CONSIDERATI

LEGAL | PUBLIC AFFAIRS | RESPONSIBLE TECH

Raamwerk Online Leeftijdsverificatie

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

10-10-2023

Bart W. Schermer LLM PhD

Partner Legal & Responsible Tech

Marianne Schoenmakers MSc

Senior Consultant Responsible Tech

Jord Goudsmit MSc

Consultant Responsible Tech

Jules van Stralendorff LLM

Senior Legal Consultant Privacy & Data Protection

Versiebeheer

Datum	Eigenaar	Wijzigingen
22-08-2023	Considerati	Conceptversie
14-09-2023	Considerati	Definitieve versie
10-10-2023	Considerati	Definitieve versie

Inhoudsopgave

1 Inleiding 4

2 Afwegingen bij verantwoorde online leeftijdsverificatie 6

3 Juridisch kader 8

4 Methoden online leeftijdsverificatie 15

5 Risico's voor kinderen online 17

6 Relevante aspecten bij de toepassing van leeftijdsclassificatie 19

7 Classificatie robuustheid leeftijdsverificatie 23

8 Nadere analyse leeftijdsverificatiemechanismen 30

9 Conclusies en aanbevelingen 40

Bijlagen 43

Voorbeeld online verkoop alcoholhoudende dranken 43

Figuur stappenplan afweging online leeftijdsverificatie 46

1 Inleiding

Minderjarigen kunnen online in aanraking komen met voor hen ongepaste online content, schadelijke middelen kopen, of schadelijke activiteiten ondernemen. Leeftijdsverificatie kan voorkomen dat minderjarigen in aanraking komen met schadelijke content, middelen of activiteiten.

Helaas zijn bestaande leeftijdsverificatie mechanismen veelal inadequaat. De meeste digitale diensten gebruiken bijvoorbeeld enkel een ´zelfverklaring´ waarbij de gebruiker zelf moet aangeven hoe oud hij/zij is. Door online leeftijdsverificatie te verbeteren kunnen minderjarigen beter beschermd worden.

Bescherming van kinderen online is één van de speerpunten van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Een van de onderdelen binnen het beleid van BZK is het versterken van de methodes van online leeftijdsverificatie. De huidige gebruikte methodes zijn niet altijd voldoende adequaat, met risico's voor kinderen tot gevolg. BZK heeft meerdere rondetafelgesprekken georganiseerd met experts om te komen tot een aanzet voor een lijst van eisen aan online leeftijdsverificatie. In dit rapport wordt deze aanzet verder uitgewerkt. Onderzocht wordt hoe de eisen aan online leeftijdsverificatie kunnen worden gekoppeld aan de zwaarte van de risico's zoals geformuleerd in het Kinderrechten Impact Assessment ("**KIA**") –dat mede is ontwikkeld door Considerati.

De uitdaging hierbij is dat er geen *one-size-fits-all* verificatiemethode is die in alle gevallen de beste oplossing biedt. Wat de eisen zijn aan een verificatiesysteem is contextafhankelijk. Daarbij spelen de specifieke risico's voor het kinderwelzijn een rol, de aard van de digitale dienst en daarmee samenhangende afwegingen op het gebied van bijvoorbeeld privacy, veiligheid, inclusiviteit en transparantie.

1.1 Scope

Om structuur te geven aan dit onderzoek zijn de volgende onderzoeksvragen geformuleerd:

1. Welke eisen moeten er worden gesteld aan online leeftijdsverificatie systemen op het gebied van robuustheid, privacy, veiligheid, inclusiviteit en transparantie?
2. Welke overwegingen zijn noodzakelijk om tot de meest geschikte methode van leeftijdsverificatie te komen?

1.2 Leeftijdsverificatie als instrument

Leeftijdsverificatie geldt als een van de maatregelen die kan worden ingezet om het welzijn van kinderen te beschermen en de negatieve impact van digitale diensten op kinderrechten te beperken. Aan de hand van de KIA kan een inschatting worden gemaakt van de mogelijke risico's bij de inzet van digitale diensten. Wanneer deze risico's zijn geïdentificeerd, moet er een afweging worden gemaakt welke maatregelen het meest effectief zijn om deze risico's te mitigeren. Leeftijdsverificatie is één van de maatregelen die de risico's kan verminderen, maar zal zeker niet in alle gevallen de enige of beste maatregel zijn.

Leeftijdsverificatie kan ook ongewenste neveneffecten hebben, zoals bijvoorbeeld een toename van het toezicht op het kind, of uitsluiting van groepen die geen toegang hebben tot de gekozen vorm van leeftijdsverificatie. Bij de keuze voor risico-beperkende maatregelen zoals leeftijdsverificatie moet ook met deze neveneffecten rekening worden gehouden.

Dit rapport beschrijft het kader van eisen en overwegingen met betrekking tot de verschillende methoden van leeftijdsverificatie. Wanneer leeftijdsverificatie wordt gezien als meest geschikte mitigerende maatregel, moet worden bepaald welke methode van leeftijdsverificatie het beste past in de specifieke context. Dit kan bijvoorbeeld worden bepaald aan de hand van het niveau van robuustheid dat gewenst is.

1.3 Aanpak

Om de hierboven besproken doelen te realiseren hanteren wij de volgende aanpak.

In **hoofdstuk 2** presenteren wij een stappenplan op hoofdlijnen, dat kan helpen om tot een afweging te komen met betrekking tot een systeem van leeftijdsverificatie.

In **hoofdstuk 3** beschrijven wij de wettelijke bepalingen die leeftijdsbeperkingen voorschrijven. Deze wetten verplichten in sommige gevallen ook het verifiëren van de leeftijd van kinderen. In **hoofdstuk 4** zetten wij uiteen wat online leeftijdsverificatie is en welke verschijningsvormen online leeftijdsverificatie op dit moment kent.

In **hoofdstuk 5** bespreken wij de categorieën risico's waaraan kinderen blootgesteld kunnen worden in een online omgeving. Hierbij hanteren wij de categorisering die wordt gebruikt in de Kinderrechten Impact Assessment (KIA). Op basis van de geïdentificeerde risico's en verplichtingen kunnen we beoordelen welke vormen van leeftijdsverificatie relevant zijn.

In **hoofdstuk 6** bespreken wij de verschillende aspecten die relevant zijn bij de keuze voor een leeftijdsverificatiemethode. Daarbij geven wij ook aan welke minimumvereisten er zijn als het gaat om deze overwegingen.

Omdat robuustheid een belangrijk criterium is voor een adequate leeftijdsverificatie bespreken wij eisen aan de robuustheid in meer detail in **hoofdstuk 7**. Omdat de robuustheid van een verificatiemethode nauw samenhangt met de veiligheid, komt ook dit onderwerp aan bod.

In **hoofdstuk 8** bespreken wij vervolgens de vier categorieën leeftijdsverificatie in het licht van de in hoofdstuk 7 besproken overwegingen.

We eindigen met een conclusie in **hoofdstuk 9**.

2 Afwegingen bij verantwoorde online leeftijdsverificatie

Om richting te geven een verantwoord en adequaat leeftijdsverificatiesysteem doen wij in dit hoofdstuk een eerste aanzet voor een afwegingskader. Er zijn diverse methoden voor online leeftijdsverificatie (zie hoofdstuk 4). Zoals we in de hoofdstukken 6, 7 en 8 zullen laten zien kunnen diverse methoden sterk variëren qua robuustheid, maar ook qua impact op andere belangen zoals privacy en inclusiviteit. Om te kunnen vaststellen aan welke eisen een leeftijdsverificatie systeem in een specifieke context moet voldoen is het raadzaam om onderstaande stappen te doorlopen.

Stap 1: Stel risico's vast

1. Breng de risico's voor kinderwelzijn door gebruik van de digitale dienst in kaart (zie hoofdstuk 5 of voer een Kinderrechten Impact Assessment uit)
2. Bepaal hoe hoog het risico voor het kinderwelzijn is (zeer hoog, hoog, midden, laag)

Stap 2: Beoordeel of er andere methoden zijn die het risico beperken

3. Beoordeel welke risico beperkende maatregelen genomen kunnen worden naast of in plaats van leeftijdsverificatie om de geïdentificeerde risico's te beperken.

Stap 3: Stel het gewenste/noodzakelijke niveau van robuustheid vast

4. **Robuustheid:** Stel op basis van de risicobeoordeling vast wat het minimaal gewenste/noodzakelijke robuustheidsniveau is (*zero, basic, standard, enhanced of strict*). Zie nadere uiteenzetting in hoofdstuk 7.

Stap 4: Breng de overige belangen in kaart

5. **Veiligheid:** Aan welke beveiligingsrisico's worden gebruikers mogelijk blootgesteld?
6. **Privacy en gegevensbescherming:** Wat is de impact van de gekozen verificatiemethode op privacy en de bescherming van persoonsgegevens?
7. **Inclusiviteit en toegankelijkheid:** Hoe beïnvloedt de gekozen verificatiemethode de inclusiviteit en toegankelijkheid van een dienst? Moet gezien de aard van de dienst extra aandacht worden besteed aan vrije / laagdrempelige toegang? Is de verificatiemethode bruikbaar voor iedereen?
8. **Transparantie:** Hoe duidelijk is de werking van het verificatiesysteem voor de gebruikers?
9. **Minimale vereisten:** Bekijk op basis van uw analyse aan welke minimale vereisten een systeem van leeftijdsverificatie zou moeten voldoen. Verdere uitwerking van de aspecten en de bijbehorende eisen staan in hoofdstuk 6.

Stap 5: Weeg de belangen af

10. Weeg op basis van de verschillende vereisten af welke methode(n) voor leeftijdsverificatie het meest geschikt zijn, kies daarbij de variant die het minst ingrijpt in de andere belangen (inclusiviteit, privacy, veiligheid).
11. Beoordeel of de inzet van de gekozen methode proportioneel is, indachtig de invloed die de verificatiemethode heeft op de andere belangen.

3 Juridisch kader

3.1 Relevante wetgeving

Er zijn verschillende wetten die ingaan op leeftijd en toegang tot digitale producten en diensten. Dit juridisch kader bevat een overzicht van verschillende relevante wetten en de mogelijke implicaties die daaruit volgen voor de inzet van leeftijdsverificatie ten behoeve van het reguleren van de toegang tot onlineplatforms.

Er zijn verschillende fundamentele rechten die hierbij van belang zijn, zoals de rechten van het kind, het recht op bescherming van de persoonlijke levenssfeer, het recht op informatie en de vrijheid van meningsuiting. Paragraaf 3.1.1 legt deze grondrechten uit aan de hand van het Handvest van de grondrechten van de Europese Unie ("**EU Handvest**").

Sommige content of zaken worden geacht zo schadelijk te zijn voor minderjarigen dat bij wet is verboden deze content of zaken aan hen aan te bieden. Paragrafen 3.1.2, 3.1.3 en 3.1.4 gaan derhalve in op respectievelijk de **Wet op de Kansspelen**, het **Tabaks – en Rookwarenbesluit** en de **Alcoholwet**.

De Digital Services Act ("**DSA**") en de Richtlijn Audiovisuele Media Diensten ("**AVMD-richtlijn**" en "**Mediawet**") stellen dat aanbieders van onlineplatformdiensten passende en evenredige maatregelen moeten nemen om minderjarigen te beschermen, door bijvoorbeeld leeftijdscontroles te gebruiken. Paragrafen 3.1.5 en 3.1.6 leggen beide stukken wetgeving nader uit. Hierbij gaan we ook in op de strafrechtelijke bepalingen ter bescherming van kinderen.

Om leeftijdscontroles op een betrouwbare manier uit te voeren op afstand, is het waarschijnlijk dat er persoonsgegevens worden verwerkt. Op grond van de Algemene Verordening Gegevensbescherming ("**AVG**)" worden persoonsgegeven rechtmatig verwerkt wanneer zij voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verwerkt en er een passende rechtsgrond (grondslag) voor de verwerking aan te wijzen is.[1] Bovendien gelden er strengere eisen wanneer er sprake is van de verwerking van persoonsgegevens van minderjarigen en wanneer er bijzondere categorieën van persoonsgegevens worden verwerkt. Paragraaf 3.1.8 gaat in op algemene verplichtingen die volgen uit de AVG en biedt belangrijke kaders voor de verantwoorde inzet van online leeftijdsverificatie.

Bij identificatie op afstand is het voor zowel de organisatie die de identificatie inzet als voor de persoon die geïdentificeerd wordt belangrijk om te kunnen vertrouwen dat persoonsgegevens veilig zijn en dat de verificatie op afstand betrouwbaar en robuust is. De eIDAS-Verordening ("**eIDAS**") tracht harmonisatie aan te brengen binnen de EU op het gebied van digitale identificatie (ook wel e-Identificatie) en beoogt vertrouwen te creëren in de betrouwbaarheid van identificatiemehoden door middel van gemeenschappelijke technische standaarden en certificeringsmechanismen. Paragraaf 3.1.8 legt in het kort uit wat de eIDAS-Verordening inhoudt.

[1] Raadpleeg artikel 5, eerste lid, onder a en b van de AVG en artikel 6 AVG.

3.1.1 Handvest van de grondrechten van de Europese Unie

In het EU Handvest worden de grondrechten uiteengezet die personen binnen de Europese Unie genieten.[2] In het Handvest wordt onderscheid gemaakt tussen positieve en negatieve verplichtingen, waarbij positieve verplichtingen inmenging vereisen van de overheid om een bepaald recht van burgers te beschermen, terwijl een negatieve verplichting inhoudt dat de overheid zich niet mag bemoeien met de burger. Dergelijke verplichtingen werken niet alleen verticaal (tussen overheid en burger) maar ook horizontaal (tussen bijvoorbeeld het kind en de ouders en het platform). Bij online leeftijdsverificatie bij kinderen speelt een aantal van deze grondrechten een rol.

Er zijn mogelijk verschillende grondrechten in het geding bij het gebruik van digitale diensten door kinderen. Allereerst kent het Handvest een zelfstandig grondrecht gericht op de bescherming van kinderen.[3] Daarnaast gelden de overige grondrechten zoals het recht op privacy, het recht op de vrijheid van meningsuiting en de vrijheid van gedachte, geweten en godsdienst ook voor kinderen bij het gebruik van digitale diensten. Daarbij hebben overheden en private organisaties een positieve verplichting, zoals het beschermen van kinderen tegen schadelijke content online. Een methode om kinderen te beschermen tegen schadelijke content is het instellen van online leeftijdsverificatie, omdat op die manier voorkomen kan worden dat minderjarigen toegang krijgen tot de schadelijke content. Tegelijkertijd kunnen verschillende methoden van online leeftijdsverificatie ook gevolgen hebben voor de bescherming van andere fundamentele rechten, bijvoorbeeld het recht op privacy en bescherming van persoonsgegevens van het kind.[4]

Het beperken van de online vrijheid van kinderen kan daarnaast hun zelfexpressie, persoonlijke ontwikkeling en persoonlijke autonomie belemmeren. Er kan bijvoorbeeld sprake zijn van een beperking van de persoonlijke ontwikkeling en persoonlijke autonomie van minderjarigen wanneer zij toestemming nodig hebben van hun ouders of verzorgers voordat zij toegang verkrijgen tot bepaalde informatie online.[5] Indien er bij de verificatiemethoden persoonsgegevens worden verwerkt op basis van de grondslag toestemming, dient de toestemming te worden gegeven door personen met het ouderlijk gezag.[6] Mogelijk voelen kinderen zich niet vrij hun ouders of verzorgers te verzoeken om toestemming voor de verwerking van hun persoonsgegevens wanneer deze toestemming gevraagd wordt om toegang tot bepaalde content te reguleren die gevoelig ligt binnen hun gezinssituatie, zoals bijvoorbeeld informatie over seksualiteit, religie of andere vormen van zelfexpressie.

