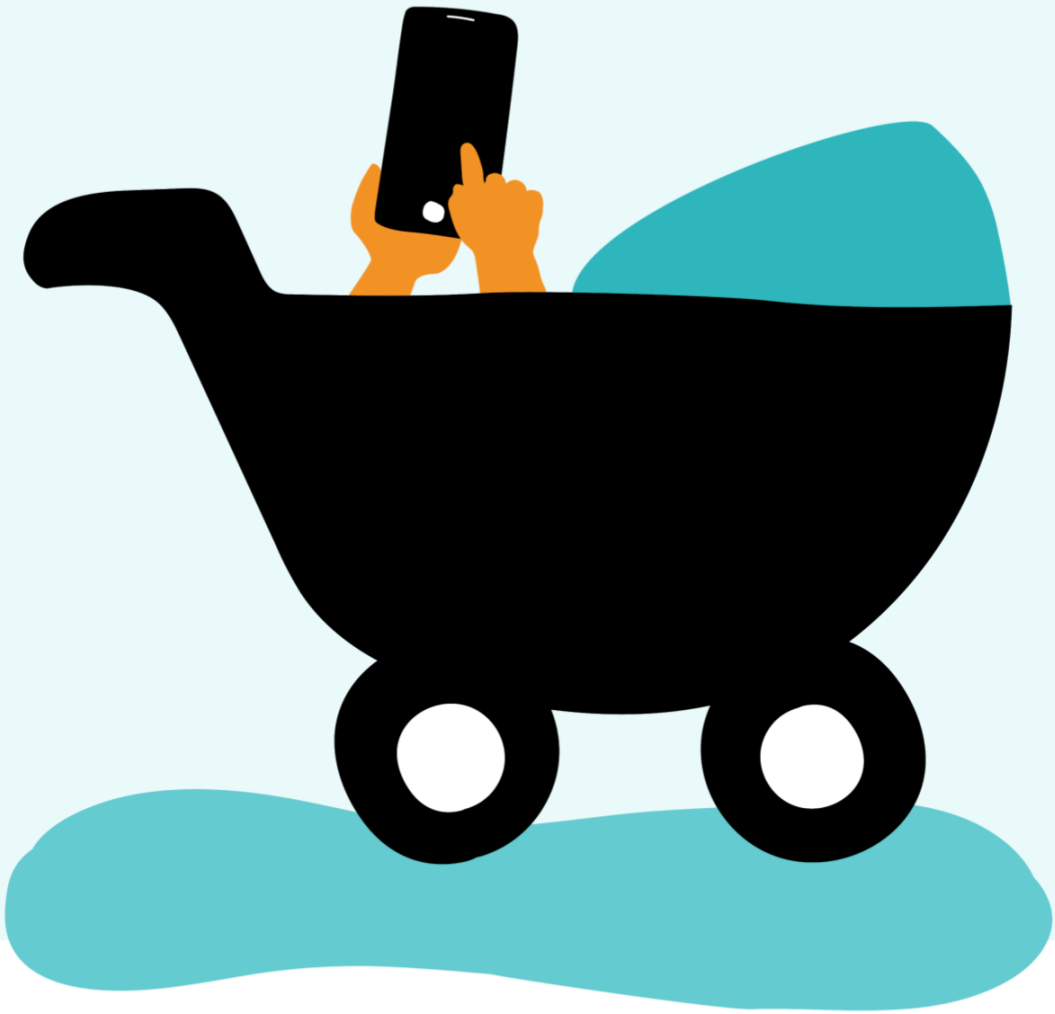


code voor kinderrechten

Code voor kinderrechten

De code voor Kinderrechten is opgesteld door
Universiteit Leiden en Waag in opdracht van het
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Inhoudsopgave

De code in een oogopslag

Beginsel 1

Zet het belang van het kind voorop bij het ontwerp

Beginsel 2

Betrek kinderen en hun verwachtingen bij het ontwerp

Beginsel 3

Verwerk persoonsgegevens op een voor kinderen rechtmatige manier

Beginsel 4

Zorg voor transparantie op een voor kinderen begrijpelijke en toegankelijke manier

Beginsel 5

Voer een op kinderrechten gebaseerde privacy impact assessment uit

Beginsel 6

Zorg voor een kindvriendelijk privacy ontwerp

Beginsel 7

Voorkom het profileren van kinderen

Beginsel 8

Voorkom te allen tijde economische exploitatie van kinderen

Beginsel 9

Voorkom te allen tijde voor kinderen schadelijk ontwerp

Beginsel 10

Ontwikkel richtlijnen voor de branche die zijn gericht op de bescherming van de belangen en rechten van kinderen

De code voor kinderrechten helpt ontwikkelaars en ontwerpers om de rechten van het kind voorop te stellen bij het ontwikkelen van digitale diensten. De code bestaat uit tien beginselen, geoperationaliseerd aan de hand van implementatievoorbeelden. De beginselen zijn op zichzelf niet juridisch afdwingbaar, maar gebaseerd op wet- en regelgeving (zoals het VN Verdrag inzake de Rechten van het Kind 1989) die wel degelijk juridisch bindend is.

Beginsel 1: Zet het belang van het kind voorop bij het ontwerp. Het vooropstellen van het belang van het kind bij alle digitale activiteiten met een impact op kinderen is het leidend beginsel in de gehele code. Een digitale dienst die mogelijk door kinderen wordt gebruikt, moet rekening houden met dit beginsel en alle andere beginselen in deze code. Een kind-impact-assessment voorafgaand aan de ontwikkeling en tijdens de levenscyclus van de dienst kan dit beginsel zorgvuldig wegen tegenover andere belangen. **Belangrijkste wet- en regelgeving**: art. 3 IVRK, art. 24 (2) EU handvest.

Beginsel 2: Betrek kinderen en hun verwachtingen bij het ontwerp. Om invulling te kunnen geven aan het belang van het kind moeten kinderen op enige wijze kunnen participeren in het ontwerp en de ontwikkeling van digitale diensten die een impact op hen hebben. Zorg dat je zicht hebt op de doelgroep (waaronder hun leeftijdscategorie) die je aan wilt spreken en ontwerp vanuit de groep die de meeste beperkingen ondervindt. Zoek aansluiting bij de leefwereld van kinderen en communiceer op een wijze die past bij desbetreffende ontwikkelfase. **Belangrijkste wet- en regelgeving**: art. 12 IVRK.

Beginsel 3: Verwerk persoonsgegevens op een voor kinderen rechtmatige wijze. De persoonsgegevens van kinderen mogen alleen verwerkt worden voor zover dat gebeurt in overeenstemming met de wet, waarbij zowel algemene als kind-specifieke regels gelden. Het principe van dataminimalisatie is leidend bij de verwerking van persoonsgegevens. Voor de implementatie is het in sommige gevallen belangrijk om te weten in welke leeftijdscategorie een kind valt; bij jongere kinderen kan het nodig zijn ouders te betrekken. **Belangrijkste wet- en regelgeving**: art. 16 IVRK, art 8 (1) Handvest Grondrechten EU, art. 16(1) Verdrag Werking EU, en art. 5 e.v. AVG.

Beginsel 4: Zorg voor transparantie op een voor kinderen begrijpelijke en toegankelijke manier. Informatie over het gebruik van een digitale dienst moet herkenbaar en makkelijk te begrijpen zijn voor het kind. De aanbieder is met name over het gebruiken en delen van persoonsgegevens tot transparantie verplicht. Maak informatie over privacy toegankelijk en begrijpelijk en ontwerp binnen de digitale dienst hulpmiddelen, zodat kinderen hun (gegevensbeschermings-)rechten kunnen uitoefenen. Houd daarbij rekening te houden met de leeftijd en ontwikkelingsfase van het kind. **Belangrijkste wet- en regelgeving**: art. 3 (1) IVRK, art. 5 (1) AVG en art. 6:230 m en 6:193c en d BW.

Beginsel 5: Voer een op kinderrechten gebaseerde privacy impact assessment uit. Voer een standaard op kinderrechten gebaseerde privacy impact assessment (PIA) uit wanneer digitale diensten mogelijk door kinderen worden gebruikt. Aangezien kinderen kwetsbare gebruikers zijn, is het risico op het schenden van de gegevensbeschermingsrechten hoog. Maak geregeld gebruik van de PIA om de impact van de dienst goed te blijven kunnen beoordelen. **Belangrijkste wet- en regelgeving**: art. 16 IVRK, art. 8 EVRM, art. 7 en 8 EU Handvest, art. 35 AVG.

Beginsel 6: Zorg voor een kindvriendelijk privacyontwerp. Verwerk niet meer persoonsgegevens dan strikt noodzakelijk voor het bereiken van het specifieke doel van de dienst. Neem privacy mee in het ontwerp (privacy by design) en stel de standaardinstellingen zo privacyvriendelijk mogelijk af (privacy by default). Geef dit op een kindvriendelijke manier vorm met bijvoorbeeld een 'opt-in' regime, standaard toegankelijke ingebouwde opties om je gegevens te wissen en meldingen wanneer geolocatie of microfoon aan staan. **Belangrijkste wet- en regelgeving**: art. 16 IVRK, art. 7 en 8 EU Handvest en art. 5 en 25 AVG.

Beginsel 7: Voorkom het profileren van kinderen. Het profileren van gebruikers is een vorm van gegevensverwerking met hoog risico. Er ontstaat een privacygevoelig (en soms onterecht) beeld van iemand op basis van correlaties. Kinderen zijn kwetsbaar, aangezien profilering kan leiden tot stereotypering, stigmatisering en discriminatie. Het inzetten van profilering zet gebruikers bovendien (impliciet) aan tot overmatig gebruik van de dienst. Functies voor profilering moeten standaard uitstaan, tenzij er vanuit het belang van het kind een dwingende reden voor is. Daar moeten dan passende maatregelen bij genomen zijn. **Belangrijkste wet- en regelgeving**: art. 2 IVRK en art. 22 AVG.

Beginsel 8: Voorkom te allen tijde economische exploitatie van kinderen. Voorkom op exploitatie gerichte vormgeving van digitale diensten, zoals het aanmoedigen van in-app aankopen, het gebruik van gokelementen en persoonsgerichte datagedreven marketing. Wees transparant over de commerciële aspecten van een dienst en vermijd oneerlijke handelspraktijken. **Belangrijkste wet- en regelgeving:** art. 3, 13, 32 IVRK, art. 6, 7, 8, 21 en 22 AVG, 6:193 BW, art. 3 Mediawet en art. 21 Wet kansspelen.

Beginsel 9: Voorkom te allen tijde voor kinderen schadelijk ontwerp. Een digitale dienst kan schadelijk voor kinderen zijn als het ontwerp de kwetsbaarheid van kinderen misbruikt of kinderen onvoldoende beschermt tegen mogelijke schadelijke content en gedragingen. Het is schadelijk als de (mentale, sociale, cognitieve of fysieke) ontwikkeling van het kind negatief wordt beïnvloedt, zoals bij excessief gebruik van de dienst. Het is daarom raadzaam de voorzorgsbenadering ('better safe than sorry') te hanteren. **Belangrijkste wet- en regelgeving**: art. 6, 17 en 24 IVRK, art. 5 (1) AVG en art. 4 (1) Mediawet.

Beginsel 10: Ontwikkel richtlijnen voor de branche gericht op de bescherming van de belangen en rechten van kinderen. De private sector speelt een belangrijke rol in het ontwikkelen en aanbieden van digitale diensten. Bedrijven kunnen zelf bijdragen aan het welzijn van kinderen door het opstellen van richtlijnen binnen de branche - bij voorkeur in samenspraak met kinderen. **Belangrijkste wet- en regelgeving**: art. 3 IVRK, art. 5 (2) en 40 AVG en art. 6:193c (2) BW.

Code voor Kinderrechten

Apps en games spelen een belangrijke rol in het leven van kinderen. En ze brengen er steeds meer tijd mee door.

Digitale technologie levert een waardevolle bijdrage aan de ontwikkeling van kinderen. Maar de praktijk wijst uit dat in het ontwerp van technologieën ook keuzes zijn gemaakt die niet in het belang van kinderen zijn.

De code voor kinderrechten bestaat uit tien beginselen met praktische voorbeelden waarmee ontwerpers en ontwikkelaars de fundamentele rechten van kinderen kunnen waarborgen in digitale diensten.

Waarom een code voor kinderrechten?

Deze code helpt ontwikkelaars en ontwerpers om de rechten van het kind bij het ontwerpen en ontwikkelen van apps, games, slimme apparaten en andere digitale technologie te implementeren.

Kinderrechten moeten waarborgen dat kinderen voldoende vrijheid hebben om zich te ontwikkelen en mee te doen in de maatschappij (participatie), terwijl ze worden beschermd tegen mogelijk schadelijke invloeden, zoals misbruik en verslaving. Dat participeren gebeurt steeds vaker met behulp van digitale diensten. Het is daarom belangrijk dat deze diensten op een kindvriendelijke wijze zijn ontworpen.

Deze code biedt handvatten die helpen om de rechten van kinderen te begrijpen en toe te passen bij de ontwikkeling van een digitale dienst. Alle beginselen zijn te herleiden naar de fundamentele rechten van kinderen in het VN Verdrag inzake de Rechten van het Kind 1989 (IVRK). Verder zijn de beginselen gebaseerd op wet- en regelgeving. De beginselen zijn op zichzelf weliswaar geen juridisch afdwingbare regels, maar de onderliggende wet- en regelgeving is wel juridisch bindend.

Wie bedoelen we met kinderen?

In de code hebben we het over ‘kinderen’ en daarmee bedoelen we alle mensen jonger dan 18 jaar (artikel 1 IVRK). Soms spreekt de wet van minderjarigen, maar wij zullen ook dan het begrip kinderen gebruiken. Soms noemt de wet specifieke leeftijden (bijvoorbeeld artikel 8 AVG) en dan gelden de regels in zo’n bepaling dus voor die leeftijdsgroep. Ook wanneer de groep niet duidelijk is gedefinieerd op basis van hun leeftijd moet er volgens het IVRK rekening worden

gehouden met de zich ontwikkelende vermogens van kinderen (artikel 5 IVRK). Bij de toepassing of implementatie van een regel kan het zijn dat dan alsnog verschillende leeftijden in acht moeten worden genomen, ook al noemt de wet dit niet met zoveel woorden.

Op wat voor digitale technologie is de code van toepassing?

De code gaat over het ontwerpen en ontwikkelen van 'digitale diensten'. Hieronder worden alle diensten begrepen die op enige wijze gebruik maken van digitale technologie, waaronder apps, games, websites, met het netwerk verbonden apparaten (waaronder speelgoed en smart assistants), online platforms, enzovoorts. Het gaat hierbij om alle digitale diensten waar kinderen mogelijk gebruik van zouden kunnen maken, ook als deze niet nadrukkelijk op kinderen gericht zijn.

Tot wie richt de code zich?

Deze code richt zich in de eerste plaats tot bedrijven, overheden, organisaties en zelfstandigen die digitale diensten ontwerpen en ontwikkelen. Ontwerpers en ontwikkelaars krijgen concrete handvatten aangereikt om zich te houden aan de rechten van kinderen bij het ontwerpen en ontwikkelen van diensten.

Ook voor anderen is de code relevant, zoals een opdrachtgever en een merkhouder. Het ontwerp van een digitale dienst vraagt om commerciële beslissingen van bijvoorbeeld een bestuurder of investeerder die consequenties hebben voor het ontwerp. En evenzo is het voor de bedrijfsjurist of functionaris gegevensbescherming in een organisatie nuttig om kennis te nemen van specifieke regels voor kinderen. De code heeft ook een toegevoegde waarde voor digitale platforms of app stores die software van derden aanbieden en willen weten aan welke op kinderrechten gebaseerde standaarden apps moeten voldoen. Verder is de code relevant voor organisaties die software gebruiken voor of met kinderen en willen weten waar ze specifiek op moeten letten bij de aanschaf en het gebruik. Denk dan bijvoorbeeld aan overheden, scholen of jeugdzorgorganisaties. Tenslotte richt de code – en in het bijzonder beginsel 10 – zich tot brancheorganisaties met het verzoek om op kinderrechten gebaseerde gedragscodes te ontwikkelen.

De code is uiteindelijk voor eenieder die digitale technologie gebruikt, waaronder natuurlijk kinderen en ouders, of verantwoordelijk is voor de implementatie van kinderrechten in beleid en regelgeving.

Hoe zijn we tot deze code gekomen?

De eerste twee beginselen zijn overkoepelende beginselen die direct volgen uit twee van de vier fundamentele beginselen van het VN Verdrag inzake de Rechten van het Kind 1989 (IVRK): het belang van het kind en het recht van het kind om gehoord te worden. Deze rechten werken door binnen de overige beginselen. De overige beginselen zijn ook gebaseerd op de rechten in het IVRK en andere wet- en regelgeving.

De code beperkt zich tot die wet- en regelgeving en meer specifiek de daarin opgenomen bepalingen waarin kinderen *in het bijzonder* worden beschermd (bijvoorbeeld bepalingen met betrekking tot de verwerking van persoonsgegevens, oneerlijke handelspraktijken en schadelijke content) of het belang van het kind is meegenomen bij de uitleg van de regels.

De beginselen in deze code hangen met elkaar samen en zijn in hun geheel relevant voor het ontwerp en de ontwikkeling van digitale diensten die door kinderen worden gebruikt. Het is dus geen pick-and-choose model waarbij slechts enkele, willekeurige beginselen worden geïmplementeerd. De concrete implementatie is wel afhankelijk van het specifieke doel en beoogde ontwerp van een app of game. Waar mogelijk verwijzen we naar best practices voor de implementatie.

De Code is opgesteld in samenspraak met experts op het snijvlak kind en technologie, en met ontwerpers, ontwikkelaars en jongeren.

Terminologie

De code heeft het over de ‘gebruiker’ (bijvoorbeeld het kind en/of de ouder) en ‘aanbieder’ van een digitale dienst (het bedrijf dat de digitale dienst ontwerpt, ontwikkelt en/of aanbiedt). We gebruiken deze termen ook op plaatsen waar de wetgeving meer specifieke begrippen gebruikt. Denk bijvoorbeeld aan ‘betrokkene’ of ‘verwerkingsverantwoordelijke’ in het gegevensbeschermingsrecht of ‘consument’ en ‘handelaar’ in het consumentenrecht. Wetgeving heeft het soms over ‘diensten van de informatiemaatschappij’ en bedoelt dan commerciële digitale diensten. Verder vallen onder het begrip ‘ouders’ ook eventuele andere wettelijke vertegenwoordigers of verzorgers van een kind.

Beginsel 1: Zet het belang van het kind voorop bij het ontwerp

Toelichting

Bij alle digitale activiteiten met een impact op individuele kinderen, groepen kinderen of kinderen in het algemeen, staat het belang van het kind voorop. Bij de uitleg van alle beginselen in de code – en daarmee alle aspecten van het ontwerp – is het belang van het kind dus het leidende beginsel. Het beginsel beoogt zo bij te dragen aan het volledig en effectief waarborgen van de fundamentele rechten van kinderen. Het belang van het kind staat daarmee niet op zich, maar moet je in het licht zien van alle relevante rechten van het kind in een concrete situatie. In de meest brede zin houdt het belang van het kind in dat activiteiten die een impact hebben op kinderen het welzijn en de ontwikkeling van het kind moeten waarborgen.

Digitale technologie kan een belangrijke bijdrage leveren aan de ontwikkeling van een kind, bijvoorbeeld door het faciliteren van sociale interactie of het stimuleren van creativiteit. De praktijk wijst echter uit dat in het ontwerp van technologieën vaak keuzes worden gemaakt die niet in het belang zijn van kinderen zijn of die zelfs schadelijk voor hen kunnen zijn. Het is dan ook niet voldoende om enkel schade of negatieve consequenties voor kinderen te voorkomen. Het belang van het kind betekent ook dat het kind een even ‘rijke’ online ervaring moet kunnen hebben als een volwassene. Je mag als kind niet zomaar uitgesloten of een bepaalde ervaring ontnomen worden.

Het belang van het kind is een voortdurend punt van aandacht bij het ontwerp en gebruik van een digitale dienst, vanaf het moment dat een start wordt gemaakt met de uitwerking van het idee en gedurende de gehele levenscyclus van de digitale dienst.

Implementatie

Ga ervan uit dat een digitale dienst die mogelijk door kinderen wordt gebruikt, rekening moet houden met het belang van het kind en alle overige beginselen in deze code. Ga er ook van uit dat je – ongeacht een leeftijdsgrens die bijvoorbeeld in de servicevoorwaarden wordt genoemd – maatregelen moet nemen om hun belangen te waarborgen als er geen adequate leeftijdsverificatie is.

Voorafgaand aan het ontwerp van digitale diensten moet je de belangen van kinderen in kaart brengen en afwegen tegen andere belangen, waaronder belangen van andere kinderen, ouders en bedrijven zelf. Het belang van het kind is ook een eerste overweging ten opzichte van het

commerciële belang dat een bedrijf heeft bij het aanbieden van een digitale dienst. Dat betekent niet dat een digitale dienst geen commercieel belang mag nastreven, maar in de belangenafweging wordt nadrukkelijk verantwoord dat het belang van het kind een eerste overweging is. Bij de belangenafweging wordt rekening gehouden met de verschillende stadia van ontwikkeling van kinderen op basis van hun leeftijd en sociale, mentale en cognitieve ontwikkeling. Concreet bestaat de belangenafweging en de implementatie van het belang van het kind-beginsel voorafgaand aan de ontwikkeling van een digitale dienst uit twee fasen. We noemen deze exercitie een kind-impact-assessment[1]. Bij het kind-impact-assessment wordt een team van belanghebbenden en deskundigen betrokken die meedenken of besluiten over allerlei aspecten van de dienst, denk daarbij aan ontwerpers, ontwikkelaars, investeerders, privacy-officers, marketeers, (bedrijfs-)juristen en, waar mogelijk, kinderen zelf.

Fase 1: evaluatiefase

In deze fase worden *alle* factoren die relevant zijn in het licht van het belang van het kind in kaart gebracht en geëvalueerd. Daarbij wordt rekening gehouden met de leeftijd van het kind [2] (zie ook de pagina meer informatie[3] over de ontwikkelfasen van een kind of beginsel 3 voor manieren voor het nagaan van leeftijd van een gebruiker).

Relevante factoren zijn onder meer:

a. mogelijke impact op het welzijn en de ontwikkeling van kinderen;
b. mogelijke impact op de rechten van kinderen. Denk daarbij onder andere aan de volgende rechten:
    - recht op non-discriminatie,
    - recht op vrijheid van informatie,
    - recht op vrije menings- en gedachtevorming,
    - vrijheid van vereniging en identiteitsvorming en
    - recht op spel en ontspanning;
c. mogelijke impact op de veiligheid van kinderen. Denk onder meer aan:
    - het waarborgen van de privacy (waaronder ook de vertrouwelijkheid en integriteit van persoonsgegevens en de identiteit van kinderen),
    - de bescherming tegen allerlei vormen van uitbuiting, waaronder commerciële of seksuele uitbuiting en seksueel misbruik,
    - bescherming tegen sociale risico's, waaronder digitaal pesten en
    - voorkomen van de confrontatie met schadelijke informatie;

[1] https://sites.unicef.org/csr/css/Children_s_Rights_in_Impact_Assessments_Web_161213.pdf
[2]https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/
[3] https://codevoorkinderrechten.nl/meer-informatie/

d. de rol van ouders bij het waarborgen van het belang van het kind, waaronder bij de bescherming tegen potentiële risico's en bij het ondersteunen van een veilig en vruchtbaar gebruik van de digitale dienst.

