

Richtsnoeren



Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679

Versie 1.1

Vastgesteld op 4 mei 2020

Translations proofread by EDPB Members.

This language version has not been proofread.

Versiegeschiedenis

Versie 1.1	13 mei 2020	Formatteringscorrecties
Versie 1.0	4 mei 2020	Vaststelling van de richtsnoeren

Inhoudsopgave

0	Vooraf.....	4
1	Inleiding.....	5
2	Toestemming in artikel 4, punt 11, van de AVG.....	6
3	Elementen van geldige toestemming.....	7
3.1	Vrij/vrijelijk gegeven.....	7
3.1.1	Wanverhouding.....	8
3.1.2	Conditionaliteit.....	10
3.1.3	Granulariteit.....	13
3.1.4	Nadeel.....	14
3.2	Specifiek.....	15
3.3	Geïnformeerd.....	16
3.3.1	De minimale inhoudelijke eisen inzake “geïnformeerde” toestemming.....	17
3.3.2	Hoe moet informatie worden verstrekt?.....	18
3.4	Ondubbelzinnige wilsuiting.....	20
4	Het verkrijgen van de uitdrukkelijke toestemming.....	22
5	Aanvullende voorwaarden voor het verkrijgen van geldige toestemming.....	25
5.1	Toestemming aantonen.....	25
5.2	Intrekking van toestemming.....	26
6	Wisselwerking tussen toestemming en andere rechtsgronden in artikel 6 AVG.....	28
7	Specifieke aandachtspunten in de AVG.....	29
7.1	Kinderen (artikel 8).....	29
7.1.1	Dienst van de informatiemaatschappij.....	30
7.1.2	Rechtstreeks aanbod aan een kind.....	31
7.1.3	Leeftijd.....	31
7.1.4	Toestemming van kinderen en ouderlijke verantwoordelijkheid.....	32
7.2	Wetenschappelijk onderzoek.....	35
7.3	De rechten van betrokkenen.....	37
8	Toestemming verkregen overeenkomstig Richtlijn 95/46/EG.....	38

Het Europees Comité voor gegevensbescherming (*European Data Protection Board, EDPB*)

Gezien artikel 70, lid 1, onder e), van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna “AVG” genoemd),

Gezien de EER-overeenkomst en in het bijzonder bijlage XI en protocol 37 van die overeenkomst, als gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018¹,

Gezien de artikelen 12 en 22 van zijn reglement van orde,

Gezien de richtsnoeren van de Groep artikel 29 (*Article 29 Working Party, WP29*) inzake toestemming overeenkomstig Verordening 2016/679, WP259 versie 01,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD

0 VOORAF

Op 10 april 2018 heeft de Groep artikel 29 zijn richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 (WP259 versie 1) vastgesteld, die de EDPB op zijn eerste plenaire vergadering heeft goedgekeurd. Dit document is een licht bijgewerkte versie van die richtsnoeren. Elke verwijzing naar de WP29-richtsnoeren inzake toestemming (WP259 versie 1) dient voortaan als een verwijzing naar de onderhavige richtsnoeren te worden opgevat.

De EDPB heeft vastgesteld dat er behoefte is aan nadere verduidelijking, met name met betrekking tot twee punten:

- 1 de geldigheid van toestemming die de betrokkene verleent bij de interactie met zogenoemde “cookie walls”;
- 2 voorbeeld 16 over scrolling en toestemming.

De paragrafen over die twee zaken zijn herzien en bijgewerkt, terwijl de rest van het document ongewijzigd is gebleven, afgezien van redactionele wijzigingen. De herziening betreft met name:

-) het hoofdstuk over conditionaliteit (paragrafen 38 - 41),
-) het hoofdstuk over ondubbelzinnige wilsuiting (paragraaf 86).

¹ Verwijzingen naar “lidstaten” in dit document moeten worden gelezen als verwijzingen naar “lidstaten van de EER”.

1 INLEIDING

1. Deze richtsnoeren verschaffen een gedegen analyse van het begrip “toestemming” in de AVG. Het in de richtlijn gegevensbescherming (Richtlijn 95/46/EG) en in de e-privacyrichtlijn gehanteerde begrip “toestemming” is geëvolueerd. In de AVG zijn de vereisten voor het verkrijgen en aantonen van geldige toestemming nader toegelicht en gespecificeerd. Deze richtsnoeren gaan op die veranderingen in. 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” van de Groep artikel 29. Verwerkingsverantwoordelijken moeten nieuwe oplossingen vinden die met de wetgeving stroken en de bescherming van persoonsgegevens en de belangen van de betrokkenen beter ondersteunen.
2. Toestemming blijft een van de zes rechtsgronden voor de verwerking van persoonsgegevens, zoals beschreven in artikel 6 AVG². Bij het opzetten van activiteiten die verwerking van persoonsgegevens omvatten, moet een verwerkingsverantwoordelijke altijd de tijd nemen om na te gaan wat de passende rechtsgrond is voor de geplande verwerking.
3. In het algemeen kan toestemming alleen een passende rechtsgrond zijn als een betrokkene controle kan uitoefenen en echt een keuze heeft met betrekking tot het accepteren of afwijzen van de aangeboden voorwaarden of het afwijzen ervan zonder nadeel. Wanneer de verwerkingsverantwoordelijke om toestemming verzoekt, heeft hij de plicht om na te gaan aan alle vereisten voor het verkrijgen van geldige toestemming is voldaan. Indien de toestemming geheel overeenkomstig de AVG wordt verkregen, is toestemming een instrument dat de betrokkenen controle geeft over het al dan niet verwerken van hun persoonsgegevens. Indien dit niet het geval is, is deze controle van de betrokkene slechts schijn, en geen geldige grond voor verwerking, waardoor de verwerkingsactiviteiten onrechtmatig worden³.
4. De bestaande adviezen over toestemming van de Groep artikel 29⁴ blijven relevant, voor zover ze verenigbaar zijn met het nieuwe wetgevingskader, omdat de bestaande richtsnoeren en algemene goede praktijken van de Groep artikel 29 in de AVG zijn vastgelegd, en de meeste kernelementen van toestemming in het kader van de AVG gelijk blijven. Daarom worden door de EDPB in dit document eerdere adviezen van de Groep artikel 29 over specifieke onderwerpen, waaronder verwijzing naar toestemming overeenkomstig Richtlijn 95/46/EG, verder ontwikkeld en aangevuld en vormt dit document geen vervanging van eerdere adviezen.
5. Zoals vermeld in Advies 15/2011 van de Groep artikel 29 over de definitie van “toestemming”, moet het aan personen vragen om in te stemmen met een gegevensverwerking aan strenge eisen zijn onderworpen, omdat het hierbij gaat om de grondrechten van de betrokkenen, en de verwerkingsverantwoordelijke een gegevensverwerking wil uitvoeren die zonder de toestemming van

² 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.

³ Zie ook Advies 15/2011 van de Groep artikel 29 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.

⁴ Dit geldt met name voor Advies 15/2011 over de definitie van “toestemming” (WP 187).

de betrokkene onrechtmatig zou zijn⁵. De cruciale rol van toestemming wordt onderstreept door de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie. Het feit dat toestemming is verkregen betekent evenmin dat de verwerkingsverantwoordelijke niet langer of in mindere mate gehouden is 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. Ook als de verwerking van persoonsgegevens op de toestemming van de betrokkene is gebaseerd, wettigt dit niet het verzamelen van gegevens die niet noodzakelijk zijn voor een specifiek doel van verwerking; een dergelijke verwerking zou wezenlijk oneerlijk zijn⁶.

6. Ondertussen is de EDPB zich bewust van de herziening van de e-privacy-richtlijn (2002/58/EG). Het begrip “toestemming” in de ontwerpverordening e-privacy blijft gekoppeld aan het begrip “toestemming” in de AVG⁷. Organisaties zullen op grond van de herziene e-privacy-verordening waarschijnlijk toestemming nodig hebben voor de meeste online marketingberichten of marketingoproepen en online traceermethodes, zoals die waarvoor gebruik wordt gemaakt van cookies of apps of andere software. De EDPB heeft reeds aanbevelingen en richtsnoeren verstrekt aan de Europese wetgever voor het voorstel voor een verordening inzake e-privacy⁸.
7. Met betrekking tot de bestaande e-privacy-richtlijn merkt de EDPB op dat verwijzingen naar de ingetrokken Richtlijn 95/46/EG moeten worden gelezen als verwijzingen naar de AVG⁹. 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 was. Overeenkomstig artikel 95 AVG mogen er geen aanvullende verplichtingen worden opgelegd met betrekking tot verwerking in verband met het verstrekken van openbare elektronische communicatiediensten in openbare communicatienetwerken, voor zover zij op grond van de e-privacy-richtlijn onderworpen zijn aan specifieke verplichtingen met dezelfde doelstelling. De EDPB merkt op dat de vereisten voor toestemming overeenkomstig de AVG niet worden beschouwd als een “aanvullende verplichting”, maar als randvoorwaarden voor rechtmatige verwerking. Daarom zijn de vereisten van de AVG voor het verkrijgen van geldige toestemming van toepassing in situaties die binnen het toepassingsgebied van de e-privacy-richtlijn vallen.

2 TOESTEMMING IN ARTIKEL 4, PUNT 11, VAN DE AVG

8. Artikel 4, punt 11, van de AVG definieert toestemming als: “elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een

⁵ Advies 15/2011 over de definitie van “toestemming” (WP 187), blz. 8.

⁶ Zie ook Advies 15/2011 over de definitie van “toestemming” (WP 187) en artikel 5 AVG.

⁷ 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.

⁸ Zie [EDBP-verklaring over ePrivacy - 25/05/2018](#) en [EDPB-verklaring 3/2019 over een ePrivacy-verordening](#).

⁹ Zie artikel 94 AVG.

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

9. Het basisconcept van toestemming blijft vergelijkbaar met dat van Richtlijn 95/46/EU en toestemming is een van de rechtsgronden waarop verwerking van persoonsgegevens moet zijn gebaseerd overeenkomstig artikel 6 van de AVG¹⁰. Naast de gewijzigde definitie in artikel 4, punt 11, verstrekt de AVG aanvullende richtsnoeren in artikel 7 en in de overwegingen 32, 33, 42 en 43 over hoe de verwerkingsverantwoordelijke moet handelen om te voldoen aan de belangrijkste elementen van het vereiste van toestemming.
10. 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

11. Overeenkomstig artikel 4, punt 11, van de AVG wordt onder toestemming van de betrokkene verstaan:
 -) elke 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.
12. In de onderstaande hoofdstukken wordt geanalyseerd in hoeverre de formulering van artikel 4, punt 11, vereist dat verwerkingsverantwoordelijken hun toestemmingsverzoeken/-formulieren wijzigen om naleving van de AVG te waarborgen¹¹.

