerkingsverantwoordelijke of de woonplaats van de betrokkene te gebruiken als referentiepunt. In de eerste plaats moeten de lidstaten rekening houden met het belang van het kind tijdens het maken van zijn of haar keuze. De Groep moedigt de lidstaten aan om een geharmoniseerde oplossing te zoeken voor deze kwestie.

Bij het aanbieden van diensten van de informatiemaatschappij aan kinderen op basis van toestemming wordt van verwerkingsverantwoordelijken verwacht dat zij zich naar redelijkheid inspannen om te controleren dat de gebruiker de leeftijd voor digitale toestemming heeft bereikt, en deze maatregelen moeten in verhouding staan tot de aard en de risico's van de verwerking.

⁶² Zie Hof van Justitie, 2 december 2010 in zaak C-108/09 (*Ker-Optika*), punten 22 en 28. Ten aanzien van "samengestelde diensten", verwijst WP29 ook naar zaak C-434/15 (*Asociacion Profesional Elite Taxi tegen Uber Systems Spain SL*), punt 40, waarin wordt bepaald dat een dienst van de informatiemaatschappij die een integrerend deel is van een integrerend deel van een dienstenpakket waarvan het hoofdelement geen dienst van de informatiemaatschappij is, (in dit geval een vervoersdienst) niet kan worden gekwalificeerd als een "dienst van de informatiemaatschappij".

Als de gebruikers aangeven dat ze de leeftijd voor digitale toestemming hebben bereikt, kan de verwerkingsverantwoordelijke passende controles uitvoeren om na te gaan of deze bewering klopt. Hoewel de noodzaak om redelijke inspanningen te betrachten om de leeftijd te verifiëren niet uitdrukkelijk in de AVG is opgenomen, is deze wel impliciet vereist, omdat in het geval een kind toestemming geeft wanneer het niet oud genoeg is om zelfstandig geldige toestemming te geven, dit de verwerking van gegevens onrechtmatig maakt.

Als de gebruiker verklaart dat hij of zij de leeftijd voor digitale toestemming nog niet heeft bereikt, kan de verwerkingsverantwoordelijke deze verklaring zonder verdere controles accepteren, maar moet hij vervolgens ouderlijke toestemming verkrijgen en controleren of de persoon die deze toestemming verleent de ouderlijke verantwoordelijkheid heeft.

Leeftijdscontrole mag niet leiden tot overmatige gegevensverwerking. Het mechanisme dat wordt gekozen om de leeftijd van een betrokkene te controleren dient een beoordeling te omvatten van het risico van de voorgenomen verwerking. In sommige situaties kan het zinvol zijn om een nieuwe abonnee op een dienst te verplichten om zijn of haar geboortjaar te vermelden of om een formulier in te vullen waarin verklaard wordt dat hij of zij (geen) minderjarige is⁶³. Bij twijfel dient de verwerkingsverantwoordelijke zijn mechanismen voor leeftijdscontrole in bepaalde gevallen te herzien en na te gaan of alternatieve controles nodig zijn⁶⁴.

7.1.4. Toestemming van kinderen en ouderlijke verantwoordelijkheid

Met betrekking tot de toestemming van de persoon die de ouderlijke verantwoordelijkheid draagt, verschaft de AVG geen praktische manieren vast waarop de toestemming van de ouder moet worden verzameld of om vast te stellen dat iemand gerechtigd is om deze handeling uit te voeren⁶⁵. Daarom beveelt WP29 aan om een proportionele aanpak te volgen, in lijn met artikel 8, lid 2, AVG en artikel 5, lid 1, onder c) AVG (gegevensminimalisering). Een proportionele aanpak kan gericht zijn op het verkrijgen van een beperkte hoeveelheid gegevens, zoals contactgegevens van een ouder of voogd.