Naast de rechten van het kind kunnen ook de rechten van andere personen in de samenleving worden geraakt. Leeftijdsverificatie betekent dat iedereen die van de dienst gebruik maakt aan de verificatie moet worden onderworpen. Daarmee is bijvoorbeeld niet alleen de privacy van het kind in het geding, maar ook die van andere gebruikers van de dienst.

---

[2] Naast het Handvest speelt het Europees Verdrag voor de Rechten van de Mens (EVRM) een zeer belangrijke rol binnen de Europese en Nederlandse rechtsorde.
[3] Artikel 24 van het EU Handvest.
[4] Artikel 8 van het EU Handvest.
[5] Artikel 6 van het EU Handvest.
[6] Dit volgt uit artikel 8, eerste lid, van de AVG. Andere grondslagen die gebruikt zouden kunnen worden voor leeftijdsverificatie zijn het gerechtvaardigd belang (6f AVG), of wanneer er sprake is van een wettelijk verplichte leeftijdsverificatie, de wettelijke plicht (6c AVG). Tenslotte zou de uitvoer van de overeenkomst (6b AVG) een grondslag kunnen bieden, maar daarvoor is het wel van belang dat een kind bekwaam wordt geacht om dergelijke overeenkomsten te sluiten.

3.1.2 Wet op de kansspelen

De Wet op de kansspelen stelt regels voor aanbieders van goksites. Het doel van deze wet is om mensen te behoeden voor risico's van dergelijke goksites, zoals het risico op verslaving en het verliezen van geld. Minderjarigen zijn, in lijn met de AVG, een bijzonder kwetsbare groep die aanvullende bescherming behoeven tegen dergelijke risico's. Er gelden strenge regels met betrekking tot (leeftijds)verificatie om toegang tot kansspelen te beperken. Het Besluit Kansspelen op afstand geeft nadere invulling aan de Wet op de kansspelen in een online context en legt aan vergunninghouders de verplichting op om het BSN-nummer te verwerken. Dit is een zeer robuuste wijze van leeftijdsverificatie en tegelijkertijd een wijze die zeer ingrijpend is voor de privacy van betrokkenen. Het BSN wordt beschouwd als een van de meest gevoelige persoonsgegevens en mag slechts worden verwerkt wanneer daar een wettelijke plicht toe is.

3.1.3 Alcoholwet

De Alcoholwet verbiedt het om alcohol te verkopen aan jongeren onder de achttien jaar, ook online. De nieuwe alcoholwet stelt echter niet al te strenge eisen aan online leeftijdsverificatie. De wet schrijft wel voor dat er een leeftijdsverificatiesysteem moet worden gehanteerd op het moment van aankoop, maar het aanvinken van een '18+ checkbox' of het invoeren van de geboortedatum is al voldoende. Het is aan de bezorger om vervolgens het WID-document te controleren of de klant de daadwerkelijke leeftijd heeft bereikt. Het Ministerie van Volksgezondheid, Welzijn en Sport heeft aangegeven in de toekomst te willen kijken naar andere opties voor leeftijdsverificatie waarmee de verkoper op afstand op een betrouwbare en eenduidige wijze de leeftijd van de koper kan verifiëren.[7]

3.1.4 Digital Services Act

De DSA bevat regels voor online platforms om de online verspreiding van illegale en schadelijke content tegen te gaan, om minderjarigen beter te beschermen en gebruikers meer keuze en betere informatie te geven. Online platforms kunnen al snel worden beschouwd als toegankelijk voor kinderen, wat ervoor zorgt dat deze platforms rekening moeten houden met de belangen van minderjarigen.[8] Zeer grote online platforms moeten de 'systemische risico's' van hun dienst in kaart brengen. Daar vallen ook risico's voor de rechten van minderjarigen onder.[9]

Aanbieders van zeer grote online platforms dienen te onderzoeken hoe kinderen via het platform kunnen worden blootgesteld aan inhoud die schadelijk kan zijn voor hun gezondheid en lichamelijke, geestelijke en morele ontwikkeling.[10] Dit kan bijvoorbeeld het geval zijn wanneer online interfaces zo ontworpen zijn dat zij opzettelijk of onopzettelijk misbruik maken van de zwakke punten of onervarenheid van minderjarige gebruikers, of die kunnen leiden tot verslaving.

De DSA stelt dat aanbieders van onlineplatforms die door minderjarigen worden gebruikt, passende en evenredige maatregelen moeten nemen om minderjarigen te beschermen, met inbegrip van instrumenten voor leeftijdscontrole en ouderlijk toezicht, of instrumenten om minderjarigen te helpen misbruik te melden of steun te krijgen.[11] Dit kan bijvoorbeeld worden gedaan door interfaces of delen daarvan zodanig

[7] Nota van toelichting over wijziging regels ter uitvoering van de Alcoholwet hoofdstuk 2.1, beschikbaar op https://www.rijksoverheid.nl/documenten/publicaties/2021/01/29/concept-nota-van-toelichting.
[8] Rechtsoverweging 71 van de preambule van de DSA
[9] Artikel 34 van de DSA
[10] Artikel 34 lid 1 sub a van de DSA
[11] Artikel 35 lid 1 sub j van de DSA

te ontwerpen dat standaard de hoogste mate van privacy, veiligheid en beveiliging voor minderjarigen wordt gewaarborgd.[12] Enerzijds noemt de DSA dat leeftijdscontroles gewenst zijn, terwijl anderzijds ook de hoogste mate van privacy gewaarborgd dient te worden. Dit kan een spanningsveld opleveren. Als bij leeftijdscontroles persoonsgegevens verwerkt moeten worden van minderjarigen, kan dat negatieve gevolgen hebben voor de bescherming van privacy.

3.1.5 Mediawet (AVMD Richtlijn)

De AVMD-richtlijn stelt, net als de DSA, dat passende maatregelen moeten worden genomen om minderjarigen tegen schadelijk content te beschermen, bijvoorbeeld leeftijdscontrole.[13] De AVMD-richtlijn stelt dat aanbieders van bijvoorbeeld videoplatformdiensten passende maatregelen moeten treffen ter bescherming van minderjarigen. Aanbieders moeten ervoor zorgen dat het media-aanbod de lichamelijke, geestelijke of morele ontwikkeling van minderjarigen niet aantast en dat aanbod alleen zo beschikbaar wordt gesteld dat minderjarigen dit normaliter niet te horen of te zien krijgen. De maatregelen die kunnen worden genomen zijn de selectie van tijd van de uitzending, instrumenten voor leeftijdscontrole, doeltreffend ouderlijk toezicht of andere maatregelen. Net als de DSA biedt de AVMD-richtlijn een grondslag om leeftijdsverificatie in te zetten voor de bescherming van minderjarigen ter voorkoming van blootstelling aan schadelijke content.

De AMVD-richtlijn is in de Mediawet geïmplementeerd. Hoofdstuk 4 van de Mediawet 2008 regelt de bescherming van jeugdigen daar waar het gaat om het tonen van content die schade kan toebrengen aan de lichamelijke, geestelijke of morele ontwikkelingen van de jeugdige. Wat als aanstootgevend voor minderjarigen moet worden beschouwd wordt via het systeem van leeftijdsclassificatie bepaald (artikel 4.2 Mediawet). In Nederland zijn de Kijkwijzer en de PEGI-rating de belangrijkste instrumenten voor leeftijdsclassificatie.[210] De Kijkwijzer biedt de Nederlandse consument een leeftijdsclassificatie voor films, series en televisieprogramma's. Voor interactieve media (games) wordt het Pan European Game Information System (PEGI) gehanteerd. De instelling die verantwoordelijk is voor het aanbod van audio-visuele inhoud (zoals bijvoorbeeld een omroep) moet zich verplicht aansluiten bij een van overheidswege goedgekeurd systeem van leeftijdsclassificatie (artikel 4.1 Mediawet).

3.1.6 Het Wetboek van Strafrecht[14]

Artikel 240a Sr stelt het tonen van aanstootgevende afbeeldingen en het aanbieden van dragers met deze afbeeldingen aan personen onder de 16 jaar strafbaar. Naast het tonen van beelden is ook het aanbieden of verstrekken van beelden aan minderjarigen strafbaar, alsmede het verstrekken van voorwerpen of dragers waarop deze beelden staan. Hierbij moet wel worden aangetekend dat de redactie van artikel 240a Sr een opzetvereiste impliceert. Dit betekent dat deze bepaling doorgaans niet van toepassing is op online diensten (omdat deze niet opzettelijk deze content zullen aanbieden aan jongeren).[15]

[12] Rechtsoverweging 71 van de preambule van de DSA
[13] Raadpleeg artikel 6 bis lid 1 van de AVMD richtlijn
[14] Tekst ontleend aan het Considerati rapport Immersieve technologieën (Schermer, B. W., van der Ham, J. (2021), *Regulering van immersieve technologieën*, WODC)
[15] Zie: Tekst & Commentaar Strafrecht, commentaar op Artikel 240 Sr

3.1.7 AVG

De AVG is van toepassing wanneer er sprake is van een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens.[16] Persoonsgegevens zijn gegevens die betrekking hebben op direct of indirect te identificeren persoon.[17] Een verwerking van persoonsgegevens is toegestaan wanneer daar een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel voor is,[18] er een rechtsgrond voor de verwerking is aan te wijzen[19] en de verwerking voorts voldoet aan bepaalde zorgvuldigheidsvereisten die zijn neergelegd in de AVG.[20]

De verwerking van persoonsgegevens dient noodzakelijk te zijn om de vooraf vastgestelde doeleinden te verwezenlijken, hetgeen betekent dat het niet is toegestaan om meer of meer gevoelige persoonsgegevens te verwerken dan nodig.[21] De afweging of een verwerking van persoonsgegevens 'noodzakelijk' is wordt gedaan aan de hand van een proportionaliteits- en subsidiariteitstoets. Een verwerking is proportioneel wanneer de inbreuk op de privacy van betrokkenen in verhouding staat tot het te bereiken doel. Een verwerking voldoet aan het subsidiariteitsbeginsel wanneer er geen minder ingrijpende manier voorhanden is om het beoogde doel te bereiken.

De AVG kwalificeert minderjarigen als een kwetsbare groep die extra bescherming behoeft.[22] Jongeren onder de 16 zijn zich mogelijk minder bewust van de risico's en gevolgen in verband met de verwerking van hun persoonsgegevens. Het is daarom ook in lijn met de AVG om online leeftijdsverificatie toe te passen. Tegelijkertijd ligt een disproportionele of overmatige verwerking van persoonsgegevens op de loer, bijvoorbeeld wanneer aanbieders van online platforms vanwege de leeftijdsverificatie meer of meer gevoelige persoonsgegevens gaan verwerken dan zij normaalgesproken zouden doen.

Om leeftijdsverificatie in te zetten, dienen aanbieders van onlineplatforms persoonsgegevens te verwerken. Om dit te kunnen doen heeft een aanbieder een grondslag nodig. Een van de grondslagen die passend is in de context van online leeftijdsverificatie is *toestemming*.[23] De persoon op wie de persoonsgegevens betrekking hebben dient voorafgaand aan de verwerking van de persoonsgegevens toestemming te verlenen. Op grond van artikel 5 lid 1 van de UAVG kunnen minderjarigen pas geldig toestemming verlenen wanneer zij de leeftijd van 16 jaar hebben bereikt. Kinderen onder de 16 jaar die toegang willen verkrijgen tot online diensten kunnen niet zelf toestemming verlenen voor het verwerken van persoonsgegevens ten behoeve van online leeftijdsverificatie om toegang te verkrijgen tot die online diensten. Een persoon die de ouderlijke verantwoordelijkheid draagt van het kind dient in plaats daarvan toestemming te verlenen.

Wanneer voor de verwerking van persoonsgegevens ten behoeve van online leeftijdsverificatie toestemming van een ouder of verzorgen nodig is kan het een uitdaging zijn om aan te tonen dat de

[16] Artikel 2 eerste lid van de AVG.
[17] Zie artikel 4 onder 1 van de AVG.
[18] Artikel 5 eerste lid onder b van de AVG.
[19] Zie artikel 5 eerste lid onder a AVG en een limitatieve opsomming van de rechtsgronden in artikel 6 eerste lid van de AVG.
[20] Zie artikel 5 eerste en tweede lid van de AVG voor een overzicht van de gegevensbeschermingsbeginselen die door de gehele AVG doorwerken. Deze beginselen worden in dit rapport nader uitgewerkt onder paragraaf 5.2.1.
[21] Het beginsel van dataminimalisatie (artikel 5, eerste lid onder c, AVG) houdt in dat verwerkingsverantwoordelijken niet meer persoonsgegevens mogen verwerken dan noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.
[22] Zij bijvoorbeeld overweging 75 bij de AVG.
[23] Afhankelijk van de situatie komen daarnaast de grondslagen noodzakelijk voor de uitvoering van de overeenkomst (6b AVG), wettelijke plicht (6c AVG) en het gerechtvaardigd belang van de verwerkingsverantwoordelijke (6f AVG) in beeld.

toestemming daadwerkelijk is verleend door de ouder of verzorger.[24] De AVG verplicht de verwerkingsverantwoordelijke om redelijke inspanningen te leveren om te controleren of de ouder toestemming heeft gegeven. Aannemelijk is dat de *redelijkheid* van de inspanning afhangt van de grootte van de risico's die gepaard gaan met de gegevensverwerking. Voor de verwerking van emailgegevens voor een nieuwbrief is in mindere mate inspanning nodig dan voor het verwerken van bijvoorbeeld gezondheidsgegevens.

Er geldt in beginsel een verwerkingsverbod op bijzondere categorieën van persoonsgegevens.[25] Binnen de context van online leeftijdsverificatie is met name de verwerking van de bijzondere categorie 'biometrische gegevens met het oog op de unieke identificatie van een persoon' relevant.[26] Het is slechts toegestaan bijzondere categorieën van persoonsgegevens te verwerken indien er een uitzonderingsgrond voor aan te wijzen valt.[27] Ook voor het verwerken van een BSN stelt de AVG nadere regels: dit moet gebaseerd zijn op een wettelijke verplichting. Dit kan ertoe leiden dat bepaalde technieken die betrouwbaar zijn voor de leeftijdsverificatie (zoals directe identificatie) moeilijker zijn toe te passen omdat het wringt met de bescherming van de persoonsgegevens.