De evaluatie van de factoren wordt voor zover beschikbaar onderbouwd met wetenschappelijk onderzoek. Bovendien worden verwachtingen, inzichten en zienswijzen van kinderen waar mogelijk meegenomen in de evaluatie (zie beginsel 2).

Fase 2: vaststellingsfase

Op basis van de evaluatie in fase 1 wordt concreet vastgesteld welke organisatorische en technische maatregelen noodzakelijk zijn om het belang van het kind (en daarmee de rechten van kinderen) adequaat te waarborgen bij het ontwerp en aansluitend gebruik van de digitale dienst. Daarbij zijn de volgende vragen mede richtinggevend:

a. Welke specifieke waarborgen vereisen wet- en regelgeving met het oog op het belang van het kind?
b. Welke ontwerpkeuzes zijn het meest in het belang van het kind? Grijp daarbij terug op de uitkomsten van de evaluatiefase.

De tweede fase is een verantwoordingsfase waarin betrokken partijen concreet laat zien hoe het belang van het kind is geïmplementeerd in de digitale dienst.

Het manipuleren van kinderen (ook in het uitoefenen van hun rechten) op een wijze die slechts of vooral het commerciële belang dient, is niet toegestaan (zie beginsel 8). Een commercieel belang nastreven met een digitale dienst mag, zolang kan worden aangetoond dat het belang van het kind een eerste overweging is wanneer een digitale dienst (mogelijk) een impact heeft op kinderen. De aanbieder zal dus aantoonbaar rekening moeten hebben gehouden met het belang van het kind in een kind-impact assessment zoals hiervoor uiteengezet.

Een kind-impact-assessment (bestaande uit fase 1 en fase 2) is geen eenmalige exercitie, maar dient voortdurend te worden bijgehouden. Het concrete gebruik alsmede de verdere ontwikkeling van de digitale dienst kunnen aanleiding geven tot een aanpassing van de concrete maatregelen of ontwerpkeuzes in het belang van het kind. Soms wordt de impact die een app of game heeft op kinderen namelijk pas duidelijk door hoe hun gebruikers ermee omgaan. Denk bijvoorbeeld aan apps zoals Pokémon Go waarbij kinderen in fysiek in contact komen met gebruikers van allerlei leeftijden. Stel ook bij elke vernieuwde toepassing of update van de digitale dienst opnieuw de vraag of het belang van het kind voorop staat.

Relevante wet- en regelgeving

Kinderrechtenperspectief

De verplichting om rekening te houden met het belang van het kind bij alle activiteiten die een impact hebben op kinderen is te vinden in artikel 3, lid 1 van het VN Verdrag voor de rechten van het kind[4] en artikel 24, lid 2 van het Handvest van de grondrechten van de Europese Unie[5]. De implementatie van het belang van het kind vraagt om een concretisering van alle relevante kinderrechten bij het ontwerpen van een digitale dienst met een impact op kinderen. Relevante kinderrechten kunnen zijn: recht op vrijheid van informatie, recht op toegang tot (niet-schadelijke) media, recht op vrije menings- en gedachtevorming, recht op vrijheid van vereniging, recht op privacy en gegevensbescherming, recht op identiteitsvorming, spel en ontspanning, recht op bescherming tegen geweld (inclusief pesten en seksueel misbruik) en tegen economische exploitatie.

Bij het implementeren van relevante kinderrechten moet een evenwicht worden gevonden tussen de gegevensbeschermingsrechten van kinderen en hun andere rechten, waaronder hun rechten op ontwikkeling (artikel 6 IVRK), vrijheid van meningsuiting en informatie (artikel 13 IVRK) en vereniging (artikel 15 IVRK). Bovendien moet je rekening houden met de leeftijd van kinderen en hun zich ontwikkelende vermogens (artikel 5 IVRK). Sommige ontwerpkeuzes kunnen in het belang van een 16-jarige zijn maar niet in het belang van een 6-jarige. Bij jongere kinderen kan het gerechtvaardigd zijn om een grotere nadruk op hun beschermingsrechten te leggen, terwijl bij oudere kinderen de vrijheidsrechten belangrijker worden. Speciale aandacht moet er zijn voor het toegankelijk maken van digitale diensten voor kinderen met een fysieke beperking.

Kinderen vinden het zelf ook belangrijk dat aanbieders van digitale diensten zich in hun belang beter houden aan de rechten die kinderen hebben op basis van het VN Verdrag inzake de Rechten van het Kind 1989. Volgens het Kinderrechtencomité moeten overheden erop toezien dat aanbieders voorkomen dat de veiligheid en het welzijn van kinderen in het gedrang komen door het gebruik van digitale diensten. Aanbieders dienen gedegen onderzoek te doen naar de impact van hun producten en diensten op kinderen en hun onderliggende kind- impact-assessment bekend te maken aan het publiek.

[4] https://wetten.overheid.nl/BWBV0002508/
[5] https://wetten.overheid.nl/BWBV0002508/

Gegevensbeschermingsrecht

De Algemene Verordening Gegevensbescherming[6] (AVG) beoogt onder andere aan het “welzijn van natuurlijke personen” bij te dragen (overweging 2). Het belang van het kind komt echter het meest duidelijk tot uitdrukking in overweging 38 waarin staat dat kinderen specifieke bescherming genieten in het licht van hun fundamentele recht op gegevensbescherming: “Kinderen hebben met betrekking tot hun persoonsgegevens recht op specifieke bescherming, aangezien zij zich allicht minder bewust zijn van de betrokken risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking”.

Ook andere overwegingen in de AVG benadrukken de specifieke bescherming van kinderen: overweging 58 (transparantie van gegevensverwerkingen), overweging 65 (recht op vergetelheid), overweging 71 (geautomatiseerde besluitvorming en profilering), overweging 75 (verwerking van persoonsgegevens van kinderen is risicovol). Deze overwegingen zijn grotendeels nader uitgewerkt in de bepalingen van de AVG.

Los van het feit of kinderen expliciet worden genoemd in overwegingen of bepalingen van de AVG zal bij gegevensverwerkingen die een impact hebben op kinderen altijd rekening moeten worden gehouden met het belang van het kind. Het belang van het kind-beginsel als ook de AVG werkt door in alle navolgende beginselen in deze code.

Consumentenrecht

Kinderen worden niet altijd specifiek genoemd in het consumentenrecht, maar het belang van het kind-beginsel vereist in het geval van een (vermoedelijke) impact op kinderen dat het consumentenrecht zo wordt uitgelegd dat de ontwikkeling en het welzijn van kinderen in acht worden genomen.

Een uitzondering in het consumentenrecht waar wel nadrukkelijk rekening wordt gehouden met kinderen is bij de regulering van oneerlijke handelspraktijken (6:193a BW e.v.) (zie beginsel 8). Deze wetgeving beschermt de gemiddelde consument tegen commerciële praktijken die zijn economische gedrag verstoort door bijvoorbeeld misleiding of het uitoefenen van druk . De mate van invloed kan gemeten worden door een fictieve gemiddelde consument als uitgangspunt te nemen. Wanneer een handelspraktijk gericht is op een specifieke groep consumenten, zoals kinderen, wordt het effect van de praktijk beoordeeld vanuit het perspectief van het gemiddelde lid van de groep in kwestie (artikel 6:193a lid 2 BW). Kinderen kunnen in dat verband als bijzonder kwetsbaar worden beschouwd, gezien hun leeftijd en hun specifieke ontwikkeling (artikel 5 IVRK). Wanneer een app of game dus gericht is op kinderen,

[6] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679

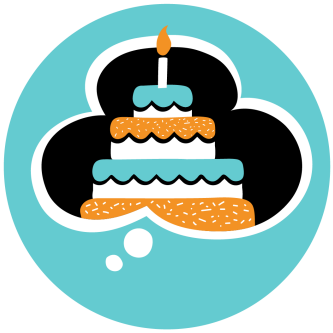
dan is het gemiddelde kind in de betreffende leeftijdsgroep de maatstaf voor de mate van bescherming.

Daarnaast moet de aanbieder rekening houden met het gemiddelde lid van de groep waarvan redelijkerwijs kan worden voorzien dat deze bijzonder vatbaar is voor de handelspraktijk of het onderliggende product. Om vast te stellen of een digitale dienst inderdaad rekening dient te houden met kinderen (van een bepaalde leeftijd) moet worden onderzocht in hoeverre de aanbieder redelijkerwijs had kunnen verwachten dat deze praktijk (met name) kwetsbare groepen zou aanspreken of dat deze groepen vanwege hun kwetsbaarheid, waaronder hun mentale of lichamelijke handicap, leeftijd of goedgelovigheid, in het bijzonder vatbaar zijn voor de praktijk.

Overige wetgeving

Schadelijke audiovisuele content - De Mediawet 2008 beschermt kinderen tegen de confrontatie met schadelijke audiovisuele content via bijvoorbeeld video on demand-diensten. Sinds 2020 moeten ook videoplatforms of social media die worden gebruikt voor het delen van video's kinderen beschermen tegen schadelijke content, het aanzetten tot haat en geweld en reclame (zie beginsel 9).

Beginsel 2: Betrek kinderen en hun verwachtingen bij het ontwerp



Toelichting

Kinderen moeten worden gehoord of op enige wijze kunnen participeren in de ontwikkeling van digitale diensten (die een impact op hen hebben) om invulling te kunnen geven aan het belang van het kind. Digitale diensten hebben die impact als het waarschijnlijk is dat ze feitelijk door kinderen worden gebruikt. Kinderen zijn creatief en hebben veel ideeën die van waarde kunnen zijn voor het ontwerp van een digitale dienst. Door kinderen te betrekken kan je beter aansluiten bij hun belevingswereld en inzicht krijgen in welke obstakels zij ervaren bij het gebruik van een app.

Om kinderen te laten participeren in het ontwerpproces is het belangrijk om te begrijpen welke mogelijkheden er zijn, afhankelijk van de leeftijd van kinderen. Hiervoor is speciale kennis als ook ervaring met het werken met kinderen nodig. Het participeren van kinderen gaat verder dan het uitvoeren van een gebruikerstest. Het omvat ook de vraag of een digitale dienst een bijdrage kan leveren aan de mentale, sociale en cognitieve ontwikkeling van het kind, ook op langere termijn. Daarbij moet je uiteraard ook rekening houden met maatschappelijke en culturele factoren. Vergeet ook niet om kinderen te betrekken die speciale wensen en behoeften hebben vanwege bijvoorbeeld een beperking of omdat ze in mindere mate toegang hebben tot digitale technologie. Voor daadwerkelijke participatie door kinderen in het ontwerpproces is het noodzakelijk dat zij goed worden geïnformeerd over het idee en de keuzes die er zijn.

De betrokkenheid van kinderen heeft ook een procedurele kant. Deze houdt in dat kinderen in de gelegenheid moeten zijn om kwalijke zaken die zich voordoen bij het gebruik van de app te kunnen rapporteren. Ook daarbij moet je rekening houden met de leeftijd van kinderen. Bijvoorbeeld: wat is aanstootgevend voor kinderen van welke leeftijd en op welke leeftijd zijn zij in staat hun belangen zelfstandig te behartigen?

Jongeren (van 14-16 jaar oud) die zijn betrokken tijdens het opstellen van deze code bevestigen dat zij het leuk vinden om mee te denken. Zij hebben op basis van eigen ervaring allerlei concrete ideeën over hoe een dienst eruit zou moeten zien. Zoals een van hen zei: “Ik vind het leuk dat ons een keer iets hierover gevraagd wordt.” Ter illustratie zullen in de code opmerkingen van hen worden vermeld.

Implementatie

Betrek kinderen vanaf het begin van de ontwerpfase. Zorg ervoor dat je zicht hebt op de doelgroep die je wilt aanspreken en gaat betrekken bij het ontwerp. Ga daarbij uit van het kind dat de meeste beperkingen ondervindt in de gekozen doelgroep. Probeer daarnaast verschillende personages te ontwerpen en stereotype representaties (zoals genderrollen) te vermijden, en geef kinderen de mogelijkheid verschillende karakters en rollen aan te nemen.

Maak gebruik van de Web Content Accessibility Guidelines (WCAG[7]) om de dienst toegankelijk te maken voor kinderen met een functiebeperking, zoals slechtziendheid, doofheid en gehoorverlies.

Er zijn veel voorbeelden om kinderen te betrekken bij het ontwerp en de ontwikkeling van diensten. Belangrijke adviezen van ontwerpers en ontwikkelaars tijdens het gezamenlijk ontwerp:

- Stel kinderen op hun gemak. Kinderen moeten zich veilig voelen en het idee hebben dat er naar hen geluisterd wordt. Dat kun je doen door tijdens de sessie nadruk te leggen op het goede in mensen en verhalen te vertellen in de eerste persoon over negatieve emoties of ervaringen. Richt je in je communicatie op de sterke punten en het potentieel van het kind.
- Kies je woorden zorgvuldig bij het uitleggen van een opdracht, gebruik geen vakjargon, zoals de taal van een ontwerper. Zoek aansluiting bij het vocabulaire en de leefwereld van een kind. Kinderen krijgen uitleg over digitale technologieën graag van mensen in hun directe omgeving, zoals een docent, directeur of een ouder.
- Begin concreet, bijvoorbeeld over de meest of laatst gebruikte apps of over schermtijd.
- Geef zo min mogelijk hints. De inzichten van kinderen zijn waardevoller wanneer je kinderen vrijuit laat spreken.
- Vraag kinderen eerst of hun ervaring goed, middelmatig of slecht is. Zo'n indeling van antwoorden helpt kinderen op gang bij het delen van hun ervaring. Aan de hand van deze classificatie vraag je een kind verder door.
- Test iedere fase met een verschillende groep kinderen (het betrekken van dezelfde groep kinderen kan leiden tot vals positieve uitkomsten).

De richtlijnen van UNICEF[8] en de recent uitgebrachte Britse Age Appropriate Design Code[9] met richtlijnen voor het communiceren met kinderen kunnen van pas komen.

[7] https://wcag.nl/
[8] https://sites.unicef.org/cwc/files/CwC_Final_Nov-2011.pdf
[9] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/

Het betrekken van kinderen geldt niet alleen tijdens de ontwerpfase voorafgaand aan het bouwen van een applicatie, maar is een iteratief proces (zoals ook benoemd onder beginsel 1). Ook tijdens de ontwikkeling van alle opvolgende updates en aanpassingen is het waardevol om kinderen actief te betrekken, waarbij je klachten en feedback uit gebruikerservaringen kunt meenemen. Het is dus aan te raden een feedback-mechanisme in te bouwen voor na de ontwerpfase van een dienst.

Wanneer je kinderen gaat betrekken bij je ontwerp, kun je bijvoorbeeld de Digiraad[10] en de kinderministers van Digitale Zaken raadplegen die al op een georganiseerde manier meedenken over het betrekken van kinderrechten bij het ontwerp van digitale diensten.

Relevante wet- en regelgeving

Kinderrechtenperspectief

Het recht van kinderen om te worden gehoord (artikel 12 IVRK) is een van de fundamentele beginselen van het IVRK. Het beginsel is onlosmakelijk verbonden met het belang van het kind (artikel 3 lid 1 IVRK) (zie beginsel 1). Om het belang van het kind te kunnen implementeren bij activiteiten die een impact hebben op kinderen is het noodzakelijk om te weten wat de verwachtingen, zorgen, wensen en behoeften van kinderen zijn. Om die te achterhalen moeten kinderen op enige wijze worden betrokken. Daarbij moet rekening worden gehouden met de ontwikkeling van kinderen (artikel 5 IVRK): vanaf de leeftijd dat ze in staat zijn om inzichten te hebben en te delen, moet dit recht worden gerespecteerd. Het recht van kinderen om gehoord te worden is verder ook verbonden met alle andere rechten van het kind in het IVRK. Denk aan het recht op ontwikkeling (artikel 6 IVRK), de vrijheid van meningsuiting en informatie (artikel 13 en 17 IVRK) en de vrijheid van vereniging (artikel 15 IVRK). Het recht om gehoord te worden draagt bij aan respect voor de menselijke waardigheid en een gezonde ontwikkeling van kinderen.

De Raad van Europa geeft in het Handboek over participatie van kinderen[11] aan dat het recht van kinderen om gehoord te worden inhoudt dat het recht van kinderen op veilig participeren betrekking heeft op digitale technologie. Meer in het bijzonder verwacht de Raad dat “belanghebbenden kinderen actief (...] betrekken bij het op zinvolle wijze meewerken aan het

[10] https://saferinternetcentre.nl/digiraad/
[11] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046c478

opstellen, uitvoeren en evalueren van … technologieën die erop gericht zijn de rechten van het kind in de digitale omgeving te eerbiedigen, te beschermen en na te leven”[12] [vertaling auteurs].

Ook het Kinderrechtencomité erkent dat de overheid moet zekerstellen dat “ontwerpers en aanbieders van digitale technologieën en diensten kinderen actief betrekken, passende waarborgen toepassen en bij de ontwikkeling van hun diensten terdege rekening houden met hun standpunten” (General Comment 25). Om van zich te kunnen laten horen, is het volgens de Raad van Europa ook belangrijk dat kinderen worden geïnformeerd “over mechanismen en diensten die passende steun bieden, en over procedures voor klachten, rechtsmiddelen of verhaal indien hun rechten worden geschonden. Deze informatie moet ook ter beschikking worden gesteld aan hun ouders of verzorgers, zodat zij de kinderen kunnen ondersteunen bij het uitoefenen van hun rechten”[13][vertaling auteurs].

Bij het betrekken van kinderen moet ook rekening worden gehouden met kinderen in achtergestelde of kwetsbare situaties, alsmede met kinderen die op enige wijze schade hebben ondervonden van het gebruik van digitale diensten.

Gegevensbeschermingsrecht

Kinderen kunnen ook worden betrokken bij de bescherming van hun persoonsgegevens volgens het gegevensbeschermingsrecht.

Bij een Privacy Impact Assessment (PIA) (artikel 35 AVG) (zie beginsel 5) kan aan kinderen en hun ouders de kans worden geboden voor inspraak in de wijze waarop hun gegevens worden gebruikt. Dat kan het vertrouwen in de digitale dienst ten goede komen. Ook helpt het om te begrijpen welke wensen, behoeften en zorgen zij hebben ten aanzien van de digitale dienst en in het bijzonder de manier waarop persoonsgegevens worden gebruikt.

Daarnaast is het ook van belang om inzicht te hebben in de privacyverwachtingen van kinderen als gerechtvaardigd belang in artikel 6(1)(f) AVG de wettelijke grondslag is voor het verwerken van hun persoonsgegevens (zie beginsel 3). Bij die wettelijke grondslag wordt een belangenafweging gemaakt waarbij je alleen een gerechtvaardigd belang hebt als je belang belangrijker is dan dat van de persoon van wie je gegevens verwerkt. Je kunt het belang van het kind alleen kennen als kinderen op enige wijze gehoord zijn (zie beginsel 1). Maar meer in het algemeen is het een vereiste onder deze bepaling dat je rekening houdt met de redelijke verwachtingen van de persoon van wie persoonsgegevens worden verwerkt.

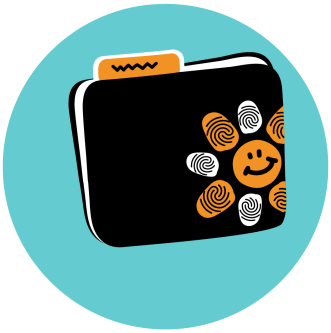
Verder is het van belang kinderen te betrekken bij het vinden van de voor hen meest geschikte en herkenbare manier om informatie te geven over de verwerking van persoonsgegevens

[12] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a
[13] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

(ziebeginsel 4). Dit moet namelijk gebeuren op een wijze die beknopt, transparant, begrijpelijk, in een gemakkelijk toegankelijke vorm en duidelijke en eenvoudige taal, waarbij in bijzonder aandacht wordt geschonken aan wat geschikt is voor kinderen (artikel 12 AVG). Adequaat geïnformeerd zijn is ook een voorwaarde voor de geldigheid van toestemming (artikel 7 (2) AVG) als wettelijke grondslag (artikel 6 (1) (a) AVG) voor de verwerking van persoonsgegevens (zie beginsel 3) en om te kunnen weten wat werkt bij kinderen zal je hen moeten betrekken.

Tot slot overweegt de AVG in het kader van gedragscodes (zie beginsel 10) dat “Bij de opstelling van een gedragscode, of bij wijziging of uitbreiding van een dergelijke code, moeten verenigingen en andere organen die categorieën van [aanbieders] vertegenwoordigen, o*verleg plegen met de belanghebbenden ter zake, waaronder waar mogelijk met [gebruikers], en rekening houden met bijdragen en standpunten naar aanleiding van dit overleg* (overweging 99). Verder heeft de European Data Protection Board in haar richtlijnen aangegeven dat een consultatie in sectoren met een hoog risico, waaronder die waar de gegevens van kinderen worden verwerkt, uitgebreider mag zijn.

Beginsel 3: Verwerk persoonsgegevens op een voor kinderen rechtmatige wijze



Toelichting

De persoonsgegevens van kinderen mag je alleen verwerken voor zover dat gebeurt in overeenstemming met de wet. Daarin staan, naast de algemene regels die gelden ongeacht de leeftijd van de gebruiker, ook regels die specifieke bescherming bieden aan kinderen. Dat geldt voor het gegevensbeschermingsrecht, maar ook voor het consumentenrecht. Die specifieke beschermingsregels zijn er omdat kinderen extra kwetsbaar kunnen zijn. Bijvoorbeeld omdat ze minder goed begrijpen wat er onder de motorkap van een app of game gebeurt met persoonsgegevens of omdat ze makkelijker kunnen worden beïnvloed bij het maken van keuzes in digitale diensten.

Om de bijzondere, op kinderen gerichte regels goed te kunnen toepassen is het noodzakelijk om te weten wie van de gebruikers jonger dan 18 is. En om die regels met het oog op een voor de - mogelijk verschillende - leeftijden van de minderjarige gebruikers geschikte manier te implementeren, is het belangrijk om te weten in welke leeftijdscategorie een kind valt. Jongere kinderen kunnen om een andere implementatie van de regels vragen dan oudere kinderen. In het eerste geval kan het bijvoorbeeld nodig zijn om de ouders te betrekken bij beslissingen of om bepaalde keuzes standaard af te schermen.

Implementatie

Hanteer het principe van dataminimalisatie: verwerk zo min mogelijk gegevens van het kind.

- Stel van elk separaat onderdeel van je dienst vast welke persoonsgegevens je nodig hebt om deze te kunnen aanbieden. Ga voor elk individueel onderdeel van jouw dienst afzonderlijk na welke persoonsgegevens je nodig hebt en voor hoe lang om het betreffende onderdeel te kunnen aanbieden. Vraag en verwerk in principe alleen de hoogst noodzakelijke gegevens. Geef het kind vervolgens waar mogelijk de keuze welke onderdelen ze van hun dienst willen gebruiken.
- Verzamel alleen de persoonsgegevens wanneer het kind actief en bewust dat betreffende onderdeel van jouw dienst gebruikt. Voor elk aanvullend doeleinde moet de keuze worden voorgelegd aan de gebruiker als de wettelijke grondslag toestemming is.