3.1 Vrij/vrijelijk gegeven¹²

¹⁰ 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”, en deze toestemming dient “ondubbelzinnig” te zijn, wil de verwerking van persoonsgegevens rechtmatig zijn (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 dat advies heeft WP29 richtsnoeren verstrekt om onderscheid te maken tussen situaties waarin toestemming een passende rechtsgrond is en situaties waarin de grond van rechtmatige belangen (misschien met een mogelijkheid tot opt-out) voldoende is, of een contractuele relatieaanbeveling verdient. 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.

¹¹ 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.

¹² In diverse adviezen heeft de Groep artikel 29 zich gebogen over de grenzen van toestemming in situaties waarin deze niet vrijelijk kan worden verleend. 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

13. Het element “vrij” impliceert werkelijke keuze en controle voor de 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 niet toestemt, de toestemming niet geldig is¹³. Indien toestemming is opgenomen als een niet-onderhandelbaar onderdeel van de voorwaarden, wordt deze verondersteld niet vrijelijk te zijn verleend. Bijgevolg wordt toestemming niet geacht vrijelijk te zijn verleend, indien de betrokkene zijn toestemming niet zonder nadelige gevolgen kan weigeren of intrekken¹⁴. De AVG besteedt ook aandacht aan het concept van een wanverhouding tussen de verwerkingsverantwoordelijke en de betrokkene.
14. Bij het beoordelen of toestemming vrijelijk is verleend, moet ook rekening worden gehouden met de specifieke situatie waarin toestemming wordt gekoppeld aan overeenkomsten of dienstverlening zoals beschreven in artikel 7, lid 4. Artikel 7, lid 4, is niet-limitatief geformuleerd, wat blijkt uit de woorden “onder meer”; d.w.z. dat er wellicht meer situaties zijn waarop deze bepaling van toepassing is. In het algemeen wordt de toestemming ongeldig door elk element dat ongepaste druk of invloed op de betrokkene inhoudt (wat op veel verschillende manieren tot uiting kan komen) en waardoor een betrokkene zijn vrije wil niet kan uitoefenen.

15. Voorbeeld 1: Gebruikers van een mobiele app voor fotobewerking wordt gevraagd om hun GPS-locatie te activeren. De app deelt zijn gebruikers ook mee dat de verzamelde gegevens zullen worden gebruikt voor gerichte reclame op basis van surfgedrag (behavioural advertising). Geolokalisatie en behavioural advertising zijn niet nodig voor het verlenen van de fotobewerkingsdienst en vallen buiten de verstrekking 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 verleend.

3.1.1 Wanverhouding

16. Overweging 43¹⁵ geeft duidelijk aan dat **overheidsinstanties** er niet zonder meer van kunnen uitgaan dat er toestemming is voor verwerking, omdat er vaak een duidelijke wanverhouding bestaat tussen de betrokkene en de verwerkingsverantwoordelijke als die laatste een overheidsinstantie is. In de meeste gevallen is het ook duidelijk dat de betrokkene geen realistische alternatieven heeft voor het aanvaarden van de verwerking(svoorwaarden) van deze verwerkingsverantwoordelijke. De EDPB is

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, 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).

¹³ Zie Advies 15/2011 over de definitie van “toestemming” (WP187), blz. 12

¹⁴ Zie overwegingen 42 en 43 AVG en WP29 Advies 15/2011 over de definitie van “toestemming”, vastgesteld op 13 juli 2011, (WP 187), blz. 12.

¹⁵ 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. (...)”.

van mening dat er andere rechtsgronden zijn die in principe meer geschikt zijn voor de activiteiten van overheidsinstanties¹⁶.

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

18. 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 (uitsluitend) voor dit doel te gebruiken. Inwoners die geen toestemming verlenen, lopen geen basisdiensten van de gemeente mis en er wordt geen afbreuk gedaan aan de uitoefening van hun rechten; zij zijn dus in staat om hun toestemming voor dit gebruik van gegevens vrijelijk te verlenen of te weigeren. Alle informatie over de wegwerkzaamheden zal ook beschikbaar zijn op de website van de gemeente.

19. Voorbeeld 3: De eigenares 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 beide overheidsorganen om dezelfde informatie, en de landeigenares stuurt haar gegevens naar beide organen. De gemeente en de provinciale overheid vragen hem om toestemming om de dossiers samen te voegen, zodat dubbele procedures en correspondentie worden voorkomen. Beide overheidsinstanties verzekeren dat dit facultatief is, en dat de vergunningsaanvragen gewoon afzonderlijk zullen worden verwerkt, mocht zij besluiten geen toestemming te verlenen voor het samenvoegen van haar gegevens. De landeigenaar kan de overheidsinstanties vrijelijk toestemming verlenen voor het samenvoegen van de dossiers.

20. Voorbeeld 4: Een openbare school vraagt leerlingen om toestemming om hun foto's in een gedrukte schoolkrant te gebruiken. Toestemming is in een dergelijke situatie een werkelijke keuze zolang leerlingen niet worden uitgesloten van onderwijs of diensten, en kunnen weigeren dat deze foto's worden gebruikt, zonder daarvan enig nadeel te ondervinden¹⁷.

21. Van een wanverhouding is ook sprake in het kader van **de arbeidsverhouding**¹⁸. Gezien de afhankelijkheid die voortvloeit uit de relatie tussen werkgever en werknemer, is het onwaarschijnlijk dat de betrokkene zijn werkgever toestemming voor gegevensverwerking zou kunnen weigeren, zonder te hoeven vrezen voor nadelige gevolgen of zich bloot te stellen aan de reële dreiging van nadelige gevolgen. Het is onwaarschijnlijk dat een werknemer vrijelijk zou kunnen reageren op een

¹⁶ Zie artikel 6, AVG, met name lid 1, onder c) en e).

¹⁷ 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.

¹⁸ Zie ook artikel 88 AVG, dat benadrukt dat de specifieke belangen van werknemers moeten worden beschermd en een mogelijkheid biedt om in het recht van de lidstaten afwijkingen op te nemen. Zie ook overweging 155.

verzoek voor toestemming van zijn werkgever voor, bijvoorbeeld, het activeren van toezichtsystemen zoals cameraobservatie op de werkvloer, of het invullen van beoordelingsformulieren, zonder druk te voelen om toestemming te verlenen¹⁹. Daarom is de EDPB van mening dat het voor werknemers problematisch is om persoonsgegevens van huidige of toekomstige werknemers te verwerken op basis van toestemming, omdat het onwaarschijnlijk is dat deze vrijelijk wordt verleend. In de meeste gevallen 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 werknemer²⁰.

22. Dit betekent echter niet dat werkgevers zich nooit kunnen baseren op toestemming als rechtsgrond voor verwerking. Er kunnen situaties zijn waarin de werkgever kan aantonen dat toestemming daadwerkelijk vrijelijk is verleend. Gezien de wanverhouding tussen een werkgever en zijn personeel, kunnen werknemers alleen in uitzonderlijke omstandigheden vrijelijk toestemming verlenen, wanneer het feit of zij wel of geen toestemming verlenen totaal geen negatieve gevolgen heeft²¹.

23. 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 willen worden gefilmd, worden op geen enkele wijze bestraft, maar mogen voor de duur van de opnames gelijkwaardige bureaus elders in het kantoor gebruiken.

24. Wanverhoudingen zijn niet beperkt tot overheidsinstanties en de werkgevers, ze kunnen zich ook in andere situaties voordoen. 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 evenmin aanzienlijke negatieve gevolgen (zoals aanzienlijke extra kosten) riskeert wanneer hij niet toestemt. Toestemming is niet vrij wanneer er sprake is van enige vorm van dwang of van druk of als de betrokkene zijn vrije wil niet kan uitoefenen.

3.1.2 Conditionaliteit

25. Bij het beoordelen of toestemming vrijelijk is verleend, speelt artikel 7, lid 4, AVG een belangrijke rol²².
26. Artikel 7, lid 4, AVG bepaalt onder meer dat het hoogst onwenselijk is om toestemming deel te laten uitmaken van de aanvaarding van voorwaarden, of het uitvoeren van een overeenkomst, met inbegrip

¹⁹ 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, 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.

²⁰ Zie Advies 2/2017 over gegevensverwerking op het werk, blz. 6-7.

²¹ Zie ook Advies 2/2017 over gegevensverwerking op het werk (WP249), paragraaf 6.2.

²² 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.”

van een dienstenovereenkomst, te koppelen aan een verzoek om toestemming voor de verwerking van persoonsgegevens die niet nodig zijn voor de uitvoering van de overeenkomst. Als in een dergelijke situatie toestemming wordt gegeven, wordt deze geacht niet vrijelijk te zijn verleend (overweging 43). Artikel 7, lid 4, beoogt te waarborgen dat het doel van de verwerking van persoonsgegevens niet wordt verhuisd of wordt gekoppeld aan de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, waarvoor deze persoonsgegevens niet noodzakelijk zijn. Zo verzekert de AVG dat de verwerking van persoonsgegevens waarvoor toestemming wordt gevraagd, niet direct of indirect de tegenprestatie voor een overeenkomst kan zijn. De twee rechtsgronden voor rechtmatige verwerking van persoonsgegevens, namelijk toestemming en overeenkomst, kunnen niet worden samengevoegd, waardoor het onderscheid tussen de twee rechtsgronden zou vervagen.

27. Verplichte instemming met het gebruik van persoonsgegevens voor andere dan de strikt noodzakelijke doeleinden beperkt de keuze van de betrokkene en staat vrije toestemming in de weg. Omdat de wetgeving inzake gegevensbescherming is gericht op de bescherming van de grondrechten, is het van essentieel belang dat eenieder controle heeft over zijn persoonsgegevens, en er is een sterk vermoeden dat instemming met de onnodige verwerking van persoonsgegevens niet kan worden beschouwd als een randvoorwaarde voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst.
28. Wanneer een verzoek om toestemming door de verwerkingsverantwoordelijke wordt gekoppeld aan de uitvoering van een overeenkomst, loopt een betrokkene die zijn persoonsgegevens niet beschikbaar wil stellen voor verwerking door de verwerkingsverantwoordelijke dus het risico dat hem de gevraagde diensten worden onthouden.
29. Om te beoordelen of er inderdaad sprake is van samenvoeging of koppeling, is het belangrijk om vast te stellen wat het toepassingsgebied van de overeenkomst is, en welke gegevens noodzakelijk zijn voor de uitvoering van die overeenkomst.
30. Overeenkomstig Advies 06/2014 van WP29 moet “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 mogen op deze grond bijvoorbeeld salarisgegevens en bankgegevens worden verwerkt, zodat lonen kunnen worden uitbetaald²³. Er moet een direct en objectief verband zijn tussen de verwerking van de gegevens en het doel van de uitvoering van de overeenkomst.
31. Als een verwerkingsverantwoordelijke persoonsgegevens wil verwerken die in feite noodzakelijk zijn voor de uitvoering van een overeenkomst, dan is toestemming niet de passende rechtsgrond²⁴.
32. Artikel 7, lid 4, is slechts relevant indien de gevraagde gegevens **niet** noodzakelijk 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

²³ 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).