3.1.8 eIDAS

Op Europees niveau wordt ook nagedacht over leeftijdsverificatie en privacy. De eIDAS Verordening stelt dat een gebrek aan vertrouwen ertoe leidt dat consumenten aarzelen om gebruik te maken van nieuwe diensten terwijl het opbouwen van vertrouwen in online-omgevingen als essentieel voor economische en sociale ontwikkeling worden geacht.[28] Om dit te waarborgen biedt de eIDAS de mogelijkheid tot elektronische identificatie binnen de EU. Hiermee kan men via deze elektronische identificatie online toegang krijgen tot verschillende diensten in de EU. Bij identificatie op afstand is het voor zowel de organisatie die de identificatie inzet als voor de persoon die geïdentificeerd wordt belangrijk om te kunnen vertrouwen dat persoonsgegevens veilig zijn en dat de verificatie op afstand betrouwbaar en robuust is. eIDAS tracht harmonisatie aan te brengen binnen de EU op het gebied van digitale identificatie (ook wel e-Identificatie) en beoogt vertrouwen te creëren in de betrouwbaarheid van identificatiemethoden door middel van gemeenschappelijke technische standaarden en certificeringsmechanismen. De eIDAS Verordening definieert drie niveaus van betrouwbaarheid voor stelsels van elektronische identificatie (laag, substantieel, hoog). Deze niveaus kennen specifieke vereisten qua procesmatige inrichting en beveiliging die gedefinieerd zijn in de uitvoeringshandelingen bij de eIDAS Verordening.[29] Afhankelijk van de gekozen leeftijdsverificatiemethode zijn deze vereisten direct of indirect relevant.

Er wordt momenteel in Europa gewerkt aan een opvolger voor de eIDAS Verordening: de eIDAS 2 Verordening. Deze Verordening ziet met name op het mogelijk maken van een Europese 'wallet' waarin

[24] Verwerkingsverantwoordelijken hebben op grond van artikel 5 tweede lid AVG een verantwoordingsplicht. Dit houdt in dat zij moeten kunnen aantonen te voldoen aan de verplichtingen van de AVG, waaronder in dit geval dat zij toestemming hebben verkregen van degene met het ouderlijk gezag.
[25] Raadpleeg artikel 9 eerste lid van de AVG voor een overzicht van de bijzondere categorieën van persoonsgegevens.
[26] Raadpleeg artikel 4 onder 14 van de AVG voor een definitie van biometrische gegevens.
[27] Deze uitzonderingsgronden staan opgenomen in artikel 9 tweede lid van de AVG.
[28] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[29] Zie: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32015R1502&from=EN

burgers hun identiteitsdocumenten kunnen opslaan. Deze infrastructuur zou ook voor leeftijdsverificatie kunnen worden gebruikt.

4 Methoden online leeftijdsverificatie

Online leeftijdsverificatie kan gezien worden als een beheersmaatregel (ook wel 'mitigerende maatregel') ter bestrijding van de risico's van online diensten voor kinderen. Zoals benoemd, is er geen *one-size-fits-all* methode van leeftijdsverificatie, maar is het kiezen van de juiste methode sterk afhankelijk van de context. Zo kan het voorkomen dat vanwege een hoog risico op illegale of schadelijke content een methode gewenst is met een hoog robuustheidsniveau. Content kan worden aangemerkt als mogelijk schadelijk doordat het gewelddadig is, maar bijvoorbeeld ook doordat het seksueel van aard is. In beide gevallen zou je kunnen stellen dat een hoog niveau van robuustheid gewenst is, maar toch zal niet dezelfde methode optimaal zijn. Bij gewelddadige content zou de methode van toestemming door ouderlijk gezag mogelijk een goede oplossing zijn. Met betrekking tot content van seksuele aard is dit mogelijk niet de meest geschikte methode, omdat kinderen vanaf een zekere leeftijd ook vrijheid moeten hebben om bijvoorbeeld hun seksuele geaardheid te kunnen onderzoeken. Toestemming van de ouders zou hier een te grote drempel kunnen zijn.

In dit hoofdstuk zullen we categorieën van verificatiemethoden bespreken en daarbij verwijzen naar voorbeelden van concrete methoden van leeftijdsverificatie. Wij zullen een indeling gebruiken die ook in het Verenigd Koninkrijk wordt gebruikt.[30] We bespreken nu eerst de indeling van de verschillende categorieën van leeftijdsverificatie methoden.

4.1 Identificatie

Identificatie is een methode voor het bepalen van iemands leeftijd met een hoge mate van accuraatheid. We onderscheiden twee manieren van identificatie:

Directe identificatie: dit is een methode waarbij de gebruiker zich identificeert op basis van een officieel identificatiemiddel (een *primary credential*) dat daartoe is uitgegeven door een (bij wet) aangewezen autoriteit, meestal een overheid. Het bekendste voorbeeld is het paspoort dat door de Nederlandse overheid wordt uitgegeven.

Afgeleide identificatie: de gebruiker identificeert zich met behulp van een middel (een *secondary credential*) dat aan hen is uitgereikt door een organisatie die zich bij de uitgifte van het middel heeft gebaseerd op een officieel identificatiemiddel. Een voorbeeld van leeftijdsverificatie op basis van afgeleide identificatie is de dienst iDIN.[31] Bij dit middel faciliteren banken het opvragen van de geboortedatum van een gebruiker. Deze geboortedatum is ontleend aan het officiële identificatiemiddel dat de gebruiker heeft moeten overleggen bij het openen van de rekening.

Directe identificatie vond tot enkele jaren geleden primair plaats door controle van het daadwerkelijke fysieke document (bijvoorbeeld het paspoort). Inmiddels kan ook van digitale identificatiemiddelen gebruikt worden gemaakt. Wanneer er gebruik wordt gemaakt van een digitale oplossing voor het identificeren van een persoon spreken we ook wel van *digital identity solutions*. Aanbieders van dergelijke

[30] https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf
[31] 'iDIN', https://www.idin.nl/

oplossingen worden *digital identity providers* of *identity service providers* genoemd. Het eerder genoemde iDIN is een voorbeeld van een *digital identity solution* op basis van een afgeleide identiteit.

4.2 Leeftijdsinschatting

Bij leeftijdsinschatting refereren we aan methoden die een inschatting maken van iemands leeftijd, vaak door gebruik van algoritmen. Methodes van leeftijdsinschatting zijn onder meer:

Biometrische analyse: een inschatting van leeftijd op basis van Artificiële Intelligentie (AI), denk bijvoorbeeld aan inschatting op basis van een foto.

Gedragsanalyse: gedragspatronen en interactie van de gebruiker op het platform worden gebruikt om leeftijd in te schatten.

Linguïstische analyse: inschatting van leeftijd op basis van geschreven taal.

Profilering: online activiteit of browsergeschiedenis wordt geëvalueerd om leeftijd in te schatten.

4.3 Accountbevestiging

Met accountbevestiging kan een reeds bestaande accounthouder bevestigen of een andere gebruiker ouder of jonger is dan 18 jaar. Een voorbeeld hiervan is dat in een gezinsaccount de hoofdaccounthouder (bijvoorbeeld de ouder of voogd) de leeftijd kan bevestigen van de personen die de andere accountprofielen gebruiken (zoals de kinderen). De dienst kan dan op een leeftijdsgerichte manier worden toegepast op elke gebruiker. Het is hier dan wel essentieel dat het systeem gezagsverhoudingen moet kunnen aantonen. Gezagsverhoudingen staan geregistreerd in de Basisregistratie Persoonsgegevens (BRP, BRP ontleent de gegevens over gezag aan het openbaar gezagsregister).

4.4 Zelfverklaring

Zelfverklaring is wanneer een gebruiker zijn/haar leeftijd kan aangeven, maar geen bewijs hoeft te leveren ter bevestiging ervan, bijvoorbeeld door het aanvinken van een check box.

In hoofdstuk 6 zullen we de minimale eisen en overwegingen uiteenzetten voor de verschillende categorieën van leeftijdsverificatiemethoden zoals hierboven beschreven.

5 Risico's voor kinderen online

Om een goede afweging te maken ten aanzien van een online leeftijdsverificatiesysteem is het zinvol om eerst stil te staan bij de risico's die kinderen kunnen lopen bij het gebruik van digitale diensten. Hierbij wordt uitgegaan van de risico's die zijn beschreven in de Kinderrechten Impact Assessment.

5.1 Risicoclassificatie Kinderrechten Impact Assessment

De mogelijk negatieve impact van digitale diensten op de rechten en welzijn van kinderen wordt behandeld aan de hand van de in de mediawetenschappen ontwikkelde risicoclassificatie van de 4C's (content risks, conduct risks, contact risks, consumer risks) en cross-cutting risks (advanced technology risks, health risks, privacy risks)[32]. De hieronder weergeven risico's zijn allen afkomstig uit het Kinderrechten Impact Assessment. Het betreft hier een samenvatting[33].

5.1.1 Content Risks[34]

Onder 'content risks' worden situaties begrepen waarin *"het kind passief inhoud ontvangt of wordt blootgesteld aan inhoud die beschikbaar is voor alle internetgebruikers"*[35]. Meer concreet worden kinderen blootgesteld aan inhoud die illegaal, haatdragend en potentieel schadelijk is. Illegale inhoud betreft inhoud waarvan de verspreiding algemeen bij wet verboden is om alle burgers, niet alleen kinderen, te beschermen. Schadelijke inhoud is inhoud die de wet niet overtreedt en dus strikt genomen niet illegaal is, maar niettemin een risico vormt voor kinderen omdat zij een negatief effect kunnen hebben op de gezondheid en het welzijn van kinderen.

5.1.2 Conduct risk[36]

Onder 'conduct risks' worden situaties begrepen waarbij kinderen risico's creëren voor zichzelf of andere kinderen[37]. Deze gedragingen kunnen bestaan uit het zelf plaatsen van illegale, haatdragende of schadelijke inhoud. Ook kan er sprake zijn van anderszins problematisch gedrag, zoals het meedoen aan gevaarlijke online challenges.

5.1.3 Contact risk[38]

Onder 'contact risks' vallen de situaties waarin kinderen risico lopen tijdens de interactie met anderen[39]. Het gaat dan bijvoorbeeld om seksueel misbruik, cyberpesten, hatelijke of toxische gedragingen van

[32] Children in the Digital Environment: Revised Typology of Risks. OECD; 2021 Jan. Available: https://www.oecd-ilibrary.org/docserver/9b8f222e-en.pdf? expires=1678964855&id=id&accname=guest&checksum=D7F9A773A74CAD9FBA981F43DA9B348E
[33] Zie voor een verder uitwerking van de risico's het rapport Hof, Simone van der & Mr. J. de Bruin (2023) Impact en juridische analyse t.b.v. de ontwikkeling van de KIA, p. 9-21
[34] Hof, Simone van der & Mr. J. de Bruin (2023) Impact en juridische analyse t.b.v. de ontwikkeling van de KIA, p. 9-11
[35] The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. Paris: OECD; 2011. Report No.: . doi:10.1787/5kgcjf71pl28-en.
[36] Hof, Simone van der & Mr. J. de Bruin (2023) Impact en juridische analyse t.b.v. de ontwikkeling van de KIA, p. 11-12
[37] The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. Paris: OECD; 2011. Report No.: . doi:10.1787/5kgcjf71pl28-en
[38] Prof. Dr. Mr. Van der Hof, S & Mr. de Bruin, J. (2023) Impact en juridische analyse t.b.v. de ontwikkeling van de KIA, p. 13
[39] OECD. (2021). Children in the Digital Environment: Revised Typology of Risks. OECD; 2021 Jan. Available: https://www.oecd-ilibrary.org/ docserver/9b8f222e-en.pdf? expires=1678964855&id=id&accname=guest&checksum=D7F9A773A74CAD9FBA981F43DA9B348E.

anderen of online fraude. Kinderen die zelf content maken kunnen ook te maken krijgen met 'contact risks' wanneer ze hun activiteiten online streamen of publiceren.

5.1.4 Consumer risks[40]

Onder 'consumer risks' worden situaties begrepen waarin kinderen in hun hoedanigheid als consument risico lopen[41]. In beginsel zijn kinderen bij het gebruik van digitale diensten per definitie consument, aangezien deze diensten vrijwel zonder uitzondering commercieel worden aangeboden. Consumentenrisico's kunnen zich onder andere voordoen in de vorm van oneerlijke handelspraktijken, zoals het verleiden of dwingen van kinderen tot het doen van in-app aankopen die ze liever niet hadden gedaan, of het gebruiken van virtuele valuta waardoor de daadwerkelijke waarde van virtuele items niet altijd duidelijk is.

5.1.5 Cross-cutting risks[42]

'Cross-cutting risks' zijn risico's die zich door alle voorgaande categorieën risico's kunnen voordoen en die deze risico's – in onderlinge samenhang – voor kinderen mogelijk kunnen vergroten. Hieronder vallen:

- *Advanced technology risks*; situaties waarin risico's ontstaan voor kinderen met het voortschrijden van de technologie.
- *Privacy risks*; het verwerken van persoonsgegevens van kinderen.
- *Health risks*; risico's waarbij de specifieke vormgeving van digitale diensten schadelijk zijn voor de fysieke en mentale gezondheid van kinderen.

5.2 Online leeftijdsverificatie als beheersmaatregel bij risico's

Wie gebruik maakt van de Kinderrechten Impact Assessment wordt gevraagd om voor hun digitale dienst een inschatting te maken van de risico's die een minderjarige gebruiker van de betreffende dienst mogelijk loopt. Na het in kaart brengen van deze risico's formuleert de ontwikkelaar van een digitale dienst zogenaamde 'mitigerende maatregelen'. Dit zijn maatregelen die kunnen helpen bij het voorkomen of verminderen van de gedetecteerde risico's. Het invoeren van een systeem van online leeftijdsverificatie is daarbij een van de mogelijke opties.

Het instellen van een adequaat leeftijdsverificatiesysteem kan een goede beheersmaatregel zijn om bovengenoemde risico's te voorkomen. Of dit ook daadwerkelijk nodig is hangt af van een aantal factoren. Denk daarbij aan de hoogte van het risico (= kans x impact) en daarnaast eventuele anderen maatregelen die genomen zijn om dit risico op een andere manier te verkleinen. Ook kan leeftijdsverificatie ongewenst zijn. Denk aan situaties waarbij privacy en anonimiteit op internet van het allergrootste belang zijn, bijvoorbeeld voor jongeren die hun seksuele, levensbeschouwelijke of politieke identiteit aan het verkennen zijn en daarover informatie willen zoeken op internet.