Wat redelijk is, zowel in termen van het controleren of een gebruiker oud genoeg is om zelf toestemming te verlenen, als in termen van het controleren of een persoon die namens een kind toestemming verleent de ouderlijke verantwoordelijkheid draagt, kan afhankelijk zijn van de risico's die de verwerking met zich meebrengt en de beschikbare technologie. In gevallen met weinig risico kan controle van de ouderlijke verantwoordelijkheid via e-mail volstaan. In risicovolle gevallen kan het daarentegen zinvol zijn om te vragen om meer bewijs, zodat de verwerkingsverantwoordelijke de informatie kan controleren en bewaren overeenkomstig artikel 7, lid 1, AVG⁶⁶. Controlediensten

⁶³ Hoewel dit niet in alle gevallen een waterdichte oplossing zal zijn, is het wel een voorbeeld hoe met deze bepaling kan worden omgegaan.

⁶⁴ Zie WP29 Advies 5/2009 over online sociale netwerken (WP163).

⁶⁵ WP29 merkt op dat het niet altijd zo is dat de houder van de ouderlijke verantwoordelijkheid ook de natuurlijke ouder van het kind is, en dat de ouderlijke verantwoordelijkheid kan worden gedragen door meerdere partijen, waaronder zowel rechtspersonen als natuurlijke personen.

⁶⁶ Een ouder of voogd kan bijvoorbeeld worden gevraagd om, via een overboeking, een betaling van € 0,01 aan de verwerkingsverantwoordelijke uit te voeren, inclusief een korte bevestiging in de omschrijving van de transactie dat de

die worden uitgevoerd door vertrouwde derden kunnen oplossingen bieden die de hoeveelheid persoonsgegevens minimaliseren die de verwerkingsverantwoordelijke zelf moet verwerken.

[Voorbeeld 23] Een online gamingplatform wil er zeker van zijn dat zijn minderjarige klanten zich alleen abonneren op zijn diensten met toestemming van hun ouders of voogd. De verwerkingsverantwoordelijke volgt de onderstaande stappen:

Stap 1: De gebruiker vragen of hij jonger of ouder is dan 16 jaar (of de alternatieve leeftijd voor digitale toestemming)

Als de gebruiker verklaart dat hij jonger is dan de vereiste leeftijd voor digitale toestemming:

Stap 2: De dienst informeert het kind dat een ouder of voogd toestemming moet verlenen of akkoord moet gaan met de verwerking voordat de diensten aan het kind kunnen worden aangeboden. De gebruiker wordt gevraagd om een e-mailadres van een ouder of voogd te verstrekken.

Stap 3: De dienst neemt contact op met de ouder of voogd en verkrijgt via e-mail zijn of haar toestemming voor verwerking en neemt redelijke maatregelen om te bevestigen dat de volwassene de ouderlijke verantwoordelijkheid heeft.

Stap 4: In geval van klachten voert het platform extra stappen uit om de leeftijd van de abonnee te controleren.

Indien het platform heeft voldaan aan de overige eisen voor toestemming, kan het platform voldoen aan de aanvullende criteria van artikel 8 AVG door deze stappen te volgen.

Dit voorbeeld toont aan dat de verwerkingsverantwoordelijke zich in een positie kan plaatsen waarin hij in staat is om aan te tonen dat redelijke inspanningen zijn betracht om te controleren dat geldige toestemming is verkregen met betrekking van de aan het kind aangeboden diensten. Artikel 8, lid 2 voegt specifiek toe dat *"Met inachtneming van de beschikbare technologie doet de verwerkingsverantwoordelijke redelijke inspanningen om in dergelijke gevallen te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend."*

Het is aan de verwerkingsverantwoordelijke om te bepalen welke maatregelen in een bepaald geval passend zijn. Als algemene regel geldt dat verwerkingsverantwoordelijken controlemethodes die op zichzelf buitensporige verzameling van persoonsgegevens omvatten moeten vermijden.

WP29 erkent dat zich gevallen kunnen voordoen waarin controle een uitdaging is (bijvoorbeeld in het geval dat kinderen die zelf toestemming verlenen nog geen 'identiteitsvoetafdruk' hebben, of waarin het niet gemakkelijk is om ouderlijke verantwoordelijkheid te controleren. Hiermee kan rekening worden gehouden bij het bepalen welke inspanningen redelijk zijn, maar er wordt wel van verwerkingsverantwoordelijken verwacht dat ze hun processen en de beschikbare technologie doorlopend toetsen.