²⁴ 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.

33. Voorbeeld 6: Een bank vraagt klanten om toestemming om derden toe te staan hun betalingsgegevens te gebruiken voor directmarketingdoeleinden. Deze verwerkingsactiviteit is niet noodzakelijk voor de uitvoering van de overeenkomst met de klant en de verlening van gewone bankdiensten. Indien de weigering van de klant om toestemming te verlenen voor deze 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.

34. Dat de wetgever ervoor kiest om onder meer conditionaliteit uitdrukkelijk te noemen als een factor die doet vermoeden dat toestemming niet vrijelijk kan worden verleend, houdt in dat zorgvuldig moet worden onderzocht of er sprake is van conditionaliteit. In artikel 7, lid 4, suggereert “ten sterkste rekening gehouden” dat de verwerkingsverantwoordelijke extra voorzichtig moet zijn wanneer aan een overeenkomst (die een dienstenovereenkomst kan omvatten) een verzoek tot toestemming voor de verwerking van persoonsgegevens is gekoppeld.
35. Omdat artikel 7, lid 4, niet op absolute wijze is geformuleerd, is er wellicht een zeer beperkte ruimte voor gevallen waarin deze conditionaliteit de toestemming niet ongeldig zou maken. Uit het woord “verondersteld” in overweging 43 blijkt echter duidelijk dat deze gevallen zeer uitzonderlijk zijn.
36. Hoe dan ook ligt de bewijslast in artikel 7, lid 4, bij de verwerkingsverantwoordelijke²⁵. Deze specifieke regel weerspiegelt het algemene beginsel van verantwoording dat in de hele AVG tot uiting komt. Indien artikel 7, lid 4, van toepassing is, is het voor de verwerkingsverantwoordelijke echter moeilijker om te bewijzen dat de betrokkene vrijelijk toestemming heeft verleend²⁶.
37. De verwerkingsverantwoordelijke zou kunnen aanvoeren dat zijn organisatie de 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, aangeboden door dezelfde verwerkingsverantwoordelijke, die geen toestemming omvat voor het gebruik van gegevens voor aanvullende doeleinden anderzijds. Zolang de mogelijkheid bestaat deze verwerkingsverantwoordelijke de overeenkomst te laten uitvoeren of de dienst te laten verlenen zonder dat er toestemming te hoeft te worden verleend voor ander of aanvullend gebruik van de betreffende gegevens, is er geen sprake van een voorwaardelijke dienst. Beide diensten moeten echter daadwerkelijk gelijkwaardig zijn.
38. De EDPB 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

²⁵ Zie ook artikel 7, lid 1, AVG, waarin staat dat de verwerkingsverantwoordelijke moet aantonen dat de betrokkene vrijelijk toestemming heeft verleend.

²⁶ Tot op zekere hoogte vormt de toevoeging van dit lid een codificatie van de bestaande richtsnoeren van WP29. Zoals beschreven in Advies 15/2011, kan het geval waarin een betrokkene zich in een situatie van afhankelijkheid jegens de verwerkingsverantwoordelijke bevindt, een sterk vermoeden inhouden dat de vrijheid om toestemming te verlenen in deze omstandigheden beperkt is bv. in een arbeidsverhouding of als het verzamelen van gegevens wordt uitgevoerd door een overheidsinstantie). 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: Groep artikel 29 Advies 15/2011 over de definitie van “toestemming” (WP 187), blz. 12-17.

voor het gebruik van persoonsgegevens voor aanvullende doeleinden enerzijds, en een gelijkwaardige dienst die wordt aangeboden door een andere verwerkingsverantwoordelijke anderzijds. Of er sprake is van keuzevrijheid zou er in een dergelijk geval van afhangen wat andere spelers op de markt doen, en of een individuele betrokkene de diensten van de andere verwerkingsverantwoordelijke echt gelijkwaardig vindt. Ook zouden de verwerkingsverantwoordelijken de ontwikkelingen op de markt moeten volgen om te waarborgen dat de toestemming voor hun verwerkingsactiviteiten nog geldig is, omdat een concurrent zijn diensten in een later stadium zou kunnen wijzigen. Toestemming afleiden uit het bestaan van een alternatief dat wordt aangeboden door een derde, strookt dus niet met de AVG; een dienstverlener mag de betrokkenen een dienst niet ontzeggen omdat zij geen toestemming verlenen.

39. Wil toestemming vrijelijk worden verleend, dan mag toegang tot diensten en functies niet afhankelijk worden gesteld van de toestemming van een gebruiker voor het bewaren van informatie, dan wel het verkrijgen van toegang tot informatie die reeds is opgeslagen, in de eindapparatuur van een gebruiker (de zogenaamde cookie walls)²⁷.

40. Voorbeeld 6a: De aanbieder van een website maakt gebruik van een script waardoor er geen inhoud zichtbaar is, behalve een verzoek om cookies te accepteren en informatie over de betrokken cookies en de doeleinden waarvoor de gegevens worden verwerkt. De inhoud kan niet worden weergegeven zonder op de knop “cookies accepteren” te klikken. Omdat de betrokkene niet echt een keus heeft, verleent hij zijn toestemming niet vrijelijk.
41. Deze toestemming is niet geldig, aangezien de dienst alleen wordt verleend als de betrokkene de cookies aanvaardt. Hem wordt geen echte keuzemogelijkheid geboden.

3.1.3 Granulariteit

42. Een dienst kan meerdere verwerkingsactiviteiten voor meerdere doeleinden omvatten. In dergelijke gevallen zouden de betrokkenen vrij moeten kunnen kiezen welk doeleinde zij accepteren, in plaats van toestemming te moeten verlenen voor een pakket verwerkingsdoeleinden. Zo kan het volgens de AVG nodig zijn om voor meerdere zaken toestemming te verkrijgen voor met het aanbieden van een dienst kan worden begonnen.
43. Overweging 43 verduidelijkt dat de toestemming vermoedelijk niet vrijelijk is verleend als de betrokkenen bij het proces/de procedure voor het verkrijgen van toestemming geen afzonderlijke toestemming kunnen verlenen voor verschillende persoonsgegevensverwerkingen (bv. voor bepaalde verwerkingen wel en voor andere niet), 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”.
44. 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 besproken in paragraaf 3.2 hieronder. Als gegevensverwerking plaatsvindt ter verwezenlijking van meerdere doeleinden, kan aan de

²⁷ Zoals hierboven is uiteengezet, zijn de vereisten van de AVG voor het verkrijgen van geldige toestemming van toepassing in situaties die binnen het toepassingsgebied van de e-privacy-richtlijn vallen.

voorwaarden voor geldige toestemming worden voldaan door granulariteit, d.w.z. de scheiding van deze doeleinden en het verkrijgen van toestemming voor elk doeleinde.

45. Voorbeeld 7: In hetzelfde verzoek om toestemming vraagt een detailhandelaar zijn klanten zowel om toestemming voor het gebruiken van hun gegevens voor marketing via e-mail als om toestemming voor het delen van hun gegevens met andere ondernemingen binnen zijn groep. Deze toestemming is niet granulaair, omdat er geen sprake is van afzonderlijke toestemming voor deze twee afzonderlijke doeleinden; de toestemming is derhalve 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 bekendgemaakt bij het verkrijgen van zijn toestemming, voor zover deze gegevens aan hen worden doorgegeven voor hetzelfde doel (in dit voorbeeld: een marketingdoel).

3.1.4 Nadeel

46. 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.

47. 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 hij zijn toestemming kon intrekken zonder daarvan nadeel te ondervinden.

48. Indien een verwerkingsverantwoordelijke kan aantonen dat een dienst de mogelijkheid omvat om toestemming in te trekken zonder negatieve gevolgen (de uitvoering van de dienst wordt bijvoorbeeld niet ten nadele van de gebruiker bijgesteld), kan dit dienen om aan te tonen dat de toestemming vrijelijk verleend is. De AVG verbiedt niet elke stimulans, maar het is wel aan de verwerkingsverantwoordelijke om aan te tonen dat toestemming onder alle omstandigheden vrijelijk is verleend.

49. Voorbeeld 8: Tijdens het downloaden van een lifestyle-app voor mobiele telefoons, vraagt de app om toestemming voor toegang 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 verplaatsingen en mate van activiteit van de gebruikers. Wanneer een gebruiker deze toestemming later intrekt, merkt hij 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 op geldige wijze is verkregen (en dat de verwerkingsverantwoordelijke dus alle op deze wijze verzamelde persoonsgegevens over de verplaatsingen van de gebruiker moet verwijderen).

50. 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 winkelvoorkeuren om de aanbiedingen daarop af te stemmen, op basis van zijn aankoopgeschiedenis of een vragenlijst die vrijwillig kan worden ingevuld. Wanneer de betrokkene zijn toestemming later intrekt, zal hij weer niet-gepersonaliseerde aanbiedingen ontvangen. Dit vormt geen nadeel, omdat de betrokkene alleen het mogelijke extra voordeel verliest.

51. Voorbeeld 10: Een modetijdschrift biedt zijn lezers de mogelijkheid om nieuwe make-upproducten te kopen vóór de officiële productpresentatie.

52. De producten zullen binnenkort in de verkoop komen, maar de lezers van dit tijdschrift kunnen er nu al exclusief mee kennismaken. Om gebruik te kunnen maken van dit voordeel, moeten mensen hun postadres opgeven 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 en T-shirts te versturen.
53. Het bedrijf verklaart de gegevens van de mailinglijst alleen zelf te zullen gebruiken voor het verzenden van goederen en reclamedrukwerk en dus niet te delen met andere organisaties.
54. Ingeval de lezer zijn adres om deze reden niet bekend wil maken, is er geen nadeel, omdat de producten evengoed voor hem beschikbaar zijn.