[40] Prof. Dr. Mr. Van der Hof, S & Mr. de Bruin, J. (2023). Impact en juridische analyse t.b.v. de ontwikkeling van de KIA, p. 14-15
[41] OECD. (2021). Children in the Digital Environment: Revised Typology of Risks. OECD; 2021 Jan. Available: https://www.oecd-ilibrary.org/docserver/9b8f222e-en.pdf?expires=1678964855&id=id&accname=guest&checksum=D7F9A773A74CAD9FBA981F43DA9B348E & OECD. (2011). The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. Paris: OECD; 2011. Report No.: . doi:10.1787/5kgcjf71pl28-en.
[42] Prof.dr.mr. van der Hof, S. & Mr. de Bruin, J. (2023) Impact en juridische analyse t.b.v. de ontwikkeling van de KIA, p. 16-20

6 Relevante aspecten bij de toepassing van leeftijdsclassificatie

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft in het voorjaar van 2023 een aantal experttafels georganiseerd om globaal in kaart te brengen welke eisen aan leeftijdsverificatie gesteld moeten worden. Uit de rondetafelgesprekken zijn vier aspecten (belangen of waarden) naar voren gekomen die belangrijk zijn om in overweging te nemen bij het implementeren van online leeftijdsverificatiesystemen: robuustheid, privacy, veiligheid en inclusiviteit. Op basis van *desk research* kan hier nog een vijfde aspect aan worden toegevoegd: transparantie.

Deze aspecten kunnen een rol spelen bij de keuze voor een methode van leeftijdsverificatie in een concreet geval. Wat daarbij in het bijzonder relevant is, is dat deze aspecten op gespannen voet met elkaar kunnen staan. Bij de keuze voor een verificatiemethode in een specifiek geval moet telkens worden gewogen welke aspecten (belangen) zwaarder wegen. In concreto gaat het met name om de weging van het aspect robuustheid ten opzichte van de andere aspecten. Zo kan een zeer robuuste verificatiemethode bijvoorbeeld botsen met privacy of inclusiviteit.

6.1 Robuustheid

Bij robuustheid gaat het om de mate waarin de leeftijd van een gebruiker met zekerheid kan worden vastgesteld. Enerzijds gaat het dan om de accuraatheid van het systeem zelf, anderzijds om de vraag of het systeem gemakkelijk te omzeilen is. Hoe robuust een systeem moet zijn, is afhankelijk van de aard van de dienst en de risico's die daarmee gepaard gaan. Als het risico op schadelijke content laag is, of reeds via andere maatregelen gemitigeerd is, dan is het wellicht niet nodig om een strenge leeftijdsverificatie toe te passen. Het is zinvol om hier per geval tot een afweging te komen, omdat een strenge vorm van leeftijdsverificatie nadelen kan hebben op het gebied van privacy of toegankelijkheid.

6.1.1 Minimale eisen

Niet elk leeftijdsverificatiesysteem is even robuust. ISO werkt momenteel aan een classificatie van de robuustheid voor leeftijdsverificatiesystemen. Wij bespreken deze classificatie en de koppeling daarvan in het volgende hoofdstuk.

6.2 Privacy en gegevensverwerking

Een essentieel onderwerp voor de inzet van leeftijdsverificatie is de invloed die het heeft op de bescherming van persoonsgegevens van betrokkenen en die van minderjarigen in het bijzonder. Hoewel de verschillende methoden van leeftijdsverificatie gericht zijn op het beschermen van kinderen en minderjarigen is het van belang te realiseren dat iedereen die toegang wil hebben tot bepaalde online content wordt onderworpen aan de gekozen methode.

De inzet van het leeftijdsverificatiemiddel moet elke keer worden afgewogen tegen de risico's ten aanzien van de bescherming van persoonsgegevens. Hierbij dient te worden vermeld dat een zeer hoog niveau van betrouwbaarheid van leeftijdsverificatie, tegelijkertijd kan leiden tot een grotere inbreuk op privacy en de bescherming van persoonsgegevens. Dit geldt niet alleen voor minderjarigen, maar voor alle gebruikers van de digitale dienst.

6.2.1 Minimale eisen

De AVG geeft het kader voor de rechtmatige verwerking van persoonsgegevens. Om aan de AVG te voldoen moeten deze beginselen, die in artikel 5 van de AVG zijn neergelegd, in acht worden genomen. Het is voor de manier van leeftijdsverificatie dan ook van belang om deze te toetsen aan de beginselen om te zien in hoeverre de leeftijdsverificatiemechanismen de bescherming van persoonsgegevens aantasten. De AVG stelt dat de volgende eisen:

- De verwerking van persoonsgegevens dient *rechtmatig, behoorlijk en transparant* te zijn. Dit betekent dat de gebruiker van een leeftijdsverificatie systeem een rechtmatige grondslag moet hebben om de persoonsgegevens te verwerken en dat de verwerking op een transparante wijze dient te geschieden. De verwerkingsverantwoordelijke moet de betrokkenen inlichten over de wijze waarop de persoonsgegevens worden verwerkt. De informatie die wordt verstrekt over de verwerking dient eenvoudig toegankelijk en begrijpelijk te zijn.
- De persoonsgegevens dienen voor *welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden* te worden verwerkt en ook deze doeleinden dienen te worden gecommuniceerd naar de betrokkene. De verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, is alleen toegestaan indien de verwerking verenigbaar is met de doeleinden van de aanvankelijke verzameling van persoonsgegevens.
- Er moet worden voldaan aan het principe *van minimale gegevensverwerking (dataminimalisatie)*. Dit houdt in dat de verwerkingsverantwoordelijke het verzamelen van persoonsgegevens toereikend moet zijn, terzake dienend en beperkt tot wat noodzakelijk is om het vastgestelde doel te bereiken.
- Ook dient de verwerking van persoonsgegevens *juist en accuraat* te zijn. Dit betekent dat de persoonsgegevens dus ook de juiste persoonsgegevens dienen te zijn. Bij leeftijdsverificatie in het bijzonder speelt dit een grote rol.
- De persoonsgegevens mogen *niet langer worden bewaard dan noodzakelijk* is voor het doel waar de persoonsgegevens voor worden verwerkt. Een uitzondering op dit beginsel kan plaatsvinden, indien de persoonsgegevens in het algemeen belang, wetenschappelijk of historisch onderzoek, of statistische doeleinden worden gearchiveerd.
- Tot slot dienen de persoonsgegevens op een *juiste wijze te worden beschermd* door de verwerkingsverantwoordelijke tegen onrechtmatige verwerkingen. Om deze bescherming te waarborgen, dient de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen te nemen.

Of een leeftijdsverificatie methode rechtmatig is moet aan de hand van omstandigheden van het geval worden bekeken.

6.3 Veiligheid

Veiligheid ziet op de mate waarin de integriteit, vertrouwelijkheid en beschikbaarheid van het leeftijdsverificatiesysteem en de daarbinnen verwerkte (persoons)gegevens zijn gewaarborgd. Veiligheid is allereerst van belang voor de robuustheid van het systeem: wanneer het systeem niet veilig is, dan kan het ook niet robuust zijn. Daarnaast is veiligheid relevant voor de bescherming van de gegevens van de gebruikers. Bij leeftijdsverificatie kunnen gevoelige gegevens worden gebruikt, het systeem moet daarom voldoende veilig zijn.

6.3.1 Minimale eisen

- Systeem moet passende technische en organisatorische maatregelen gebruiken om persoonsgegevens te beveiligen;
- Naarmate de gevoeligheid van de gedeelde gegevens (die nodig zijn voor de leeftijdsverificatie) groter wordt, zal de veiligheid ter bescherming en zorgvuldige verwerking van deze gegevens hoger moeten zijn;
- Wanneer gekozen wordt voor de inzet van kunstmatige intelligentie (AI) voor leeftijdsverificatie, moet een organisatie over verschillende risico's nadenken met betrekking tot het verwerken van gegevens.
    - De organisatie moet een afweging maken tussen transparantie en veiligheid. Beschikbaarheid van technische informatie kan het mogelijk maken om data-subjecten te herleiden middels 'model inversion';
    - Accuraatheid: oftewel, welke mate van vals positieven of negatieven is acceptabel;
    - Bias: bij de inzet van AI kan sprake zijn van 'bias'. Dit dient zoveel mogelijk te worden voorkomen en op worden getest.

Wij gaan op iets meer detail in op de beveiligingsvereisten in het volgende hoofdstuk.

6.4 Inclusiviteit en toegankelijkheid

Bij het introduceren van een leeftijdsverificatie systeem is het essentieel dat het systeem inclusief en toegankelijk is. Binnen onze maatschappij is de toegang tot digitale diensten van groot belang, in sommige gevallen zijn er zelfs geen alternatieven meer voor digitale dienstverlening. Incorrecte uitsluiting van een digitale dienst kan daarom verstrekkende gevolgen hebben voor een persoon. Er zijn verschillende factoren die kunnen leiden tot dergelijke uitsluiting, waaronder het ontbreken van officiële documentatie, digitale ongeletterdheid en of ontoereikende toegang tot digitale apparatuur (zoals laptops en mobiele telefoons) die gebruikt worden voor leeftijdsverificatie. Vooral kwetsbare demografische groepen, zoals ouderen, mensen met beperkte financiële middelen en ongedocumenteerden worden hier sneller door getroffen. Ook is het voor een goede toegankelijkheid wenselijk dat een systeem interoperabel of gestandaardiseerd is en dat een gebruiker zelf kan kiezen voor een 'wallet' of methode die tot zijn of haar beschikking is (en dus niet gedwongen wordt om veel verschillende wallets te installeren). Het is daarom essentieel dat in het gebruik van systemen voor leeftijdsverificatie rekening wordt gehouden met de verschillende factoren die kunnen leiden tot incorrecte uitsluiting van digitale diensten.

6.4.1 Minimale eisen

- Het systeem moet voor iedereen te gebruiken zijn en zo min mogelijk drempels voor de toegang opwerpen, idealiter is het systeem gratis in het gebruik;
- Het systeem moet gebruikers zo min mogelijk afschrikken van het gebruik van de dienst;
- Het systeem moet interoperabel zijn;
- Het systeem moet makkelijk te begrijpen en te gebruiken zijn;
- De werking van het systeem moet duidelijk uitgelegd worden aan gebruikers, in het bijzonder minderjarigen;
- Gebruikers moeten niet onterecht uitgesloten worden van voor hen relevante content (accuraatheid);

Met betrekking tot met name de laatste twee eisen geldt dat de toepassing van een leeftijdsverificatie systeem in belangrijke mate contextafhankelijk is. Zo dient voorkomen te worden dat informatie die voor een kind relevant is (denk bijvoorbeeld aan informatie betreffende seksualiteit) achter een verificatie systeem verdwijnt dat hen onterecht de toegang tot deze informatie ontzegt.

6.5 Transparantie

In deze context is het waarborgen van transparantie essentieel, omdat het gebruikers in staat stelt om op de hoogte te zijn van zowel de beweegredenen van een aanbieder van een digitale dienst als de procedures die ten grondslag liggen aan leeftijdsverificatie. Het verschaffen van duidelijke informatie vergroot de waarschijnlijkheid van begrip en kans op medewerking van de gebruikers aanzienlijk. Hierdoor zijn ze beter in staat om de noodzaak van deze maatregel te begrijpen, namelijk het beschermen van minderjarigen tegen ongepaste content, met als gevolg dat ze eerder geneigd zullen zijn om (waarheidsgetrouw) deel te nemen aan het verificatieproces.

Om transparantie te bevorderen in het proces van leeftijdsverificatie, zijn de volgende minimale eisen van belang:

- Voordat gebruikers toegang krijgen tot (eventuele leeftijdsbeperkte) online content, goederen of diensten, moeten er vooraf waarschuwingen worden weergegeven, waar duidelijk aangegeven moet worden dat er een leeftijdscontrole zal plaatsvinden voordat toegang wordt verleend.[43]
- De gebruiker moet duidelijk geïnformeerd worden over welke normen en kenmerken worden gehanteerd om de leeftijd te verifiëren.[44] Hier moet ook vermeld worden welke vorm van leeftijdsverificatie wordt gehanteerd, en waarom er voor deze methode is gekozen.

6.6 Overige ontwerpprincipes

Naast de minimale eisen voor de aspecten hierboven beschreven, zijn er ook nog andere ontwerpprincipes die helpen bij het ontwikkelen van een geschikte vorm van leeftijdsverificatie.

- Monitoring en noodzakelijke aanpassingen: de methode die wordt gebruikt voor leeftijdsverificatie moet periodiek worden geëvalueerd. Bij deze evaluatie moet zowel gekeken worden naar de effectiviteit van de methode: doet het nog steeds waarvoor het bedoeld is. Daarnaast verandert de omgeving en context waarin de methode is geïmplementeerd, dus ook daar moet op worden gemonitord en indien nodig aanpassingen getroffen.

6.7 Tussenconclusie

Bij de keuze voor een leeftijdsverificatie systeem spelen verschillende overwegingen een rol. Bij deze voor een systeem moet rekening worden gehouden met de vraag hoe robuust een systeem is en welke consequenties het gekozen systeem heeft voor andere waarden en belangen. Daarbij staat de robuustheid van het systeem mogelijk tegenover belangen als privacy, inclusiviteit (toegankelijkheid) en veiligheid.

[43] Age Check Certification Scheme. (2020). Technical Requirements for Age Check Systems ACCS 4: 2020. Retrieved on 18/8/2023 at https://www.accscheme.com/media/ofnggwsn/accs-4_2020_agechecksystem.pdf
[44] Ibid.

7 Classificatie robuustheid leeftijdsverificatie

Robuustheid kan op verschillende manieren gedefinieerd worden. Er is (nog) geen internationale standaard voor het vaststellen van de robuustheid van een leeftijdsverificatiesysteem. Wel wordt in onder andere IEEE en ISO verband momenteel gewerkt aan standaarden.[45] Daarnaast zijn er gepubliceerde standaarden over de implementatie van leeftijdsverificatie, maar deze zien op de bredere implementatie, niet specifiek op de robuustheid.[46] Wij nemen de ISO Working Draft standaard voor leeftijdsverificatie als uitgangspunt voor het definiëren van robuustheidsniveaus omdat deze specifiek gaat over robuustheid en publiek toegankelijk is.

ISO spreekt van *age assurance systems*. Deze systemen hebben tenminste twee onderdelen:

1) Eén of meer 'age assurance components'.
2) Een sub-systeem dat de mate van betrouwbaarheid van deze componenten vaststelt.

Age assurance systemen kennen vijf niveaus van robuustheid:

1. **Zero:** Dit niveau is alleen geschikt voor laag risico omgevingen, waarin een leeftijdsindicatie relevant kan zijn.
2. **Basic:** Dit niveau is alleen geschikt voor laag risico omgevingen, waarbij toegang niet gereguleerd is.
3. **Standard:** Dit niveau is geschikt voor midden tot hoog risico omgevingen. Het is het minimale niveau voor wettelijke gereguleerde toegangscontrole, tenzij hoger gedefinieerd is.
4. **Enhanced** Dit niveau is geschikt voor hoog risico omgevingen waarbij toegang kan worden verkregen tot gevoelige goederen, inhoud of diensten.
5. **Strict** Dit niveau is geschikt voor zeer hoog risico omgevingen waarbij het waarborgen van toegangscontrole van kritiek belang is voor het waarborgen van de rechten en veiligheid van minderjarigen.