Met betrekking tot de zelfstandigheid van de betrokkene om toestemming te verlenen voor de verwerking van zijn of haar persoonsgegevens en volledige controle te hebben over de verwerking, kan de toestemming door een drager van ouderlijke verantwoordelijkheid of een machtiging tot toestemming van een drager van ouderlijke verantwoordelijkheid worden bevestigd, gewijzigd of

houder van de bankrekening een persoon is die de ouderlijke verantwoordelijkheid voor de gebruiker draagt. In voorkomende gevallen moet een alternatieve controlemethode worden aangeboden om buitensporige discriminerende behandeling van personen die geen bankrekening hebben te voorkomen.

ingetrokken nadat de betrokkene de leeftijd voor het verlenen van digitale toestemming heeft bereikt.

In de praktijk betekent dit dat als het kind geen actie onderneemt, de door een drager van ouderlijke verantwoordelijkheid verleende toestemming of machtiging tot toestemming voor de verwerking van de persoonsgegevens voorafgaand aan het door de betrokkene bereiken van de leeftijd voor het verlenen van digitale toestemming, een geldige grond voor verwerking blijft.

Nadat het kind de leeftijd voor het verlenen van digitale toestemming heeft bereikt, heeft het de mogelijkheid om de toestemming, in overeenstemming met artikel 7, lid 3), zelf in te trekken. Overeenkomstig de beginselen van behoorlijkheid en verantwoording moet de verwerkingsverantwoordelijke het kind informeren over deze mogelijkheid⁶⁷.

Het is belangrijk om erop te wijzen dat overeenkomstig overweging 38 toestemming door een ouder of voogd niet vereist is in het kader van een preventieve dienstverlening of begeleidingsdiensten die rechtstreeks aan een kind worden aangeboden. Voor het online aanbieden van diensten in verband met kinderscherming door middel van een online chatservice is bijvoorbeeld geen voorafgaande ouderlijke toestemming vereist.

Ten slotte bepaald de AVG dat de regels betreffende de eisen voor ouderlijke toestemming ten aanzien van minderjarigen geen afbreuk mogen doen aan het "algemene overeenkomstenrecht van de lidstaten, zoals de regels inzake de geldigheid, de totstandkoming of de gevolgen van overeenkomsten ten opzichte van kinderen". Daarom maken de eisen voor geldige toestemming voor het gebruik van gegevens over kinderen onderdeel uit van een wetgevingskader dat moet worden beschouwd als een kader dat los staat van nationaal overeenkomstenrecht. Daarom wordt in deze richtsnoeren niet ingegaan op de vraag of het al dan niet rechtmatig is voor een minderjarige om online overeenkomsten te sluiten. Beide rechtsregelingen kunnen tegelijk van toepassing zijn, en de werkingssfeer van de AVG omvat niet de harmonisatie van nationale bepalingen van overeenkomstenrecht.

7.2. Wetenschappelijk onderzoek

De definitie van wetenschappelijke doeleinden heeft aanzienlijke gevolgen voor het bereik van verwerkingsactiviteiten die een verwerkingsverantwoordelijke kan uitvoeren. Het begrip "*wetenschappelijk onderzoek*" wordt in de AVG niet gedefinieerd. Overweging 159 stelt "(...) Voor de toepassing van deze verordening moet de verwerking van persoonsgegevens met het oog op wetenschappelijk onderzoek ruim worden opgevat. (...)"; WP 29 is echter van mening dat het begrip niet kan verder kan worden opgerekt dan de gebruikelijke betekenis, en vat "*wetenschappelijk onderzoek*" in deze context op als een onderzoeksproject dat opgezet wordt in overeenstemming met de relevante methodologische en ethische normen van de sector, en conform goede praktijken.