- De verzameling van persoonsgegevens om de online ervaring van jouw gebruikers buiten de kerndienst te personaliseren, verbeteren, optimaliseren (enzovoort) mag niet zomaar gecombineerd worden met de persoonsgegevens die je gebruikt voor de kerndienst.
- Sluit bepaalde diensten niet uit voor gebruikers die ervoor kiezen een deel van hun gegevens niet te delen, bijvoorbeeld door niet een persoonlijke profielfoto of exacte geolocatie te vereisen (tenzij noodzakelijk voor het functioneren van de dienst en dan wellicht beperkt tot een specifieke gebruikerssessie).
- Wees terughoudend met het gebruik van webformulieren. Vraag alleen gegevens die nodig zijn voor het gebruik van een dienst. Anonimiseer waar mogelijke deze data, of pas 'datafading' toe (anonimiseer data geleidelijk: anonimiseer data na verwerking alsnog). Een andere optie is pseudonimisering; er zijn meerdere opties om de persoonsgegevens van de gebruikers met technische en organisatorische maatregelen te beschermen.
- Moedig het gebruik van adblockers aan, zoals Junkbuster, CookieCooker of de Firefox Add-on: Self-Destructing Cookies, waardoor cookies direct worden verwijderd wanneer een webpagina is afgesloten. Zie voor meer ontwerpoplossingen gericht op o.a. minimale gegevensverwerking[14].

In lijn met het principe van dataminimalisatie is het raadzaam je af te vragen of het relevant is om de leeftijd-(categorie) van jouw gebruikers te verifiëren, zeker wanneer het gaat om diensten die geen risico's met zich mee brengen (blijkens bijvoorbeeld het kind impact assessment uit beginsel 1 of de privacy impact assessment uit beginsel 5). Wanneer het gebruik van de dienst wel risico's met zich meebrengt, houd dan waar nodig rekening met de mogelijke leeftijd van jouw gebruikers. Neem daarbij de jongste leeftijdscategorie als uitgangspunt (zie voor de categorieën ook de tabel in de bijlage). De tabel over leeftijdscategorieën die de Age Appropriate Design Code ook gebruikt[15] kunnen daarbij helpen.

Er zijn verschillende manieren om de leeftijdscategorie van de gebruiker te verifiëren. Met verifiëren bedoelen we dat je achterhaalt of een kind jonger is dan een bepaalde leeftijd (bijvoorbeeld 16 of 18) of in een bepaald leeftijdscategorie valt (bijvoorbeeld 12-15 jaar) zonder dat je precies hoeft te weten hoe oud het kind is. Voorbeelden van wijzen van leeftijdsverificatie zijn:

- Eigen opgave. Vraag de gebruiker of jonger is dan een bepaalde leeftijd dan wel zich in een bepaalde leeftijdsgroep bevindt, zonder daar bewijs van te overleggen. Deze vorm van leeftijdsverificatie past bij de verwerking van gegevens met een laag risico of kan

[14] https://privacypatterns.org
[15] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/

gebruikt worden in combinatie met een andere (bijvoorbeeld onderstaande) verificatietechniek. Houd er rekening mee dat deze vorm van leeftijdsverificatie waarschijnlijk niet adequaat is wanneer er persoonsgegevens van kinderen worden verwerkt.

- Technische maatregelen. Om valse leeftijdsopgave te ontmoedigen en/of op te sporen en het openen van accounts door minderjarigen onmogelijk te maken, zoals bij digitale diensten die schadelijk kunnen zijn voor kinderen (bijvoorbeeld gok- of pornosites), kunnen ook technische maatregelen worden genomen. Denk daarbij aan een neutrale presentatie van de vensters waarin gebruikers moet aangeven in welke leeftijdscategorie ze zitten (en daarmee niet aansporen tot het kiezen van andere leeftijdscategorieën), of die er bijvoorbeeld voor zorgen dat gebruikers niet direct een andere leeftijdscategorie kunnen opgeven wanneer blijkt dat ze met de eerder opgegeven leeftijdscategorie geen toegang krijgen tot de dienst. Waar het gaat om 18+ websites is het juist raadzaam om met dezelfde technische maatregelen het opgeven van een valse leeftijd juist ontmoedigen.
- Derde partijen. Je kunt de leeftijdscontrole ook uitbesteden aan een derde partij. Dit soort diensten werken met attributen ('Attribute-Based Credentials'): je vraagt om bevestiging van een bepaald gebruikersattribuut (in dit geval de leeftijdscategorie) en de dienst antwoordt hierop met 'ja' of 'nee'. Vanzelfsprekend moet deze dienst voldoen aan de eisen voor gegevensbescherming en je moet gebruikers duidelijke informatie verstrekken over het feit dat je gebruik maakt van deze dienst. Bij voorkeur gebeurt zo'n verificatie privacyvriendelijk op het apparaat van de gebruiker. De derde partij faciliteert dan enkel de leeftijdsverificatie maar verwerkt geen persoonsgegevens. Een voorbeeld van zo'n dienst is IRMA[16].
- Bevestiging via e-mail- of SMS-link. Vraag bijvoorbeeld de ouder de leeftijd van het kind te bevestigen door te klikken op een link die wordt verstrekt in een e-mailbericht of een SMS-bericht.

Zorg ervoor dat de ingewonnen gegevens niet gebruikt worden voor doeleinden anders dan leeftijdsverificatie en verwerk dus niet meer gegevens dan absoluut noodzakelijk is. Pas de overige beginselen in deze code uitsluitend toe op de laagst geïdentificeerde leeftijdscategorie (hoogste beschermingsniveau).

Neem een LIA (Legitimate Interests Assessment) af wanneer je gegevens wilt verzamelen op grond van het gerechtvaardigd belang'. Een LIA is een eenvoudigere vorm van risicobeoordeling (dan een PIA) die je ertoe aanzet het doel van verwerking vast te stellen en na

[16] https://privacybydesign.foundation/irma/

te denken over de gevolgen voor personen[17]. Een LIA kan een aanleiding zijn om een (diepgravender) PIA (zie beginsel 5) uit te voeren maar ga er vanuit dat een PIA sowieso nodig is als een dienst waarschijnlijk door kinderen wordt gebruikt.

Verstrek alleen gegevens aan derde partijen of aan andere afdelingen binnen jouw organisatie wanneer daarvoor een aantoonbaar dwingende reden is (zoals wet- en regelgeving), rekening houdend met de belangen van het kind. Commercieel hergebruik van persoonsgegevens is (waarschijnlijk) geen aantoonbaar dwingende reden. Gebruik hiervoor de PIA (beginsel 5) en onderzoek de problemen en de risico's die daaruit voortgekomen zijn. Zorg ervoor dat je een garantie hebt van de derde partij dat deze de persoonsgegevens niet zal inzetten op een manier die schadelijk is voor het welzijn van het kind.

Maak het voor kinderen even gemakkelijk om zich in te schrijven als uit te schrijven bij een digitale dienst. Zorg er dan ook voor dat persoonsgegevens die niet langer noodzakelijk zijn worden gewist.

Relevante wet- en regelgeving

Kinderrechtenperspectief

Het Kinderrechtencomité geeft aan dat het IVRK, met name artikel 16 over het recht op privacy, een recht van kinderen op gegevensbescherming bevat. Europese burgers, waaronder kinderen, hebben een fundamenteel recht op gegevensbescherming (artikel 8 (1) Handvest van de grondrechten van de Europese Unie (EU Handvest), artikel 16 (1) Verdrag betreffende de werking van de Europese Unie).

Het fundamentele recht op gegevensbescherming is in de Europese Unie uitgewerkt in de Algemene Verordening Gegevensbescherming (AVG): "De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht" (overweging 1 AVG) en de AVG "eerbiedigt alle grondrechten alsook de vrijheden en beginselen [...], met name de eerbiediging van het privéleven en het familie- en gezinsleven, woning en communicatie, de bescherming van persoonsgegevens, de vrijheid van gedachte, geweten en godsdienst, de vrijheid van meningsuiting en van informatie, de vrijheid van ondernemerschap, het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, en het recht op culturele,

[17] Voor een voorbeeld: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

godsdienstige en taalkundige verscheidenheid" (overweging 4 AVG). "Alle grondrechten" omvat ook de rechten van kinderen en in het bijzonder het belang van het kind (artikel 3 IVRK, artikel 24 EU Handvest) (zie beginsel 1) en het recht van kinderen om gehoord te worden (artikel 12 IVRK) (zie beginsel 2) .

De AVG onderkent nadrukkelijk dat het kinderrechtenperspectief van belang is: "[k]inderen hebben met betrekking tot hun persoonsgegevens recht op specifieke bescherming, aangezien zij zich allicht minder bewust zijn van de betrokken risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van persoonsgegevens" (overweging 38 AVG).

Gegevensbeschermingsrecht

De grondbeginselen van het gegevensbeschermingsrecht

Aanbieders van digitale diensten die persoonsgegevens verwerken moeten voldoen aan de regels van de AVG. Wanneer hun diensten een impact hebben op kinderen zijn er bijzondere aandachtspunten voor de bescherming van de persoonsgegevens van kinderen onder de AVG. Dat begint al bij de toepassing van de zeven grondbeginselen van het gegevensbeschermingsrecht. Dit zijn de beginselen van behoorlijkheid, transparantie, doelbinding, dataminimalisatie, juistheid, opslagbeperking, integriteit, vertrouwelijkheid en de verantwoordingsplicht (artikel 5 (1) (a) - (f) AVG). De grondbeginselen van gegevensbescherming in artikel 5 van de AVG zijn heel belangrijk omdat ze ten grondslag (vandaar ook grondbeginselen) liggen aan de rechten en plichten in de AVG. Bovendien kan het schenden van deze beginselen tot hogere boetes leiden, dan wanneer in strijd wordt gehandeld met sommige verplichtingen in de AVG (artikel 83 (5) (a) AVG).

Deze grondbeginselen kunnen hogere eisen stellen aan de gegevensverwerking bij kinderen, bijvoorbeeld omdat nadrukkelijk rekening moet worden gehouden met het belang van het kind. (zie beginsel 1) Zo is bij de toepassing van het behoorlijkheidsbeginsel relevant of er een onevenwichtige machtsrelatie bestaat tussen de aanbieder van een digitale dienst en de gebruiker. Bij kinderen kan vanwege hun kwetsbare positie eerder sprake zijn van onevenwichtigheid of van een grotere evenwichtigheid dan in het geval van volwassenen. Ook zal de leeftijd van kinderen een rol kunnen spelen bij de vraag naar de mate van onevenwichtigheid in de machtsrelatie tussen hen en de aanbieder. Verder kan bijvoorbeeld de verantwoordingsplicht - dat wil zeggen de verplichting om aan te tonen dat een bedrijf aan de AVG voldoet (artikel 5 (2) AVG) - een zwaardere invulling krijgen bij kinderen vanwege hun kwetsbare positie en bijzondere behoefte aan bescherming.

De uitwerking van het beginsel van rechtmatigheid van de verwerking van persoonsgegevens vraagt ook om speciale aandacht bij kinderen. Het beginsel vereist dat de verwerking rechtmatig is (artikel 5 (1) (a) AVG) en de verwerking van persoonsgegevens is in ieder geval

niet rechtmatig als deze niet is gebaseerd op een van de zes wettelijke grondslagen als genoemd in artikel 6 van de AVG: toestemming, overeenkomst, wettelijke verplichting, algemeen belang, vitale belangen van de betrokkene of gerechtvaardigde belangen van de verantwoordelijke (artikel 6 (1) (a)-(f) AVG).

Wettelijke grondslagen

Persoonsgegevens mogen alleen worden verwerkt als er een wettelijke grondslag is. De wettelijke grondslagen staan uitputtend vermeld in artikel 6 (1) (a)-(f) van de AVG. Om te kunnen bepalen wat de meeste geschikte grondslag is vanuit het oogpunt van behoorlijkheid zal je eerst moeten bepalen met welk specifieke doel de gegevens worden verwerkt. Ieder specifieke doel vraagt om een afzonderlijke wettelijke grondslag. Hieronder wordt aandacht besteedt aan drie van deze grondslagen: 'toestemming', 'noodzakelijk voor de uitvoering van een overeenkomst' en 'gerechtvaardigd belang'.

Toestemming (artikel 6(1)(a) AVG, artikel 7 AVG, artikel 8 AVG))

De verwerking van persoonsgegevens kan rechtmatig zijn als de gebruiker daarvoor toestemming heeft gegeven voor een of meer specifieke doeleinden. Geldige toestemming wordt door gebruikers gegeven met een duidelijke actieve handeling (schriftelijke/ mondelinge verklaring, ook met elektronische middelen), waaruit blijkt dat zij vrijelijk, specifiek, geïnformeerd en ondubbelzinnig de betreffende verwerking van persoonsgegevens aanvaarden (artikel 7 AVG). Bij digitale diensten die door kinderen worden gebruikt zal in het bijzonder moeten worden onderzocht of aan voorwaarden voor toestemming is voldaan. Is er bijvoorbeeld een voor kinderen geschikte manier gekozen om hen te informeren over de gegevensverwerking (geïnformeerde toestemming) (zie beginsel 4)? Is de toestemming wel vrijelijk gegeven gelet op het feit dat de machtsrelatie tussen kinderen en een aanbieder van digitale diensten mogelijk onevenwichtiger is (vrije toestemming)? Toestemming is niet vrijelijk gegeven als er geen daadwerkelijke keuze is. De reden kan contextueel zijn (bijvoorbeeld voor de burger of scholier verplichte gegevensverwerkingen door de overheid respectievelijk in het onderwijs) of er zijn economische overwegingen (zoals verdienmodellen gebaseerd op datagedreven marketing waarbij er met persoonsgegevens moet worden "betaald" om de digitale dienst te gebruiken (zie artikel 7 (4) AVG) (zie beginsel 8). Een daadwerkelijke keuze ontbreekt dus bijvoorbeeld als het gebruik van een dienst afhankelijk is van privacyvoorwaarden ten aanzien van verwerkingen die daarvoor niet strikt noodzakelijk zijn. In al dat soort gevallen - toestemming is geen vrije keuze - kan toestemming niet de wettelijke grondslag zijn, maar zal een andere geschikte grondslag moeten worden gevonden in artikel 6 AVG.

Specifieke toestemming betekent dat er moet worden ingestemd met de verwerking van een bepaald soort, specifieke activiteit. De toestemming die wordt gegeven moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel dienen. Als er meerdere doelen zijn voor de

verwerking, moet iemand ook afzonderlijk instemmen met ieder van deze doelen of er moet een andere wettelijke grondslag van toepassing zijn. Ook moet de toestemming ondubbelzinnig zijn, wat inhoudt dat hetgeen waarmee iemand instemt duidelijk moet zijn; de tekst waarmee de persoon instemt moet maar vatbaar zijn voor één uitleg. Deze voorwaarde houdt in dat bijvoorbeeld het gebruik van reeds aangekruiste vakjes of inactiviteit niet als toestemming mag gelden. Iemand die toestemming heeft gegeven voor een gegevensverwerking moet die toestemming ook net zo eenvoudig weer kunnen intrekken (artikel 7 (3) AVG). De aanbieder van digitale diensten moet kunnen aantonen dat de toestemming rechtsgeldig is gegeven door de gebruiker (verantwoordingsplicht, artikel 5 (2) AVG).

Wanneer toestemming de wettelijke grondslag is, kunnen kinderen van 16 jaar en ouder zelf toestemming geven (artikel 8 AVG jo. artikel 5 UAVG). Let echter op: andere Europese lidstaten kunnen andere leeftijden (15, 14 of 13 en ouder) hanteren en in de Verenigde Staten is de leeftijd vastgesteld op 13 jaar en ouder. De veiligste optie is om alleen kinderen van 16 jaar of ouder zelfstandig om toestemming te vragen omdat je dan altijd goed zit (mits aan de andere voorwaarden voor rechtmatige toestemming is voldaan). De verwerking van persoonsgegevens van een kind jonger dan 16 jaar is slechts rechtmatig indien de toestemming wordt verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. Dat zal vaak een van de ouders zijn, maar er kan ook een andere wettelijke vertegenwoordiger zijn. Let er op dat deze leeftijdsgrens in Nederland geldt; in andere landen van de Europese Unie kan er voor een andere leeftijdsgrens zijn gekozen.

Om deze regels te kunnen toepassen moet je weten wanneer je te maken hebt met iemand die jonger is dan 16 jaar. Er is dan ook een impliciete verplichting om dat vast te stellen. De regels daarvoor zijn streng want alleen als een digitale dienst wordt aangeboden aan klanten die ouder zijn dan 18 jaar en er geen bewijs van het tegendeel is, het is bijvoorbeeld niet zo dat kinderen deze door gebrekkige leeftijdsverificatie feitelijk toch gebruiken, dan mag worden aangenomen dat de digitale dienst niet wordt aangeboden aan kinderen. In dat geval hoef je dus ook niet te onderzoeken of kinderen ouder of jonger dan 16 jaar zijn. In het geval dat een kind jonger dan 16 jaar is, dan zal niet alleen ouderlijke toestemming moeten worden gevraagd maar zal ook moeten worden geverifieerd dat het inderdaad de ouder (of andere wettelijk vertegenwoordiger) is die toestemming verleend voor de gegevensverwerking.

Er moet een redelijke inspanning worden gedaan om te verifiëren met een middel dat voldoet aan de stand van de techniek. Bij het inbouwen van leeftijdsverificatie en verificatie van ouderlijke toestemming mogen niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is (beginsel van minimale gegevensverwerking of dataminimalisatie) (zie beginsel 6). Voor preventieve en adviesdiensten aan kinderen is geen ouderlijke toestemming vereist (overweging 38). Denk aan de Kindertelefoon waarmee kinderen vertrouwelijk kunnen chatten over problemen waarmee ze worstelen. Of het de kinderen of de ouders die toestemming mogen respectievelijk moeten geven, er moet altijd aan de eerder genoemde vereisten voor

toestemming zijn voldoen. Houd er verder rekening mee dat wanneer een kind 16 jaar wordt toestemming opnieuw kan worden gevraagd maar dit keer aan het kind zelf. Bovendien kunnen kinderen er belang bij hebben om toestemming in te trekken en gegevens te laten verwijderen als ze 16 worden en zelf mogen beslissen over de verwerking van hun persoonsgegevens. Deze mogelijkheden zullen dus op voor kinderen toegankelijke en begrijpelijke wijze moeten worden ingebouwd.

Anders dan wel wordt gedacht is toestemming niet noodzakelijk voor een rechtmatige gegevensverwerking als er een andere wettelijke grondslag is. Bij digitale diensten wordt vaak gebruik gemaakt van de wettelijke grondslagen van overeenkomst (artikel 6 (1) (b) AVG) en gerechtvaardigde belangen (artikel 6 (1) (f) AVG). Gelet op de strikte voorwaarden aan toestemming als wettelijke grondslag, die nog strenger zijn bij kinderen, is toestemming wellicht ook niet de meest wenselijke grondslag voor aanbieders van digitale diensten.

Noodzakelijk voor de uitvoering van de overeenkomst (artikel 6(1)(b) Avg)

Een gegevensverwerking is ook rechtmatig als deze *noodzakelijk* is voor de uitvoering van een overeenkomst met de gebruiker van de digitale dienst. Dit is een van de wettelijke grondslagen die vaak wordt gebruikt bij digitale diensten. De aanbieder van de digitale dienst moet kunnen aantonen dat er een overeenkomst is, dat deze overeenkomst rechtsgeldig is en dat de verwerking van persoonsgegevens ook *daadwerkelijk noodzakelijk* is voor de *uitvoering* van de overeenkomst (verantwoordingsplicht, artikel 5 (2) AVG).

Deze wettelijke grondslag heeft nog een complicatie ten aanzien van kinderen omdat kinderen op grond van het toepasselijke recht wel rechtsgeldig een overeenkomst moeten kunnen afsluiten. Of een verwerking noodzakelijk is hangt samen met het specifieke doel waarvoor de gegevens worden verwerkt en er zal mede in het licht van het belang van het kind (zie beginsel 1) rekening worden gehouden met het beginsel van minimale gegevensverwerking (zie beginsel 6) en het behoorlijkheidsbeginsel (artikel 5 (1) (a) en (c) AVG). Gegevensverwerkingen die bedoeld zijn voor bijvoorbeeld datagedreven en gerichte marketing of het verbeteren van een app of website vallen hier bijvoorbeeld niet onder. Ook het opstellen van gebruikers- en persoonlijkheidsprofielen of het monitoren van het gedrag van gebruikers om fraude te bestrijden kan niet gebeuren op basis van deze wettelijke grondslag.

Gerechtvaardigd belang (artikel 6(1)(f) Avg)

Een andere wettelijke grondslag die vaak wordt toegepast bij digitale diensten is die waarbij gegevens mogen worden verwerkt als dit noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de aanbieder van zo'n dienst of een derde (artikel 6(1)(f) AVG). Gerechtvaardigde belangen kunnen bijvoorbeeld zijn: fraudebestrijding, marketing, technische

beveiliging en het tegengaan van illegale activiteiten. Sommige gerechtvaardigde belangen kunnen zwaarwegender zijn dan andere.

Deze grondslag vraagt om een belangenafweging tussen de gerechtvaardigde belangen van bedrijven en de belangen en rechten van de gebruikers van de dienst, waaronder kinderen. In die belangenafweging moeten nadrukkelijk ook het belang van het kind (artikel 3 (1) IVRK) (zie beginsel 1) en de fundamentele rechten van kinderen in onder meer het IVRK worden meegewogen. In het bijzonder het recht op privacy en gegevensbescherming van kinderen moet worden meegenomen in de belangenafweging, maar andere fundamentele (kinder)rechten, waaronder het recht op vrijheid van informatie, het recht op toegang tot media en het recht op ontwikkeling, kunnen ook relevant zijn.

De toepassing van deze wettelijke grondslag bestaat uit drie stappen:

1. Vaststellen van de gerechtvaardigde belangen van de aanbieder van een digitale dienst en daarmee het doel van de verwerking;
2. Aantonen waarom het noodzakelijk is om persoonsgegevens te verwerken voor het specifieke doel dat is vastgesteld;
3. Afwegen van de noodzakelijke gerechtvaardigde belangen tegen de belangen en fundamentele rechten van de gebruiker van een digitale dienst.

Er moet rekening worden gehouden met de impact die de gegevensverwerking heeft op kinderen (zie beginsel 1) en welke verwachtingen kinderen redelijkerwijs hebben over de manier waarop hun persoonsgegevens worden gebruikt (zie beginsel 2). Wanneer marketing als een gerechtvaardigd belang wordt opgevoerd zal bijvoorbeeld in het bijzonder rekening moeten worden gehouden met de mogelijk schadelijk impact van marketing op kinderen. Bij datagedreven vormen van marketing, waaronder het opstellen van gebruikersprofielen, online direct marketing en online gedragsgestuurde marketing, wordt de wettelijke grondslag van toestemming (artikel 6 (1) (a) AVG) geschikter geacht. De gebruiker van een digitale dienst heeft in het geval van direct marketing het recht om bezwaar te maken (artikel 21 AVG)en zal daarover op een toegankelijke en behoorlijke manier moeten worden geïnformeerd waarbij rekening moet worden gehouden met wat een kinderen op verschillende leeftijden kunnen begrijpen. Dit geldt slechts in het geval dat toepassen van deze wettelijke grondslag voor direct marketing bij kinderen rechtmatig is, omdat het niet indruist tegen hun belangen en rechten.

Ook moet de aanbieder van de digitale dienst zorgen voor adequate waarborgen om onnodige en voor kinderen nadelige gevolgen te beperken. Daarbij kan worden gedacht aan privacy by design-oplossingen (zie beginsel 6) en extra aandacht voor transparantie (zie beginsel 4). Aanbieders moeten kunnen aantonen dat zij de belangen van kinderen als een eerste overweging hebben meegenomen in de belangenafweging en rekenschap hebben gegeven van de bescherming van de rechten van kinderen die worden beïnvloed door het gebruik van de dienst, in het bijzonder de vanuit het gerechtvaardigd belang van de aanbieder noodzakelijke

gegevensverwerking (verantwoordingsplicht, artikel 5 (2) AVG). In de privacyvoorwaarden moeten gerechtvaardigde belangen worden toegelicht (zie beginsel 4). Ook wanneer een dienst niet specifiek bedoeld is voor kinderen, zal de aanbieder moeten onderzoeken of het waarschijnlijk is dat kinderen deze gebruiken.