Deze niveaus zijn gekoppeld aan 'assurance components' oftewel, manieren waarop iemand kan (laten) aantonen dat hij of zij een bepaalde leeftijd heeft. Er zijn verschillende assurance componenten:

1. Processen of systemen die een leeftijdsattribuut afleiden uit een officieel identiteitsdocument (directe identificatie).
2. Processen of systemen die een leeftijdsattribuut afleiden uit een secundair attribuut (afgeleide identificatie).
3. Een systeem dat kunstmatige intelligentie gebruikt om biometrische- of gedragskenmerken vast te stellen.
4. Een proces waarmee op basis van iemands gedrag en sociale omgeving wordt vastgesteld wat diens leeftijd is (social proofing).
5. Een systeem dat is gebaseerd op een medeling van een derde partij (ouder of voogd)
6. Een menselijke controle gebaseerd op voorkomen, gedrag en betrouwbaarheid
7. Een proces, systeem of methode erkend in internationale standaarden.

Deze methoden worden toegepast in de vier categorieën beschreven in dit rapport.

[45] Zie: https://standards.ieee.org/ieee/2089.1/10700/?utm_source=beyondstandards&utm_medium=post&utm_campaign=diita-2022; https://www.iso.org/standard/80399.html en https://euconsent.eu/download/iso-working-draft-age-assurance-systems-standard/

[46] IEEE SA IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children. Beschikbaar via: https://ieeexplore.ieee.org/document/9627644

7.1 Robuustheidseisen per niveau

Hieronder beschrijven wij de robuustheidseisen per niveau. Omwille van de omvang geven wij een versimpeld overzicht van de niveaus. Voor een volledig overzicht van de eisen verwijzen wij naar de ISO Working Draft.

Niveau Zero

- Op dit niveau volstaat een mededeling van de persoon omtrent diens leeftijd.
- De verstrekte informatie wordt niet gevalideerd.

Niveau Basic

- Op dit niveau wordt gebruikt gemaakt van zelfverklaring door het individu in combinatie met tenminste één ander age assurance component.
- Het component moet geëvalueerd worden met een 'basisniveau van vertrouwen'.[47]
- De verstrekte informatie mag op een simpele wijze gevalideerd worden.
- Voor dit niveau mogen de *false accept rate* (foutief toegelaten) en de *false reject rate* (foutief geweigerd) niet groter zijn dan 5%.

Niveau Standard

- Op dit niveau wordt gebruikt gemaakt van zelfverklaring door het individu in combinatie met tenminste één ander age assurance component.
- Het component moet geëvalueerd worden met een 'standaardniveau van vertrouwen'
- De verstrekte informatie *moet* gevalideerd worden. Voor dit niveau mogen de *false accept rate* (foutief toegelaten) en de *false reject rate* (foutief geweigerd) niet groter zijn dan 1%.
- Wanneer de verificatie op afstand plaatsvindt, dan moet gecontroleerd worden of de persoon levend is. Met andere woorden, een foto controleren is onvoldoende.
- Wanneer voor dit niveau gebruik wordt gemaakt van kunstmatige intelligentie, dan moet speciale rekening worden gehouden met beschermde attributen van personen (bijzondere persoonsgegevens).

Niveau Enhanced

- Op dit niveau wordt gebruikt gemaakt van zelfverklaring door het individu in combinatie met tenminste twéé andere age assurance componenten die worden verkregen van onafhankelijke bronnen, waarvan er tenminste één gebaseerd is op een primair attribuut (een identiteitsdocument) of een afgeleid attribuut (attribuut afgeleid van een identiteitsdocument).
- De componenten moeten geëvalueerd worden met een 'hoog niveau van vertrouwen'

[47] De evaluatie vindt plaats conform de 'Common Criteria Evaluation Methodology', een ISO methodologie voor het testen van systemen. Zie ISO/IEC 15408 1 tot en met 3.

- De verstrekte informatie *moet* gevalideerd worden. Voor dit niveau mogen de *false accept rate* (foutief toegelaten) en de *false reject rate* (foutief geweigerd) niet groter zijn dan 0,1%.
- Wanneer de verificatie op afstand plaatsvindt, dan moet gecontroleerd worden of de persoon levend is. Met andere woorden, een foto controleren is onvoldoende.
- Wanneer voor dit niveau gebruik wordt gemaakt van kunstmatige intelligentie, dan moet speciale rekening worden gehouden met beschermde attributen van personen (bijzondere persoonsgegevens).
- Het omzeilen van het systeem moet actief worden ontmoedigd en manieren om het systeem te omzeilen moeten tegengegaan worden.

Niveau Strict

- Op dit niveau wordt gebruikt gemaakt van zelfverklaring door het individu in combinatie met tenminste twéé ander age assurance componenten die worden verkregen van onafhankelijke bronnen, waarvan er tenminste één is gebaseerd op een primair attribuut.
- Het component moet geëvalueerd worden met een 'strikt niveau van vertrouwen'
- De verstrekte informatie *moet* gevalideerd worden. Voor dit niveau mogen de *false accept rate* (foutief toegelaten) en de *false reject rate* (foutief geweigerd) niet groter zijn dan 0,01%.
- Wanneer de verificatie op afstand plaatsvindt, dan moet gecontroleerd worden of de persoon levend is. Met andere woorden, een foto controleren is onvoldoende.
- Wanneer voor dit niveau gebruik wordt gemaakt van kunstmatige intelligentie, dan moet speciale rekening worden gehouden met beschermde attributen van personen (bijzondere persoonsgegevens).
- Het omzeilen van het systeem moet actief worden ontmoedigd en manieren om het systeem te omzeilen moeten tegengegaan worden.

7.2 Robuustheidseisen beschouwd per methode

Op basis van het bovenstaande geven wij hieronder onze inschatting in hoeverre de genoemde methoden kunnen voldoen aan de beschreven niveaus van robuustheid.

Zelfverklaring is alleen geschikt voor niveau *zero*.

Leeftijdsinschatting kan geschikt zijn als assurance component voor elk niveau, maar alleen voor de niveaus *standard*, *enhanced* en *strict* als deze voldoende accuraat is. Op zichzelf is leeftijdsinschatting nooit geschikt voor de niveaus *enhanced* en *strict*, omdat er geen gebruik wordt gemaakt van primaire of afgeleide attributen. Naast gedragsanalyse moet er dan bijvoorbeeld gebruik worden gemaakt van directe identificatie.

Accountbevestiging kan geschikt zijn als assurance component voor elk niveau. Op zichzelf is accountbevestiging nooit geschikt voor de niveaus *enhanced* en *strict*, omdat er geen gebruik wordt gemaakt van primaire of afgeleide attributen. Naast accountbevestiging moet er dan bijvoorbeeld gebruik worden gemaakt van directe identificatie.

Identificatie is, afhankelijk van de gekozen methode, als assurance component geschikt voor alle niveaus, inclusief de niveaus *standard*, *enhanced* en *strict*. Directe identificatie is geschikt voor de niveaus *standard*, *enhanced* en *strict*. Bij afgeleide identificatie is het afhankelijk van de zekerheid waarmee vastgesteld kan worden dat de houder van het afgeleide attribuut (bijvoorbeeld een token) deze rechtmatig in het bezit heeft. Voor het niveau *strict* is deze methode op zichzelf ontoereikend. Voor digital identity solutions is het afhankelijk van de robuustheid van de gekozen methode (waarop baseren de partijen hun identiteitscontrole) maar kan tot en met het niveau *enhanced* bereikt worden. Digital identity solutions die niét direct gebruik maken van een primair attribuut zullen op zichzelf mogelijk onvoldoende zijn voor het niveau *strict*, omdat op dit niveau identificatie op basis van een primair attribuut vereist is.

7.3 Robuustheid in relatie tot risico

Op grond van het bovenstaande concluderen wij dat voor (wettelijk) verplichte leeftijdsverificatie alleen de niveaus *Standard*, *Enhanced* of *Strict* toereikend zijn.

Verder concluderen wij dat wanneer uit de risico-inschatting voor de dienst blijkt dat er kans is op een hoog risico voor kinderen, leeftijdsverificatie overwogen moet worden van tenminste de niveaus *standard*, *enhanced* of *strict*.

Voor de genoemde categorieën leeftijdsverificatie betekent dat het volgende:

Zelfverklaring is sowieso onvoldoende voor de niveaus *standard*, *enhanced* en *strict*.

Veel verschijningsvormen van **Leeftijdsinschatting** zullen gezien de huidige stand van de techniek waarschijnlijk ook ontoereikend zijn voor het niveau *standard*, omdat zij een te hoge foutmarge hebben. Wel kan deze techniek een belangrijke aanvulling vormen op andere verificatiemethoden, omdat de methode geschikt is om gedurende het gebruik van de dienst blijvend te verifiëren of een persoon daadwerkelijk meerderjarig is. Voor de niveaus *enhanced* and *strict* is de methode ook ontoereikend, omdat voor deze niveaus vertrouwd moet worden op officiële identiteitsdocumenten (*strict*) dan wel op daar van afgeleide attributen (*enhanced*).

Bij **Accountbevestiging** hangt het af van de concrete implementatie, maar deze methode is in beginsel voldoende voor het niveau *standard*. Voor de niveaus *enhanced* en *strict* is de methode ontoereikend, omdat voor deze niveaus vertrouwd moet worden op officiële identiteitsdocumenten (*strict*) dan wel op daar van afgeleide attributen (*enhanced*). Bij accountbevestiging hangt het natuurlijk ook af van de vraag hoe robuust het identificatie- en verificatieproces is voor de hoofdaccounthouder. Tenslotte moet rekening worden gehouden met het feit dat de hoofdaccounthouder de minderjarige in strijd met een wettelijk voorschrift alsnog toegang kan geven tot verboden producten of diensten (bijvoorbeeld de ouder staat toe dat het minderjarige kind toegang krijgt tot een site die alcohol verkoopt). Afhankelijk van de concrete situatie moet daarom bekeken worden of een striktere vorm van verificatie noodzakelijk is.

Identificatie in alle verschijningsvormen is geschikt voor tenminste het niveau *standard* en biedt daarnaast ook mogelijkheden voor de niveaus *enhanced* en *strict*. Directe identificatie is geschikt is voor het niveau *strict*, omdat er daarbij direct vertrouwd moet worden op een identiteitsdocument. Voor afgeleide identificatie methoden geldt dat *enhanced* het hoogst haalbare niveau is, omdat daar vertrouwd mag worden op van identiteitsdocumenten afgeleide attributen. Voor digital identity providers hangt het af van de methode die zij gebruiken en hun status als betrouwbare derde partij (trusted third party). In ieder geval lijkt het niveau *strict* niet haalbaar.

Tenslotte is het van belang om nogmaals te onderstrepen dat bij de keuze voor één of meer 'assurance components' telkens gekeken moet worden wat de betrouwbaarheid is van het gekozen component. Dit is altijd afhankelijk van de concrete toepassing en de gekozen implementatie.

Het bovenstaande kan als volgt schematisch worden weergegeven:

Tabel: Benodigde robuustheid per risicocategorie

	Robuustheid verificatie				
	Zero	Basic	Standard*	Enhanced	Strict
Laag risico	X				
Gemiddeld risico		X			
Hoog risico			X	X	X
Zeer hoog risico					X

* = minimale niveau om te voldoen aan (wettelijke) verificatieplicht, tenzij hoger niveau is gedefinieerd.

Tabel: Te halen robuustheidniveau per verificatiemethode.

	Robuustheid verificatie				
	Zero	Basic	Standard	Enhanced	Strict
Zelfverklaring	X				
Leeftijdsinschatting					
- biometrie	X	X	-/+*		
- gedrag	X	X	-/+*		
- linguïstiek	X	X	-/+*		
- profilering	X	X	-/+*		
Accountbevestiging	X	X	X		
Identificatie					
Directe identificatie	X	X	X	X	X
Afgeleide Identificatie	X	X	X	X	

* = Indien voldoende accuraat

7.4 Beveiligingsvereisten

Het te kiezen niveau van beveiliging is afhankelijk van het gewenste niveau van robuustheid, alsmede de gevoeligheid van de gegevens die gebruikt worden voor de gekozen verificatiemethode. Deze beoordeling is sterk afhankelijk van de omstandigheden van het geval. Wel kunnen wij in algemene zin een aantal aandachtspunten formuleren voor de beveiliging op grond van de gekozen verificatiemethode en het gewenste niveau van robuustheid.

7.4.1 Zelfverklaring

Het beveiligingsniveau voor deze methode hoeft niet heel hoog te zijn. Allereerst worden weinig gevoelige attributen opgevraagd ter verificatie van de leeftijd.[48] Daarnaast worden dit soort systemen meestal gekoppeld aan de sessie van een gebruiker (bijvoorbeeld bij het binnenkomen van een website) en is er dus geen (langdurige) koppeling tussen de daadwerkelijke identiteit van de betrokkene en de ingevoerde leeftijd / geboortedatum.

7.4.2 Leeftijdsinschatting

Leeftijdsinschatting kan -afhankelijk van het aard en het type analyse- zeer gevoelig zijn.

Bij biometrische analyse is zoals besproken in het juridisch kader doorgaans sprake van de verwerking van bijzondere persoonsgegevens.

Om de leeftijd van een persoon op basis van online gedrag in te schatten met een redelijk accuraatheidsniveau zal naar verwachting een relatief rijk profiel moeten worden opgebouwd van een persoon. Hiermee zou een min of meer compleet beeld van bepaalde aspecten van iemands persoonlijke levenssfeer verkregen kunnen worden. Hierdoor is er sprake van een hoog risico.

Naar verwachting is voor dit soort methoden een Data Protection Impact Assessment (DPIA) verplicht. Uit deze DPIA vloeien risico-beperkende maatregelen voort, onder andere op het gebied van beveiliging.

Voor wat betreft de beveiligingseisen kan aangesloten worden bij de vereisten voor een Information Security Management System (ISMS) uit ISO/IEC 27001 en de security controls uit ISO/IEC 27002.

Wanneer van biometrie gebruik wordt gemaakt moet worden aangesloten bij de eisen uit de ISO/IEC 19989 standaarden aangaande informatiebeveiliging en biometrie.

7.4.3 Accountbevestiging

Voor accountbevestiging gelden in beginsel dezelfde technische en organisatorische maatregelen als er gelden voor de beveiliging van het account van de gebruiker. Los van de wetenschap dat een bepaalde persoon in een (gezags)relatie staat tot een andere persoon, is er geen hoger beveiligingsrisico voor de accounts als zodanig.

7.4.4 Identificatie

Voor directe (online) identificatie moeten strenge beveiligingsmaatregelen gelden omdat er gebruik wordt gemaakt van identiteitsdocumenten, daarvan afgeleide attributen en mogelijk biometrie. Bij het verwerken van identiteitsdocumenten kan ook (onbedoeld) het BSN nummer verwerkt worden, bijvoorbeeld omdat deze automatisch meekomt bij het uitlezen van de chip in het identiteitsdocument of omdat deze onvoldoende is afgeschermd bij het verwerken van een digitale kopie.