Wanneer toestemming de rechtsgrond is voor het uitvoeren van onderzoek in overeenstemming met de AVG, moet deze toestemming voor het gebruik van persoonsgegevens worden onderscheiden

⁶⁷ Betrokkenen moeten zich ook bewust zijn van het recht op vergetelheid, zoals vastgelegd in artikel 17, wat met name relevant is voor toestemming die is gegeven toen de betrokkene nog een kind was, zie overweging 63.

van andere eisen voor toestemming die dienen als een ethische norm of een procedurele verplichting. Een voorbeeld van een dergelijke procedurele verplichting, waarbij verwerking niet gebaseerd is op toestemming maar op een andere rechtsgrond, is te vinden in de verordening inzake klinische proeven. In het kader van de wetgeving inzake gegevensbescherming kan deze vorm van toestemming worden beschouwd als een extra waarborg⁶⁸. Tegelijkertijd beperkt de AVG met betrekking tot de verwerking van gegevens voor onderzoeksdoeleinden de toepassing van artikel 6 niet tot alleen toestemming. Zolang passende waarborgen zijn ingesteld, zoals de eisen op grond van artikel 89, lid 1, en de verwerking behoorlijk, rechtmatig en transparant is en in overeenstemming met de normen voor gegevensminimalisering en individuele rechten, kunnen andere rechtsgronden, zoals artikel 6, lid 1, onder e) of f) worden gebruikt⁶⁹. Op grond van de uitzondering van artikel 9, lid 2, geldt dit ook voor bijzondere categorieën gegevens⁷⁰.

Overweging 33 lijkt een zekere mate van flexibiliteit te verschaffen voor de mate van specificering en granulariteit van toestemming in het kader van wetenschappelijk onderzoek. Overweging 33 stelt: *"Het is vaak niet mogelijk op het ogenblik waarop de persoonsgegevens worden verzameld, het doel van de gegevensverwerking voor wetenschappelijke onderzoeksdoeleinden volledig te omschrijven. Daarom moet de betrokkenen worden toegestaan hun toestemming te geven voor bepaalde terreinen van het wetenschappelijk onderzoek waarbij erkende ethische normen voor wetenschappelijk onderzoek in acht worden genomen. Betrokkenen moeten de gelegenheid krijgen om hun toestemming alleen te geven voor bepaalde onderzoeksterreinen of onderdelen van onderzoeksprojecten, voor zover het voorgenomen doel zulks toelaat."*

Ten eerste moet worden opgemerkt dat overweging 33 de verplichtingen ten aanzien van de eis van specifieke toestemming niet buiten toepassing laat. Dit betekent dat wetenschappelijke onderzoeksprojecten in beginsel alleen persoonsgegevens op basis van toestemming mogen omvatten als een dergelijk project een goed omschreven doel heeft. Voor gevallen waarin de doeleinden voor gegevensverwerking binnen een wetenschappelijk onderzoeksproject aanvankelijk niet kunnen worden gespecificeerd, staat overweging 33 als uitzondering toe dat het doel op een meer algemeen niveau kan worden omschreven.

Gezien de strenge eisen die door artikel 9 AVG worden gesteld betreffende de verwerking van bijzondere categorieën gegevens, merkt WP29 op dat in het geval bijzondere categorieën gegevens worden verwerkt op basis van uitdrukkelijke toestemming, op de toepassing van de flexibele aanpak van overweging 33 een striktere interpretatie van toepassing is een hoge mate van controle vereist.

Als één geheel beschouwd kan de AVG niet worden uitgelegd om een verwerkingsverantwoordelijke toe te staan om rond het belangrijke uitgangspunt van het specificeren van doeleinden waarvoor toestemming van de betrokkene wordt gevraagd te laveren.

⁶⁸ Zie ook overweging 161 van de AVG.

⁶⁹ Artikel 6, lid 1, onder c), kan ook van toepassing zijn op delen van verwerkingsactiviteiten die uitdrukkelijke wettelijk verplicht zijn, zoals het verzamelen van betrouwbare en eerlijke gegevens op grond van het protocol dat door de lidstaat aangenomen is op grond van de verordening inzake klinische proeven.

⁷⁰ Op grond van artikel 9, lid 2, onder i), kunnen specifieke tests van geneesmiddelen kunnen worden uitgevoerd op basis van communautaire of nationale wetgeving.