3.2 Specifiek

55. Volgens artikel 6, lid 1, onder a), moet de toestemming van de betrokkene worden verleend met betrekking tot “een of meer specifieke” doeleinden, en dient een betrokkene een keuze te hebben ten aanzien van elk van deze doeleinden²⁸. De eis dat de toestemming “specifiek” moet zijn, beoogt te zorgen voor een zekere mate van controle door 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 verkrijgen²⁹. Kortom, wil de toestemming “specifiek” zijn, dan moet de verwerkingsverantwoordelijke zorgen voor:
- i specificatie van doeleinden als een bescherming tegen “function creep”,
 - ii granulariteit in toestemmingsverzoeken, en
 - iii een duidelijk onderscheid tussen informatie over het verkrijgen van toestemming voor verwerkingsactiviteiten en informatie over andere zaken.
56. **Ad. i):** Overeenkomstig artikel 5, lid 1, onder b) AVG, wordt het verkrijgen van geldige toestemming altijd voorafgegaan door de vaststelling van een welbepaald, uitdrukkelijk omschreven gerechtvaardigd doel voor de beoogde verwerkingsactiviteit³⁰. 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 de betrokkenen,

²⁸ Nadere richtsnoeren voor het bepalen van “doeleinden” zijn te vinden in Advies 3/2013 over doelbinding (WP 203).

²⁹ Overweging 43 AVG stelt dat in voorkomende gevallen afzonderlijke toestemming voor verschillende persoonsgegevensverwerkingen nodig is. Er moeten granulaire toestemmingsopties worden aangeboden om de betrokkenen in staat te stellen om afzonderlijk in te stemmen met verschillende doeleinden.

³⁰ 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”.”

omdat het kan leiden tot onvoorzien gebruik van persoonsgegevens door de verwerkingsverantwoordelijke of door derden en verlies van controle door de betrokkene.

57. Als de verwerkingsverantwoordelijke zich baseert op artikel 6, lid 1, onder a), moeten de betrokkenen altijd toestemming geven voor een bepaald doel van verwerking³¹. In lijn met het concept van *doelbinding* (artikel 5, lid 1, onder b), en overweging 32) kan toestemming voor verschillende werkzaamheden gelden, 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.
58. Onverminderd de bepalingen inzake compatibiliteit van doeleinden moet toestemming specifiek voor het doel zijn. De betrokkenen verlenen hun toestemming in 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 bij de situatie past.

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

60. **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.
61. **Ad. iii):** Ten slotte moeten verwerkingsverantwoordelijken 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 zij 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 (zie paragraaf 3.3).

3.3 Geïnformeerd

62. 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 nauw verwant aan de beginselen van behoorlijkheid en rechtmatigheid. Het verstrekken van informatie aan de betrokkenen voorafgaand aan het verkrijgen van hun toestemming is noodzakelijk om hen in staat te stellen 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 toegankelijke informatie verstrekt, wordt de controle van de betrokkene slechts schijn en is toestemming een ongeldige grond voor verwerking.

³¹ Dit is in overeenstemming met WP29 Advies 15/2011 over de definitie van “toestemming” (WP 187), bijvoorbeeld op blz. 17.

63. Als niet wordt voldaan aan de eisen inzake geïnformeerde toestemming, is de toestemming ongeldig en schendt de verwerkingsverantwoordelijke mogelijk artikel 6 van de AVG.

3.3.1 De minimale inhoudelijke eisen inzake “geïnformeerde” toestemming

64. Opdat 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 de EDPB van mening dat ten minste de volgende informatie nodig is voor het verkrijgen van rechtmatige toestemming:

- i. de identiteit van de verwerkingsverantwoordelijke³²,
- ii. het doel van elk van de verwerkingen waarvoor toestemming wordt gevraagd³³,
- iii. welk(e) (soort) gegevens worden verzameld en gebruikt³⁴,
- iv. het bestaan van het recht om toestemming in te trekken³⁵,
- v. informatie over het gebruik van de gegevens voor geautomatiseerde besluitvorming overeenkomstig artikel 22, lid 2, onder c)³⁶, indien van toepassing, en
- vi. informatie over de risico's van dergelijke doorgiften bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen, zoals beschreven in artikel 46³⁷.

65. Ten aanzien van de punten i) en iii) merkt de EDPB op dat ingeval meerdere (gezamenlijke) verwerkingsverantwoordelijken zich op de gevraagde toestemming willen baseren of als de gegevens zullen worden doorgegeven aan of verwerkt door andere verwerkingsverantwoordelijken die zich op de oorspronkelijke toestemming willen baseren, al deze organisaties moeten worden genoemd. De verwerkingsverantwoordelijken hoeven niet te worden genoemd als onderdeel van de eisen inzake 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 de EDPB op dat, afhankelijk van de omstandigheden en de context van een geval, meer informatie nodig kan zijn om de betrokkene in staat te stellen de betreffende verwerkingsactiviteiten goed te begrijpen.

³² Zie ook overweging 42 AVG. [...] Van geïnformeerde toestemming van de betrokkene kan slechts sprake zijn indien deze ten minste bekend is met de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking van de persoonsgegevens [...].

³³ Zie wederom overweging 42, AVG.

³⁴ Zie ook WP29 Advies 15/2011 over de definitie van “toestemming” (WP 187), blz. 19-20.

³⁵ Zie artikel 7, lid 3 AVG.

³⁶ Zie ook WP29-richtsnoeren betreffende geautomatiseerde individuele besluitvorming en profilering in de zin van Verordening 2016/679 (WP251), paragraaf IV.B, blz. 20 e.v.

³⁷ Volgens 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.

3.3.2 Hoe moet informatie worden verstrekt?

66. 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 aan geïnformeerde toestemming, voornamelijk in artikel 7, lid 2, en overweging 32. Dit leidt tot een hogere norm voor de duidelijkheid en toegankelijkheid van de informatie.
67. Bij het vragen om toestemming moeten verwerkingsverantwoordelijken 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 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 mag worden verborgen in algemene voorwaarden³⁸.
68. 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 gevraagd³⁹.
69. 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 om gevolg te geven aan de dubbele verplichting om enerzijds nauwkeurig en volledig, en anderzijds begrijpelijk te zijn.
70. 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 minderjarigen⁴⁰. Nadat een verwerkingsverantwoordelijke heeft vastgesteld om wat voor publiek het gaat, moet hij bepalen welke informatie hij moet verstrekken, en vervolgens hoe deze informatie aan de betrokkenen wordt gepresenteerd.
71. 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 (schriftelijke) overeenkomst, moet het verzoek om toestemming duidelijk te onderscheiden zijn van de andere zaken. Als de schriftelijke 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

³⁸ De verklaring van toestemming moet als zodanig worden aangeduid. Formuleringen zoals "Ik weet dat..." voldoen niet aan de eis van duidelijke taal.

³⁹ Zie artikel 4, punt 11, en artikel 7, lid 2, AVG.

⁴⁰ Zie ook overweging 58 betreffende voor kinderen begrijpelijke informatie.

geldt dat als toestemming wordt gevraagd via elektronische middelen, het verzoek om toestemming afzonderlijk en gescheiden moet zijn: uit overweging 32 volgt dat het niet eenvoudigweg een paragraaf in de algemene voorwaarden mag zijn⁴¹. Om tegemoet te komen aan kleine schermen of situaties met beperkte ruimte voor informatie, kan, in voorkomende gevallen, een gelaagde presentatie van informatie worden overwogen om buitensporige verstoring van de gebruikerservaring of het productontwerp te voorkomen.

72. Om te voldoen aan de AVG moet een verwerkingsverantwoordelijke die zich baseert op de toestemming van de betrokkene, ook voldoen aan de verplichtingen inzake afzonderlijk te verstrekken informatie die omschreven zijn in artikel 13 en 14. In de praktijk kan de naleving van de informatieverplichtingen en het voldoen aan de eis van geïnformeerde toestemming in veel gevallen tot een geïntegreerde aanpak leiden. Deze paragraaf is echter geschreven in de veronderstelling dat geldige “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 de privacyverklaring van een onderneming). WP29 heeft afzonderlijke richtsnoeren verstrekt betreffende de eis van transparantie.

73. Voorbeeld 12: Bedrijf X is een verwerkingsverantwoordelijke die klachten heeft ontvangen dat het voor de betrokkenen onduidelijk is voor welke doeleinden van gegevensgebruik hun wordt gevraagd om toestemming te verlenen. Het bedrijf onderkent dat het nodig is om na te gaan of de informatie in het verzoek om toestemming begrijpelijk is voor de betrokkenen. X organiseert vrijwillige testpanels van specifieke categorieën van zijn afnemers en legt aan dit testpubliek nieuwe versies van zijn informatie inzake toestemming voor, voordat deze informatie naar buiten wordt gebracht. De selectie van het panel voldoet aan het beginsel van onafhankelijkheid en wordt uitgevoerd op basis van normen 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 relevantie. 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 illustreert hoe X kan aantonen dat de betrokkenen duidelijke informatie ontvangen voordat ze toestemming verlenen voor de verwerking van hun persoonsgegevens door X.

74. Voorbeeld 13: Een bedrijf voert gegevensverwerking uit op basis van toestemming. Het bedrijf maakt gebruik van een gelaagde privacyverklaring die een verzoek om toestemming omvat. Het bedrijf maakt alle basisgegevens van de verwerkingsverantwoordelijke en de voorgenomen verwerkingsactiviteiten bekend⁴². Het bedrijf geeft in de eerste informatielaag van de privacyverklaring echter niet aan hoe contact kan worden opgenomen met zijn functionaris voor gegevensbescherming. Om te beschikken over een geldige rechtsgrond zoals bedoeld in artikel 6 heeft deze verwerkingsverantwoordelijke

⁴¹ 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 dan nog steeds zinnig is, anders is de volledige overeenkomst ongeldig).

⁴² Wanneer de identiteit van de verwerkingsverantwoordelijke of het doel van de verwerking niet blijkt uit de eerste informatielaag van de gelaagde privacyverklaring (en opgenomen is in de volgende lagen), zal het voor de verwerkingsverantwoordelijke moeilijk 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.

geldige “geïnformeerde” toestemming verkregen, hoewel de contactgegevens van de functionaris voor gegevensbescherming, niet aan de betrokkene zijn doorgegeven (in de eerste informatielaag) zoals verplicht is op grond van artikel 13, lid 1, onder b), of artikel 14, lid 1, onder b), AVG.