Afhankelijk van de aard van de gekozen identificatietoepassing kunnen (internationale) standaarden gelden voor het gebruiken en verwerken van deze toepassingen.

[48] Wel kan een geboortedatum relatief gevoelig zijn. Het is daarom wenselijker om te vragen naar een geboortejaar + maand in plaats van naar een geboortedatum.

Voor de beveiliging van biometrische toepassingen kan aansluiting worden gezocht bij onder andere de ISO/IEC 19989 standaarden.

7.5 Conclusie

Op grond van het voorgaande concluderen wij dat voor hoog risico toepassingen er op grond van de criteria die de ISO momenteel hanteert een leeftijdsverificatiemethode moet worden gekozen met relatieve strenge eisen aan de robuustheid. Dat betekent dat zelfverklaring sowieso afvalt, terwijl methoden als gedragsanalyse en accountbevestiging (op zichzelf) veelal onvoldoende zullen zijn voor hoog-risico toepassingen of situaties waarin er een wettelijke verificatieplicht bestaat.

Systemen die werken met directe identificatie en/of afgeleide identificatie zijn het meest geschikt voor hoog risico toepassingen en/of toepassingen die wettelijk afgedwongen verificatie vereisen.

Voor alle niveaus geldt dat passende technische en organisatorische maatregelen moeten worden genomen ter beveiliging van de gegevens. Dat is enerzijds relevant voor het waarborgen van de robuustheid van de verificatie en anderzijds voor het beschermen van de privacy en persoonsgegevens van de betrokkenen nu afhankelijk van de gekozen methode meer of minder gevoelige gegevens worden verwerkt.

8 Nadere analyse leeftijdsverificatiemechanismen

In voorgaande hoofdstukken hebben we vier categorieën van leeftijdsverificatie besproken, namelijk zelfverklaring, leeftijdsinschatting, accountbevestiging en identificatie. In het vorige hoofdstuk zijn we in detail ingegaan op de robuustheidseisen die kunnen/moeten worden gesteld aan de verschillende verificatiemethoden.

De keuze voor een verificatiemethode op grond van robuustheidsvereisten betekent echter wel dat andere aspecten zoals inclusiviteit en privacy in het gedrang kunnen komen. In dit hoofdstuk kijken wij naar de verschillende methoden in relatie tot de aspecten robuustheid, privacy, veiligheid en inclusiviteit zoals beschreven in hoofdstuk 6. Aangezien de eisen met betrekking tot transparantie voor elke methode van leeftijdsverificatie gelden, zullen wij die hieronder niet apart bespreken.

We spreken hier van overwegingen, omdat een optimale invulling van deze aandachtspunten sterk afhankelijk is van de context. Zo kan het zijn dat een hoog niveau van robuustheid gewenst is op basis van het risico dat is geïdentificeerd. Er kan echter alsnog gekozen worden voor een methode die een lager niveau van robuustheid heeft, omdat privacy of inclusiviteit in die specifieke context zwaar weegt. Bij het kopen van alcohol wordt een andere overweging gemaakt dan voor het toegankelijk maken van content die bijdraagt aan de seksuele ontwikkeling van een kind of minderjarige.

8.1 Zelfverklaring

Zelfverklaring is wanneer een gebruiker zijn/haar leeftijd kan aangeven, maar geen bewijs hoeft te leveren ter bevestiging ervan, bijvoorbeeld door het aanvinken van een check box. Hieronder beschrijven we de overwegingen die moeten worden gemaakt wanneer voor deze methode wordt gekozen.

8.1.1 Robuustheid

Deze vorm is onbetrouwbaar, aangezien er geen enkele bevestiging is op basis van objectieve factoren, maar enkel een bevestiging van de gebruiker zelf. Het is voor een minderjarige erg makkelijk om een dergelijk 'verificatiesysteem' te omzeilen. Om die reden is deze methode alleen geschikt voor het robuustheidsniveau *zero*. ISO geeft in dit verband aan dat deze methode meer geschikt is als leeftijdsindicatie, die vervolgens gebruikt kan worden om bijvoorbeeld de interface af te stemmen op de gebruiker.

8.1.2 Privacy

De robuustheid van zelfverklaring is laag, maar daartegenover staat dat er geen tot weinig inbreuk wordt gemaakt op de privacy, afhankelijk van de methode. In het geval van het aanvinken van een check box worden geen persoonsgegevens verzameld. Indien de zelfverklaring bestaat uit het doorgeven van de geboortedatum is er mogelijk wel sprake van een verwerking van persoonsgegevens, omdat de persoonsgegevens in combinatie met andere (meta)gegevens van het platform wel te herleiden kunnen zijn tot een persoon. Bij deze methode is het daarentegen gemakkelijk een valse geboortedatum door te geven.

8.1.3 Veiligheid

Gezien er geen tot nauwelijks persoonsgegevens worden verzameld bij het gebruik van deze methode, is er ook geen tot nauwelijks risico voor de gebruiker.

8.1.4 Inclusiviteit

Zelfverklaring is meest gebruikte vorm van leeftijdsverificatie. Er zijn bij deze vorm geen speciale aandachtspunten als het gaat om inclusiviteit. Er is hierbij geen (digitale) identiteit nodig. Daarnaast zijn er geen speciale digitale vaardigheden of middelen nodig om aan deze vorm van verificatie deel te nemen.

8.2 Leeftijdsinschatting

Leeftijdsinschatting is, zoals eerder beschreven, het inschatten van iemands leeftijd, vaak met behulp van kunstmatige intelligentie. We zullen hieronder de overwegingen bespreken die noodzakelijk wanneer een methode wordt gekozen uit deze categorie van methoden.

8.2.1 Robuustheid

De robuustheid van gedragsanalyse, linguïstische analyse, profilering, biometrische analyse is hoger dan zelfverklaring. Maar omdat de methoden gebaseerd zijn op *inschatting* kunnen ze vatbaar zijn voor onnauwkeurigheden en discriminatie (bias).

Omdat biometrische leeftijdsinschatting wordt gedaan met behulp van AI is de robuustheid van deze methode (de accuraatheid) sterk afhankelijk van de kwaliteit van het model. Er is nog weinig bekend over de foutmarges van modellen voor leeftijdsverificatie en deze zullen ook per gekozen techniek en toepassing verschillen. Het lijkt echter aannemelijk dat net als bij andere AI toepassingen die gebaseerd zijn op probabiliteit, er rekening moet worden gehouden met een (aanzienlijke) foutmarge.

Tenslotte moet voor een aantal technieken (zoals gedragsanalyse) rekening worden gehouden met de mogelijkheden om het systeem te omzeilen (*gaming the system*). Zo zou een minderjarige die toegang wil krijgen tot een dienst bijvoorbeeld het gedrag kunnen simuleren of een foto kunnen gebruiken van een oudere broer of zus.

8.2.2 Privacy

Onder de AVG wordt de verwerking van persoonsgegevens door middel van de inzet van biometrie *met het oog op unieke identificatie van een persoon* beschouwd als een verwerking van bijzondere persoonsgegevens waarvoor in beginsel een verwerkingsverbod geldt, tenzij een van de uitzonderingen uit artikel 9, tweede lid, AVG voor aan te wijzen is. Deze uitzonderingsgrond is nodig om het verwerkingsverbod te doorbreken. Daarnaast is er ook een rechtsgrond uit artikel 6 van de AVG nodig om te kunnen spreken van een rechtmatige verwerking van biometrie met het oog op de unieke identificatie van een persoon. In het kader van leeftijdsinschatting is er mogelijk niet altijd sprake van biometrie *met het oog op de unieke identificatie van een persoon*. In de gevallen waarin de inzet van biometrie niet het oogmerk heeft om iemand uniek de identificeren is het verwerkingsverbod van artikel 9 AVG niet van toepassing. Toch zal bij leeftijdsverificatie al snel sprake zijn van identificatie in de zin van de AVG omdat degene van wie de leeftijd moet worden vastgesteld uniek van andere personen onderscheiden moet kunnen worden. Daarnaast zijn voor een accuraat profiel waarschijnlijk dusdanig veel datapunten nodig dat deze in hun gezamenlijkheid de betrokkene kunnen identificeren. Of er sprake is van de verwerking van bijzondere persoonsgegevens is daarmee sterk afhankelijk van de concrete toepassing.

Bij algoritmische besluiten, waaronder profilering, heeft de betrokkene het recht op een menselijke tussenkomst.[49] Hierop geldt een uitzondering indien er sprake is van een contractuele noodzaak, een wettelijke verplichting of als er toestemming is gegeven door de betrokkene. Bij toestemming als grondslag dient, zoals eerder vermeld, ook toestemming van de ouders te worden gegeven voor de profilering. De andere twee rechtsgronden, namelijk de contractuele noodzaak of de wettelijke verplichting zijn lastig om als wettelijke grondslag te gebruiken. Het zal daarom veelal het geval zijn dat er bij profilering, gedragsanalyse en linguïstische analyse een menselijke tussenkomst vereist is.[50]

Een van de gegevensbeschermingsbeginselen is het beginsel van juistheid. Dit houdt in dat verwerkingsverantwoordelijken alle redelijke maatregelen dienen te treffen om ervoor te zorgen dat de persoonsgegevens waarmee zij werken accuraat zijn. De betrouwbaarheid van geautomatiseerde leeftijdsinschatting is sterk afhankelijk van de data waarmee de algoritmen zijn getraind, waardoor er een groot risico op bias bestaat tegen bepaalde bevolkingsgroepen.

Bij gedragsanalyse speelt verder het probleem dat er veel bekend moet zijn over het gedrag van de betrokkene alvorens een inschatting kan worden gegeven van de leeftijd. Dit brengt een potentieel zeer grote privacyschending met zich mee.

Op grond van het bovenstaande kunnen we vooralsnog concluderen dat vanuit privacy-perspectief de inzet van leeftijdsinschatting door middel van biometrie, geautomatiseerde besluitvorming en profilering op zijn minst problematisch kan worden genoemd.

8.2.3 Veiligheid

Aangezien de genoemde methoden voornamelijk gebaseerd zijn op dataverzameling en analyse, en de kwestie van veiligheid in gelijke mate van toepassing is op deze methoden, wordt hier een meer overkoepelende beschrijving gegeven.

Voor de benaderingen rondom leeftijdsinschatting is een aanzienlijke hoeveelheid gebruikersgegevens vereist als input voor de AI-toepassingen die nodig zijn bij gedrags-, linguïstische en biometrische analyses en profilering. Deze informatie die hiervoor verzameld wordt is gedetailleerder en omvangrijker dan informatie die bijvoorbeeld in een paspoort wordt verstrekt. Daarom is het essentieel dat er passende technische en organisatorische maatregelen worden genomen om de gegevens te beschermen. [51]

8.2.4 Inclusiviteit

Het voordeel van leeftijdsinschatting ten opzichte van leeftijdsverificatie is dat voor deze vorm geen (digitale) identiteit noodzakelijk is. Dat kan voordelen hebben voor gebruikers die niet over een dergelijk document beschikken (zie ook overweging 5.1.4). Echter, leeftijdsinschatting is vaak gebaseerd op algoritmische methoden die veel data nodig hebben om tot een classificatie te komen. Hierbij ligt het risico op discriminatie (bias) en uitsluiting op basis van geautomatiseerde besluitvorming op de loer. Dergelijke situaties kunnen aanzienlijke gevolgen hebben voor de inclusiviteit en toegankelijkheid van de digitale dienstverlening.

[49] Raadpleeg artikel 22 AVG.
[50] Mogelijk zou de profilering met het oog op de leeftijdsverificatie gezien kunnen worden als een noodzakelijke maatregel ter uitvoering van de overeenkomst, nu de levering van de dienst afhankelijk is van een bepaalde leeftijd.
[51] Denk aan risico's zoals identiteitsfraude, zie ook Autoriteit Persoonsgegevens 'Slachtoffer van een datalek? Dit kunt u doen' https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/slachtoffer-van-een-datalek-dit-kunt-u-doen

Biometrische analyse:

Om een biometrische analyse uit te voeren is het noodzakelijk om een AI-toepassing te trainen op het detecteren van gezichten om hier vervolgens een leeftijd aan toe te wijzen. Eerdere incidenten leren dat gezichtsherkenningsmodellen kans hebben tot het genereren van discriminerende resultaten, waarbij aanzienlijk meer fouten worden gemaakt bij het herkennen van vrouwen met een donkere huidskleur dan bij mannen met een lichte huidskleur.[52] Deze bias kan leiden tot onnauwkeurige identificatie van een persoon en hun leeftijd resulterend in potentiële beperkt toegang tot digitale dienstverleningen.

Daarnaast is het aannemelijk dat niet alle gebruikers over de vereiste technische vaardigheden of benodigde 'apparatuur' beschikken om een foto te maken en te uploaden die voldoet aan de kwaliteitseisen voor een biometrische analyse. Deze situatie doet zich met name voor bij ouderen en mensen met een lagere sociaaleconomische status, die mogelijk niet over persoonlijke digitale apparatuur beschikken, en daarom genoodzaakt zijn om gebruik te maken van openbare faciliteiten zoals de bibliotheek om toegang tot internet te krijgen. Of slechts over defecte of ontoereikende digitale apparatuur beschikken en daarom niet kunnen voldoen aan de eisen voor een biometrische analyse.

Gedragsanalyse:

De uiting van gedrag is sterk afhankelijk van cultuur, context, opvoeding en persoonlijkheid. Een gedragsanalyse is vatbaar voor vooroordelen, omdat de complexiteiten van menselijk gedrag lastig te bevatten zijn in een algoritmische analyse. Bovendien moet in de analyse ook rekening worden gehouden met digitale ongeletterdheid. Volgens het INSEE, het Franse Instituut voor Statistiek, beschikte in 2019 tussen de 16% en 22% van de Franse bevolking (inwoners van 15 jaar en ouder) niet over digitale basisvaardigheden.[53] Het is plausibel dat digitale ongeletterdheid zich zal uitdrukken in een ander online gedrag dan bij gebruikers die wel digitaal geletterd zijn. Wanneer gedragsanalyse gebaseerd is op het referentiekader van digitale geletterdheid, bestaat de mogelijkheid dat dit aanzienlijke gevolgen kan hebben voor de betrouwbaarheid van leeftijdsverificatie bij gebruikers die afwijken van deze norm. Denk hierbij aan situaties van digitale ongeletterdheid, maar ook aan gebruikers met fysieke of mentale beperkingen.[54] Daarnaast kan culturele achtergrond ook een rol spelen bij online gedrag van gebruikers van het internet.[55][56]

Linguïstische analyse:

[52] Gentzel, M. (2021). Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy. Philos. Technol. 34, 1639–1663 (2021). https://doi.org/10.1007/s13347-021-00478-z

[53] *Branche-Seigeot, A. (2023). More Digital Illiteracy in Territories Away From Cities and Small Urban Centres. Retrieved at 18/8/2023 on: https://www.insee.fr/en/statistiques/7647949*

[54] *W3 Web Accessibility Initiative. (2023, 16 augustus). Stories of Web Users. In: How People with Disabilities Use the Web. https://www.w3.org/WAI/people-use-web/user-stories/*

[56] Mazaheri E., Richard M., Laroche M., Ueltschy L. C. 'The influence of culture, emotions, intangibility, and atmospheric cues on online behavior' 2014, https://doi.org/10.1016/j.jbusres.2013.05.011

Verschillende factoren, zoals bijvoorbeeld dyslexie,[57] hebben de potentie om aanzienlijke invloed uit te oefenen op de taalvaardigheid van een individu. Hierdoor is het aannemelijk dat er bij het gebruik van de linguïstische analyse onnauwkeurigheden zullen opduiken wat kan leiden tot een verkeerde inschatting, waardoor een persoon onterecht wordt uitgesloten van deelname aan een digitale dienst.