Wanneer onderzoeksdoeleinden niet kunnen worden gespecificeerd, moet een verwerkingsverantwoordelijke andere manieren vinden om ervoor te zorgen dat zo goed mogelijk wordt voldaan aan de eisen voor toestemming, bijvoorbeeld door betrokkenen toe te staan om in algemenere termen toestemming te geven voor een onderzoeksdoelstelling en voor specifieke fases van een onderzoeksproject waarvan bij aanvang reeds bekend is dat deze zullen worden uitgevoerd. Naarmate het onderzoek vordert, kan toestemming voor verdere stappen in het project verkregen worden voordat een volgende fase van start gaat. Dergelijke toestemming moet echter nog steeds in overeenstemming zijn met de geldende ethische normen voor wetenschappelijk onderzoek.

Bovendien kan de verwerkingsverantwoordelijke in dergelijke gevallen nadere waarborgen instellen. Zo wijst artikel 89, lid 1, bijvoorbeeld op de noodzaak voor waarborgen voor verwerkingsactiviteiten voor wetenschappelijke of historisch onderzoek of statistische doeleinden. Deze doeleinden *"zijn onderworpen aan passende waarborgen in overeenstemming met deze verordening voor de rechten en vrijheden van de betrokkene"*. Als mogelijke waarborgen worden gegevensminimalisering, anonimisering en gegevensbeveiliging genoemd.⁷¹ Wanneer het doel van het onderzoek kan worden gerealiseerd zonder de verwerking van persoonsgegevens, is anonimisering de aangewezen oplossing.

Transparantie is een extra waarborg wanneer de omstandigheden van het onderzoek specifieke toestemming niet mogelijk maken. Een gebrek aan specificatie van een doel kan worden gecompenseerd door het regelmatige verstrekken van informatie over de ontwikkeling van het doel door de verwerkingsverantwoordelijken in de loop van het onderzoeksproject, zodat de toestemming na verloop van tijd zo specifiek mogelijk is. Wanneer dit gebeurt, heeft de betrokkene ten minste een basiskennis van de stand van zaken, wat hem of haar in staat stelt om te kunnen beslissen om bijvoorbeeld al dan niet gebruik te maken van het recht om toestemming in te trekken op grond van artikel 7, lid 3⁷².

Ook een uitgebreid onderzoeksplan dat betrokkenen kunnen inzien alvorens zij toestemming verlenen, kan bijdragen tot het compenseren van een gebrek aan specificatie van doeleinden⁷³. In dit

⁷¹ Zie bijvoorbeeld overweging 156. De verwerking van persoonsgegevens voor wetenschappelijke doeleinden dient ook te voldoen aan andere relevante wetgeving, zoals de wetgeving inzake klinische proeven, zie overweging 156, waarin Verordening (EU) 536/2014 van het Europees parlement en de Raad van 16 april 2014 inzake klinische proeven met geneesmiddelen voor menselijk gebruik wordt genoemd. Zie ook WP29 Advies 15/2011 over de definitie van 'toestemming' (WP 187), blz. 7: *"Bovendien ontslaat het verkrijgen van toestemming de voor de verwerking verantwoordelijke niet van de in artikel 6 neergelegde verplichtingen met betrekking tot eerlijkheid, noodzaak en proportionaliteit en de kwaliteit van gegevens. Ook als het verwerken van persoonsgegevens met toestemming van de betrokkene gebeurt, mogen bijvoorbeeld niet meer gegevens worden verzameld dan voor een bepaald doeleinde noodzakelijk is."* [...] *'Toestemming' moet niet worden gezien als een uitzondering op de andere beginselen van gegevensbescherming, maar als een waarborg. Het is allereerst een rechtmatigheidsgrond en ontheft de voor de verwerking verantwoordelijke niet van het toepassen van de andere beginselen."*

⁷² Ook andere maatregelen met betrekking tot transparantie kunnen zinvol zijn. Wanneer verwerkingsverantwoordelijken gegevensverwerking voor wetenschappelijke doeleinden uitvoeren en bij aanvang van het onderzoek geen volledige informatie kan worden verstrekt, kunnen ze een specifieke contactpersoon aanwijzen waarmee betrokkenen contact kunnen opnemen als ze vragen hebben.