3.4 Ondubbelzinnige wilsuiting

75. De AVG bepaalt duidelijk dat voor toestemming een verklaring van de betrokkene of een ondubbelzinnige actieve handeling van de betrokkene is vereist, wat betekent dat toestemming altijd 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.
76. 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, punt 11, AVG bouwt voort op deze definitie door te verduidelijken dat voor geldige toestemming een *ondubbelzinnige wilsuiting* door middel van een *verklaring of ondubbelzinnige actieve handeling* is vereist, overeenkomstig de eerder door WP29 verstrekte richtsnoeren.
77. Een “ondubbelzinnige actieve handeling” betekent dat de betrokkene een opzettelijke handeling moet hebben verricht om toestemming te verlenen voor de specifieke verwerking⁴³. Overweging 32 bevat aanvullende richtsnoeren. Toestemming kan door middel van een schriftelijke of een (opgenomen) mondelinge verklaring worden verkregen, bijvoorbeeld op elektronische wijze.
78. 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 precies instemt. Dit is echter vaak niet realistisch. Schriftelijke verklaringen kunnen in vele soorten en maten aan de AVG voldoen.
79. Onverminderd het bestaande (nationale) overeenkomstenrecht kan toestemming worden verkregen door middel van een geregistreerde mondelinge verklaring, hoewel rekening moet worden gehouden met de informatie die de betrokkene ter beschikking staat vóórdat hij zijn toestemming verleent. Het gebruik van vooraf aangevinkte opt-invakjes is op grond van de AVG ongeldig. Stilzwijgen of inactiviteit van de betrokkene kan evenmin als het louter verder benutten van een dienst worden beschouwd als het actief kenbaar maken van een keuze.

⁴³ Zo staat in het Werkdocument van de diensten van de Commissie, Effectbeoordeling, bijlage 2, blz. 20 en ook blz. 105-106 (or. Engels): “Zoals ook aangegeven in het door WP29 vastgestelde advies inzake toestemming, lijkt het absoluut noodzakelijk om te verduidelijken dat dat het vereiste van geldige toestemming vraagt om het gebruik van mechanismen die er geen twijfel over laten bestaan dat de betrokkene metterdaad wilde toestemmen, waarbij het duidelijk moet worden gemaakt dat – in de context van de online omgeving – mechanismen waarbij “toestemming” wordt verkregen via standaardinstellingen die de betrokkene moet wijzigen als hij niet wil dat zijn gegevens worden verwerkt (“wie zwijgt, stemt toe”) op zichzelf geen ondubbelzinnige toestemming opleveren. Dit zou personen meer controle over hun eigen gegevens geven ingeval 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 geldige 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.”

80. 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 gelaagde privacyverklaring waarin de noodzakelijke informatie wordt verstrekt. Door actief het optionele vakje met “Ik ga akkoord” aan te vinken, kan de gebruiker op geldige wijze een “ondubbelzinnige actieve handeling” uitvoeren om toestemming te verlenen voor de verwerking.

81. 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 duidelijke actieve handeling waarmee toestemming wordt gegeven voor het gebruik van persoonsgegevens. De AVG staat verwerkingsverantwoordelijken niet toe om te werken met vooraf aangevinkte vakjes of opt-outconstructies waarbij de betrokkene een handeling moet verrichten om instemming te voorkomen (bijvoorbeeld “opt-outvakjes”)⁴⁴.
82. Wanneer toestemming moet worden gegeven naar aanleiding van een verzoek langs elektronische weg, mag het verzoek om toestemming niet *onnodig* verstorend zijn voor het gebruik van de dienst waarvoor de toestemming wordt verleend⁴⁵. 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 een verzoek om toestemming de gebruikerservaring tot op zekere hoogte verstoort om dit verzoek effectief te maken.
83. 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.
84. Verwerkingsverantwoordelijken moeten mechanismen voor toestemming op een dusdanige manier ontwerpen dat ze voor de betrokkenen duidelijk zijn. Verwerkingsverantwoordelijken moeten dubbelzinnigheid vermijden en ervoor zorgen dat de handeling waarmee toestemming wordt verleend, kan worden onderscheiden van andere handelingen. Het louter blijven gebruiken van een website is daarom geen gedrag dat kan worden opgevat als een wilsuiting waarmee de betrokkene kenbaar maakt dat hij toestemming geeft voor een voorgenomen gegevensverwerking.

85. Voorbeeld 15: Het over een scherm vegen van een balk, wuiven voor een slimme camera, een smartphone met de klok mee draaien of in een achtje bewegen, kunnen mogelijkheden zijn om toestemming kenbaar te maken, zolang 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 de betrokkenen moeten hun toestemming net zo eenvoudig kunnen intrekken als verlenen.

⁴⁴ Zie artikel 7, lid 2. Zie ook Werkdocument 02/2013 inzake het verkrijgen van toestemming voor cookies (WP 208), blz. 3-6.

⁴⁵ Zie overweging 32, AVG.

86. Voorbeeld 16: Uit overweging 32 volgt dat handelingen als het scrollen of vegen door een website en soortgelijke gebruikersactiviteiten onder geen beding voldoen aan het vereiste van een duidelijke actieve handeling: dergelijke handelingen kunnen moeilijk te onderscheiden zijn van andere activiteiten van of interactie met een gebruiker; er kan dus niet worden vastgesteld dat ondubbelzinnig toestemming is verkregen. In een dergelijk geval is het bovendien lastig om het voor de gebruiker net zo gemakkelijk te maken zijn toestemming in te trekken als het was om deze te verlenen.

87. In de digitale context hebben veel diensten persoonsgegevens nodig om te werken, en daarom ontvangen de 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.

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

89. Een vaak aangehaald voorbeeld van een manier om dit binnen de online context te doen, is om toestemming van internetgebruikers te verkrijgen via hun browserinstellingen. Deze instellingen moeten worden ontwikkeld in overeenstemming met de voorwaarden voor geldige 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 bevatten.

90. In ieder geval moet toestemming altijd worden verkregen voordat de verwerkingsverantwoordelijke begint met de verwerking van persoonsgegevens waarvoor toestemming nodig is. WP29 heeft zich in eerdere adviezen consequent op het standpunt gesteld dat toestemming moet worden verleend voordat wordt begonnen met de verwerking⁴⁶. Hoewel de AVG in artikel 4, lid punt 11, niet letterlijk voorschrijft dat toestemming moet worden verleend voordat begonnen wordt met de verwerkingsactiviteiten, wordt dit duidelijk verondersteld. Het kopje van artikel 6, lid 1, en de tekst “heeft gegeven” in artikel 6, lid 1, ondersteunen deze interpretatie. Uit artikel 6 en overweging 40 volgt logischerwijs dat er een geldige rechtsgrond moet bestaan voordat begonnen wordt met gegevensverwerking. Daarom moet toestemming worden gegeven vóór aanvang van de verwerkingsactiviteiten. In beginsel kan het volstaan 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

91. Uitdrukkelijke toestemming is vereist in bepaalde situaties waarin zich een ernstig risico voor gegevensbescherming voordoet en waarbij derhalve een hoog niveau van individuele controle over persoonsgegevens passend wordt geacht. In het kader van de AVG speelt uitdrukkelijke toestemming

⁴⁶ WP29 heeft dit standpunt consequent ingenomen vanaf Advies 15/2011 over de definitie van “toestemming” (WP 187), blz. 30-31.

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 ontbreken van de passende waarborgen als bedoeld in artikel 49⁴⁷, en artikel 22 betreffende geautomatiseerde individuele besluitvorming, waaronder profilering⁴⁸.

92. De AVG bepaalt dat “een verklaring of een 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 overeenkomstig de AVG de *uitdrukkelijke* toestemming van de betrokkene te verkrijgen.
93. 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 weg te nemen en mogelijk gebrek aan bewijs in de toekomst uit te sluiten⁴⁹.
94. Een dergelijke ondertekende verklaring is echter niet de enige manier om uitdrukkelijke toestemming te verkrijgen, en het is niet zo dat de AVG bepaalt dat in alle omstandigheden waarin geldige uitdrukkelijke toestemming nodig is, een schriftelijke en ondertekende verklaring vereist is. 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 verklaringen ook voldoende zijn om geldige uitdrukkelijke toestemming te verkrijgen; het kan echter voor de verwerkingsverantwoordelijke moeilijk te bewijzen zijn dat bij het registreren van de verklaring voldaan werd aan alle voorwaarden voor geldige uitdrukkelijke toestemming.
95. 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

⁴⁷ Volgens artikel 49, lid 1, onder a), AVG kan uitdrukkelijke toestemming het verbod opheffen op doorgifte van gegevens bij ontstentenis van een adequaat beschermingsniveau van gegevensbeschermingswetgeving. Zie ook het werkdokument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995 (WP 114), blz. 11, waarin WP29 stelt dat toestemming voor gegevensdoorgiften die periodiek of op regelmatige basis plaatsvinden ongepast is.

⁴⁸ Artikel 22 van de AVG bevat bepalingen om de betrokkenen te beschermen tegen besluitvorming die uitsluitend is gebaseerd op geautomatiseerde verwerking, waaronder profilering. Besluiten die op deze basis worden genomen, zijn onder bepaalde wettelijke voorwaarden toegestaan. Toestemming speelt in dit beschermingsmechanisme een sleutelrol, omdat artikel 22, lid 2, onder c), AVG duidelijk maakt dat een verwerkingsverantwoordelijke mag overgaan tot geautomatiseerde besluitvorming, waaronder profilering, 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).

⁴⁹ Zie ook WP29 Advies 15/2011 over de definitie van “toestemming” (WP 187), blz. 25.

specifieke bevestiging van de betrokkene (bijvoorbeeld door een knop in te drukken of een mondelinge bevestiging te verschaffen).

96. Voorbeeld 17: Een verwerkingsverantwoordelijke kan ook uitdrukkelijke toestemming van een bezoeker van zijn website verkrijgen via een scherm voor het verlenen van uitdrukkelijke toestemming, 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.
97. Voorbeeld 18: Een kliniek voor cosmetische chirurgie vraagt een patiënt om uitdrukkelijke toestemming voor de doorgifte van zijn medisch dossier 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 informatie 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 verkregen⁵⁰.
98. 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 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 specifieke informatie voor een specifiek 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 de toestemming kan bevestigen.
99. 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, nagaan 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 op grond waarvan deze gegevens kunnen worden verwerkt.
100. Voorbeeld 19: De luchtvaartmaatschappij Holiday Airways biedt extra assistentie aan voor passagiers die, bijvoorbeeld vanwege een beperking, niet zelfstandig kunnen reizen. Een klant boekt een vlucht van Amsterdam naar Boedapest en vraagt 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 meerdere mogelijkheden, bijvoorbeeld een rolstoel bij de gate van aankomst, of een medewerker die samen met haar van A naar B reist). Holiday Airways vraagt om uitdrukkelijke toestemming voor het verwerken van de medische gegevens van deze klant 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.

⁵⁰ Dit voorbeeld doet geen afbreuk aan 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.

Bovendien blijven er vluchten naar Boedapest zonder extra assistentie beschikbaar. NB: aangezien er gegevens nodig zijn voor de verlening van de gevraagde dienst, is artikel 7, lid 4, niet van toepassing.