Bijzondere persoonsgegevens

Als er ook zogeheten bijzondere persoonsgegevens worden verwerkt dan zal naast de wettelijke grondslag van artikel 6 van de AVG ook moeten worden voldaan aan de speciale en strengere regels in artikel 9 AVG alsmede artikel 22 jo. art 23 UAVG. Het gaat dan om gegevens die onder andere iemands seksualiteit, etniciteit of gezondheid betreffen. Daarnaast vallen er ook biometrische gegevens onder. Het verwerken van deze persoonsgegevens is niet toegestaan, tenzij er sprake is van één van de tien wettelijke verwerkingsgronden (artikel 9 (2) AVG).

Een van die verwerkingsgronden is uitdrukkelijke toestemming. Uitdrukkelijk ziet op de manier waarop de toestemming tot uitdrukking wordt gebracht. Een uitdrukkelijke manier van toestemmen is het ondertekenen van een schriftelijke verklaring en dit kan ook door middel van een elektronisch formulier of een e-mailbericht. De toestemming moet uitdrukkelijk zijn om te voorkomen dat er in de toekomst twijfel en/of gebrek aan bewijs is over het bestaan van toestemming voor dit soort gegevensverwerkingen. Uitdrukkelijke toestemming is vanwege het expliciete karakter dus strenger dan de toestemming van artikel 6(1)(a) AVG. Verder gelden voor deze vorm van toestemming ook de eerder al behandeld voorwaarden (artikel 7 AVG) voor toestemming waarbij er speciale regels zijn in het geval van kinderen onder de 16 jaar (artikel 8 AVG).

Beginsel 4: Zorg voor transparantie op een voor kinderen begrijpelijke en toegankelijke manier

Toelichting

Wettelijke verplichtingen in het gegevensbeschermingsrecht en het consumentenrecht bepalen dat een digitale aanbieder op verschillende wijzen transparant moet zijn voor gebruikers. Niet in de laatste plaats om het vertrouwen in een digitale dienst te waarborgen. In het gegevensbeschermingsrecht is transparantie zelfs een grondbeginsel en dus van groot belang. Als digitale aanbieder moet je duidelijk aangeven voor welk (rechtmatig) doel je welke persoonsgegevens gebruikt en met wie je ze eventueel deelt. Ook moet je voor ieder doel aangeven op basis van welke grondslag er wordt verwerkt en je gebruikers informeren over hun rechten.

Bij kinderen is er de extra verplichting om al die informatie te geven op een manier die voor kinderen herkenbaar, toegankelijk en begrijpelijk is. Omdat kinderen gezien worden als een kwetsbare groep in het gegevensbeschermingsrecht, heb je als aanbieder van een digitale dienst een extra verantwoordelijkheid om te zorgen dat je dit juist ook voor hen goed doet. Het is dan belangrijk om rekening te houden met de leeftijd van kinderen.

Het consumentenrecht vereist transparantie over alle aspecten van een transactie. Dat betekent bijvoorbeeld dat de aanbieder van een digitale dienst duidelijk moet zijn over de kosten in apps of games voor bijvoorbeeld extra functionaliteiten, levens of virtuele goederen (denk aan skins) die worden gekocht. Voor kinderen moet het ook duidelijk zijn dat er met echt geld wordt betaald voor deze aankopen. Dat is met name relevant wanneer een game een eigen betaalmiddel heeft (bijvoorbeeld V-Bucks in Fortnite). Dan is de link tussen echt geld en de aankoop namelijk lastiger te leggen, zeker ook voor kinderen. Ook binnen het consumentenrecht hebben aanbieders soms een grotere zorgplicht bij kinderen, omdat ze worden gezien als extra kwetsbare consumenten.

Transparantie is een voortdurende verantwoordelijkheid van aanbieders die niet alleen bij het aanmelden bij een digitale dienst, maar ook tijdens het gebruik ervan gegarandeerd moet blijven. Zelfs wanneer ouders op enige wijze betrokken zijn (bijvoorbeeld omdat ze toestemming moeten geven voor de gegevensverwerking), zijn aanbieders toch verantwoordelijk voor het bieden van transparantie gericht op kinderen en moeten zij ervoor zorgen dat kinderen begrijpen wat er met hun gegevens gebeurt en welke impact dat heeft. Dat is overigens niet altijd eenvoudig uit te leggen. Het is wellicht gemakkelijker om iemand bewust te maken van sociale privacyrisico's, bijvoorbeeld in de omgang met ouders of leeftijdsgenoten,

dan van de impact van het verwerken van persoonsgegevens door aanbieders van digitale diensten die meestal niet direct zichtbaar is.

Jongeren zien wel degelijk de risico's in van gegevensverwerking, zoals bleek uit een opmerking in een van de sessies die we organiseerden voor het opstellen van deze code: "**Een app is schadelijk als ze mijn privégegevens opslaan en niet verwijderen als ik het account niet meer heb of als ze het doorgeven aan andere mensen**". Tegelijkertijd leest vrijwel niemand de privacyvoorwaarden; deze vonden jongeren **een "te lang verhaal vol met technische taal**" en "**vaak lastig te begrijpen**". Ze zouden op een meer toegankelijke manier gepresenteerd moeten worden.

Implementatie

Laat informatie over privacy duidelijk zichtbaar zijn voor de (minderjarige) gebruiker.

- Voeg een voor kinderen begrijpelijk privacy-dashboard toe, zodat je in een oogopslag kunt zien wat er is afgesproken.
- Zorg ervoor dat de voorwaarden beknopt zijn, duidelijk in het oog vallen en in heldere taal geformuleerd zijn.
- Dwing zoveel mogelijk af dat de voorwaarden volledig gelezen worden, door bijvoorbeeld de gebruiker met elk onderdeel apart akkoord te laten gaan.
- Om het voor gebruikers makkelijker te maken de privacy settings te volgen is het aan te raden gebruik te maken van visuele elementen die het niveau van privacy bepalen. Maak bijvoorbeeld gebruik van (drop-down) lijsten om de verschillende niveaus van privacy aan te geven.
- Maak gebruik van de 'just-in-time'-notice. Op het moment dat de applicatie gebruik gaat maken van de persoonsgegevens moet de gebruiker duidelijk gemaakt worden wat er met de persoonsgegevens gebeurt. Voordat dit is aangegeven mogen de persoonsgegevens nog niet gebruikt worden. Al naar gelang het risico moet het kind ook aangespoord worden een ouder te raadplegen voordat het nieuwe gebruik van gegevens wordt geactiveerd. Overweeg in alle fasen van het gebruikerstraject of een dergelijke just-in-time-notice passend zou zijn.
- Voorkom beïnvloedingstechnieken ('nudging'). Gebruik bijvoorbeeld geen visueel misleidende informatie door de knoppen om te kiezen voor meer gegevensverwerking duidelijker weer te geven dan die voor gegevensminimalisatie.
- Wees transparant over het doorvoeren van patches en updates, en eventuele implicaties hiervan op privacy.

- Metadata die niet direct zichtbaar zijn voor de gebruiker (en niet begrijpelijk voor het kind) moeten verwijderd worden. (Zie Privacy Patterns[18] van Jaap Henk Hoepman)
- Een praktische tool voor het inzichtelijk maken van de verzameling, verwerking en het delen van data is Privacy Label[19].

Houd bij het verschaffen van deze informatie rekening met de leeftijd van het kind.

- Kies voor kindvriendelijke bewoordingen. Denk aan het gebruik van diagrammen, cartoons, afbeeldingen, video- en audiocontent, spelelementen en interactieve content die de aandacht van kinderen trekken, anders dan schriftelijke communicatie. Test deze aanpak bij kinderen en vraag hen om input.
- Als sommige algemene voorwaarden uitsluitend in juridische bewoordingen geformuleerd kunnen worden, overweeg dan een kindvriendelijke toelichting ernaast te zetten.
- Maak meerdere versies van deze informatie, rekening houdend met de leeftijd van het kind. Maak daarbij gebruik van de tips in beginsel 3 (passende informatie over privacy voor iedere leeftijdscategorie) en zoals hieronder omschreven.

Wij raden aan om bij het informeren van kinderen rekening te houden met hun ontwikkelingsfase volgens de door de Britse Age Appropriate Design Code voorgestelde indeling (zie ook de bijlage voor een uitgebreide toelichting per leeftijdscategorie):

- 0 - 5: ongeletterdheid en ontluikende geletterdheid (gebruik eenvoudige taal, herhaling, leg uit aan de hand van ritme en zang met dieren en mensen, gebruik rijmpjes en raadsels)
- 6 - 9: middenbouw basisschool (gebruik verhalen over vriendschap, het creëren van vaardigheden, dagelijkse gebeurtenissen die gaan over iemands waarden en kritisch denkvermogen)
- 10-12: overgangsjaren (gebruik rolmodellen, vertel verhalen over de invloed van familie, vrienden en media op het kind, stimuleer kinderen in hun behoefte om op deze leeftijd om te experimenteren en onafhankelijke keuzes te durven maken)
- 13-15: vroege tienerjaren (gebruik rolmodellen, vertel verhalen over de invloed van familie, vrienden en media op de jongere, stimuleer kinderen in hun behoefte om op deze leeftijd om te experimenteren en onafhankelijke keuzes te durven maken)
- 16-17: overgangsfase naar volwassenheid (gebruik rolmodellen, vertel verhalen over de invloed van familie, vrienden en media op de jongere, stimuleer kinderen in hun behoefte om op deze leeftijd om te experimenteren en onafhankelijke keuzes te durven maken)

[18] https://privacypatterns.org/patterns/
[19] https://privacylabel.org/

Bovenstaande indeling is gemaakt op basis van de zich ontwikkelende vermogens, vaardigheden en interesses van het kind. Wanneer de kans bestaat dat kinderen die jonger zijn dan de beoogde leeftijdscategorie gebruik zullen maken van jouw dienst, houdt dan rekening met die leeftijdscategorie in je ontwerp.

Geef de mogelijkheid aan kinderen om hun rechten uit te oefenen op het gebied van gegevensbescherming; geef dit een prominente plek in het ontwerp.

- Maak deze hulpmiddelen eenvoudig in gebruik en leeftijdsrelevant (denk aan een chatbot, waarbij gesprekken na afloop automatisch worden gewist). Maak daarbij gebruik van de tips in beginsel 2 (over aantrekkelijke, heldere uitleg aan kinderen), de tips hierboven en uit de bijlage.
- Stem hulpmiddelen af op rechten die ze ondersteunen, zoals:
    - een 'download al mijn gegevens'-hulpmiddel ter ondersteuning van het recht op inzage en het recht op dataportabiliteit;
    - een 'verwijder al mijn gegevens'- of 'selecteer gegevens om te verwijderen'-hulpmiddel ter ondersteuning van het recht op vergetelheid;
    - een 'stop met het gebruik van mijn gegevens'-hulpmiddel ter ondersteuning van het recht op beperking van de verwerking en het recht om bezwaar te maken tegen verwerking; en
    - een 'wijzigen'-hulpmiddel ter ondersteuning van het recht op rectificatie.
- Maak duidelijk hoe kinderen een klacht kunnen indienen over de verwerking van hun persoonsgegevens (ook bij de toezichthouder[20]) of onrechtmatig/compromitterend gebruik van hun persoonlijke informatie eenvoudig kunnen rapporteren. Zorg voor mechanismen waarin de voortgang van een klacht/verzoek tot verwijdering van (onrechtmatige/compromitterende) persoonlijke informatie kan worden gevolgd en creëer de optie dat kinderen kunnen aangeven dat hun klacht of verzoek urgent is. Neem alle informatie in aanmerking die zij verstrekken. Zorg voor procedures om snel actie te kunnen ondernemen als verstrekte informatie wijst op een acuut risico op de bescherming van persoonsgegevens.
- Maak bij speelgoed gebruik van een herkenbaar symbool (of knop) die kinderen gemakkelijk kunnen vinden wanneer ze hun rechten willen uitoefenen. Vermeld in het geval een verbonden speelgoed apparaat het symbool op de verpakking.
- Maak eventuele gedragscodes waaraan je gebonden bent en de daarin neergelegde richtlijnen op een begrijpelijke manier eenvoudig toegankelijk voor kinderen (zie beginsel 10).

[20] https://autoriteitpersoonsgegevens.nl/nl/over-privacy/jouw-privacy-voor-jongeren

Relevante wet- en regelgeving

Kinderrechtenperspectief

Transparantie is in het belang van het kind (artikel 3 (1) IVRK) (zie beginsel 1), omdat met het kunnen en leren begrijpen van wat er in digitale diensten gebeurt je weet wat de impact op jou en je omgeving kan zijn. Op die manier kun je enige mate van controle uitoefenen door het maken van keuzes bij het gebruik van digitale diensten en het uitoefenen van je rechten. Transparantie is van belang voor onder meer het recht om gehoord te worden (artikel 12), de vrijheid van informatie en meningsuiting (artikel 13), het recht op vrijheid van gedachtevorming (artikel 14) en het recht op toegang tot de media en op bescherming tegen schadelijke content (artikel 17 IVRK).

Transparantie gaat over het geïnformeerd worden over de kansen en mogelijkheden van digitale diensten, zodat deze kunnen bijdragen aan het welzijn van kinderen. Kinderen moeten echter ook worden geïnformeerd over de mogelijke risico's en beperkingen van digitale diensten. Die beperkingen kunnen bijvoorbeeld gericht zijn op het beschermen van kinderen tegen schadelijke content (artikel 14 (4) IVRK). Bij het informeren van kinderen moet rekening worden gehouden met de zich ontwikkelende vermogens van kinderen (artikel 5 IVRK) en het feit dat iets wat oudere kinderen begrijpen mogelijk nog niet te bevatten is voor jonge kinderen. Het bieden van transparantie ten aanzien van de digitale dienstverlening moet daarom ook gericht zijn op het informeren van ouder, verzorgers en anderen die kinderen ondersteunen.

Gegevensbeschermingsrecht

Het beginsel van transparantie is een van de grondbeginselen van de AVG (artikel 5 (1)(a) AVG). Het beginsel "betreft met name het informeren van de betrokkenen over de identiteit van de [aanbieder] en de doeleinden van de verwerking, alsook verdere informatie om te zorgen voor behoorlijke en transparante verwerking met betrekking tot de [gebruiker] in kwestie en hun recht om bevestiging en mededeling te krijgen van hun persoonsgegevens die worden verwerkt. [Gebruikers] 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" (overweging 39 AVG). Het transparantiebeginsel is uitgewerkt in afdeling 1 en 2 van hoofdstuk III van de AVG en omvat bepalingen over het recht op informatie (hoe en wanneer welke informatie over de gegevensverwerking moet worden verstrekt) (artikel 12-14 AVG) en over het recht op inzage van gebruikers (artikel 15 AVG).

Over de wijze van verstrekken van informatie (het hoe) zijn er de volgende aandachtspunten: "[o]vereenkomstig het transparantiebeginsel moet informatie die bestemd is voor het publiek

of voor de betrokkene beknopt, eenvoudig toegankelijk en begrijpelijk zijn en moet duidelijke en eenvoudige taal en, in voorkomend geval, aanvullende visualisatie worden gebruikt. Die informatie kan elektronisch worden verstrekt, bijvoorbeeld wanneer die tot het publiek is gericht, via een website. Dit geldt in het bijzonder voor situaties, waarin het vanwege zowel het grote aantal actoren als de technologische complexiteit van de praktijk voor een betrokkene moeilijk is te weten en te begrijpen of, door wie en met welk doel zijn persoonsgegevens worden verzameld, zoals bij online advertenties" (overweging 58 AVG).

Vooral relevant voor deze code is de volgende overweging: "aangezien kinderen specifieke bescherming verdienen, dient de informatie en communicatie, wanneer de verwerking specifiek tot een kind is gericht, in een zodanig duidelijke en eenvoudige taal te worden gesteld dat het kind deze makkelijk kan begrijpen" (overweging 58 AVG; artikel 12 AVG). Het is van belang om dit samen te lezen met de suggesties voor de wijze van presenteren van informatie, aangezien sommige kinderen wellicht een voorkeur hebben voor tekst maar veel kinderen vermoedelijk juist voor meer visuele informatie (video's, games, comics, icons enzovoorts). Ook moet rekening worden gehouden met de zich ontwikkelende vermogens van kinderen (artikel 5 IVRK) en zal de informatie dus geschikt moeten zijn voor kinderen van verschillende leeftijden. Daarbij moet er aandacht zijn voor woord-, taalgebruik en stijl om ervoor te zorgen dat kinderen zich ook daadwerkelijk aangesproken voelen (zie beginsel 2).

Consumentenrecht

Het beginsel van transparantie is ook relevant in het consumentenrecht. Je kunt alleen een geïnformeerd besluit nemen over een transactie (bijvoorbeeld een in-app aankoop) als je precies weet wat de kosten en functionaliteiten zijn (zie bijvoorbeeld artikel 6:230m BW). Het belang van het kind (zie beginsel 1) kan betekenen dat je de informatie op een voor kinderen begrijpelijke en herkenbaar manier presenteert als het waarschijnlijk is dat een transactiemogelijkheid ook door kinderen wordt gebruikt. Houd er overigens wel rekening mee dat kinderen alleen met toestemming van hun ouders rechtsgeldig een overeenkomst kunnen afsluiten (artikel 1:234 BW).

Wanneer je niet transparant bent over de specifieke kenmerken of voorwaarden van een transactie, kan dat een oneerlijke handelspraktijk opleveren (artikel 6:193b BW). Een handelspraktijk is oneerlijk als de gebruiker wordt misleid, bijvoorbeeld door het geven van feitelijk onjuiste informatie (artikel 6:193c BW) (zie beginsel 8). Ook is het misleidend om informatie die essentieel is om een geïnformeerd besluit te nemen over een transactie, niet te vermelden (artikel 6:193d BW). Daarbij wordt specifiek rekening gehouden met hetgeen in het bijzonder kwetsbare consumenten, waaronder kinderen, mochten begrijpen, wanneer een digitale dienst (mede) voor hen ontwikkeld is.

Beginsel 5: Voer een op kinderrechten gebaseerde privacy impact assessment uit

Toelichting

Bij een gegevensverwerking die een potentieel hoog risico vormt, moet je eerst een privacy impact assessment (PIA) uitvoeren. Van een hoog risico kan bijvoorbeeld sprake zijn als gebruikers worden geprofileerd (zie beginsel 7) of hun gedrag systematisch wordt gevolgd.

Bij kinderen loop je eigenlijk altijd een hoog risico, aangezien de kwetsbaarheid van de degene wiens gegevens je verwerkt een criterium is op basis waarvan verwerkingen als risicovol kunnen worden aangemerkt. Dat is zo, omdat de machtsrelatie tussen aanbieder en gebruiker (nog) onevenwichtiger is als er factoren zijn die de gebruiker kwetsbaar maken. Kwetsbare gebruikers, waaronder kinderen, kunnen mogelijk minder goed bewust en weloverwogen besluiten om in te stemmen dan wel bezwaar te maken tegen gegevensverwerkingen. Het is daarom raadzaam om bij digitale diensten die waarschijnlijk door kinderen worden gebruikt standaard een PIA uit te (laten) voeren.

Het doel van zo'n PIA is om in kaart te brengen welke gegevens op welke wijze worden verwerkt en met welke risico's (voor de rechten en vrijheden van de persoon om wiens het gegevens het gaat) dat mogelijk gepaard gaat. Bij kinderen ligt het voor de hand dat in die beoordeling ook hun specifieke fundamentele rechten worden betrokken. Vervolgens moet je vaststellen met welke maatregelen je de risico's effectief kunt ondervangen. Bij maatregelen met een impact op kinderen, hun rechten en persoonsgegevens zal je rekening moeten houden met hun specifieke belangen (zie beginsel 1).

Implementatie

Gebruik de richtlijnen van de Autoriteit Persoonsgegevens[21] en de Europese toezichthouder[22] voor het uitvoeren van een verplichte PIA.

[21] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia
[22] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf

Een op kinderrechten gebaseerde privacy impact assessment bevat in ieder geval de volgende zeven stappen (onderstaand voorbeeld is afkomstig uit de Britse Age Appropriate Design Code[23]):

- stap 1. Bepaal het moment voor uitvoering.
    - Rond de PIA af voor ingebruikname van de dienst
    - Voer een nieuwe PIA is verplicht als je belangrijke wijzigingen aanbrengt in de verwerkingsactiviteiten.
    - Voer ook een nieuwe PIA uit in het geval van externe aanleiding zoals een nieuw beveiligingslek, of nieuwe risico's voor kinderen.
- stap 2. Beschrijf de verwerking (aard, toepassingsgebied, context, doel van de verwerking). Adresseer daarbij de volgende vragen:
    - of je jouw dienst ontwerpt voor kinderen, en zo niet, of kinderen desondanks waarschijnlijk jouw dienst zullen gebruiken;
    - de leeftijdscategorieën van die kinderen;
    - jouw eventuele plannen voor ouderlijk toezicht;
    - jouw eventuele plannen voor het vaststellen van de leeftijd van jouw individuele gebruikers;
    - de beoogde voordelen voor kinderen;
    - de commerciële belangen (van jezelf of derde partijen) die je in aanmerking hebt genomen;
    - eventuele profilering of automatische besluitvorming;
    - geolocatie-elementen; het gebruik van beïnvloedingstechnieken ('nudging');
    - verwerking van speciale categorieën gegevens; verwerking van afgeleide gegevens;
    - actuele kwesties van openbaar belang ten aanzien van online risico's voor kinderen;
    - relevante normen en gedragsregels in de branche;
    - relevante richtlijnen of onderzoek met betrekking tot de ontwikkelingsbehoeften, het welzijn of de capaciteit van kinderen in de relevante leeftijdscategorie.
- stap 3. Raadpleeg kinderen en ouders (zie beginsel 2)
    - Overweeg aanvullend of je onafhankelijk advies moet inwinnen bij deskundigen op het gebied van kinderrechten en ontwikkelingsbehoeften.
- stap 4. Beoordeel noodzaak, proportionaliteit en conformiteit van het verzamelen van persoonsgegevens. Behandel daarin ook de volgende punten
    - de wettelijke verwerkingsgrondslag;

[23] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/2-data-protection-impact-assessments/

    - de voorwaarde voor de verwerking van gegevens uit speciale categorieën;
    - maatregelen om nauwkeurigheid te waarborgen, vertekening te vermijden en het gebruik van AI uit te leggen; en
    - specifieke details van de technologische beveiligingsmaatregelen (bijv. hashing en versleutelingsstandaarden).
- stap 5. Identificeer en beoordeel de risico's bij kinderen. Onderzoek in het bijzonder of de verwerking van persoonsgegevens de volgende risico's kan veroorzaken, mogelijk kan maken, aan kan bijdragen, of in andere gevallen juist kan helpen vermijden:
    - lichamelijk letsel;
    - stereotypering of discriminatie van kinderen of anderen;
    - online-grooming of andere seksuele uitbuiting;
    - sociale angst, gebrek aan eigenwaarde, pesten of sociale druk;
    - toegang tot schadelijke of ongepaste inhoud;
    - misleidende informatie of ongepaste informatiebeperking; aanzetten tot het nemen van buitensporige risico's of ongezond gedrag;
    - ondermijning van ouderlijk gezag of verantwoordelijkheid;
    - verlies van autonomie of rechten (inclusief controle over gegevens, risico van verstrekking van persoonsgegevens van het kind door anderen dan het kind, en privacy ten opzichte van derden, waaronder ook ouders);
    - verslaving of aandachtsstoornissen;
    - overmatig schermgebruik;
    - onderbroken of onvoldoende slaap;
    - economische uitbuiting of onbillijke commerciële druk; of
    - elk ander aanmerkelijk nadeel op economisch, sociaal of ontwikkelingsvlak.
- stap 6. Bepaal maatregelen om risico's te beperken. Onderzoek of je vastgestelde risico's in het ontwerp kunt beperken of vermijden of dat je een aanvullende bescherming moet inbouwen.
- stap 7. Registreer de conclusie. Wanneer je beschikt over een gegevens functionaris, moet je de uitkomst en eventuele maatregelen van de PIA registreren. Het is aan te bevelen de uitkomsten te publiceren.