Profilering:

Gebruikers hebben beperkte controle over welke informatie wordt vastgelegd. Bovendien gaat deze benadering uit van individueel gebruik van een apparaat waarbij alle activiteiten terug te leiden zijn naar één persoon, terwijl dit in de werkelijkheid niet het geval hoeft te zijn.

8.3 Accountbevestiging

Met accountbevestiging kan een reeds bestaande accounthouder een leeftijd van een andere gebruiker bevestigen. Hieronder beschrijven we de overwegingen wanneer voor deze methode wordt gekozen.

8.3.1 Robuustheid

De robuustheid van accountbevestiging is gemiddeld. De methode is robuuster dan zelfverklaring, maar biedt geen garanties over de leeftijd / meerderjarigheid van een persoon. Ook zijn bijvoorbeeld ouders of verzorgers niet altijd in staat om ouderlijke controlemechanismen effectief te gebruiken.

8.3.2 Privacy

Bij deze methode bevestigt een ouder of verzorger die reeds over een account op het platform beschikt de leeftijd van het kind. Als de ouder of verzorger enkel een checkbox hoeft aan te vinken waarmee deze laat weten dat het kind de juiste leeftijd heeft, levert dat een geringe inbreuk op de privacy van het kind op. Als de ouder de geboortedatum moet invullen en daarnaast zelf moet verifiëren dat hij of zij de ouder is, dan worden er meer persoonsgegevens verwerkt en is de inbreuk op de privacy van zowel de ouder als het kind groter.

Het betrekken van ouders/voogden bij het proces vereist dat kinderen bepaalde informatie moeten delen, wat mogelijk gevoelig van aard kan zijn, zoals bijvoorbeeld apps die verband houden met identiteit, politieke of levensbeschouwelijke overtuiging, of seksuele voorkeur en geaardheid. Dit kan een potentieel punt van zorg zijn, aangezien het delen van dergelijke informatie mogelijk kan leiden tot privacyrisico's. Bovendien is het niet altijd mogelijk om de relatie te verifiëren tussen een ouder en het kind waarvoor de volwassene garant staat, aangezien dit vaak afhangt van documentatie of andere vormen van bewijsmateriaal.[58] De relatie verifiëren kan op zijn beurt weer leiden tot inbreuken op de privacy.

8.3.3 Veiligheid

Voor wat betreft de veiligheid zijn er geen aanvullende aandachtspunten bij dit type verificatie.

[57] Morken, F. & Helland, T. (2013). Writing in Dyslexia: Product and Process. In: Dyslexia International Journal of Research and Practice. Vol 19(3). 131-188. https://doi.org/10.1002/dys.1455

[58] Nash, V., O'Connell, R., Zevenbergen, B. & Mishkin, A. (2013). Effective Age Verification Techniques: Lessons to Be Learnt from the Online Gambling Industry. Available at SSRN: https://ssrn.com/abstract=2658038 or http://dx.doi.org/10.2139/ssrn.2658038.

8.3.4 Inclusiviteit

Het betrekken van ouders bij het goedkeuringsproces voor digitale diensten kan leiden tot beperking van de autonomie van het kind. Dit kan vooral plaatsvinden als ouders de volledige controle hebben over welke inhoud het kind mag bekijken of welke interacties ze kunnen hebben. Daarnaast speelt de digitale geletterdheid van de ouders een grote rol bij deze methode. Het vermogen van ouders om te begrijpen hoe digitale diensten werken, het beheren van de privacy-instellingen en hoe ze de online ervaring van hun kinderen kunnen begeleiden, kan sterk variëren. Dit kan resulteren in aanzienlijke verschillen in de mate van toegang en interactie die verschillende kinderen hebben, afhankelijk van de kennis en vaardigheden van hun ouders.

8.4 Identificatie

Identificatie is een groep van methoden gebaseerd op het verifiëren van de leeftijd door het matchen van een persoon met een attribuut dat de identiteit (en leeftijd) van de persoon bevat. Hieronder beschrijven we de overwegingen wanneer voor deze methode wordt gekozen.

8.4.1 Robuustheid

De robuustheid van directe identificatie en afgeleide identiteit kan, afhankelijk van de gekozen implementie, hoog zijn. Sterker nog, identificatie is de enige methode die geschikt is voor de robuustheidsniveaus *enhanced* en *strict*. Dit komt doordat bij identificatie gebruik gemaakt wordt van primaire attributen (officiële identiteitsdocumenten) dan wel afgeleide attributen (ontleend aan officiële identiteitsdocumenten). Wanneer de implementatie goed is, wordt met deze methode de meest robuuste leeftijdsverificatie gerealiseerd.

8.4.2 Privacy

De AVG is van toepassing wanneer er persoonsgegevens worden verwerkt om de leeftijd van een persoon te verifiëren. Dit is het geval omdat verificatie gekoppeld is aan identificatie. Er bestaan verschillende identificatiemethoden ten behoeve van het achterhalen van de leeftijd van een persoon. De AVG schept regels ter bescherming van het recht op privacy en de zorgvuldige verwerking van persoonsgegevens voor ieder van deze methoden.

Directe identificatie:

Voor deze verificatiemethode is het noodzakelijk dat een persoon persoonsgegevens overdraagt die hem direct identificeren, zoals bijvoorbeeld paspoortgegevens. Deze vorm van identificatie en verificatie is bij een juiste implementatie weliswaar zeer accuraat en robuust, maar is ook privacygevoelig, omdat (zeer) gevoelige gegevens verwerkt kunnen worden en inzichtelijk worden voor de dienstverlener.

Wanneer een identiteitsdocument direct wordt gebruikt geldt dat alleen de noodzakelijke gegevens mogen worden verwerkt. De Autoriteit Persoonsgegevens laat weten dat een kopie van een paspoort of ID,

waarbij het BSN en de pasfoto onzichtbaar zijn gemaakt, enkel mogelijk is als er echt geen andere manier is om het beoogde doel te bereiken.[59]

Een bijkomend probleem is dat voor paspoorten die vóór 2021 zijn uitgegeven het BSN staat opgenomen in de MRZ-code op de voorpagina van het paspoort en het BSN standaard wordt uitgelezen bij het elektronisch openen van de chip op het paspoort. Uit de AVG en de Nederlandse Uitvoeringswet AVG volgt dat de verwerking van een BSN alleen mogelijk is in gevallen waarin dit wettelijk verplicht is gesteld.[60] De Wet op de kansspelen bijvoorbeeld biedt een dergelijke wettelijke verplichting voor de verwerking van het BSN ten behoeve van een deugdelijke identificatie. Maar, zonder wettelijke grondslag voldoet de verwerking van een BSN niet aan het beginsel van rechtmatigheid, waardoor de (geautomatiseerde) verwerking van het paspoort in veel gevallen (nog) geen geschikt middel is voor leeftijdsverificatie.

Wat voorts relevant is, is dat voor de niveaus *standard*, *enhanced* en *strict* geverifieerd moet worden dat de persoon die geïdentificeerd wordt daadwerkelijk leeft. Bij fysieke identificatie is dit als het ware 'ingebakken' in het identificatieproces (de persoon van wie het paspoort is geeft het aan de partij die de identiteit wil verifiëren), maar omdat dit niet noodzakelijkerwijs het geval is bij een identificatie op afstand, wordt deze aanvullende eis gesteld. Hiermee wordt voorkomen dat een kwaadwillende derde die wederrechtelijk in het bezit is van een wettelijk identificatiemiddel een foto van de daadwerkelijke houder kan laten zien en zich zo kan uitgeven als deze persoon. Het is dus niet voldoende om identificerende gegevens op te sturen, deze moeten direct gekoppeld worden aan de persoon. Dit betekent dat bijvoorbeeld met behulp van een webcam een match gemaakt moet worden tussen de persoon en het document en er dus aanvullend (biometrische) persoonsgegevens worden verwerkt.

Verificatie gekoppeld aan identificatie is dus afhankelijk van de gekozen implementatie robuust, maar tegelijkertijd ook privacygevoelig en afhankelijk van de concrete implementatie alleen mogelijk als er sprake is van een wettelijke grondslag. De gevoeligheid neemt navenant toe wanneer de dienstverlener de verificatie wil documenteren voor bijvoorbeeld bewijsdoeleinden (denk bijvoorbeeld aan een kopie paspoort).

Wanneer voor de verificatie gebruik wordt gemaakt van een derde partij (bijvoorbeeld een digital identity provider), dan bestaat er het risico dat deze derde partij weet welke dienst(en) de betrokkene allemaal gebruikt.

Afgeleide identiteit:

Een afgeleide identiteit of secundair attribuut kan gecreëerd worden op basis van een primair attribuut (een identiteitsdocument). Ook kan er een meer afgeleide identiteit worden gebruikt, door de verificatie te koppelen aan een dienst waar de identiteit en leeftijd reeds geverifieerd is, zoals bijvoorbeeld een bankrekening. Dit kan bijvoorbeeld via een 1-centbetaling van een bankrekeningnummer, waarbij de naam van de rekeninghouder en aanvullende gegevens zoals de geboortedatum worden vergeleken met de

[59] Autoriteit Persoonsgegevens. (2023).'Kopie van uw ID-bewijs: wat kunt u doen? Retrieved on 22/8/2023 at https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/paspoort-en-identiteitskaart/kopie-van-uw-id-bewijs-wat-kunt-u-doen#:~:text=Watermerk%20of%20schrijven%20op%20kopie%20ID,-Om%20het%20risico&text=Op%20een%20papieren%20kopie%20kunt%20u%20schrijven%20voor%20welke%20organisatie,kopie%20aan%20het%20eind%20terugvragen.

[60] Artikel 87 van de AVG in combinatie met artikel 46 van de UAVG.

naam van de accounthouder op een platform. Dit is een bruikbare methode wanneer de verwerkingsverantwoordelijke reeds beschikt over betaalinformatie. Wanneer de verwerkingsverantwoordelijke niet al beschikt over betaalinformatie kan er sprake zijn van een overmatige verwerking van persoonsgegevens. Het is van belang te beoordelen of de 1-centbetaling proportioneel is ten opzichte van het te bereiken doel en binnen de context waarbinnen deze wordt verwerkt. Het zij opgemerkt dat het doelbindingsprincipe verbiedt dat persoonsgegevens die voor leeftijdsverificatie worden verwerkt vervolgens voor andere, niet-verenigbare doeleinden worden verwerkt. Dit is een waarborg om misbruik van de gegevens te voorkomen.

De toepassing van digitale identificatie (zoals self-sovereign identity-oplossingen) kan een goed en robuust alternatief opleveren voor de elektronische verwerking van het paspoort. Bij een aantal digitale identiteit oplossingen wordt er lokaal op de smartphone van de gebruiker een kopie van een paspoort of een ander identificatiemiddel opgeslagen, de gebruiker kan diens identiteit vervolgens verifiëren door het maken van een biometrische match tussen de foto op het paspoort en een live gezichtsopname, er zijn echter ook andere technische oplossingen denkbaar om vast te stellen of de gebruiker is wie hij zegt dat hij is.

De gebruiker beslist vervolgens welke attributen van diens identiteit (met uitzondering van het BSN) er worden gedeeld met de aanbieder van het online platform. De gebruiker behoudt in dit geval de controle over diens persoonsgegevens. Het is zelfs mogelijk met ‘zero knowledge proof’ te werken, waarbij de aanbieder van het online platform uitsluitend de melding krijgt dat de leeftijd akkoord of niet akkoord bevonden is. Dit is met het oog op dataminimalisatie en een verantwoorde verwerking van persoonsgegevens een uitstekende oplossing.

Op dit moment wordt er vanuit de EU gewerkt aan een herziening van de eIDAS-verordening, daarmee ontstaat voor alle lidstaten de verplichting om binnen 2,5 jaar na inwerkingtreding van de verordening tenminste één (open source) wallet beschikbaar te stellen waarmee burgers en ondernemers die dat willen kunnen inloggen, identificeren, elektronisch kunnen ondertekenen en gewaarmerkte gegevens/attributen kunnen opslaan c.q. delen met andere partijen in de publieke en private sector.”

8.4.3 Veiligheid

De veiligheid van een leeftijdsverificatie heeft betrekking op de maatregelen en procedures die worden gevolgd om ervoor te zorgen dat het proces van het vaststellen van iemands leeftijd veilig verloopt. Het gaat om het minimaliseren van risico's, het voorkomen van misbruik en het beschermen van de integriteit van zowel de verificatiegegevens als de betrokken partijen.

Directe identificatie:

De gebruiker moet voor dit niveau van accuraatheid mogelijk gevoelige persoonsgegevens delen. Deze gegevens kunnen ook worden opgeslagen door de dienstverlener. Het beveiligingsniveau van deze data moet dan ook hoog zijn, zodat het risico op eventuele datalekken of inbreuken zo klein mogelijk is.

Afgeleide identiteit:

Om tot een afgeleide identiteit te komen dient een wettelijk identificatiemiddel geverifieerd te worden. Dit kan resulteren in het prijsgeven van (bijzondere) persoonsgegevens. Hierdoor kan informatie zoals de

afkomst van een persoon onthuld worden, terwijl alleen de geboortedatum van de persoon essentieel is voor het doel van de verificatie. Het risico dat gepaard gaat met het delen van dit soort gegevens, is dat deze onbevoegd hergebruikt kunnen worden, of kunnen lekken. Met betrekking tot identificatie door middel van bankgegevens stelt de CNIL dat de ingevoerde systemen de veiligheid van de verificatie moeten garanderen om de risico's van phishing die ermee gepaard gaan te voorkomen.[61]

Bij een digital identity solution wordt er gebruik gemaakt van een digitale identiteit. Zoals eerder vermeld kan de oplossing zo zijn ingericht dat persoonsgegevens alleen lokaal zijn opgeslagen en is het aan de gebruiker te bepalen wat er wordt gedeeld met de derde partij (het platform dat leeftijdsverificatie gebruikt). De gebruiker heeft dan controle over de persoonsgegevens en kan zelf kiezen met wie welke gegevens worden gedeeld. Zo kunnen gebruikers via een eID aantonen dat ze de juiste leeftijd hebben.[62] Uiteraard dienen dan ook de persoonsgegevens die lokaal zijn opgeslagen goed te worden beschermd. Omdat de persoonsgegevens lokaal worden opgeslagen, is het risico met betrekking tot de beveiliging doorgaans wel minder groot dan wanneer de persoonsgegevens worden overgedragen.[63]

Een specifiek aandachtspunt bij lokaal opgeslagen gegevens is wel dat de minderjarige zelf verantwoordelijk is voor de bescherming van het randapparaat. Dit kan mogelijk een kwetsbaarheid opleveren, omdat minderjarigen zich misschien minder bewust zijn van beveiligingsrisico's die voortvloeien uit bijvoorbeeld phishing, het gebruik van zwakke wachtwoorden of verlies of diefstal van hun apparaat.