101. 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.
102. Om zijn op maat gemaakte producten te kunnen leveren aan bijziende klanten, verzoekt de verwerkingsverantwoordelijke om toestemming voor het gebruik van de informatie over de oogafwijking van de klanten. Klanten verstrekken bij het online plaatsten van hun bestelling de benodigde medische gegevens, zoals de sterkte van hun bril. Zonder deze gegevens kunnen de gewenste maatbrillen 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

103. De AVG verplicht verwerkingsverantwoordelijken ertoe om aanvullende maatregelen te nemen om ervoor te zorgen dat zij geldige toestemming verkrijgen en behouden, en kunnen aantonen dat zij daarover beschikken. Artikel 7 AVG omschrijft deze aanvullende voorwaarden voor geldige toestemming en bevat specifieke bepalingen over het bijhouden van registers inzake toestemming en het recht toestemming gemakkelijk te kunnen intrekken. Artikel 7 geldt ook voor toestemming zoals bedoeld in de andere artikelen van de AVG, bijvoorbeeld de artikelen 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

104. 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.
105. Overweging 42 luidt: “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.”
106. 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 informatie mogen verzamelen dan nodig is.
107. 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 toestemming heeft verleend. De verplichting te kunnen aantonen dat toestemming bestaat, geldt zolang 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).

108. De verwerkingsverantwoordelijke kan bijvoorbeeld een register bijhouden van ontvangen verklaringen van toestemming, zodat hij kan aantonen hoe de toestemming is verkregen, wanneer de toestemming is verkregen en welke informatie destijds 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 reden voor deze verplichting in de AVG is dat verwerkingsverantwoordelijken verantwoording moeten afleggen met betrekking tot het verkrijgen van geldige toestemming van de betrokkenen en de mechanismen die zij hebben ingevoerd voor het verkrijgen van die toestemming. In een online context kan een verwerkingsverantwoordelijke bijvoorbeeld gegevens bewaren over de sessie waarin toestemming kenbaar is gemaakt, tezamen met de documentatie over de werkstroom voor het verkrijgen van 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.

109. 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 er vrijwillig mee hebben ingestemd om te worden opgenomen op een lijst van kandidaten die voor dit doel kunnen worden benaderd. De verwerkingsverantwoordelijke vraagt de betrokkenen om uitdrukkelijke toestemming 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 instemt met het gebruik van zijn gegevens voor de doeleinden van project X.

110. In de AVG wordt geen specifieke termijn gesteld aan de geldigheidsduur van de toestemming. Hoelang toestemming geldig blijft, hangt af van de context, het toepassingsgebied van de oorspronkelijke toestemming en de verwachtingen van de betrokkene. Wanneer de verwerkingsactiviteiten veranderen of sterk evolueren, is de oorspronkelijke toestemming niet meer geldig. Indien dit het geval is, moet opnieuw toestemming worden verkregen.

111. De EDPB adviseert als een beste praktijk om met passende tussenpozen opnieuw om toestemming te vragen. Ook hier helpt het verstrekken van alle informatie om ervoor te zorgen dat de betrokkene goed geïnformeerd blijft over hoe zijn gegevens worden gebruikt, en hoe hij zijn rechten kan uitoefenen⁵¹.

5.2 Intrekking van toestemming

112. 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 deze kwestie in WP29 adviezen⁵².

⁵¹ Zie de richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679 (WP 260 versie 1) van de Groep artikel 29, bekrachtigd door de EDPB.

⁵² 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

113. Artikel 7, lid 3, AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de betrokkene zijn toestemming te allen tijde moet kunnen intrekken en dat dit net zo eenvoudig moet zijn als het geven ervan. De AVG bepaalt niet dat het geven en intrekken van informatie altijd moet plaatsvinden door middel van dezelfde handeling.
114. Wanneer toestemming echter wordt verkregen via elektronische middelen, door middel van slechts één muisklik, veeg of toetsaanslag, 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 e-mail), lijdt het geen twijfel dat de betrokkene zijn toestemming moet kunnen intrekken via dezelfde elektronische interface, omdat overschakelen naar een andere interface enkel voor het intrekken van toestemming onnodige moeite zou kosten. Voorts moet de betrokkene zijn toestemming kunnen intrekken zonder daarvan nadeel te ondervinden. Dit betekent onder meer dat een verwerkingsverantwoordelijke het mogelijk moet maken dat toestemming kosteloos of zonder verslechtering van het serviceniveau wordt ingetrokken⁵³.
115. Voorbeeld 22: Een muzikfestival verkoopt kaartjes via een online ticketservice. Bij elke online verkoop van kaartjes wordt toestemming gevraagd om de contactgegevens voor marketingdoeleinden te gebruiken. Klanten kunnen hierop reageren door “Nee” of “Ja” te 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 vergt meer moeite dan de ene muisklik die nodig is voor het geven van toestemming via de online ticketservice, die dag en nacht open is.
116. 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 artikel 7, lid 3, van de AVG. Daarnaast moet de verwerkingsverantwoordelijke als onderdeel van de transparantieplichting de betrokkenen informeren hoe zij hun rechten kunnen uitoefenen⁵⁴.
117. Als algemene regel geldt dat als toestemming wordt ingetrokken, alle gegevensverwerkingen die overeenkomstig de AVG waren gebaseerd op toestemming en plaatsgevonden hebben voordat de

5/2005 over het gebruik van locatiegegevens voor het verstrekken van diensten met toegevoegde waarde (WP 115), blz. 7).

⁵³ 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).

⁵⁴ Overweging 39 AVG, waarin wordt verwezen naar de artikelen 13 en 14 van deze verordening, bepaalt: “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.”

toestemming werd ingetrokken, rechtmatig blijven, maar de verwerkingsverantwoordelijke wel moet stoppen met de desbetreffende verwerkingsactiviteiten. Als er voor de verwerking van de gegevens geen andere rechtsgrond is (bijv. verdere opslag), moeten deze door de verwerkingsverantwoordelijke worden gewist⁵⁵.

118. Zoals reeds vermeld in deze richtsnoeren is het zeer belangrijk dat verwerkingsverantwoordelijken de doeleinden waarvoor de gegevens daadwerkelijk worden verwerkt en de rechtsgrond 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 worden verwerkt 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 op welke rechtsgrond men zich daartoe baseert.
119. Verwerkingsverantwoordelijken zijn verplicht om gegevens te wissen die zijn verwerkt op basis van toestemming nadat deze toestemming is ingetrokken, gesteld dat er geen ander doel is dat het bewaren van deze gegevens rechtvaardigt⁵⁶. Naast deze situatie, die bestreken wordt door artikel 17, lid 1, onder b), kan een individuele betrokkene verzoeken om het wissen van andere hem betreffende persoonsgegevens die zijn verwerkt op basis van een andere rechtsgrond, bijvoorbeeld op basis van artikel 6, lid 1, onder b)⁵⁷. Verwerkingsverantwoordelijken zijn verplicht om na te gaan of verdere verwerking van de betreffende gegevens passend is, ook zonder een verzoek tot wissen door de betrokkene⁵⁸.
120. In gevallen waarin de betrokkene zijn toestemming intrekt en de verwerkingsverantwoordelijke op basis van een andere rechtsgrond door wil gaan met de verwerking van de persoonsgegevens, mag de verwerkingsverantwoordelijke de toestemming (die ingetrokken is) niet stilzwijgend verruilen voor deze andere rechtsgrond. Elke wijziging van de rechtsgrond voor verwerking moet aan de betrokkene worden meegedeeld overeenkomstig de informatievereisten van 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

121. Artikel 6 bevat de voorwaarden voor rechtmatige verwerking van persoonsgegevens en beschrijft zes rechtsgronden waarop een verwerkingsverantwoordelijke zich kan baseren. Voordat begonnen wordt

⁵⁵ Zie artikel 17, lid 1, onder b), en lid 3, AVG.

⁵⁶ In dat geval moet het andere doel dat de verwerking rechtvaardigt een eigen, afzonderlijke rechtsgrond hebben. Dit betekent dat de verwerkingsverantwoordelijke toestemming kan verruilen voor een andere rechtsgrond, zie onderstaand punt 6.

⁵⁷ Zie artikel 17, inclusief eventueel toepasselijke uitzonderingen, en overweging 65 AVG.

⁵⁸ Zie ook artikel 5, lid 1, onder e), AVG.

met de verwerkingsactiviteiten moet worden bepaald welke van deze zes gronden van toepassing is en met betrekking tot welk specifiek doel⁵⁹.

122. Het is belangrijk om hier op te merken dat als een verwerkingsverantwoordelijke ervoor kiest zich te baseren op toestemming voor een deel van de verwerking, hij bereid moet zijn om de keuzen inzake die toestemming te respecteren, en te stoppen met dat deel van de verwerking als een persoon zijn toestemming intrekt. Het doen voorkomen dat gegevens worden verwerkt op basis van toestemming, terwijl men zich in werkelijkheid op een andere rechtsgrond baseert, zou wezenlijk oneerlijk zijn ten aanzien van de betrokkenen.
123. Met andere woorden, de verwerkingsverantwoordelijke kan toestemming niet voor andere rechtsgronden verruilen. Het is bijvoorbeeld niet toegestaan om, wanneer de geldigheid van toestemming problemen oplevert, achteraf de rechtsgrond “rechtmatig belang” te gebruiken ter rechtvaardiging van verwerking. Wegens de verplichting de rechtsgrond te vermelden waarop de verwerkingsverantwoordelijke zich bij het verzamelen van persoonsgegevens baseert, moet hij alvorens te beginnen met verzamelen, hebben beslist wat de passende rechtsgrond hiervoor is.

7 SPECIFIEKE AANDACHTSPUNTEN IN DE AVG

7.1 Kinderen (artikel 8)

124. Ten opzichte van de huidige richtlijn creëert de AVG een extra beveiligingslaag voor situaties waarin persoonsgegevens van kwetsbare natuurlijke personen, met name kinderen, worden verwerkt. Artikel 8 bevat aanvullende verplichtingen die 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 [...]” In overweging 38 staat ook: “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 “verzamen van persoonsgegevens over kinderen” omvat.
125. 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 draagt⁶⁰. Ten aanzien van de leeftijdsgrens voor geldige

⁵⁹ Overeenkomstig artikel 13, lid 1, onder c), en/of artikel 14, lid 1, onder c), moet de verwerkingsverantwoordelijke de betrokkene hiervan in kennis stellen.

⁶⁰ Onverminderd de mogelijkheid voor lidstaten om bij wet af te wijken van de leeftijdsgrens, zie artikel 8, lid 1.

toestemming is de AVG flexibel: lidstaten kunnen bij wet een lagere leeftijd vaststellen, maar deze leeftijd mag niet lager zijn dan 13 jaar.