Overigens is een PIA niet een eenmalige exercitie, maar zal je voortdurend moeten beoordelen wat de impact van de digitale dienst is op de rechten en vrijheden van gebruikers. De doorontwikkeling en het gebruik van een digitale dienst kan de impact van de dienst doen veranderen en vraagt mogelijk om aanpassing van de waarborgen.

Relevante wet- en regelgeving

Kinderrechtenperspectief

Een op kinderrechten gebaseerde privacy impact assessment is eigenlijk een bijzondere vorm van de kind-impact-assessment die het belang van het kind-beginsel vergt van digitale dienstaanbieders (zie beginsel 1). De PIA is bedoeld om op een zorgvuldige wijze - lees: met effectieve waarborgen omklede - invulling te geven aan het recht op gegevensbescherming en privacy van kinderen (artikel 16 IVRK, artikel 8 EVRM, artikel 7 en 8 EU Handvest). Die waarborgen mogen echter geen onterechte beperking van andere kinderrechten, zoals hun recht op vrijheid van informatie en meningsuiting (artikel 13 IVRK) en op vrijheid van vereniging (artikel 15 IVRK), dan wel een inbreuk op andere rechten, waaronder hun recht op bescherming tegen discriminatie (artikel 2 IVRK), opleveren. De op kinderrechten gebaseerde PIA wordt dus uitgevoerd in samenhang met de in beginsel 1 besproken kind-impact-assessment wanneer een digitale dienst waarschijnlijk door kinderen wordt gebruikt.

Gegevensbeschermingsrecht

Als aanbieder van een digitale dienst moet je in bepaalde gevallen een privacy impact assessment of PIA (ook wel gegevensbeschermingseffectbeoordeling) uitvoeren (artikel 35 AVG). Dat houdt in dat er een beoordeling moet worden gemaakt van de impact van gegevensverwerkingen met een mogelijk hoog risico voor (de inperking van) de fundamentele rechten en vrijheden van de gebruiker van de dienst. Het gaat dus ook om andere rechten dan het recht op gegevensbescherming en bij kinderen meer specifiek hun bijzondere rechten. Een PIA moet worden gedaan als er sprake is van het gebruik van nieuwe technologieën, het opstellen van profielen van gebruikers en het voortdurend en systematisch online volgen van hun gedrag. Ga er vanuit dat in het geval van kinderen een PIA verplicht is.

Kinderen worden niet genoemd, maar het verwerken van gegevens van personen die als kwetsbaar worden aangemerkt, vormt een hoog risico vanwege de mogelijk extra onevenwichtige machtsrelatie. Kinderen vallen in de categorie kwetsbare personen (overweging 38 AVG) en het is dan ook raadzaam - en waarschijnlijk ook verplicht - om een PIA te doen wanneer kinderen de digitale dienst kunnen gebruiken. In ieder geval vraagt het belang van het kind om een impact assessment en moet met dat beginsel en andere kinderrechten rekening worden gehouden wanneer een digitale dienst waarschijnlijk een impact heeft op kinderen (zie beginsel 1). Ook de verwachtingen van kinderen en ouders als belanghebbende partijen moeten worden meegenomen in de PIA (artikel 12 en 18 IVRK) (zie beginsel 2).

In de PIA moeten ook bredere risico's worden afgewogen die de verwerking kan opleveren voor de rechten en vrijheden van kinderen, zoals de kans op aanmerkelijke materiële, fysieke,

psychologische of sociale schade. Er moet bovendien rekening worden gehouden met de verschillende leeftijden, vermogens en ontwikkelingsbehoeften van kinderen (artikel 5 IVRK). In een PIA kan ook worden vastgesteld welke stappen moeten worden ondernomen om leeftijd en ouderlijke toestemming adequaat en privacyvriendelijk te verifiëren. Ook kan een PIA beantwoorden aan de vraag of het eventueel beperken van de vrijheidsrechten van kinderen (zoals de vrijheid van kinderen om te leren, zich te ontwikkelen en te ontdekken) met het oog op het waarborgen van hun beschermingsrechten proportioneel is. Denk aan de situatie waarin kinderen alleen worden uitgesloten van (een deel van) een dienst als deze aantoonbaar of vermoedelijk schadelijk voor hen is. Ook moet daarbij rekening worden gehouden met hun zich ontwikkelende vermogens en leeftijd (artikel 5 IVRK).

Het gebruik van een PIA heeft zowel voordelen voor de aanbieder van een digitale dienst als voor kinderen. Voor de verwerker kan een PIA uiteindelijk kostenbesparend werken, omdat vanaf het begin van het ontwerpproces adequaat rekening kan worden gehouden met gegevensbescherming alsmede andere fundamentele rechten. Dat kan onder andere door gegevensbescherming op adequate wijze mee te nemen in het ontwerp van de digitale dienst. Ook kan reputatieschade worden voorkomen in een latere fase. Voor kinderen en ouders kan het gebruik van een PIA geruststellend werken, omdat er reeds in de ontwerpfase aantoonbaar aandacht wordt besteed aan het belang en de rechten van kinderen.

Beginsel 6: Zorg voor een kindvriendelijk privacyontwerp

Toelichting

Je mag niet meer persoonsgegevens verwerken dan strikt noodzakelijk is voor het bereiken van het specifieke doel van je digitale dienst (bijvoorbeeld het aanbieden van een chat-app). Met andere woorden, je hebt de verplichting om privacy mee te nemen in het ontwerp van je app of game (privacy by design) en de standaardinstellingen zo privacyvriendelijk mogelijk af te stellen (privacy by default). In het belang van het kind (zie beginsel 1) is het raadzaam om deze verplichting op een kindvriendelijke manier vorm te geven in het ontwerp. Kindvriendelijk privacyontwerp kan ook bijdragen aan andere privacybeginselen (denk aan veiligheid en integriteit) en de bescherming van de gegevensbeschermingsrechten van kinderen.

Buiten het minimaliseren van het aantal persoonsgegevens tot wat echt nodig (maar wel toereikend) is voor het specifieke doel van je dienst, kun je privacy op andere manieren op een kindvriendelijke manier implementeren in het ontwerp. Je kunt gegevensstromen en keuzes bij het gebruik van persoonsgegevens op een kindvriendelijke manier transparant maken (zie beginsel 4) en kinderen op eenvoudige en begrijpelijke wijze inzage geven in hun gegevensverwerkingen. De jongeren die tijdens het opstellen van deze code hebben meegedacht, willen unaniem kunnen inzien wat voor gegevens er van hen online staan (“**omdat het belangrijk is om te weten wat voor informatie andere mensen van je kunnen zien [...] zodat ik voor een volgende keer weet wat ik wel of niet moet accepteren**”), en geven aan daar graag controle over te hebben.

Je kunt bovendien opties inbouwen om gegevens eenvoudig te wissen (recht op vergetelheid). De meeste van de jongeren die we hebben gevraagd zouden gebruik maken van de mogelijkheid om al hun foto’s en gegevens van een account te verwijderen (zolang je ze wel op een andere manier kunt opslaan), “**want dan kunnen die gegevens niet meer zomaar worden gebruikt zonder mijn toestemming**”. Daarnaast kun je de optie inbouwen dat je op toegankelijke wijze bezwaar kan worden gemaakt tegen direct marketing (zie beginsel 3) en je toestemming net zo eenvoudig intrekken als die is gegeven (zie beginsel 3). Ook is het raadzaam om de digitale dienst zodanig te ontwerpen dat kinderen *niet* standaard worden geprofileerd (zie beginsel 7). Een kindvriendelijk privacyontwerp draagt zo bij aan de verwezenlijking van andere beginselen in deze code en het vertrouwen dat kinderen en ouders hebben in de dienst.

Implementatie

De resultaten van de PIA (zie beginsel 5) om de risico's voor de verwerking van persoonsgegevens weg te nemen of zoveel mogelijk te verkleinen moeten, zo mogelijk worden meegenomen in het ontwerp van de dienst.

Maak gebruik van standaardinstellingen voor een kindvriendelijk ontwerp.

- Kies voor een 'opt-in' regime bij de standaardinstellingen (privacy by default). Zorg ervoor dat instellingen standaard zo privacy-vriendelijk mogelijk staan afgesteld.
- Zorg ervoor dat de standaardinstellingen van jouw dienst geschikt zijn voor kinderen van alle leeftijden, d.w.z. de standaardinstellingen hebben het hoogste 'beschermingsniveau', tenzij het mogelijk is om te differentiëren naar verschillende leeftijden van kinderen. Bij jongere kinderen kies je dan het hoogste 'beschermingsniveau', terwijl tieners bijvoorbeeld meer vrijheid krijgen. In dat laatste geval is het wel goed om te weten wat hun ervaringen met je dienst zijn en of die vragen om bijstelling van de het 'beschermingsniveau'.
- Elke vorm van optioneel gebruik van persoonsgegevens (ook door derde partijen), inclusief elk gebruik met als doel personalisering van de dienst, moet afzonderlijk door het kind worden geselecteerd en geactiveerd. Een uitzondering op deze regel is als je over een aantoonbare dwingende reden beschikt om voor een andere standaardinstelling te kiezen, bijvoorbeeld wanneer de belangen van het kind in het geding zijn.
- Overweeg om maatregelen in te bouwen voor het moment dat een kind de standaardinstelling probeert te wijzigen op een wijze die mogelijk afbreuk doet aan zijn of haar veiligheid, bijvoorbeeld een waarschuwing op het moment dat de gebruiker zijn profiel als 'openbaar' wil instellen. Het afnemen van een PIA voor kinderen (zie beginsel 5) kan daarbij helpen.
- Geef het kind de keuze om van deze instellingen permanent gebruik te maken of om hier alleen per individuele sessie over te besluiten. Zorg ervoor dat bij softwareupdates de standaardinstellingen bewaard blijven. Gebruik bij voorkeur geen automatische updates, maar laat het kind - of de ouder/verzorger - hier expliciet mee instemmen.
- Maak het mogelijk om op apparaten die door meerdere gebruikers worden gebruikt verschillende gebruikerskeuzes in te stellen. Zorg dat de bescherming van gegevens gewaarborgd is op alle apparaten waar jouw dienst gebruikt kan worden.
- Geef bij aankoop en bij installatie van met internet verbonden speelgoed duidelijke informatie over het gebruik van persoonsgegevens. Voorzie je apparaat van functies die voor het kind of de ouder duidelijk maken wanneer je persoonsgegevens verzamelt.
- Maak het mogelijk om bij gebruik van een ouderaccount de ouder inzicht te geven in de maatregelen, waaronder standaardinstellingen, die zijn ingesteld bij de daaraan gelieerde kind-accounts.

- Verzamel geen gegevens als de applicatie of het speelgoed niet wordt gebruikt; aan het einde van de gebruikerssessie worden de toegang tot gegevens en internetverbinding uitgeschakeld.
- Bouw een laagdrempelige 'verwijder al mijn gegevens'-knop in (zoals ook onderbouwd onder beginsel 4), waar kinderen op elk moment gebruik van kunnen maken. Gegevens dienen ook automatisch te worden verwijderd indien het kind de applicatie verwijdert

Zorg ervoor dat de geolocatie, microfoon en camera standaard uit staan en laat kinderen en/of ouders handmatig toestemming voor geven voordat deze worden aangezet.

- Na afloop van elke sessie waarin de geolocatie gebruikt wordt, moet de optie weer uitgeschakeld zijn.
- Op het moment dat het kind gebruik maakt van geolocatie, moet dat het kind duidelijk gemaakt worden, op ieder moment: moment van abonneren, iedere keer dat dienst wordt geopend. Zorg ervoor dat het kind niet onbewust of per ongeluk geolocatie aan kan laten staan.
- Overweeg om op een andere manier locatie op te vragen dan via geolocatie (bijvoorbeeld door wijk/stadsdeel in te vullen) als je toch de applicatie wilt koppelen aan een locatie.

Maak gebruik van technieken die de privacy van kinderen bevorderen. Gebruik dus geen nudgetechnieken om kinderen ertoe te bewegen of aan te moedigen om opties te activeren die niet in hun belang zijn/ertoe leiden dat je meer persoonsgegevens van ze krijgt, of om privacybeschermingen uit te schakelen.

- Geef kinderen de mogelijkheid om van de dienst gebruik te maken onder een pseudoniem of om anoniem gebruik te maken van jouw platform.
- Maak standaard gebruik van een VPN (of ORBOT of TOR) bij het opstarten van een app.
- Zorg ervoor dat het kind een duidelijk, opvallend signaal krijgt wanneer ze gemonitord of gevolgd worden (ook als bijvoorbeeld een ouder meekijkt).
- Gebruik dummies. Dummies maken gebruik van de website en zijn niet te onderscheiden van echte gebruikers. Het gebruik van kinderen op een dienst bevat veel privacygevoelige informatie. Dit gedrag kan 'verborgen' worden door deze te 'vermengen' met het gedrag van nepgebruikers.
- Verwijder cookies op regelmatige basis, bijvoorbeeld bij het opstarten van het besturingssysteem, door ze per geval in te schakelen, door te bepalen of de bezochte website al dan niet betrouwbaar is en door een cookie alleen voor de huidige sessie te aanvaarden. Zie ook de website voor Privacy Patterns van Jaap Henk Hoepman[24].

[24] https://privacypatterns.org/patterns/

- Zie voor praktische handvatten voor het vormgeven van Privacy by Design het PbD framework op de website van Privacy Company[25].

Betrek bij een kindvriendelijk ontwerp ook de relatie van kinderen tot hun ouders. Kinderen hebben een recht op privacy, ook ten opzichte van hun ouders. Dit kan in voorkomende gevallen ook gelden voor andere volwassenen die met kinderen te maken hebben, waaronder leerkrachten en docenten.

- Zeker bij tieners is het raadzaam om hen een optie te geven om het meekijken door ouders te autoriseren in plaats van dit standaard in te bouwen.
- Ook jongere kinderen kunnen behoefte aan privacy hebben. Als een omgeving voor hen veilig is vormgegeven of ouders vooraf op hun leeftijd afgestemde keuzes kunnen maken van wat kinderen te zien krijgen, dan zouden zij daar verder zonder toezicht moeten kunnen 'rondhangen' en spelen. Overweeg binnen de applicatie een deel te ontwerpen dat niet toegankelijk is voor ouders of andere verzorgers. Let op dat het kind-deel van de applicatie dan niet openstaat voor communicatie met onbekenden, waaronder eventuele kwaadwillenden.

Relevante wet- en regelgeving

Kinderrechtenperspectief

Volgens het Kinderrechtencomité is het belang van het kind bijzonder relevant omdat digitale technologieën (oorspronkelijk) niet specifiek zijn ontworpen voor kinderen, terwijl ze inmiddels wel door veel kinderen in hun dagelijks leven worden gebruikt. Bij het ontwerpen van digitale diensten zal dan ook rekening moeten worden gehouden met het belang en de rechten van het kind, in het bijzonder het recht op privacy (artikel 16 IVRK, artikel 7 en 8 EU Handvest). Met name privacy en veiligheid, waaronder end-to-end encryptie, moeten onderdeel zijn van het ontwerp van digitale diensten.

De Raad van Europa erkent bovendien dat het recht van kinderen op privacy en gegevensbescherming niet alleen geldt in de relatie tot aanbieders van digitale diensten, maar ook in relatie van kinderen tot hun ouders en verzorgers, leeftijdsgenoten en leerkrachten. Ook deze rechten zouden by design kunnen worden ingebouwd door bijvoorbeeld tieners controle te geven over de privacy settings in onderwijsapps waar ouders ook gebruik van maken. In het geval van preventieve of adviesdiensten is het relevant om de privacy van kinderen ten opzichte van anderen, waaronder hun ouders, te waarborgen. Kinderen moeten de mogelijkheid

[25] https://www.privacycompany.eu/knowledge-base-nl/privacy-by-design-framework

hebben om gevoelige onderwerpen in vertrouwen te kunnen bespreken met bijvoorbeeld een hulpverlener, zeker ook omdat de thuissituatie niet altijd een veilige hoeft te zijn. Het ontwerp van een app kan ook ongewenste neveneffecten hebben, zoals misbruik van onbedoeld gedeelde locatiegegevens van kinderen, die in ieder geval moeten worden voorkomen (zie beginsel 5).

Gegevensbeschermingsrecht

Het grondbeginsel van minimale gegevensverwerking, ook wel dataminimalisatie genoemd, houdt in dat het verwerken van persoonsgegevens tot het minimale beperkt moet blijven. De gegevensverwerking moet "toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt" (artikel 5 (1) (c) AVG). Dat betekent onder meer dat de opslagperiode van de persoonsgegevens tot een strikt minimum moet worden beperkt (overweging 39 AVG). Het beginsel staat niet op zich en houdt verband met andere grondbeginselen, zoals het beginsel van rechtmatigheid, het doelbindingsbeginsel, het beginsel van opslagbeperking en de verantwoordingsplicht (artikel 5 AVG).

Het beginsel van minimale gegevensverwerking kan je implementeren door rekening te houden met het beginsel van gegevensverwerking door ontwerp (ook wel dataprotectie/privacy by design) en van gegevensbescherming door standaardinstellingen (dataprotectie/privacy by default) (artikel 25 AVG).

De verplichting om het principe van *privacy by design* te implementeren houdt onder meer in dat er bij het ontwerp van een digitale dienst rekening moet worden gehouden met de beginselen uit artikel 5 van de AVG (en dus niet alleen het beginsel van dataminimalisatie). Het belang van het kind, waarbij de belangen van kinderen een eerste overweging zijn, betekent dat ook bij het ontwerpen van de digitale dienst in het bijzonder rekening dient te worden gehouden met kinderen. Een effectieve manier om in de ontwerpfase rekening te houden met kinderen, kan door het ontwerp af te stemmen op de percepties, ervaringen en verwachtingen van kinderen. Dit vereist dan wel onderzoek naar deze percepties, ervaringen en verwachtingen van (en met) kinderen in verschillende leeftijdscategorieën (zie beginsel 2), omdat de ontwikkelende vermogens van kinderen mogelijk om andere maatregelen per leeftijdscategorie vragen.

Als digitale dienstaanbieder moet je passende *technische en organisatorische maatregelen* nemen bij de bepaling van de verwerkingsmiddelen en de verwerking zelf (artikel 25 lid 1 AVG). Een passende maatregel kan bijvoorbeeld pseudonimisering zijn (artikel 4 (5) AVG), wat inhoudt dat het verwerken van persoonsgegevens op zodanige wijze wordt gedaan, dat de persoonsgegevens niet meer aan een specifieke gebruiker kunnen worden gekoppeld zonder dat er aanvullende gegevens of speciale technieken worden gebruikt. Verder moeten er passende maatregelen worden genomen om ervoor te zorgen dat alleen persoonsgegevens

worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking (artikel 25 (2) AVG). Onder dergelijke maatregelen vallen bijvoorbeeld:

- het minimaliseren van de verwerking van persoonsgegevens,
- het zo spoedig mogelijk pseudonimiseren van persoonsgegevens,
- transparantie met betrekking tot de functies en de verwerking van persoonsgegevens,
- het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking, en
- uit het in staat stellen van de [aanbieder] om beveiligingskenmerken te creëren en te verbeteren" (overweging 78).

De aanbieder van een digitale dienst moet aantonen te voldoen aan het beginsel van privacy by design en by default (verantwoordingsplicht, artikel 5 (2) AVG).

Hoewel de *privacy by design*-verplichting in de AVG niet specifiek is toegespitst op kinderen, biedt het interessante kansen om het expliciete doel van de AVG waar te maken, namelijk kinderen en hun persoonlijke data extra goed beschermen (overweging 38).

Passende maatregelen kunnen voor kinderen ook iets anders inhouden dan voor volwassenen. In ieder geval moet rekening worden gehouden met het belang van het kind (zie beginsel 1) bij het vaststellen en ontwerpen van maatregelen om de beginselen en rechten in de AVG te waarborgen. Denk onder meer aan het op kindvriendelijke wijze visualiseren van gegevensverwerkingen en het inbouwen van voor hen toegankelijke en begrijpelijke mogelijkheden om daar controle op uit te oefenen. Daarbij kan worden meegenomen wat voor kinderen zelf belangrijk is (zie beginsel 2). Het Kinderrechtencomité noemt het innoveren vanuit het belang van het kind een belangrijke stap voorwaarts in de ontwikkeling van digitale diensten. Een op kinderen gerichte privacy impact assessment kan daarbij ondersteunen (zie beginsel 5).

Een aantal van onderstaande onderwerpen kan als voorbeeld dienen van mogelijkheden om juist (maar niet uitsluitend) bij kinderen in het ontwerp rekening te houden met privacybeginselen en -rechten. Dit is geen uitputtende lijst.

Leeftijdsverificatie - Als aanbieder van digitale diensten moet je om twee redenen weten of kinderen je dienst gebruiken. Ten eerste moet je ervan op de hoogte zijn of de gebruikers van je dienst onder de 18 jaar zijn, omdat in dat geval sprake is van specifieke gegevensbescherming (overweging 38 AVG) en een uitleg van de AVG in het belang van het kind (artikel 3 (1) IVRK) wordt vereist (zie beginsel 1). Ten tweede moet in het geval dat toestemming als wettelijke grondslag wordt gebruikt, worden vastgesteld of een kind zelf toestemming kan geven (kind is 16 jaar en ouder) of dat ouderlijke toestemming (kind is jonger dan 16) vereist is (zie beginsel 3). In beide gevallen mogen er niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om leeftijdsverificatie mogelijk te maken.

Recht op vergetelheid - Op grond van de AVG bestaat het recht op gegevenswissing, ook wel recht op vergetelheid genoemd, bijvoorbeeld wanneer gegevens niet langer noodzakelijk zijn voor het verwerkingsdoel, de gebruiker van de dienst toestemming intrekt of bezwaar maakt (artikel 17 AVG). Het recht is met name ook in het belang van kinderen, omdat zij wellicht gegevens hebben gedeeld toen ze zich nog niet (voldoende) bewust waren van de verwerkingsrisico's en deze later - ook of juist wanneer zij geen kind meer zijn - liever weer (van het Internet) wil laten verwijderen (overweging 65 AVG). Je wilt niet dat kinderen zogezegd worden achtervolgd door hun jeugdzonden. Ze moeten op enig moment weer met een schone lei kunnen beginnen. Als gebruikers vragen om wissing van gegevens die zijn verstrekt toen zij een kind waren, dan moet je als aanbieder van een digitale dienst dus zoveel mogelijk aan die wensen voldoen. Dat geldt vooral als het waarschijnlijk is dat ze hun persoonlijke gegevens hebben verstrekt zonder de implicaties hiervan volledig te begrijpen. Bovendien moet je derde partijen aan wie de persoonsgegevens zijn verstrekt inlichten over het wissingsverzoek. Wanneer kinderen zelf toestemming mogen geven of hun rechten uitoefenen, mag aan een verzoek van de ouder (of andere wettelijk vertegenwoordiger van het kind) om gegevens te wissen niet worden voldaan zonder het kind erbij te betrekken. Aangezien gegevens eenvoudig moeten kunnen worden gewist als gebruikers daar recht op hebben, is het raadzaam om dit mee te nemen in het ontwerp van de digitale dienst. Houd er daarbij ook rekening mee dat toestemming net zo eenvoudig moet kunnen worden ingetrokken als het wordt gegeven, en het intrekken van toestemming een grond is om ook meteen gegevens te verwijderen.