⁷³ Een dergelijke mogelijkheid kan bijvoorbeeld worden gevonden in artikel 14, lid 1, in de huidige Wet inzake persoonsgegevens van Finland (*Henkilötietolaki*, 523/1999)

onderzoeksplan moeten de voorziene onderzoeksvragen en werkwijze zo duidelijk mogelijk worden beschreven. Het onderzoeksplan kan ook bijdragen aan naleving van artikel 7, lid 1, omdat verwerkingsverantwoordelijken moeten aantonen welke informatie voor betrokkenen beschikbaar was op het moment dat ze toestemming verleenden, om te kunnen aantonen dat de toestemming geldig is.

Het is belangrijk om in gedachten te houden dat in het geval toestemming wordt gebruikt als de rechtsgrond voor verwerking, de betrokkene een mogelijkheid moet hebben om deze toestemming in te trekken. WP29 merkt op dat het intrekken van toestemming zou kunnen leiden tot ondermijning van bepaalde soorten wetenschappelijk onderzoek waarvoor aan personen gekoppelde gegevens nodig zijn, de AVG is echter duidelijk dat toestemming moet kunnen worden ingetrokken en dat verwerkingsverantwoordelijken hiernaar moeten handelen – voor wetenschappelijk onderzoek geldt geen uitzondering op deze eis. Wanneer een verwerkingsverantwoordelijke een verzoek tot intrekking ontvangt, moet hij in beginsel de persoonsgegevens meteen wissen als hij de gegevens wil blijven gebruiken voor de onderzoeksdoeleinden⁷⁴.

7.3. De rechten van betrokkenen

Als de gegevensverwerking is gebaseerd op toestemming van de betrokkene, dan heeft dit gevolgen voor de rechten van de persoon. Wanneer de verwerking is gebaseerd op toestemming, hebben betrokkenen mogelijk het recht op overdraagbaarheid van gegevens (artikel 20). Tegelijkertijd is het recht van bezwaar (artikel 21) niet van toepassing wanneer verwerking is gebaseerd op toestemming, hoewel het recht om op elk gewenst moment de toestemming in te trekken een vergelijkbaar resultaat kan hebben.

Artikel 16 tot en met 20 van de AVG geeft aan dat (bij gegevensverwerking op basis van toestemming) betrokkenen het recht hebben op het wissen van gegevens wanneer toestemming is ingetrokken, alsmede het recht op beperking, rectificatie en inzage⁷⁵.

8. Toestemming verkregen krachtens Richtlijn 95/46/EG

Verwerkingsverantwoordelijken die momenteel gegevens verwerken op basis van toestemming in overeenstemming met nationale wetgeving inzake gegevensbescherming worden niet automatisch verplicht om alle bestaande relaties op basis van toestemming bij de voorbereiding op de AVG te hernieuwen. Tot op heden verkregen toestemming blijft geldig voor zover deze in overeenstemming is met de voorwaarden die zijn vastgelegd in de AVG.

Het is belangrijk dat verwerkingsverantwoordelijken de bestaande werkprocessen en registratiemethodes vóór 25 mei 2018 nauwgezet evalueren om er zeker van te zijn dat de toestemming voldoet aan de standaard van de AVG (zie overweging 171 van de AVG⁷⁶). In de

⁷⁴ Zie ook WP29 Advies 05/2014 over anonimiseringstechnieken (WP216).

⁷⁵ In gevallen waarin bepaalde verwerkingsactiviteiten worden beperkt overeenkomstig artikel 18 AVG, kan toestemming van de betrokkene nodig kan zijn op de beperkingen op te heffen.

⁷⁶ Overweging 171 van de AVG stelt: "*Richtlijn 95/46/EG dient door deze verordening te worden vervangen. Verwerkingen die al gaande zijn op de datum van toepassing van deze verordening, dienen overeenkomstig deze*

praktijk legt de AVG ten aanzien van het instellen van mechanismen voor toestemming de lat hoger en voert verschillende nieuwe eisen in waardoor verwerkingsverantwoordelijken mechanismen voor toestemming moeten veranderen, en alleen het herschrijven van privacybeleid niet voldoende is⁷⁷.