126. Zoals vermeld in paragraaf 3.1 over geïnformeerde toestemming moet de informatie begrijpelijk zijn voor het publiek waartoe de verwerkingsverantwoordelijke zich richt, en moet er bijzondere aandacht zijn 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 hoe hij voornemens is de verzamelde gegevens te verwerken⁶¹. Als de ouder toestemming moet geven, kan informatie nodig zijn om volwassenen in staat te stellen een geïnformeerde beslissing nemen.
127. 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.^{62, 63}
 -) De verwerking is gebaseerd op toestemming.

7.1.1 Dienst van de informatiemaatschappij

128. Voor het bepalen van het toepassingsgebied van de term “dienst van de informatiemaatschappij” in de AVG wordt in artikel 4, punt 25, AVG verwezen naar Richtlijn 2015/1535.
129. Voor de beoordeling van het toepassingsgebied van deze definitie verwijst de EDPB tevens naar jurisprudentie van het Europees Hof van Justitie⁶⁴. Het Hof oordeelde dat *diensten van de informatiemaatschappij* overeenkomsten en andere diensten omvatten die online gesloten of doorgegeven worden. Als een dienst twee economisch zelfstandige onderdelen omvat, waarvan er één

⁶¹ In overweging 58 AVG wordt opgemerkt dat een verwerkingsverantwoordelijke er in voorkomende gevallen voor moet zorgen dat de verstrekte informatie begrijpelijk is voor kinderen, hetgeen deze verplichting bevestigt.

⁶² Volgens artikel 4, punt 25, AVG is een dienst van de informatiemaatschappij een dienst zoals gedefinieerd in artikel 1, lid 1, onder b), van Richtlijn 2015/1535: ““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, doorgeleid 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 vallende diensten opgenomen. Zie ook overweging 18 van Richtlijn 2000/31/EG.

⁶³ Volgens het VN-Verdrag inzake de bescherming van het kind, artikel 1, wordt “[...] onder een kind [...] verstaan ieder mens jonger dan achttien jaar, tenzij volgens het op het kind van toepassing zijnde recht de meerderjarigheid eerder wordt bereikt”, zie resolutie 44/25 van 20 november 1989 van de Algemene Vergadering van de Verenigde Naties (Verdrag inzake de bescherming van het kind).

⁶⁴ Zie Hof van Justitie, 2 december 2010 in zaak C-108/09 (*Ker-Optika*), punten 22 en 28. Voor wat betreft “samengestelde diensten” verwijst de EDPB ook naar zaak C-434/15 (*Asociación 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 dienstenpakket waarvan het hoofdelement geen dienst van de informatiemaatschappij is (in die zaak een vervoersdienst), niet kan worden gekwalificeerd als een “dienst van de informatiemaatschappij”.

de online component is, zoals het aanbod en de aanvaarding van een aanbod in het kader van het sluiten van een overeenkomst of de informatieverstrekking 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 of distributie van goederen, niet onder het begrip “dienst van de informatiemaatschappij”. De online levering van een dienst valt dus binnen het toepassingsgebied van het begrip “dienst van de informatiemaatschappij” in artikel 8 AVG.

7.1.2 Rechtstreeks aanbod aan een kind

130. 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

131. De AVG bepaalt: “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 van kan uitgaan dat het volstaat 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 in zijn nationale wetgeving de plaats van de belangrijkste vestiging van de verwerkingsverantwoordelijke of de woonplaats van de betrokkene te gebruiken als referentiepunt. Ten eerste moeten de lidstaten bij die keuze rekening houden met het belang van het kind. De EDPB moedigt de lidstaten aan om een geharmoniseerde oplossing te zoeken voor deze kwestie.
132. 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 zich ervan te vergewissen dat de gebruiker de leeftijd voor digitale toestemming heeft bereikt, en de betrokken maatregelen moeten in verhouding staan tot de aard en de risico's van de verwerking.
133. Als de gebruikers verklaren dat zij de leeftijd voor digitale toestemming hebben bereikt, kan de verwerkingsverantwoordelijke passende controles uitvoeren om na te gaan of dat waar is. Hoewel niet expliciet in de AVG staat dat redelijke inspanningen moet worden geleverd om de leeftijd te verifiëren, is dat wel impliciet vereist, omdat de verwerking van gegevens onrechtmatig is als deze berust op toestemming die is verleend door een kind dat niet oud genoeg is om zelfstandig geldige toestemming te geven.
134. Als de gebruiker verklaart dat hij 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.
135. 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 met een gering risico kan het passend

zijn om een nieuwe abonnee op een dienst te verplichten om zijn geboortjaar te vermelden of door middel van een formulier te verklaren dat hij (niet) minderjarig is⁶⁵. Bij twijfel dient de verwerkingsverantwoordelijke zijn mechanismen voor leeftijdscontrole in voorkomend geval te herzien en na te gaan of alternatieve controles nodig zijn⁶⁶.

7.1.4 Toestemming van kinderen en ouderlijke verantwoordelijkheid

136. Met betrekking tot de toestemming van de persoon die de ouderlijke verantwoordelijkheid draagt, is in de AVG niet vastgelegd hoe in de praktijk de toestemming van de ouder moet worden verkregen of moet worden vastgesteld dat iemand gerechtigd is om deze handeling uit te voeren⁶⁷. Daarom beveelt de EDPB aan om een proportionele aanpak te volgen, overeenkomstig 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 informatie, zoals contactgegevens van een ouder of voogd.
137. Wat redelijk is, zowel voor het controleren of een gebruiker oud genoeg is om zelf toestemming te verlenen, als voor 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 een gering 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, AVG⁶⁸. Controlediensten die worden uitgevoerd door vertrouwde derden kunnen oplossingen bieden die de hoeveelheid persoonsgegevens minimaliseren die de verwerkingsverantwoordelijke zelf moet verwerken.

138. 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:
139. Stap 1: De gebruiker vragen of hij jonger of ouder is dan 16 jaar (of een alternatieve leeftijd voor digitale toestemming). Als de gebruiker verklaart dat hij jonger is dan de vereiste leeftijd voor digitale toestemming:
140. Stap 2: De dienst informeert het kind dat een ouder of voogd toestemming moet verlenen voor 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.

⁶⁵ Dit zal niet in alle gevallen een waterdichte oplossing zijn, maar illustreert wel hoe met deze bepaling kan worden omgegaan.

⁶⁶ Zie WP29 Advies 5/2009 over online sociale netwerken (WP163).

⁶⁷ WP29 merkt op dat de persoon die de ouderlijke verantwoordelijkheid draagt niet altijd de natuurlijke ouder van het kind is, en dat de ouderlijke verantwoordelijkheid kan worden gedragen door meerdere partijen, waaronder zowel rechtspersonen als natuurlijke personen.

⁶⁸ Een ouder of voogd kan bijvoorbeeld worden gevraagd om € 0,01 over te maken aan de verwerkingsverantwoordelijke, met in de omschrijving van de transactie een korte bevestiging dat de 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 ongeoorloofde discriminatie van personen die geen bankrekening hebben te voorkomen.

141. 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 zich ervan te vergewissen dat de volwassene de ouderlijke verantwoordelijkheid heeft.
142. Stap 4: In geval van klachten neemt het platform extra stappen om de leeftijd van de abonnee te controleren.
143. Indien het platform de overige eisen inzake toestemming heeft vervuld, kan het platform voldoen aan de aanvullende criteria van artikel 8 AVG door deze stappen te volgen.
144. Uit dit voorbeeld blijkt dat de verwerkingsverantwoordelijke ervoor kan zorgen dat hij in staat is om aan te tonen dat hij redelijke inspanningen heeft geleverd om zich ervan te vergewissen dat geldige toestemming is verkregen met betrekking van de aan het kind aangeboden diensten. Artikel 8, lid 2, voegt specifiek toe: “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.”
145. Het is aan de verwerkingsverantwoordelijke om te bepalen welke maatregelen in een bepaald geval passend zijn. Als algemene regel geldt dat verwerkingsverantwoordelijken moeten afzien van controlemethodes waarbij buitensporig veel persoonsgegevens worden verzameld.
146. De EDPB erkent dat zich gevallen kunnen voordoen waarin controle een uitdaging is (bijvoorbeeld als kinderen die zelf toestemming verlenen, nog geen “identiteitsvoetafdruk” hebben, of als het niet gemakkelijk is om de ouderlijke verantwoordelijkheid te controleren). Hiermee kan rekening worden gehouden bij het bepalen van welke inspanningen redelijk zijn, maar van verwerkingsverantwoordelijken worden ook verwacht dat zij hun processen en de beschikbare technologie doorlopend toetsen.
147. Met betrekking tot de mogelijkheid van de betrokkene om zelfstandig toestemming te verlenen voor de verwerking van zijn persoonsgegevens en volledige controle te hebben over de verwerking, kan de toestemming door een drager van de ouderlijke verantwoordelijkheid of een machtiging tot toestemming van een drager van ouderlijke verantwoordelijkheid worden bevestigd, gewijzigd of ingetrokken, wanneer de betrokkene de leeftijd voor het verlenen van digitale toestemming heeft bereikt.
148. In de praktijk betekent dit dat als het kind geen actie onderneemt, de toestemming of machtiging tot toestemming voor de verwerking van de persoonsgegevens die door een drager van de ouderlijke verantwoordelijkheid is verleend toen de betrokkene nog niet oud genoeg was om zelf digitale toestemming te verlenen, een geldige grond voor verwerking blijft.
149. Wanneer het kind de leeftijd voor het verlenen van digitale toestemming heeft bereikt, heeft het de mogelijkheid om de toestemming overeenkomstig artikel 7, lid 3, zelf in te trekken. Overeenkomstig de beginselen van behoorlijkheid en verantwoording moet de verwerkingsverantwoordelijke het kind informeren over deze mogelijkheid⁶⁹.

⁶⁹ De betrokkenen moeten zich ook bewust zijn van het in artikel 17 vastgelegde recht op vergetelheid, dat met name relevant is voor toestemming die is gegeven toen de betrokkene nog een kind was, zie overweging 63.

150. Het is belangrijk om erop te wijzen dat overeenkomstig overweging 38 in de context van preventieve of adviesdiensten die rechtstreeks aan een kind worden aangeboden, de toestemming van de persoon die de ouderlijke verantwoordelijkheid draagt, niet vereist is. Voor het online aanbieden van diensten in verband met kindbescherming via een online chatservice is bijvoorbeeld geen voorafgaande ouderlijke toestemming vereist.
151. Ten slotte bepaalt de AVG dat de regels betreffende de eisen inzake 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 rechtskader dat moet worden beschouwd als losstaand van het nationaal overeenkomstenrecht. In deze richtsnoeren wordt dan ook 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 harmonisatie van nationale bepalingen van overeenkomstenrecht behoort niet tot het toepassingsgebied van de AVG.