Inzagerecht - de gebruiker van een digitale dienst heeft het recht om persoonsgegevens die over hem of haar worden verwerkt in te zien (artikel 15 AVG). Dit is een recht dat "eenvoudig en met redelijke tussenpozen" (overweging 63 AVG) moet kunnen worden uitgeoefend. Door via bijvoorbeeld een privacydashboard inzage te geven in gegevensverwerkingen wordt in het ontwerp van de digitale dienst meteen rekening gehouden met het recht. Daarmee worden het recht op informatie en op inzage gezamenlijk vormgegeven.

Beveiliging - het spreekt wellicht voor zich maar de verplichting om persoonsgegevens adequaat te beveiligen (artikel 32 AVG) is iets om rekening mee te houden bij het ontwerp van een digitale dienst. Betrek daar vooral ook kinderen zelf bij (zie beginsel 2) om te achterhalen of zij niet tegen bijzondere kwetsbare situaties aanlopen en bepaalde wensen hebben. Een interessant fenomeen is het delen van inloggegevens met vrienden: iets dat indruist tegen veilig internetgebruik, maar wel voorziet in een sociale behoefte. Het is dus goed om hier aandacht voor te hebben en uit te zoeken of beide toch op enige wijze met elkaar verenigd kunnen worden, zodat dat wat als sociaal wenselijk wordt gevoeld, niet de veiligheid van een app of game ondermijnd.

Beginsel 7: Voorkom het profileren van kinderen

Toelichting

“Ik vind een app schadelijk als het schadelijk tegen minderheden is”
- een jongere die deelnam aan een sessie voor het opstellen van de Code.

Het profileren van gebruikers wordt gezien als een verwerking met een hoog risico waarvoor bijvoorbeeld een PIA (zie beginsel 5) vereist is. Bovendien gelden er beperkingen bij het profileren van kinderen. Zij genieten extra bescherming bij het opstellen van gebruikersprofielen en persoonlijkheidsprofielen. Profilering gebeurt voor uiteenlopende doeleinden. Je kan het bijvoorbeeld gebruiken om op de persoon gerichte marketing en diensten aan te bieden of om interessante klanten te onderscheiden van klanten die een risico vormen voor een bedrijf.

Profielen kunnen worden gemaakt op basis van over personen of groepen personen verzamelde gegevens. Vaak gaat het dan om online of offline gedragsgegevens. Uit die gegevens of op basis van associaties met andere gebruikers kunnen voorkeuren of kenmerken van personen worden afgeleid. Het plaatje dat zo ontstaat van een gebruiker kan heel indringend en privacygevoelig zijn. Bovendien is het niet per se een beeld dat overeenkomt met de werkelijkheid als het is gebaseerd op correlaties. Daarin schuilt dan het gevaar dat iemand onterecht een bepaald etiket opgeplakt krijgt. Dat kan schadelijk zijn als het leidt tot stereotypering, stigmatisering en ongewenste of oneerlijke bejegening (bijvoorbeeld vooroordelen of onterechte uitsluiting van diensten) of zelfs discriminatie van personen.

Kinderen worden als kwetsbaar gezien als het gaat om profilering. Profielen van gebruikers worden nauwkeuriger wanneer zij veel tijd steken in een digitale dienst dan wel daar steeds weer terugkeren, zodat zoveel mogelijk gedragsgegevens kunnen worden verzameld. Dat kan leiden tot obsessief gebruik, waardoor kinderen bijvoorbeeld minder tijd aan schoolwerk besteden of tijdens het leren continu worden gestoord en hun schoolresultaten onder druk komen te staan. Bovendien zijn kinderen mogelijk gemakkelijker te beïnvloeden. Kwetsbaarheden kunnen gericht worden benut voor marketingdoeleinden op een manier die indruist tegen hun vrijheid van informatie, hun vrijheid van gedachtevorming of hun recht op een plek om te spelen en te ontspannen vrij van commerciële boodschappen. Tenslotte zijn de lange termijn-effecten van profilering op kinderen vaak nog onvoldoende bekend.

Implementatie

Zorg ervoor dat functies voor profilering standaard uitstaan, tenzij er vanuit het belang van het kind een dwingende reden voor profilering is .

- Een dwingende reden is bijvoorbeeld dat profileren nodig is, omdat je ten behoeve van het welzijn van kinderen aan bepaalde wet- en regelgeving moet voldoen (om bijvoorbeeld seksuele uitbuiting en misbruik te voorkomen).

Wanneer je toch genoodzaakt bent te profileren, neem dan de volgende maatregelen:

- Geef aantoonbaar aan waarom het profileren in het belang van het kind is (zie beginsel 1).
- Maak duidelijk welk type profilering voor welk doeleinde wordt gebruikt. Waar passend moeten er afzonderlijke privacyinstellingen zijn voor iedere vorm van profilering. Verschillende vormen van profilering mogen niet gebundeld worden onder een en dezelfde privacyinstelling.
- Op het punt dat profilering wordt aangezet moet voor passende interventies gezorgd worden (denk aan leeftijdsrelevante informatie over wat er met de persoonsgegevens van het kind gebeurt, eventuele aansporing een volwassene erbij te halen al naar gelang leeftijd van het kind)
- Neem passende maatregelen om te waarborgen dat dit niet resulteert in eventuele psychische of fysieke schade voor het kind. Test daarbij de effecten van de wijze van profileren aan de hand van (menselijke) moderatie en meldprocedures.
- Evalueer of profilering geen effecten heeft die afdoen aan het belang van het kind en hun rechten. Zorg voor specifieke waarborgen om het belang en de rechten van het kind te beschermen (zie beginsel 1 en 5).

Relevante wet- en regelgeving

Kinderrechtenperspectief

Zowel de Raad van Europa als het Kinderrechtencomité roepen op tot grote terughoudendheid door online profilering van kinderen te verbieden, tenzij dat in het belang van het kind is. De keuze voor zo'n benadering is begrijpelijk, omdat de (lange termijn-)impact van online profilering op kinderen, ook voor marketingdoeleinden, nog onbekend is. Profilering van kinderen zou dan ook niet moeten gebeuren, tenzij het in hun belang is doordat het bijdraagt aan hun welzijn en de gebruikte middelen proportioneel zijn en niet onnodig inbreuk maken op de (privacy-)rechten van kinderen. Bijzondere aandacht moet er zijn voor het recht van kinderen op non-discriminatie (artikel 2 IVRK). Besluitvorming op basis van profilering kan leiden tot vooringenomenheid, stereotypering en discriminatie van (groepen) mensen, waaronder

kinderen. Discriminatie kan leiden tot materiële en immateriële schade en is verboden. Overigens kan ook discriminatie van ouders als gevolg van profilering een impact hebben op hun kinderen.

Gegevensbeschermingsrecht

Profilering behelst iedere vorm van geautomatiseerde verwerking van persoonsgegevens ter beoordeling van persoonlijke aspecten van een gebruiker, met name kenmerken als beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene te analyseren of te voorspellen (overweging 71 AVG). Profilering kan voor uiteenlopende doeleinden worden gebruikt, zoals het aanbieden van op de persoon gerichte content of marketing of het personaliseren van digitale diensten.

Kinderen verdienen extra bescherming, omdat zij de risico's van gegevensverwerkingen minder goed kunnen inschatten. Dat wordt in het bijzonder onderkend ten aanzien van het opstellen van persoonlijkheids- en gebruikersprofielen (overweging 38 AVG). De AVG overweegt dan ook dat profilering geen betrekking mag hebben op een kind wanneer deze rechtsgevolgen heeft of kinderen in aanmerkelijke mate treft (overweging 71 AVG). Ook op basis van de grondbeginselen van rechtmatigheid, behoorlijkheid en transparantie (artikel 5 AVG) moet een aanbieder van digitale diensten terughoudend zijn met profilering. Profilering is doorgaans niet direct zichtbaar voor de gebruiker, waardoor het lastig is om te begrijpen wat er eigenlijk gebeurt en welke consequenties dat heeft. Voor kinderen is dat zo mogelijk nog bezwaarlijker. Niet alleen omdat voldoende begrip van de situatie ontbreekt, maar ook omdat zij minder goed in staat zijn om de (lange termijn-)consequenties te overzien.

Profilering is niet toegestaan, wanneer daaraan voor iemand rechtsgevolgen zijn verbonden of deze hem of haar anderszins in aanmerkelijke mate treft (artikel 22 AVG). Een gebruiker heeft namelijk het recht om niet te worden onderworpen aan een geautomatiseerd besluit, waaronder profilering, zonder menselijke tussenkomst. Zonder menselijke tussenkomst betekent dat een besluit uit de computer komt rollen en er geen betekenisvolle controle meer plaatsvindt door een mens om te toetsen of het besluit wel terecht is.

De kans dat profilering iemand in aanmerkelijke mate treft, kan bij kinderen groter zijn vanwege hun kwetsbaarheid. Van 'in aanmerkelijke mate treffen' is sprake als profilering schadelijk is voor de ontwikkeling van kinderen. Dit kan het geval zijn bij op de persoon gerichte marketing. Profilering van kinderen voor marketingdoeleinden wordt dan ook afgeraden. Overigens hoeft een daadwerkelijk effect niet te worden aangetoond om te kunnen spreken van een aanmerkelijke impact.

Er zijn ook uitzonderingen op het profileringsverbod in artikel 22 AVG. Een uitzondering kan bijvoorbeeld zijn dat de gebruiker van een dienst expliciet heeft ingestemd met profilering of het noodzakelijk is voor de uitvoering van een overeenkomst (artikel 22 (2) AVG). Aangenomen wordt dat deze uitzonderingsgronden ten aanzien van kinderen restrictief moeten worden uitgelegd en profilering alleen moet worden toegestaan als dit in het belang van het kind is. Zo'n belang kan er zijn als profilering bijdraagt aan de gezondheid of de educatie van kinderen. Ook in dat geval moeten er wel voor kinderen passende waarborgen ter bescherming van hun rechten worden gegeven.

Beginsel 8: Voorkom te allen tijde economische exploitatie van kinderen

Toelichting

Kinderen hebben het recht om te spelen en te ontspannen in een omgeving die vrij is van commercie. Digitale technologie (die wordt gebruikt voor spel en ontspanning) wordt echter vanuit een commercieel oogmerk aangeboden door bedrijven. Nu mogen bedrijven natuurlijk geld verdienen met een hun app of game, maar er zijn wel bijzondere aandachtspunten wanneer deze door kinderen worden gebruikt om economische exploitatie te voorkomen.

Digitale diensten genereren vaak inkomsten met in app-aankopen. Bij kinderen is dan van belang dat ze in beginsel alleen met toestemming van hun ouders een overeenkomst mogen afsluiten. Ook worden kinderen soms bewust verleid of opzettelijk misleid tot het maken van keuzes, bijvoorbeeld het kopen van extra levens of levels als je bent vastgelopen in een game, die je bij nader inzien misschien liever niet had gemaakt. Daarbij kan de daadwerkelijke waarde van je in app-aankopen ook nog eens worden versluierd, doordat games een eigen virtuele valuta hanteren.

Bovendien kunnen in-app aankopen een gokelement hebben, waardoor de scheidslijn tussen gamen en gokken ondoorzichtiger wordt. Denk aan virtuele pakketjes met geheime inhoud (zogeheten loot boxes of blind boxes) die via microtransacties met echt geld gekocht worden. De verleiding van loot boxes kan groot zijn als er een kans bestaat dat de inhoud (bijvoorbeeld een krachtig wapen) kan helpen om prestaties in een game te verbeteren of dat een bijzonder kostuum het spelkarakter van de gebruiker populairder maakt.

Al dit soort praktijken dienen vooral het commerciële belang van de digitale dienst. We noemen het daarom ook wel op exploitatie gerichte vormgeving van digitale diensten of ‘dark patterns’. Niet alleen staat het commerciële belang voorop, maar het ondermijnt bovendien de autonomie van de gebruikers van een dienst om eigen keuzes te maken. De informatieasymmetrie tussen aanbieder en gebruiker van een digitale dienst wordt vergroot, doordat klanten zich vaak niet bewust zijn van de werking en het doel van dark patterns die op hen worden losgelaten. Ze doorzien niet altijd wat de impact op hun handelen is en wat de mogelijke risico’s zijn. Dark patterns kunnen misleidend, oneerlijk en daarmee onrechtmatig zijn.

Op exploitatie gerichte vormgeving van apps en games kan bovendien onderdeel zijn van op de persoon gerichte, datagedreven marketing. Dat is een vorm van marketing die als verdienmodel voor veel apps of games fungeert en gebaat is bij het verwerken van veel

gegevens. Door het ontwerp van een app of game wordt de gebruiker bijvoorbeeld “verleid” om daar veel tijd door te brengen, zodat er een grote hoeveelheid gedragsdata over hem of haar kan worden verzameld. Ook kunnen instellingen voor een privacyvriendelijk gebruik van apps en games worden verborgen of nodeloos ingewikkeld gemaakt waardoor ze voor de gebruiker, en zeker kinderen, moeilijk kunnen worden toegepast.

Met al die verzamelde gedragsgegevens kan een zeer indringend beeld van iemand ontstaan. Bovendien kunnen er kenmerken over (groepen) personen uit worden afgeleid (profilering) (zie beginsel 7). Die profielen zeggen bijvoorbeeld iets over iemands persoonlijkheid, seksuele identiteit, emotionele gesteldheid, medische aandoeningen, interesses, behoeften, en sociale contacten. De mens zelf wordt het middel tot het genereren van winst, aangezien deze gegevens en profielen een economische waarde vertegenwoordigen. Bij kinderen is dit in het bijzonder problematisch, omdat zij moeten worden beschermd tegen economische exploitatie.

Een ander voorbeeld van economische exploitatie van kinderen is de door algoritmes aangedreven informatievoorziening op bijvoorbeeld videoplatforms. De gebruiker moet zo veel mogelijk tijd achter het scherm doorbrengen om de inkomsten uit reclames te maximaliseren. Een beproefde methode om gebruikers te vermaken (en hun aandacht dus zo lang mogelijk vast te houden), is het aanbevelen van steeds sensationelere content. Met de autoplay-functie hoeven gebruikers niet meer na te denken over de volgende video die zij willen zien. Het algoritme bepaalt deze namelijk op basis van je kijkhistorie en speelt automatisch de volgende af. Volgens de jongeren die meedachten bij het opstellen van de Code zou ‘autoplay’ een van de eerste functies zijn van een videoplatform die afgeschaft moet worden.

Implementatie

Maak geen gebruik van reclame die in woord, geluid of beeld kinderen op enigerlei wijze kan misleiden. Reclame mag daarnaast geen formele of fysieke schade berokkenen en moet daarom:

- niet aanzetten tot de aankoop van een bepaald product aanzetten door te profiteren van de onervarenheid of goedgelovigheid van een kind;
- niet rechtstreeks het kind ertoe aanzetten ouders of anderen te overtuigen tot de aankoop van producten waarvoor reclame wordt gemaakt;
- niet profiteren van het speciale vertrouwen dat kinderen hebben in ouders, leerkrachten of anderen.

Reclame gericht op kinderen mag daarnaast niet suggereren dat het hebben of gebruiken van een bepaald product hen fysiek of sociaal voordeel biedt ten opzichte van andere kinderen, noch dat het niet hebben van een bepaald product tot het tegenovergestelde effect leidt. Concreet betekent dat voor het ontwerp van een digitale dienst dat bijvoorbeeld:

- In geval van een banner) en/of via een pop-up een website zichtbaar gemaakte reclame gericht op kinderen, de reclame-uiting dient te zijn voorzien van een duidelijke, in één oogopslag waarneembare, vermelding van het woord “reclame” of “advertentie”.
- Reclame in posts en overige reclame dienen door optische, virtuele en/of akoestische middelen – passend bij het bevattingsvermogen van kinderen – duidelijk herkenbaar te zijn.
- Het is niet toegestaan kinderen rechtstreeks te stimuleren tot het maken van reclame ten behoeve van de adverteerder.

Bekijk ook de Kinder- en Jeugdreclamecode[26] en de Reclamecode social media en influencer marketing[27].

Wees transparant over aankopen of andere commerciële aspecten van een game:

- Noem het spel alleen gratis wanneer het dat helemaal is. Games met in-app aankopen mogen bijvoorbeeld niet verkocht worden als ‘gratis’. Maak voor de aankoop duidelijk aan de potentiële gebruiker of er in het spel aankopen mogelijk zijn. De voorkeur gaat bij het ontwerp uit naar een eenmalige betaling vooraf (in plaats van continu in-app).
- Als er toch sprake is van in-app aankopen, moet dit in heldere taal (bijvoorbeeld met universele symbolen voor aankopen) worden uitgelegd. Vermeld de valuta (ook) in euro’s bij elke uitnodiging tot aankoop, in plaats van enkel in de unieke valuta van de app of game. En herhaal ‘dit kost echt geld’ of een vergelijkbare boodschap op het moment dat dit van toepassing is, bijvoorbeeld bij de aankoop zelf.
- Overweeg, als een game of app voornamelijk door kinderen wordt gespeeld of gebruikt, betaalinstellingen zo vorm te geven dat kinderen geen aankopen kunnen doen zonder ouderlijk toezicht. Dat kun je bijvoorbeeld doen door voor elke aankoop - of voor aankopen boven een bepaald bedrag - een wachtwoord te vereisen.
- Laat gebruikers bij een ‘early acces’-game bij aanvang meteen weten waar zij aan beginnen. Het moet voor de gebruiker duidelijk zijn dat het spel mogelijk niet verder ontwikkeld wordt. Het moet voor de potentiële gebruiker ook duidelijk zijn wanneer het spel al langere tijd een ‘early-acces’-game is of (mogelijk) niet meer ontwikkeld wordt.

Bekijk ook de leidraad Bescherming online consument van de ACM[28].

Vermijd het gebruik van loot boxes of andere technieken die gebruikt worden om aankopen bij gebruikers te stimuleren, zoals aanbiedingen die beperkt geldig zijn, verborgen reclame, microtransacties, gebruik van andere valuta, prijspersonalisatie en algoritmen die de beste verkoopstrategie bepalen.

[26] https://www.reclamecode.nl/nrc/kinder-en-jeugdreclamecode-kjc/
[27] https://www.reclamecode.nl/nrc/reclamecode-social-media-rsm/
[28] https://www.acm.nl/nl/publicaties/leidraad-bescherming-online-consument

Laat de content die kinderen creëren, op bijvoorbeeld videoplatforms en in social media apps, eigendom blijven van de kinderen zelf.

Relevante wet- en regelgeving

Kinderrechtenperspectief

Kinderen hebben het recht op bescherming tegen economische exploitatie (artikel 32 IVRK). Economische exploitatie is onrechtvaardig voordeel halen uit kinderen voor het eigen gewin van een bedrijf. Hieronder kan ook vallen het manipuleren van kinderen om economisch voordeel te behalen, waaronder door op exploitatie gerichte vormgeving van digitale diensten. Het Kinderrechtencomité beschouwt dit als het tonen van een gebrek aan respect voor de harmonieuze ontwikkeling van de persoonlijkheid van kinderen. Op exploitatie gerichte vormgeving is niet in het belang van kinderen (artikel 3 IVRK) als het niet bijdraagt aan hun welzijn of zelfs schadelijk voor hen is. Daarmee heeft het ook een impact op het recht van kinderen op een optimale ontwikkeling (artikel 6 IVRK). Bovendien is bij economische exploitatie niet het belang van het kind een eerste overweging, maar staat het belang van bedrijven zelf voorop.

Op exploitatie gerichte vormgeving raakt ook aan het recht op privacy en dataprotectie van kinderen (artikel 16 IVRK), artikel 7 en 8 EU Handvest), als deze gepaard gaat met niet-noodzakelijke of zelfs excessieve gegevensverzameling. Het manipuleren van hun denkbeelden met op basis van algoritmes geselecteerde content kan in strijd zijn met hun recht op vrijheid van informatie (artikel 13 IVRK) en gedachtevorming (artikel 14 IVRK). En op exploitatie gerichte vormgeving heeft een impact op hun recht op spel en ontspanning (artikel 31 IVRK).

De Raad van Europa pleit voor maatregelen[29] om kinderen te beschermen tegen economische exploitatie bij het gebruik van digitale diensten. Bij reclame en marketing moet rekening worden gehouden met de leeftijd van kinderen. Kinderen die daar vanwege hun leeftijd nog niet aan toe zijn, verdienen bescherming. Voor kinderen die op een leeftijd zijn dat ze reclame herkennen en daar kritisch op kunnen reflecteren, is het daarentegen van belang dat ze ermee leren omgaan en valt het wellicht onder hun recht op vrijheid van informatie (artikel 13 IVRK). Het is dan wel belangrijk dat het heel duidelijk is wanneer iets is bedoeld als reclame of marketing. Het Kinderrechtencomité roept op tot grote terughoudendheid bij nieuwe vormen van marketing, omdat deze mogelijk in strijd zijn met kinderrechten.

Reclame- en marketingstrategieën worden steeds slimmer in het beïnvloeden van gebruikers, bijvoorbeeld door hen voortdurend en op verschillende platformen te bombarderen met

[29] https://rm.coe.int/09000016808d881a

reclame of door juist verborgen en/of op de affectie gerichte tactieken te gebruiken, zoals advergames, brand pushers (waaronder kinderen) en branded pop songs, zodat reclame en marketing onontkoombaar worden. Oudere kinderen kunnen zich daar cognitief net zo slecht tegen weren als jongere kinderen. Wanneer transparantie bij deze vormen van marketing niet helpt bij het beschermen van kinderen tegen negatieve effecten (denk aan oneerlijke manipulatie), dan wordt niet voldaan aan onder meer het belang van het kind-beginsel (zie beginsel 1) en het recht op ontwikkeling van kinderen (artikel 6 IVRK). Het Kinderrechtencomité noemt nog als voorbeelden van marketing die in strijd kunnen zijn met kinderrechten: datagedreven, gerichte marketing op basis van de persoonlijke en locatie-informatie van kinderen die over platformen heen wordt gegenereerd. Dat geldt temeer als die gepaard gaat met op marketing gerichte ontwerpkeuzes die kinderen naar meer of extremere content sturen of met geautomatiseerde, slaapverstorende meldingen. Sommige vormen van marketing zouden volgens het Kinderrechtencomité verboden moeten zijn, waaronder het targeten van kinderen, ongeacht hun leeftijd, op basis van profielen alsmede op kinderen gerichte neuromarketing.

Gegevensbeschermingsrecht

In het gegevensbeschermingsrecht hebben kinderen recht op specifieke bescherming, met name bij het gebruik van hun persoonsgegevens voor marketingdoeleinden of voor het opstellen van persoonlijkheids- of gebruikersprofielen (overweging 38 AVG). Zij zijn namelijk minder goed in staat zijn om marketingpraktijken te herkennen en deze kritisch te beoordelen, zeker wanneer deze gepaard gaan met (meestal) niet direct zichtbare gegevensverwerking en profilering. Voorkomen moet worden dat er misbruik wordt gemaakt van het gebrek aan besef bij kinderen van de werking en de mogelijke consequenties van deze vormen van marketing. De AVG bevat geen algemeen verbod op marketing gericht op kinderen, maar er zijn wel duidelijke beperkingen op gegevensverwerkingen voor marketingdoeleinden.