Omdat de AVG bijvoorbeeld vereist dat een verwerkingsverantwoordelijke in staat moet zijn om aan te tonen dat geldige toestemming is verkregen, worden alle veronderstelde toestemming waarover geen bewijs wordt bewaard, automatisch beschouwd als onder de standaard voor toestemming van de AVG, en moeten deze worden hernieuwd. En omdat de AVG een "verklaring of een ondubbelzinnige actieve handeling" vereist, voldoen alle veronderstelde toestemmingen die gebaseerd zijn op een meer impliciete vorm van handelen door de betrokkene (bijvoorbeeld een vooraf aangevinkte opt-invakje) eveneens niet aan de standaard voor toestemming van de AVG.

Daarnaast kan het om aan te tonen dat toestemming is verkregen of een meer granulaire indicatie van de wensen van de betrokkenen mogelijk te maken, nodig zijn om bedrijfsactiviteiten en IT-systemen te herzien. Mechanismen waarmee betrokkenen hun toestemming kunnen intrekken, moeten ook eenvoudig beschikbaar zijn, en er moet informatie worden verstrekt over hoe toestemming kan worden ingetrokken. Indien de bestaande procedures voor het verkrijgen van toestemming niet voldoen aan de standaarden van de AVG, moeten verwerkingsverantwoordelijken nieuwe toestemming in overeenstemming met de AVG verkrijgen.

Omdat voor geïnformeerde toestemming echter niet alle elementen die genoemd worden in artikel 13 en 14 altijd aanwezig moeten zijn, zijn de uitgebreide informatieverplichtingen in de AVG niet altijd in strijd met het voortbestaan van toestemming die is verleend vóór de inwerkingtreding van de AVG (zie pagina 15). Krachtens Richtlijn 95/46/EG bestond er geen verplichting om betrokkenen te informeren over de rechtsgrond waarop de verwerking werd uitgevoerd.

In het geval een verwerkingsverantwoordelijke vaststelt dat de toestemming die eerder op grond van de oude wetgeving is verkregen niet voldoet aan de standaard van de AVG, moet hij actie ondernemen om wel aan deze standaard te voldoen, bijvoorbeeld door het vernieuwen van toestemming op een manier die in overeenstemming is met de AVG. Krachtens de AVG kan niet worden overgestapt van de ene op de andere rechtsgrond. In het geval een verwerkingsverantwoordelijke niet op een met de AVG overeenstemmende wijze opnieuw toestemming kan verkrijgen, en ook niet – als een eenmalige situatie – kan voldoen aan de AVG door de gegevensverwerking te baseren op een andere rechtsgrond om ervoor te zorgen dat verdere verwerking eerlijk en verantwoord is, moet met de verwerkingsactiviteiten worden gestopt. De

verordening te worden gebracht binnen twee jaar na de inwerkingtreding ervan. Om de verwerkingsverantwoordelijke in staat te stellen na de datum van toepassing van deze verordening de verwerking voort te zetten, hoeft de betrokkene voor een verwerking waarmee hij krachtens Richtlijn 95/46/EG heeft ingestemd op een manier die aan de voorwaarden van deze verordening voldoet, niet nog eens toestemming te geven. Besluiten van de Commissie en door de toezichthoudende autoriteiten verleende toestemmingen die op Richtlijn 95/46/EG zijn gebaseerd, blijven van kracht totdat zij worden gewijzigd, vervangen of ingetrokken."

⁷⁷ Zoals in de inleiding vermeld, geeft de AVG een nadere toelichting en specificatie van de vereisten voor het verkrijgen en aantonen van geldige toestemming. Veel van de nieuwe eisen bouwen voort op *Opinie 15/2011 inzake 'toestemming'*.

verwerkingsverantwoordelijke moet in ieder geval voldoen aan de beginselen van rechtmatige, behoorlijke en transparante verwerking.

***** EINDE DOCUMENT *****