7.2 Wetenschappelijk onderzoek

152. De definitie van wetenschappelijke onderzoeksdoeleinden heeft aanzienlijke gevolgen voor het bereik van verwerkingsactiviteiten die een verwerkingsverantwoordelijke mag 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. (...)”; de EDPB is echter van mening dat het begrip niet ruimer mag worden opgevat dan de gebruikelijke betekenis en verstaat onder “wetenschappelijk onderzoek” in deze context een onderzoeksproject dat opgezet wordt volgens de relevante methodologische en ethische normen van de sector, en conform goede praktijken.
153. Wanneer toestemming de rechtsgrond is voor het uitvoeren van onderzoek conform de AVG, moet deze toestemming voor het gebruik van persoonsgegevens worden onderscheiden van andere eisen inzake 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 gegevensbeschermingswetgeving kan deze vorm van toestemming worden beschouwd als een extra waarborg⁷⁰. 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 gebruikt⁷¹. Op grond van de uitzondering van artikel 9, lid 2, onder j), geldt dit ook voor bijzondere categorieën gegevens⁷².
154. 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 luidt: “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.”
155. 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 welomschreven doel heeft. Voor gevallen waarin de doeleinden voor gegevensverwerking binnen een wetenschappelijk onderzoeksproject aanvankelijk niet kunnen

⁷⁰ Zie ook overweging 161 van de AVG.

⁷¹ Artikel 6, lid 1, onder c), kan ook van toepassing zijn op delen van de verwerkingsactiviteiten die uitdrukkelijk 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.

⁷² Op grond van artikel 9, lid 2, onder i), kunnen specifieke tests van geneesmiddelen kunnen worden uitgevoerd op basis van communautaire of nationale wetgeving.

worden gespecificeerd, staat overweging 33 als uitzondering toe dat het doel op een meer algemeen niveau mag worden omschreven.

156. Gezien de strenge eisen die door artikel 9 AVG worden gesteld aan de verwerking van bijzondere categorieën gegevens, merkt de EDPB op dat ingeval bijzondere categorieën gegevens worden verwerkt op basis van uitdrukkelijke toestemming, voor de toepassing van de flexibele aanpak van overweging 33 een striktere interpretatie geldt en een hoge mate van controle is vereist.
157. In zijn geheel bezien kan de AVG niet zodanig worden uitgelegd dat het belangrijke uitgangspunt dat de doeleinden waarvoor toestemming van de betrokkene wordt gevraagd, dienen te worden gespecificeerd, door een verwerkingsverantwoordelijke mag worden omzeild.
158. Wanneer onderzoeksdoeleinden niet volledig kunnen worden gespecificeerd, moet een verwerkingsverantwoordelijke andere manieren vinden om ervoor te zorgen dat zo goed mogelijk wordt voldaan aan de eisen inzake toestemming, bijvoorbeeld door de 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 worden verkregen voordat een volgende fase van start gaat. Zulke toestemming moet echter evengoed in overeenstemming zijn met de geldende ethische normen voor wetenschappelijk onderzoek.
159. Bovendien kan de verwerkingsverantwoordelijke in dergelijke gevallen nadere waarborgen instellen. Zo wordt in artikel 89, lid 1, bijvoorbeeld benadrukt dat er waarborgen vereist zijn voor verwerkingsactiviteiten voor wetenschappelijk of historisch onderzoek of statistische doeleinden. De verwerking voor deze doeleinden dient te 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 genoemd⁷³. Wanneer het doel van het onderzoek kan worden gerealiseerd zonder de verwerking van persoonsgegevens, is anonimisering de aangewezen oplossing.
160. Transparantie is een extra waarborg wanneer door de omstandigheden van het onderzoek specifieke toestemming niet mogelijk is. Als een doel onvoldoende bepaald is, kunnen de verwerkingsverantwoordelijken dat compenseren door in de loop van het onderzoeksproject regelmatig informatie te verstrekken over de ontwikkeling van het doel, zodat de toestemming na verloop van tijd zo specifiek mogelijk is. Wanneer dit gebeurt, heeft de betrokkene ten minste een

⁷³ 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 betreffende 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.”

basiskennis van de stand van zaken, zodat hij bijvoorbeeld kan beslissen al dan niet gebruik te maken van het recht om toestemming in te trekken op grond van artikel 7, lid 3⁷⁴.

161. Ook een uitgebreid onderzoeksplan dat de betrokkenen kunnen inzien alvorens zij toestemming verlenen, kan bijdragen tot het compenseren van een gebrek aan specificatie van doeleinden⁷⁵. In dit onderzoeksplan moeten de beoogde onderzoeksvragen en werkwijze zo duidelijk mogelijk worden beschreven. Het onderzoeksplan kan ook bijdragen tot naleving van artikel 7, lid 1, omdat verwerkingsverantwoordelijken moeten aantonen welke informatie voor de betrokkenen beschikbaar was op het moment dat ze toestemming verleenden, om te kunnen bewijzen dat de toestemming geldig is.
162. Het is belangrijk om in gedachten te houden dat ingeval toestemming wordt gebruikt als de rechtsgrond voor verwerking, de betrokkene ook de mogelijkheid moet hebben om deze toestemming in te trekken. De EDPB 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 bepaalt 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 onderzoeksdoeleinden⁷⁶.

7.3 De rechten van betrokkenen

163. Als de gegevensverwerking is gebaseerd op toestemming van de betrokkene, dan heeft dit gevolgen voor de rechten van die persoon. Wanneer de verwerking is gebaseerd op toestemming, hebben de 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 tot een vergelijkbaar resultaat kan leiden.
164. De artikelen 16 tot en met 20 AVG bepalen dat (bij gegevensverwerking op basis van toestemming) de betrokkenen het recht hebben op het wissen van gegevens wanneer toestemming is ingetrokken, alsmede het recht op beperking, rectificatie en inzage⁷⁷.

⁷⁴ Ook andere maatregelen met betrekking tot transparantie kunnen zinvol zijn. Wanneer verwerkingsverantwoordelijken persoonsgegevens verwerken voor wetenschappelijke doeleinden en bij aanvang van het onderzoek geen volledige informatie kan worden verstrekt, zouden zij een specifieke contactpersoon kunnen aanwijzen waarmee de betrokkenen contact kunnen opnemen als zij vragen hebben.

⁷⁵ Een dergelijke mogelijkheid staat bijvoorbeeld in artikel 14, lid 1, van de huidige Wet inzake persoonsgegevens van Finland (*Henkilötietolaki*, 523/1999).

⁷⁶ Zie ook WP29 Advies 05/2014 over anonimiseringstechnieken (WP216).

⁷⁷ In gevallen waarin bepaalde verwerkingsactiviteiten worden beperkt overeenkomstig artikel 18 AVG, kan toestemming van de betrokkene nodig zijn om de beperkingen op te heffen.

8 TOESTEMMING VERKREGEN OVEREENKOMSTIG RICHTLIJN 95/46/EG

165. Verwerkingsverantwoordelijken die momenteel gegevens verwerken op basis van toestemming conform nationale wetgeving inzake gegevensbescherming, worden niet automatisch verplicht om alle bestaande relaties op basis van toestemming ter voorbereiding op de AVG volledig te hernieuwen. Verkregen toestemming blijft tot op heden geldig voor zover deze in overeenstemming is met de voorwaarden die zijn vastgelegd in de AVG.
166. 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 norm van de AVG (zie overweging 171 AVG⁷⁸). In de praktijk legt de AVG de lat hoger ten aanzien van de toepassing van mechanismen voor toestemming; zo worden er verschillende nieuwe eisen ingevoerd waardoor verwerkingsverantwoordelijken mechanismen voor toestemming moeten veranderen, en alleen het herschrijven van privacyverklaringen niet voldoende is⁷⁹.
167. Omdat de AVG bijvoorbeeld bepaalt dat een verwerkingsverantwoordelijke in staat moet zijn om aan te tonen dat geldige toestemming is verkregen, gelden alle vermoede toestemmingen ten aanzien waarvan geen referenties worden bewaard, automatisch als niet in overeenstemming met de norm voor toestemming van de AVG, en moeten deze worden hernieuwd. En omdat de AVG een “verklaring of een ondubbelzinnige actieve handeling” vereist, voldoen alle vermoede toestemmingen die gebaseerd zijn op een meer impliciete vorm van handelen door de betrokkene (zoals een vooraf aangevinkt opt-invakje) evenmin aan de norm voor toestemming van de AVG.
168. Om te kunnen aantonen dat toestemming is verkregen of om een meer granulaire indicatie van de wensen van de betrokkenen mogelijk te maken, kan het bovendien nodig zijn om bedrijfsactiviteiten en IT-systemen te herzien. Er moeten ook mechanismen beschikbaar zijn waarmee betrokkenen hun toestemming eenvoudig kunnen intrekken, en er moet informatie worden verstrekt over hoe de toestemming kan worden ingetrokken. Indien de bestaande procedures voor het verkrijgen van toestemming niet voldoen aan de normen van de AVG, moeten verwerkingsverantwoordelijken nieuwe toestemming verkrijgen die wel in overeenstemming is met de AVG.
169. Omdat voor geïnformeerde toestemming echter niet alle in artikel 13 en 14 genoemde elementen altijd aanwezig hoeven te zijn, betekenen de uitgebreide informatieverplichtingen van de AVG niet

⁷⁸ Overweging 171 van de AVG luidt: “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 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.”

⁷⁹ Zoals in de inleiding vermeld, verschaft de AVG een nadere toelichting op 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”.

altijd dat toestemming die is verleend vóór de inwerkingtreding van de AVG ongeldig wordt (zie pagina 15). Richtlijn 95/46/EG voorzag niet in een verplichting om betrokkenen te informeren over de rechtsgrond waarop de verwerking werd uitgevoerd.

170. Ingeval een verwerkingsverantwoordelijke vaststelt dat de toestemming die eerder op grond van de oude wetgeving is verkregen, niet voldoet aan de norm van de AVG, moet hij actie ondernemen om wel aan deze standaard te voldoen, bijvoorbeeld door hernieuwde toestemming te verkrijgen op een manier die in overeenstemming is met de AVG. Overeenkomstig de AVG kan de ene rechtsgrond niet voor de andere worden verruild. Ingeval een verwerkingsverantwoordelijke niet op een met de AVG strokende 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 verwerkingsverantwoordelijke moet in ieder geval voldoen aan de beginselen van rechtmatige, behoorlijke en transparante verwerking.