Toestemming en marketing - als gegevensverwerking voor marketingdoeleinden een verplicht onderdeel van een app of game is, maar niet behoort de kern van de dienst, dan is toestemming voor het gebruik van die digitale dienst niet vrijelijk gegeven. Je hebt dan namelijk geen vrije keuze om er al dan niet mee in te stemmen. Toestemming is in zo'n geval niet rechtsgeldig gegeven (artikel 7 (4) AVG) (zie beginsel 3). Bovendien moet toestemming geïnformeerd zijn en in het geval van kinderen moet die informatie op een voor hen begrijpelijke en herkenbare manier worden gegeven. Datagedreven, gerichte marketingpraktijken zijn echter lastig uit te leggen aan kinderen, waardoor het twijfelachtig is of zij daar op een geïnformeerde wijze mee kunnen instemmen als zij zelf bevoegd zijn om toestemming te geven (artikel 7 en 8 AVG). Overigens kun je je ook afvragen of deze praktijken voor volwassenen - en daarmee de ouders van kinderen - steeds voldoende begrijpelijk zijn. Het kan helpen om de gegevensverwerking zo eenvoudig mogelijk te houden.

Gerechtvaardigd belang en marketing - gegevensverwerking voor directe marketingdoeleinden kan een gerechtvaardigd belang van de digitale dienstaanbieder zijn (overweging 47 AVG) (zie beginsel 3). Die gegevensverwerking moet echter een minimale impact hebben op het recht op privacy van de gebruiker. In het geval van kinderen moet het belang van het kind bovendien een eerste overweging zijn in de belangenafweging (zie beginsel 1). Is er daarentegen sprake van een omvangrijke gegevensverwerking, zoals bij het opstellen van profielen, het delen van data met data brokers, op gedrag gebaseerde marketing en online direct marketing, dan is toestemming (artikel 6 (1) (a) AVG) een mogelijk geschiktere wettelijke grondslag. Daarbij moet overigens nog steeds ook worden voldaan aan de grondbeginselen van de AVG, waaronder het beginsel van minimale gegevensverwerking (artikel 5 (1) (c) AVG).

Recht op bezwaar en direct marketing - als gebruiker kun je bezwaar maken tegen gegevensverwerking voor direct marketing (artikel 21 (2) AVG). Hierover moet de gebruiker worden geïnformeerd, waarbij er specifiek rekening mee moet worden gehouden dat informatie voor kinderen begrijpelijk en herkenbaar is.

Profilering en marketing - kinderen verdienen in het bijzonder bescherming wanneer er sprake is van het opstellen van persoonlijkheids- en gebruikersprofielen (overweging 38 AVG). Profilering is als onderdeel van geautomatiseerde besluitvorming verboden, tenzij er sprake is van een uitzonderingsgrond (artikel 22 AVG) (zie beginsel 7) Gerichte of gepersonaliseerde marketing zijn vormen van profilering die schadelijk kunnen zijn voor de ontwikkeling van kinderen en het profileren van kinderen voor marketingdoeleinden wordt afgeraden, omdat het waarschijnlijk is dat dit een aanmerkelijk effect op hen heeft. Die uitleg is ook in lijn met het belang van het kind (zie beginsel 1).

Consumentenrecht

Op exploitatie gericht ontwerp van digitale diensten kan een oneerlijke handelspraktijk zijn (6:193a BW e.v.). Een handelspraktijk is oneerlijk als gebruikers daardoor een besluit nemen over een transactie die zij anders niet hadden genomen. Het moet de gebruiker beschermen tegen praktijken die hem of haar hinderen in het nemen van een weloverwogen en geïnformeerde beslissing over een economische transactie. De (on)eerlijkheid van een handelspraktijk wordt beoordeeld aan de hand van wat de gemiddelde consument (in deze code de gebruiker van een digitale dienst) kan begrijpen.

In het geval van kinderen kijk je naar wat het gemiddelde lid van de groep kinderen kon begrijpen als de (in dit geval) aanbieder zich op deze groep richt of redelijkerwijs kon voorzien dat zij door de handelspraktijk of het onderliggende product geraakt zouden worden. De groep kan nader bepaald worden, bijvoorbeeld naar leeftijd. Een kind kan namelijk het slachtoffer worden van een praktijk die de gemiddelde volwassen consument zal wantrouwen. Er zijn factoren denkbaar die maken dat een gemiddeld kind van een groep minder redelijk

geïnformeerd, omzichtig en oplettend is. Hierbij spelen maatschappelijke, culturele en taalkundige factoren, maar ook leeftijd een rol. Als aanbieders zich richten op kinderen, dan moeten zij dus rekening houden met het feit dat kinderen informatie anders op waarde schatten dan volwassenen. Hierdoor zijn kinderen in kwetsbare situaties extra beschermd.

Er zijn ook handelspraktijken die onder alle omstandigheden oneerlijk en dus verboden zijn (artikel 6:193g en 193i BW). Er is een zogeheten zwarte lijst van misleidende handelspraktijken en een zwarte lijst van agressieve handelspraktijken. Bij misleidende handelspraktijken geeft de aanbieder feitelijk onjuiste of misleidende informatie, laat deze informatie weg of is de aanbieder er onduidelijk over. Voorbeelden van misleidende handelspraktijken zijn het als gratis aanbieden van een dienst terwijl er wel degelijk kosten aan verbonden zijn of het ten onrechte beweren dat een product maar een zeer beperkte tijd beschikbaar is.

Bij een agressieve handelspraktijk wordt de gebruiker op ongepaste wijze, door intimidatie, dwang, waaronder het gebruik van lichamelijk geweld, of ongepaste beïnvloeding aanzienlijk in zijn keuzevrijheid beperkt of kan daarin worden beperkt. Voorbeelden van agressieve praktijken op de zwarte lijst zijn het moeten betalen om een gewonnen prijs in ontvangst te mogen nemen (anders dan de noodzakelijke verzendkosten om deze naar het kind toe te laten komen), of kinderen er in reclame rechtstreeks toe aanzetten om een product, inclusief virtuele items in bijvoorbeeld games, te kopen of om hun ouders ertoe over te halen het product voor hen te kopen. Bij de beoordeling van de oneerlijke handelspraktijken kan de gehele context van een digitale dienst worden meegenomen, waaronder de situationele kwetsbaarheid van kinderen.

Overige wet- en regelgeving

Reclame - Een aanbieder van een videoplatform moet zorgen dat reclame, bijvoorbeeld in de vorm van advertenties, sponsoring of productplaatsing, herkenbaar zijn en geen subliminale technieken gebruiken (artikel 3a.5 (1)-(2) Mediawet). Sluikreclame is niet toegestaan (artikel 3a.5 (3) Mediawet). Een aanbieder van een videoplatform waarop reclame wordt gemaakt valt onder de regelingen en het toezicht van de Stichting Reclame Code (artikel 3a.4 (1) Mediawet). Ook apps en games vallen onder de Stichting Reclame Code. De Stichting stelt voorwaarden aan reclame om de geloofwaardigheid en betrouwbaarheid ervan te waarborgen. Reclame mag niet misleiden, nodeloos kwetsen of bedreigen en moet wettelijk zijn toegestaan. Zo is het verboden om de menselijke waardigheid aan te tasten, te discrimineren en aan te sporen tot gedrag dat schadelijk is voor de gezondheid, veiligheid of voor het milieu (zie o.a. Media - en

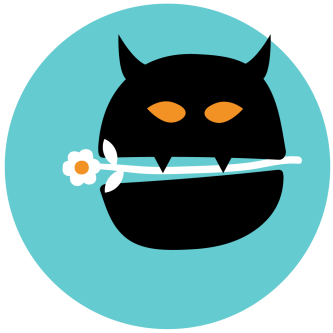
Tabaks- en rookwarenwet). Er zijn specifieke Reclame Codes waaronder voor kansspelen[30], jeugd[31] en social media & influencer marketing[32].

Kansspelen - Kansspelwetgeving beoogt kwetsbare groepen, waaronder kinderen[33], te beschermen. In 2021 wordt het voor aanbieders mogelijk om een vergunning aan te vragen voor online kansspelen. Online kansspelen mogen dan niet worden aangeboden aan kinderen (artikel 31k (2) (a) Wet kansspelen op afstand). Een vergunninghouder (dat wil zeggen een houder van een vergunning tot het organiseren van kansspelen op afstand) mag bovendien geen wervings- en reclameactiviteiten specifiek op kinderen richten.

Er moet duidelijk worden onderscheiden tussen games en kansspelen. Een vergunninghouder mag bij het aanbieden van kansspelen op afstand geen games aanbieden dan wel daar reclame voor maken. Bovendien mogen zij in diensten waar games worden aangeboden, geen reclame maken (zie toelichting[34] bij Besluit kansspelen op afstand[35]). Daarnaast heeft de Kansspelautoriteit loot boxes[36] waarmee prijzen met een economische waarde kunnen worden gewonnen in games, verboden. Overigens is de Kansspelautoriteit ook kritisch over andere gokelementen in games. In de overweging speelt mee dat kinderen extra kwetsbaar zijn vanwege hun zich nog ontwikkelende vermogens (artikel 5 IVRK) en mogelijk makkelijker gevoelig kunnen worden gemaakt voor gokken. Vanuit het belang van het kind bezien, is het dan ook aan te raden om kinderen tegen gokelementen in apps en games te beschermen (zie beginsel 1).

[30] https://www.reclamecode.nl/nrc/reclamecode-voor-kansspelen-die-worden-aangeboden-door-vergunninghouders-ingevolge-de-wet-op-de-kansspelen-rvk-2015/
[31] https://www.reclamecode.nl/nrc/kinder-en-jeugdreclamecode-kjc/
[32] https://www.reclamecode.nl/socialuitleg/
[33] https://kansspelautoriteit.nl/onderwerpen/minderjarigen/
[34] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/03/03/tk-bijlage-besluit-kansspelen-op-afstand/tk-bijlage-besluit-kansspelen-op-afstand.pdf
[35] https://kansspelautoriteit.nl/over-ons/publicaties/regels-leidraden/online-kansspelen/besluit-kansspelen/
[36] https://kansspelautoriteit.nl/onderwerpen/loot-boxes/

Beginsel 9: Voorkom te allen tijde voor kinderen schadelijk ontwerp



Toelichting

“**Ik vind een app schadelijk als je andere dingen verwaarloost erdoor of als het je slecht laat voelen.**” - een jongere die deelnam aan een sessie voor het opstellen van de Code.

Naast op economische exploitatie gericht ontwerp moet ook - anderszins - schadelijk ontwerp te allen tijde worden vermeden. Onder schadelijk ontwerp wordt onder andere verstaan een ontwerpkeuze in een digitale dienst die de kwetsbaarheid van kinderen onterecht benut of misbruikt, dan wel gedragingen met een negatieve impact voor kinderen niet of onvoldoende adequaat aanpakt. Ontwerp is schadelijk als het negatieve consequenties heeft voor de gezondheid of het welzijn van kinderen. Het welzijn van kinderen omvat alle aspecten van hun ontwikkeling, waaronder hun mentale, sociale, cognitieve en fysieke ontwikkeling.

Ontwerp kan schadelijk zijn voor de ontwikkeling van kinderen als het hen onvoldoende beschermt tegen mogelijke schadelijke content, contacten of gedragingen. Denk bij schadelijke content bijvoorbeeld aan het (geautomatiseerd) vertonen of verheerlijken van geweld, stereotypering, racisme, desinformatie of pornografische content in een app of game. Schadelijke contacten of gedragingen kunnen te maken hebben met pesten, (seksueel) misbruik, opruiing, haatzaaien, werven voor criminele praktijken en radicalisering.

Verder kan er sprake zijn van ontwerp dat een mogelijk negatieve impact heeft op hun sociale relaties. Denk bijvoorbeeld aan vaste tijdstippen in games waarop kinderen bijzondere achievements (zoals skins en wapens) kunnen behalen, waardoor andere geplande activiteiten met bijvoorbeeld familie of vrienden worden doorkruist. Een ander voorbeeld is (tijdelijke) uitsluiting van deelname in een game wanneer het spel moet worden onderbroken om te gaan eten.

Dit soort mechanismen kunnen leiden tot conflicten met ouders en sociale druk van leeftijdgenoten. Ook kan het een negatief effect hebben op het vermogen van kinderen om zich te concentreren op andere activiteiten, zoals hun schoolwerk, wanneer ze voortdurend worden gestoord door notificaties. Denk aan games die de speler continu terugroepen om de voortgang in het spel zeker te stellen. Ontwerp kan ook excessief gebruik van digitale diensten in de hand werken en zelfs leiden tot gezondheidsproblemen (waaronder slaaptekort, fysieke schade en verslaving).

Ontwerpkeuzes waarbij kinderen (onbewust) worden gedwongen tot bepaald gedrag dat zij zonder die keuzes mogelijk niet hadden vertoond en/of die een disruptieve werking hebben op hun gezondheid, sociale relaties en andere activiteiten in hun dagelijks leven, moeten bij voorkeur worden vermeden. Dat is zeker het geval als die keuzes aantoonbaar niet in hun belang of schadelijk zijn.

Wordt van bepaalde vormen van ontwerp aangenomen dat ze niet bijdragen aan het welzijn van kinderen of voor hen schadelijk zijn, maar is er geen (overtuigend) bewijs? Wees dan terughoudend en gebruik het liever niet in een dienst die waarschijnlijk ook door kinderen wordt gebruikt. We noemen dat de voorzorgsbenadering. Die benadering gaat uit van het better safe than sorry-principe: als aannemelijk is dat het ontwerp op enige wijze negatieve effecten zou kunnen hebben op kinderen, is het beter om voorzichtig te zijn met de implementatie ervan.

Implementatie

Pas de voorzorgsbenadering toe als aannemelijk is dat een bepaald ontwerp potentieel schadelijk is voor kinderen. Gebruik daarvoor bijvoorbeeld de uitkomsten van het kind-impact-assessment uit beginsel 1.

Pas voor het gebruik van beloningen, notificaties en likes de volgende regels toe:

- Vermijd het om persoonsgegevens zodanig te gebruiken dat kinderen worden gestimuleerd langer te blijven, zoals kinderen in ruil voor langer doorspelen gepersonaliseerde in-game-voordelen te bieden (gebaseerd op jouw gebruik van de persoonsgegevens van de individuele gebruiker).
- Presenteer opties om door te blijven spelen of op andere wijze gebruik van jouw dienst te blijven maken op een neutrale manier, zonder te suggereren dat kinderen zichzelf tekort doen als ze dit niet doen. Probeer de tijdsdruk te verminderen door minder of geen tijdsgebonden opdrachten op te nemen (dit kan verslavend werken).
- Vermijd functies met persoonsgegevens het gebruik van de dienst automatisch verlengen. Laat kinderen een actieve keuze maken of ze hun tijd op deze manier willen besteden (datagestuurde autoplay-functies).
- Introduceer mechanismen als pauzeknoppen, waarmee kinderen op elk moment een pauze kunnen nemen, zonder dat ze hun voortgang in een spel verliezen, of biedt leeftijdsrelevante content om bewuste keuzes over het nemen van pauzes te ondersteunen.
- Beperk het overmatig gebruik van notificaties, of zorg dat deze op simpele wijze uitgeschakeld kunnen worden.
- Zorg ervoor dat kinderen op elk moment kunnen stoppen met het gebruik van de applicatie (en hierbij al hun gegevens kunnen wissen, zie ook beginsel 4 en 5) zonder dat ze zich daarover schuldig voelen.

- Voorkom incentives voor kinderen om zoveel mogelijk (onbekende) vrienden of volgers toe te voegen.

Ontwerp de digitale dienst zo dat gebruikers zo min mogelijk in aanraking komen met schadelijke content, contacten of gedragingen.

- Promoot en communiceer de communityrichtlijnen van het ontwerp op een manier die aantrekkelijk is en past bij gebruikers van alle leeftijden. Denk hierbij aan communityrichtlijnen en gedragscodes die duidelijk maken wat voor gedrag niet welkom is in je spel of dienst.
- Zorg voor mechanismen waarmee kinderen op vertrouwelijke wijze ongepast gedrag en inbreuken op de communityrichtlijnen kunnen rapporteren en zorg dat deze gemakkelijk te vinden en gebruiken zijn.
- Wees transparant over welke content mogelijk schadelijk kan zijn voor een specifieke leeftijdscategorie en zorg ervoor dat kinderen deze content kunnen rapporteren wanneer dit mogelijk schadelijk of illegaal is.

Indien de app of game kinderen aanspoort om zich bij het gebruik van een app of game in de fysieke omgeving te verplaatsen, zorg dan dat dit op een zo veilig mogelijke manier gebeurt.

- Zorg ervoor dat kinderen zich veilig door hun fysieke omgeving kunnen verplaatsen door daar bijvoorbeeld voortdurend op te wijzen of dat spelenderwijs aan ze duidelijk te maken.
- Als gebruikers vanuit de applicatie worden gestimuleerd om specifieke fysieke locaties te bezoeken, zorg dan dat deze locaties passen bij de ontwikkeling van het kind (zie ook de classificering per ontwikkelfase onder beginsel 2).
- Als kinderen worden aangemoedigd om andere gebruikers offline te ontmoeten, richt dit dan zo in dat het past bij de leeftijd van het kind. Maak bijvoorbeeld profielen van kinderen onder een bepaalde leeftijd niet openlijk zichtbaar voor andere gebruikers.

Relevante wet- en regelgeving

Kinderrechtenperspectief

Het beschermen van kinderen tegen schadelijk ontwerp houdt direct verband met het belang van het kind: het is niet in het belang van kinderen dat digitale diensten gebruik maken van voor kinderen schadelijk ontwerp of ontwerp dat schade voor kinderen onvoldoende voorkomt. Kinderen hebben onder meer het recht op een optimale en gezonde ontwikkeling (artikel 6 IVRK), recht op gezondheid (artikel 24 IVRK) en bescherming tegen schadelijke content (artikel 17 lid 4 IVRK). Bovendien hebben zij het recht op bescherming tegen geweld (artikel 19 IVRK) (waaronder pesten) en tegen seksueel misbruik (artikel 34 IVRK).

Het waarborgen van het belang van het kind houdt bovendien in dat activiteiten, waaronder digitale diensten, die een impact op hen hebben, dienen bij te dragen aan hun welzijn. Schade moet derhalve zeker worden voorkomen en bij de waarschijnlijkheid van schade dient een voorzorgsbenadering te worden gekozen, bijvoorbeeld door een bepaalde ontwerpkeuze niet te maken. Daarbij kan rekening worden gehouden met de zich ontwikkelende vermogens van kinderen (artikel 5 IVRK): wat voor jonge kinderen schadelijk is, hoeft niet per se schadelijk te zijn voor oudere kinderen. Bovendien kan het, zeker voor oudere kinderen, ook heel leerzaam te zijn om te leren omgaan met risico's van digitale diensten. Bijvoorbeeld door hen te laten ondervinden hoe ontwerp hen kan beïnvloeden en hen te leren om daar kritisch op te reflecteren. Kritisch leren reflecteren veronderstelt wel dat kinderen weten dat bepaalde ontwerpkeuzes hen kunnen beïnvloeden en bij voorkeur ook dat zij de mogelijkheid hebben om een andere keuze te maken. Leren kritisch reflecteren op ontwerpkeuzes is niet per se een verplichting voor ontwerpers en zou onderdeel kunnen worden van bredere bewustwordingsactiviteiten rondom digitale technologie.

Wanneer veiligheidsmaatregelen worden ingebouwd in de digitale dienst (safety by design) om kinderen te beschermen tegen schadelijke content of contacten moet rekening worden gehouden met de zich ontwikkelende vermogens van kinderen (artikel 5 IVRK) en andere kinderrechten, zoals hun recht op privacy (artikel 16 IVRK) en recht op vrijheid van informatie (artikel 13 IVRK). Leeftijdsverificatie (zoals bij kansspelen) of contentclassificatie (vergelijkbaar met het systeem van de Kijkwijzer[37] voor audiovisuele media of PEGI[38] voor games) kunnen adequate instrumenten zijn om kinderen te beschermen, waarbij rekening moet worden gehouden met de zich ontwikkelende vermogens van kinderen (artikel 5 IVRK).

Gegevensbeschermingsrecht

Gegevensverwerking om gedrag van gebruikers te beïnvloeden of content gericht te laten zien, moet aantoonbaar voldoen aan het gegevensbeschermingsrecht. (zie beginsel 3, 4, 5, 6) Vanuit het oogpunt van behoorlijkheid (artikel 5 (1) (a) AVG) moet er in het bijzonder aandacht zijn voor de gegevensverwerking waarbij de persoonlijkheid, waaronder ook de kwetsbaarheid, van het kind wordt gebruikt in het ontwerp en gebruik van de digitale dienst. Zo is profilering van kinderen niet toegestaan, tenzij het in hun belang is, bijvoorbeeld doordat het bijdraagt aan hun welzijn (zie beginsel 7).

Ook bij het implementeren van safety by design-instrumenten moet aantoonbaar worden voldaan aan het gegevensbeschermingsrecht. (zie beginsel 3, 4, 6, 7) Wordt er gebruik gemaakt van leeftijdsverificatie om ervoor te zorgen dat schadelijke content niet toegankelijk is voor

[37] https://www.kijkwijzer.nl/
[38] https://www.kijkwijzer.nl/pegi

kinderen van specifieke leeftijden, dan moet rekening worden gehouden met het beginsel van minimale gegevensverwerking (artikel 5 (1) (c) AVG) (zie beginsel 5).

Overige wetgeving

Verwijderen van illegale informatie - aanbieders van digitale diensten hebben een zorgplicht om onrechtmatige informatie meteen te verwijderen of ontoegankelijk te maken als zij weten of redelijkerwijs behoren te weten van het onrechtmatige karakter ervan (artikel 6:196c lid 4 BW). Er hoeft geen controle vooraf te zijn bij het opslaan en publiceren van informatie op bijvoorbeeld een social media platform, maar de aanbieder heeft wel een onderzoeksplicht als er reden tot twijfel aan de rechtmatigheid van opgeslagen informatie is. Het Meldpunt Kinderporno, onderdeel van het Expertisebureau Online Kindermisbruik, kan bijvoorbeeld helpen bij het verwijderen van kinderporno.

Mediawet en videoplatforms - aanbieders van videoplatforms moeten maatregelen nemen om kinderen te beschermen tegen content die schadelijk is voor hun lichamelijke, geestelijke of morele ontwikkeling (artikel 4.1a Mediawet) en om gebruikers in het algemeen - kinderen en volwassenen - te beschermen tegen content die aanzet tot geweld, of haat jegens een persoon of een groep van personen op grond van godsdienst, levensovertuiging, politieke gezindheid, ras en geslacht, seksuele gerichtheid, en handicap, en tegen content waarvan de verspreiding een misdrijf vormt (bijvoorbeeld racistische content, kinderporno, of content die het plegen van een terroristisch misdrijf uitlokt) (artikel 2.88 Mediawet). De maatregelen om gebruikers, en in het bijzonder kinderen, te beschermen tegen deze drie categorieën content moeten in een gedragscode worden opgenomen (artikel 3a.3 Mediawet 2008). Ook moet het platform ervoor zorgen dat gebruikers worden geïnformeerd over door anderen geplaatste content, zogeheten user generated content, die mogelijk schadelijk is voor kinderen. Videoplatformen zullen gaan vallen onder het Kijkwijzer-systeem[39] van het NICAM.

[39] https://www.kijkwijzer.nl/

Beginsel 10: Ontwikkel richtlijnen voor de branche die zijn gericht op de bescherming van de belangen en rechten van kinderen

Toelichting

Steeds meer kinderen brengen steeds meer tijd door met digitale technologieën. Deze technologieën worden vooral ontwikkeld en aangeboden door de private sector. Bedrijven hebben daarmee een enorme impact op kinderen en hun rechten. Daarbij geldt steeds de niet vrijblijvende verplichting om de rechten van kinderen te bevorderen (zie beginsel 1). Dat vereist echter bewustwording en kan ook een uitdagende taak zijn, zoals de beginselen in deze code duidelijk laten zien.

Het Kinderrechtencomité erkent dat bedrijven ook zelf kunnen bijdragen door het opstellen van richtlijnen of gedragscodes. Dat kan op vrijwillige basis gebeuren. Daarnaast kan de wet dit soort zelfregulering door bijvoorbeeld brancheorganisaties stimuleren of voorschrijven.

Met een gedragscode is het voor een sector duidelijker hoe bepaalde regels bij kinderen moeten worden uitgelegd, zodat hun rechten goed worden gewaarborgd. Zeker voor bedrijven die producten en diensten aanbieden waarvan het waarschijnlijk is dat deze door kinderen worden gebruikt, zoals apps, games en connected toys, is het raadzaam om met de sector richtlijnen op te stellen. Een gedragscode is niet vrijblijvend en als bedrijf zul je je eraan moeten houden, omdat anders sprake kan zijn van een misleidende handelspraktijk.

Implementatie

- Raadpleeg richtlijnen uit de relevante branche, voorbeelden van geschikte richtlijnen zijn de UNICEF Children's Rights and Business Principles[40] en de UNICEF Child Online Protection Guidelines for the ICT Sector[41].
- Betrek kinderen bij het opstellen van richtlijnen en zorg ervoor dat deze openbaar zijn, zodat ouders, docenten en kinderen de richtlijnen kunnen lezen en begrijpen. Promoot en communiceer de richtlijnen vervolgens op een manier die aantrekkelijk is voor gebruikers van alle leeftijden.
- Zorg ervoor dat de richtlijnen ook daadwerkelijk worden nageleefd

[40] https://www.unicef.org/csr/resources.html
[41] https://www.unicef.org/csr/files/Training_Module_2_Child_Online_Protection_for_ICT_industry.pdf

    - Zorg ervoor dat de richtlijn zorgvuldig is ingebed in de desbetreffende keten.
    - Zorg dat naleving regelmatig gecontroleerd wordt.
    - Stel een (effectief) handhavingsmechanisme in.
- Het vooropstellen van het belang van het kind is een iteratief proces: evalueer regelmatig of nieuwe updates of ontwikkelingen nog in lijn zijn met een kindvriendelijk ontwerp. Bouw het liefst procesmatig een terugkerende evaluatie in die zich specifiek op het belang van het kind richt.
- Blijf op de hoogte van aanbevelingen of adviezen bij de relevante branche en scherp de richtlijnen zo nodig aan.

Relevante wet- en regelgeving

Kinderrechtenperspectief

Een gedragscode van een bij digitale diensten betrokken sector kan bijdragen aan de implementatie van het belang van het kind-beginsel (artikel 3, IVRK) door effectieve, op de rechten van kinderen gebaseerde gedragsregels op te stellen. Daarmee legt het verantwoording af over de keuzes die zijn gemaakt in het toepassen van de geldende wettelijke regels wanneer digitale diensten een impact hebben op kinderen. Meer specifiek geeft het gegevensbeschermingsrecht een invulling van het recht van kinderen op privacy en gegevensbescherming (artikel 16 IVRK).

Het Kinderrechtencomité wijst eveneens op het belang van gedragscodes om daarin “de hoogste normen inzake ethiek, privacy en veiligheid in acht te nemen bij het ontwerpen, de engineering, de ontwikkeling, de exploitatie, de distributie en de marketing van hun technologische producten en diensten” (vertaling door de auteurs van deze code) (General Comment No. 25). Er moet op worden toegezien dat bedrijven hoge standaarden voor transparantie en controleerbaarheid hanteren en met hun maatregelen innoveren in het belang van kinderen. Het Kinderrechtencomité wijst in het bijzonder op het belang van gedragscodes voor marketing.

Gegevensbeschermingsrecht

Sectoren kunnen door middel van het opstellen van gedragscodes duidelijk maken hoe zij invulling geven aan de normen uit de AVG. Een gedragscode is een vorm van zelfregulering door een brancheorganisatie of -vereniging. In het geval van de specifieke bescherming die kinderen moeten krijgen onder de AVG kan een gedragscode een belangrijk instrument zijn om bij te dragen aan de verantwoordingsplicht (artikel 5 lid 2 AVG) door in detail te beschrijven welke gedragsregels gelden in een sector.

Onder de AVG wordt het opstellen van gedragscodes aangemoedigd, met name ook ten aanzien van kinderen, om “doeltreffende uitvoering van deze verordening te bevorderen, rekening houdend met het specifieke karakter van de verwerkingen in sommige sectoren” en “gedragscodes zouden met name het ijkpunt kunnen zijn voor de verplichtingen van [aanbieders], rekening houdend met de aan de verwerking verbonden risico's voor de rechten en vrijheden van [gebruikers]” (overweging 98 AVG). In dat laatste geval zal er ook aandacht moeten zijn voor de risico’s voor in het bijzonder de rechten en vrijheden van kinderen die - zoals deze code laat zien - anders kunnen zijn of een andere invulling krijgen dan bij volwassenen.

Het doel van de gedragscode is dus een juiste toepassing van de AVG (ook artikel 40). In de gedragscode kunnen brancheorganisaties de toepassing van de regels van de AVG voor de betreffende sector nader toelichten (artikel 40 lid 2 AVG). Een van de onderwerpen die een gedragscode kan behelzen is “de informatie verstrekt aan en de bescherming van kinderen (inclusief wijzen waarop toestemming wordt verkregen van de personen die de ouderlijke verantwoordelijkheid voor kinderen dragen)” (Art. 40 (2) (g) AVG). Een gedragscode kan een specifieke sector betreffen, zoals de Britse Age Appropriate Design Code voor digitale diensten, maar kan zich ook richten op een specifiek onderwerp, zoals leeftijdsverificatie.

De gedragscode kan de goedkeuring van de Autoriteit Persoonsgegevens krijgen als deze adequate waarborgen biedt (artikel 40 lid 5 AVG). Sectoren met een "hoog risico", zoals die waar gegevens van kinderen worden verwerkt, worden geacht strengere waarborgen te hanteren, gelet op bijvoorbeeld de gevoeligheid van de persoonsgegevens, de kwetsbaarheid van de betrokkene of het indringende karakter van de gegevensverwerking. Toezicht op de naleving van een gedragscode wordt uitgeoefend door een orgaan dat over de passende deskundigheid met betrekking tot het onderwerp van de gedragscode beschikt en daartoe door de bevoegde toezichthoudende autoriteit, in Nederland de Autoriteit Persoonsgegevens, is geaccrediteerd (artikel 41 AVG).

Consumentenrecht

Een gedragscode is niet vrijblijvend en als bedrijf zul je je eraan moeten houden. Het niet nakomen van een verplichting in gedragscode kan een misleidende handelspraktijk zijn (artikel 6:193c, lid 2, onder a, BW).

Geraadpleegde bronnen

Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01)*, p. 28.

Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (PIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248*, 2017, p. 10, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Article 29 Working Party, *Guidelines on automated individual decision-making and profiling for the purposes of the regulation 2016/679.* WP 251, 3 October 2017, p. 29.

Autoriteit Consument & Markt, *Leidraad Bescherming van de online consument: Grenzen aan online beïnvloeding*, 2020, https://www.acm.nl/sites/default/files/documents/2020-02/acm-leidraad-bescherming-online-consument.pdf

Boom, W.H. van, *Inpassing en handhaving van de Wet oneerlijke handelspraktijken*, Tijdschrift voor Consumentenrecht en handelspraktijken, 2008.

College van Beroep voor het bedrijfsleven 15 mei 2018, ECLI:NL:CBB:2018:145.

Consumer Protection Cooperation Network, *Common position of national authorities within the CPC [related to online games],* European Commission: 2013, https://ec.europa.eu/info/sites/info/files/common-position_of_national_authorities_within_cpc_2013_en_0.pdf.

Council of Europe, *Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* Convention 108 (Guidelines), 2020, https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b.

Data Protection Commission, *Fundamentals for a Child-Oriented Approach to Data Protection* (Draft version for Public Consultation), Dublin: 2020, https://www.dataprotection.ie/en/dpc-guidance/blogs/the-children-fundamentals

Dempsey, J., Sim, G. & Cassidy, B., *Designing for GDPR - Investigating Children's Understanding of Privacy: A Survey Approach*, 2018, http://clok.uclan.ac.uk/24179/1/BHCI-2018_paper_82.pdf

Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Recommendation CM/Rec(2018)7 of the Committee of Ministers), Council of Europe: 2018, https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html.

Hof, S. van der & Hannema, T.S.P., *Veilig opgroeien in een wereld vol algoritmes. De bijzondere bescherming van kinderen onder art. 22 Algemene Verordening Gegevensbescherming*, Privacy & Informatie 2018(6): 190-198.

Hof, S. van der & Lievens, E., *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR*, Communications Law 23(1): 2018, 33-43. (DRAFT PAPER p.7, p.9)

Hof, S. van der, Lievens, E. & Milkaite, I., The protection of children's personal data in a data-driven world. A closer look at the GDPR from a children's rights perspective. In: Liefaard T., Rap S., Rodrigues P. (red.) *Monitoring Children's Rights in the Netherlands. 30 Years of the UN Convention on the Rights of the Child.* Leiden: Leiden University Press, 2019, p. 25,35,36,38,39. (DRAFT)

Information Commissioner's Office, *Age appropriate Design: a code of practice for online services,* 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.

Information Commissioner's Office, 'Right to Erasure": recital 65 GDRP. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/how-does-the-right-to-erasure-apply-to-children/

Information Commissioner's Office, *Consultation*: *Children and the GDPR guidance*, 2017, https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf.

International Telecommunication Union, *Guidelines for industry on Child Online Protection,* Geneva: 2020, https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_967b2ded811f48c6b57c7c5f68e58a02.pdf.

Kardefelt-Winther, D., Day, E., Berman, G., Winning, S.K., Bose, A., *Encryption, Privacy and Children's Right to Protection from Harm,* UNICEF Office of Research - Innocenti (Working Paper), 2020, https://www.unicef-irc.org/publications/1152-encryption-privacy-and-childrens-right-to-protection-from-harm.html.

Kennisnet, *Waarde wegen: Een ethisch perspectief op digitalisering in het onderwijs,* Zoetermeer: 2020, https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/Kennisnet-Ethiekkompas-Waardenwegen.pdf.

Kolucki, B. & Lemish, D., *Communication with Children: Principles and Practices to Nurture, Inspire, Excite, Educate and Heal,* New York: UNICEF 2011, https://sites.unicef.org/cwc/files/CwC_Final_Nov-2011.pdf.

Pijpers, R. & Bosch, N. van den (red.), *Positive Digital Content for Kids: Experts reveal their secrets.* POSCON & Mijn Kind Online, 2014, https://www.kennisnet.nl/mijnkindonline/files/Positive_digital_content_for_kids.pdf.

Richtlijn 2005/29/EG van het Europees Parlement en de Raad van 11 mei 2005 betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt en tot wijziging van Richtlijn 84/450/EEG van de Raad, Richtlijnen 97/7/EG, 98/27/EG en 2002/65/EG van het Europees Parlement en de Raad en van Verordening (EG) nr. 2006/2004 van het Europees Parlement en de Raad („Richtlijn oneerlijke handelspraktijken") (*PbEU* 2005, L 149/22).

Roosendaal, A. & Privacy Company (2016), *Privacy by Design in de praktijk!* (Jaarcongres ECP), https://docplayer.nl/44346190-Privacy-by-design-in-de-praktijk.html.

UC Berkeley School of Information, "Privacy patterns", https://privacypatterns.org/.

Verdoodt, V. (2018), *Children's rights and advertising literacy in the digital era: towards an empowering regulatory framework for commercial communication.*

UNICEF, Child Rights and Online Gaming, Opportunities and challenges for children and the industry, Discussion paper, 2019, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

UNICEF, *Training Module 2: Child Online Protection Guidelines for ICT Industry,* Powerpoint presentatie (n.d.), https://sites.unicef.org/csr/files/Training_Module_2_Child_Online_Protection_for_ICT_industry.pdf.

Wet van 25 september 2008 tot aanpassing van de Boeken 3 en 6 van het Burgerlijk Wetboek en andere wetten aan de richtlijn betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt, *Stb.* 2008, 397.

Aanvullend leesmateriaal

Amnesty International rapport ‘Surveillance Giants’ (achtergrond): https://www.amnesty-international.be/nieuws/alomtegenwoordige-surveillance-van-facebook-en-google-is-gevaar-voor-mensenrechten

Autoriteit Consument & Markt leidraad ‘Bescherming van de online consument’: https://www.acm.nl/sites/default/files/documents/2020-02/acm-leidraad-bescherming-online-consument.pdf

Data & Design by LINC (focus op GDPR): https://design.cnil.fr/en/

Defenddigitalme (focus op onderwijs): https://defenddigitalme.org/

Kinderrechten.nl: https://www.kinderrechten.nl/

OECD Council rapport ‘The protection of children online’ (aanbevelingen voor beleid): https://www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en

Tada: https://tada.city/en/home-en/

UNICEF (rapporten, artikels en workshops rond *AI for children*): https://www.unicef.org/globalinsight/featured-projects/ai-children

UNICEF (trainingsmodules): https://sites.unicef.org/csr/resources.html

Colofon

Simone van der Hof
Quirine van Eeden
Hannah Grijns
Rosalie Kok
Melis Bilgin
Hannah Volman
Tessel van Leeuwen
Sander van der Waal
Laurens Hebly

Onze speciale dank gaat uit naar Frank van der Meyden (Ministerie van BZK).

De Code is opgesteld in samenspraak met experts op het snijvlak van kind en technologie, en met ontwerpers, ontwikkelaars en jongeren. Wij willen hierbij alle deelnemers aan de expertsessies en allen die hebben meegelezen met de code bedanken voor hun waardevolle inbreng. In het bijzonder spreken wij onze dank uit aan Robert Zuiverloon en zijn klas, Alain Otjens, Anne-Jel Hoelen, Arnold Roosendaal, Astrid Poot, Douwe-Sjoerd Boschman, Eva Lievens, Fiona Venig, Lodewijk Loos, Marit Hoefsloot, Marjolijn Bonthuis, Simone Fennell-van Esch en Tom Demeyer. Fouten en onjuistheden komen voor rekening van de makers van de code.

Bijlage. Communiceren met kinderen per leeftijdscategorie

Indeling in leeftijdscategorieën en aanbevelingen zijn afkomstig uit de Britse Age Appropriate Design Code.

Communiceren met kinderen per leeftijdscategorie

Leeftijdscategorie	Aanbevelingen
0-5 Ongeletterdheid en ontluikende geletterdheid -	• gebruik eenvoudige taal, herhaling, leg uit aan de hand van ritme en zang met dieren en mensen, gebruik rijmpjes en raadsels
6-9 Middenbouw basisschool	• gebruik verhalen over vriendschap, het creëren van vaardigheden, dagelijkse gebeurtenissen die gaan over iemands waarden en kritisch denkvermogen
10-12 Overgangsjaren	• gebruik rolmodellen, vertel verhalen over de invloed van familie, vrienden en media op het kind, stimuleer kinderen in hun behoefte om op deze leeftijd om te experimenteren en onafhankelijke keuzes te durven maken
13 -15 Vroege tienerjaren	• gebruik rolmodellen, vertel verhalen over de invloed van familie, vrienden en media op de jongere, stimuleer kinderen in hun behoefte om op deze leeftijd om te experimenteren en onafhankelijke keuzes te durven maken
16-17	• overgangsfase naar volwassenheid (gebruik rolmodellen, vertel verhalen over de invloed van familie, vrienden en media

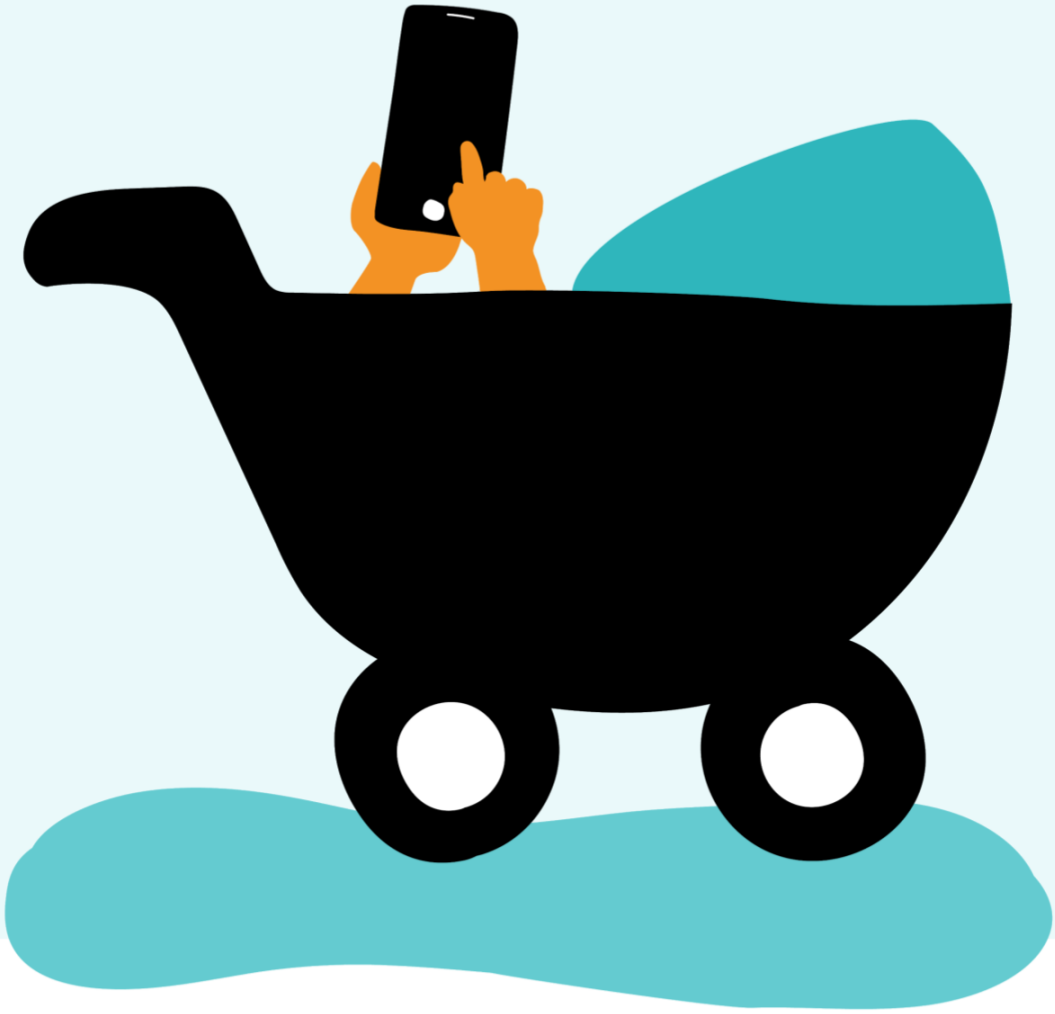
Overgangsfase naar volwassenheid	op de jongere, stimuleer kinderen in hun behoefte om op deze leeftijd om te experimenteren en onafhankelijke keuzes te durven maken

Communiceren met kinderen *over privacy* per leeftijdscategorie

Leeftijdscategorie	Aanbevelingen
0-5 Ongeletterdheid en ontluikende geletterdheid -	• Bied volledige privacy-informatie aan zoals verplicht volgens artikel 13 en 14 van de AVG, in een voor ouders geschikte vorm. • Bied audio- of videoprompts die kinderen oproepen dingen te laten zoals ze zijn of hulp in te roepen van een ouder of vertrouwde volwassene als ze standaard op hoog ingestelde privacy-instellingen proberen te wijzigen.
6-9 Middenbouw basisschool	• Bied volledige privacy-informatie aan zoals verplicht volgens artikel 13 en 14 van de AVG, in een voor ouders geschikte vorm. • Bied naast de informatie voor ouders cartoons of video- of audiomaterialen aan. • Geef uitleg over de basisprincipes van online privacy binnen jouw dienst, de privacy-instellingen die je aanbiedt, wie wat kan zien, hun informatierechten, hoe ze controle kunnen uitoefenen over hun eigen informatie en over het respecteren van de privacy van anderen. • Geef uitleg over de basiselementen van jouw dienst en hoe deze werkt, wat ze van je kunnen verwachten en wat je van hen verwacht.

10-12 *Overgangsjaren*	• Bied volledige privacy-informatie aan zoals verplicht volgens artikel 13 en 14 van de AVG, in een voor ouders geschikte vorm. • Bied volledige privacy-informatie aan zoals verplicht volgens artikel 13 en 14 van de AVG, in een voor kinderen in deze leeftijdsgroep geschikte vorm. • Bied kinderen de keuze tussen schriftelijke en video/audio-opties. • Bied kinderen de mogelijkheid om de getoonde informatie naar individuele behoeften op of af te schalen (naar materialen ontwikkeld voor een oudere of jongere leeftijdsgroep). • Bied als een kind een standaard op hoog ingestelde privacy-instelling probeert te wijzigen, cartoons of schriftelijke, video- of audiomaterialen aan om uit te leggen wat er met zijn of haar informatie gebeurt en welke risico's daarbij horen. • Vertel kinderen dat ze de dingen moeten laten zoals ze zijn of hulp moeten vragen van een ouder of een vertrouwde volwassene voordat ze de instelling wijzigen.
13 -15 *Vroege tienerjaren*	• Bied volledige privacy-informatie aan zoals verplicht volgens artikel 13 en 14 van de AVG, in een voor deze leeftijdsgroep geschikte vorm. • Bied de keuze tussen schriftelijke en video/audio-opties. • Bied de mogelijkheid om de getoonde informatie naar individuele behoeften op of af te schalen (naar materialen ontwikkeld voor een oudere of jongere leeftijdsgroep). • Bied als een kind een standaard op hoog ingestelde privacy-instelling probeert te wijzigen, schriftelijke, video- of audiomaterialen aan om uit te leggen wat er met zijn of haar informatie gebeurt en welke risico's daarbij horen. • Spoor kinderen aan om een ouder of een vertrouwde volwassene om hulp te vragen en de instelling niet aan te passen als ze twijfelen of niet begrijpen wat je ze hebt verteld. • Geef naast de op het kind gerichte informatie volledige informatie weer in een voor ouders geschikte vorm.

16-17 *Overgangsfase naar volwassenheid*	• Bied volledige informatie in een voor deze leeftijdsgroep geschikte vorm. • Bied de keuze tussen schriftelijke en video/audio-opties. • Bied de mogelijkheid om de getoonde informatie naar individuele behoeften op of af te schalen (naar materialen ontwikkeld voor een oudere of jongere leeftijdsgroep). • Bied als een kind in deze leeftijdsgroep een standaard op hoog ingestelde privacy-instelling probeert te wijzigen, schriftelijke, video- of audiomaterialen aan om uit te leggen wat er met zijn of haar informatie gebeurt en welke risico's daarbij horen. • Spoor kinderen aan om een volwassene of een andere vertrouwde informatiebron te raadplegen en de instelling niet aan te passen als ze twijfelen of niet begrijpen wat je ze hebt verteld. • Geef naast de op het kind gerichte informatie volledige informatie weer in een voor ouders geschikte vorm.



code voor
kinderrechten