8.4.4 Inclusiviteit

De inclusiviteit en toegankelijkheid van een leeftijdsverificatie ziet op het voorkomen van discriminatie en het bieden van gelijke kansen voor alle individuen, ongeacht hun achtergrond, (digitale) vaardigheden of beschikbaarheid van documentatie.

Een leeftijdsverificatie op basis van identiteit is in de meeste gevallen afhankelijk van de beschikbaarheid van officiële documenten, een bankrekening en/of een betrouwbare derde partij. Dit kan een uitdaging vormen voor bijvoorbeeld jongvolwassenen, zeker wanneer het gaat om verificatie op basis van hun betaalgegevens, aangezien zij mogelijk nog geen eigen bankrekening hebben. Ook toegang tot officiële documentatie en een goede digitale infrastructuur voor de authenticatie van deze documentatie is niet vanzelfsprekend. Hoewel in Nederland nagenoeg iedere burger (toegang tot) een identiteitsdocument heeft, is een eenvoudige toegankelijke infrastructuur voor online leeftijdsverificatie (nog) niet beschikbaar.[64] Dit ondermijnt de inclusiviteit van deze methode.

Een aandachtspunt bij het gebruik van identificatiemethoden is voorts dat kinderen sterk afhankelijk zijn van hun ouders voor hun toegang tot deze middelen. Wanneer bijvoorbeeld de ouder of voogd het gebruik

[61] CNIL 'Online age verification: balancing privacy and the protection of minors' 2022 https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

[62] Europese Commissie. (2021). 'Building a Trusted and Secure European Digital. Retrieved on 22/8/2023 at https://digital-strategy.ec.europa.eu/en/library/building-trusted-and-secure-european-digital-identity-brochure

[63] De eIDAS verordening richtsnoeren voor de beveiliging van dit soort elektronische identificatiemethoden.

[64] Nash, V., O'Connell, R., Zevenbergen, B. & Mishkin, A. (2013). Effective Age Verification Techniques: Lessons to Be Learnt from the Online Gambling Industry. Available at SSRN: https://ssrn.com/abstract=2658038 or http://dx.doi.org/10.2139/ssrn.2658038

van een digitale wallet niet toestaat, maar het gebruik daarvan is wel verplicht voor online diensten, dan wordt daarmee de minderjarige effectief de toegang tot deze diensten ontzegd.

Vanuit het perspectief van inclusiviteit is voorts nog van belang te vermelden dat wanneer een digitale dienst verificatie van een (digitale) identiteit vereist alle gebruikers daardoor geraakt worden (niet alleen de minderjarigen). Dit betekent dat personen die moeite zouden kunnen hebben met het gebruiken van digitale identificatiemethoden (denk aan ouderen, lichamelijk beperkte mensen of (licht) verstandelijk beperkte mensen) ook geraakt worden in hun vrije toegang tot een dienst.

Tenslotte zullen mensen voor eID toepassingen mogelijk ook bezwaar maken tegen het (vermeende) feit dat de overheid toegang tot digitale diensten kan controleren en reguleren met behulp van een digitale identiteit. Mogelijk mijden zij dan deze diensten hetgeen de inclusiviteit niet ten goede komt.

8.5 Conclusie

Er lijkt (nog) geen ‘silver bullet’ te bestaan voor (online) leeftijdsverificatie die tegemoet kan komen aan alle belangen die spelen. We kunnen stellen dat methoden met een hogere robuustheid zich moeilijk(er) verhouden tot de belangen privacy en inclusiviteit, terwijl de methoden die meer inclusief zijn (zoals zelfverklaring) veelal onvoldoende robuust zijn om effectief de leeftijd van een persoon te verifiëren.

Bij het kiezen voor een geschikte methode moet het risico voor de minderjarige worden vastgesteld en op basis daarvan een toereikende methode worden gekozen. Daarbij moet vervolgens worden afgewogen of het proportioneel is om leeftijdsverificatie in te zetten als een risico-beperkende maatregel.

9 Conclusies en aanbevelingen

9.1 Conclusies

In dit rapport hebben wij het speelveld rondom leeftijdsverificatie in kaart gebracht. We hebben ons hierbij specifiek twee vragen gesteld:

1. Welke eisen moeten er worden gesteld aan online leeftijdsverificatie systemen op het gebied van robuustheid, privacy, veiligheid, inclusiviteit en transparantie?

2. Welke overwegingen zijn noodzakelijk om tot de meest geschikte methode van leeftijdsverificatie te komen?

Om deze vragen te beantwoorden, hebben wij in hoofdstuk 4 de categorieën besproken van risico's waaraan kinderen kunnen worden blootgesteld. Het gaat om content, conduct, contact, consumer en cross-cutting risks. Deze categorieën zijn afkomstig uit de KIA. Leeftijdsverificatie kan een risico-beperkende maatregel zijn waarbij we kunnen stellen dat naarmate het risico hoger is, een meer robuuste leeftijdsverificatie noodzakelijk is.

Er zijn vele mogelijkheden om de leeftijd van een persoon te verifiëren die alleen, of in samenhang kunnen worden gebruikt. Wij hebben de verschillende methoden ingedeeld in vier categorieën: 1) zelfverklaring, 2) leeftijdsinschatting, 3) accountbevestiging en 4) identificatie. De indeling in deze categorieën stelde ons in staat om in de hoofdstukken daarna vereisten en overwegingen op te stellen.

De verschillende methoden hebben verschillende robuustheidsniveaus. In ISO verband wordt momenteel gewerkt aan een standaard voor de classificatie van de robuustheid van leeftijdsverificatiesystemen. Het gaat om de volgende niveaus:

1. **Zero:** Dit niveau is alleen geschikt voor laag risico omgevingen, waarin een leeftijdsindicatie relevant kan zijn.
2. **Basic:** Dit niveau is alleen geschikt voor laag risico omgevingen, waarbij toegang niet gereguleerd is**.**
3. **Standard:** Dit niveau is geschikt voor midden tot hoog risico omgevingen. Het is het minimale niveau voor wettelijke gereguleerde toegangscontrole, tenzij hoger gedefineerd is.
4. **Enhanced** Dit niveau is geschikt voor hoog risico omgevingen waarbij toegang kan worden verkregen tot gevoelige goederen, inhoud of diensten.
5. **Strict** Dit niveau is geschikt voor zeer hoog risico omgevingen waarbij het waarborgen van toegangscontrole van kritiek belang is voor het waarborgen van de rechten en veiligheid van minderjarigen.

Wanneer we deze niveaus afzetten tegen mogelijke risico's dan komen wij tot de volgende onderverdeling:

Benodigde robuustheid per risicocategorie

	Robuustheid verificatie				
	Zero	Basic	Standard*	Enhanced	Strict
Laag risico	X				

Gemiddeld risico		X			
Hoog risico			X	X	X
Zeer hoog risico					X

* = minimale niveau om te voldoen aan wettelijke verificatieplicht, tenzij hoger niveau is gedefinieerd.

Wanneer we de robuustheidsvereisten van de ISO afzetten tegen de verschillende leeftijdsverificatiemethoden dan komen we tot het onderstaande beeld:

Maximaal te halen robuustheidniveau per verificatiemethode.

	Robuustheid verificatie				
	Zero	Basic	Standard	Enhanced	Strict
Zelfverklaring	X				
Leeftijdsinschatting					
- biometrie	X	X	-/+*		
- gedrag	X	X	-/+*		
- linguïstiek	X	X	-/+*		
- profilering	X	X	-/+*		
Accountbevestiging	X	X	X		
Identificatie					
Directe identificatie	X	X	X	X	X
Afgeleide Identificatie	X	X	X	X	

* = Indien voldoende accuraat

Bij het kiezen van een leeftijdsverificatiemethode is de relatie tussen risico en robuustheid primair van belang, maar daarnaast spelen ook andere belangen een rol. Afhankelijk van de gekozen methode kan er een (negatieve) impact zijn op belangen als privacy, veiligheid, inclusiviteit en toegankelijkheid en transparantie. Hoewel de impact sterk afhankelijk is van de concrete implementatie van een verificatiemethode kunnen we in zijn algemeenheid stellen dat naarmate een methode robuuster is, andere belangen daaronder lijden. Bij de keuze voor een verificatiemethode is het dus van belang om te beoordelen of de inzet van het middel wel proportioneel is. Hiervoor kan het afwegingskader uit hoofdstuk 2 worden gebruikt.

9.2 Aanbevelingen

Op basis van de bevindingen uit dit rapport komen wij ook nog tot enkele aanbevelingen voor het beleid:

- Sluit aan bij de ontwikkeling van internationale standaarden, zoals de ISO standaard voor leeftijdsverificatie die momenteel ontwikkeld wordt. Omdat de standaard nog in ontwikkeling is, is er nog ruimte voor aanpassingen.

- Houd rekening met het feit dat leeftijdsverificatie betekent dat elke gebruiker van de digitale dienst aan de verificatie moet worden onderworpen. Of dat proportioneel is hangt met name af van het risico dat de dienst oplevert voor minderjarigen en de beschikbaarheid van alternatieven voor leeftijdsverificatie die minder ingrijpend zijn voor belangen als inclusiviteit en privacy.

- Er lijkt geen 'silver bullet' te zijn voor leeftijdsverificatie. Wees daarom terughoudend met het voorschrijven of verplichten van een specifieke leeftijdsverificatiemethode voor alle gevallen. De noodzaak en wenselijkheid van leeftijdsverificatie is sterk afhankelijk van de context en de concrete implementatie van een methode.

- Wel kan voor specifieke use-cases onderzocht worden wat de beste methode voor leeftijdsverificatie is.

- Stimuleer initiatieven die naast een robuuste verificatie ook rekening houden met andere belangen zoals privacy en inclusiviteit. Systemen die de controle hiervoor bij de gebruiker leggen (bijvoorbeeld wallet oplossingen) lijken hiertoe het meest geschikt.

Bijlagen

Voorbeeld online verkoop alcoholhoudende dranken

In voorgaande hoofdstukken hebben we gezien dat het noodzakelijk om een afweging te maken bij het instellen van leeftijdsverificatie. Gezien de context van de dienst, de aard van het specifieke risico voor kinderen en de daarbij horende overwegingen omtrent robuustheid, privacy, veiligheid en inclusiviteit is het heel goed mogelijk dat bijvoorbeeld de online verkoop van alcoholhoudende drank een andere methode van leeftijdsverificatie nodig heeft dan de toegang tot een social media platform. Om dit te illustreren laten wij door middel van een voorbeeld zien hoe zo'n afweging op hoofdlijnen in z'n werk zou kunnen gaan.

Online verkoop van alcoholhoudende dranken

Digitale diensten die digitale aankoop van alcoholhoudende dranken faciliteren kunnen negatieve impact op het kinderwelzijn en kinderrechten veroorzaken (zie content risico en consumentenrisico). Zoals we hebben gezien in hoofdstuk 3.1.3 is de verkoop van alcoholhoudende dranken aan minderjarigen verboden. Het verifiëren van de leeftijd van iemand die drank koopt is zowel offline als online verplicht. Leeftijdsverificatie wordt gezien als een mitigerende maatregel dat het risico kan helpen verminderen.

Mogelijke afweging ten aanzien van robuustheid

Omdat het in dit specifieke geval gaat om zaken die expliciet bij wet verboden zijn is een hoog niveau van robuustheid wenselijk. Hiervoor is een directe vorm van identificatie raadzaam. In de classificatie van ISO zou het dan minimaal gaan om niveau *standard* of hoger (zie hoofdstuk 7).

Mogelijke afweging ten aanzien van privacy

Het is van belang aan alle vereisten vanuit de AVG te voldoen (zie hoofdstuk 6.2.1). Bij een directe vorm van identificatie is het goed om te realiseren dat er waarschijnlijk gevoelige persoonsgegevens moeten worden verwerkt.

Ten aanzien van de verwerking van het BSN-nummer zijn daarnaast de volgende aandachtspunten van belang;

- Bij online leeftijdsverificatie mag het BSN-nummer in dit specifieke geval niet verwerkt worden omdat dit in geval van online verkoop van alcohol niet expliciet door de wet wordt voorgeschreven. Voor het verwerken van het BSN-nummer bij de online verkoop van alcohol is dus geen wettelijke grondslag.
- Wanneer een identiteitsdocument direct wordt gebruikt geldt dat alleen de noodzakelijke gegevens mogen worden verwerkt. De Autoriteit Persoonsgegevens laat weten dat een kopie van

een paspoort of ID, waarbij bijvoorbeeld het BSN en de pasfoto onzichtbaar zijn gemaakt, enkel mogelijk is als er echt geen andere manier is om het beoogde doel te bereiken.

- Op paspoorten die vóór 2021 zijn uitgegeven staat het BSN opgenomen in de MRZ-code op de voorpagina van het paspoort en het BSN standaard wordt uitgelezen bij het elektronisch openen van de chip op het paspoort. De methode voor leeftijdsverificatie op basis van directe identificatie moet daar dus een (technische) oplossing voor bieden.
- Als we uitgaan van de ISO-niveaus *standard, enhanced* en *strict* moet daarnaast geverifieerd worden dat de persoon die geïdentificeerd wordt daadwerkelijk leeft. Het is dus niet voldoende om identificerende gegevens op te sturen, deze moeten direct gekoppeld worden aan de persoon. Dit betekent dat bijvoorbeeld met behulp van een webcam een match gemaakt moet worden tussen de persoon en het document en er dus aanvullend (biometrische) persoonsgegevens worden verwerkt.

Afweging ten aanzien van beveiliging

De gebruiker moet voor dit niveau van robuustheid mogelijk gevoelige persoonsgegevens delen. Deze gegevens kunnen ook worden opgeslagen door de dienstverlener. Het beveiligingsniveau van deze data moet dan ook hoog zijn, zodat het risico op eventuele datalekken of inbreuken zo klein mogelijk is.

Afweging ten aanzien van toegankelijkheid en inclusiviteit

Voor inclusiviteit betekent dit mogelijk dat een deel van de gebruikers van de dienst worden uitgesloten, bijvoorbeeld als een (digitale) identiteit niet voorhanden is (zie hoofdstuk 8.4.4). In het geval van online alcoholverkoop moet dan ook worden afgewogen wat zwaarder weegt: het belang om kinderen te beschermen tegen de schadelijke gevolgen van alcoholische dranken of de toegankelijkheid en inclusiviteit van de dienst.

Mogelijke oplossingsrichtingen voor nader onderzoek

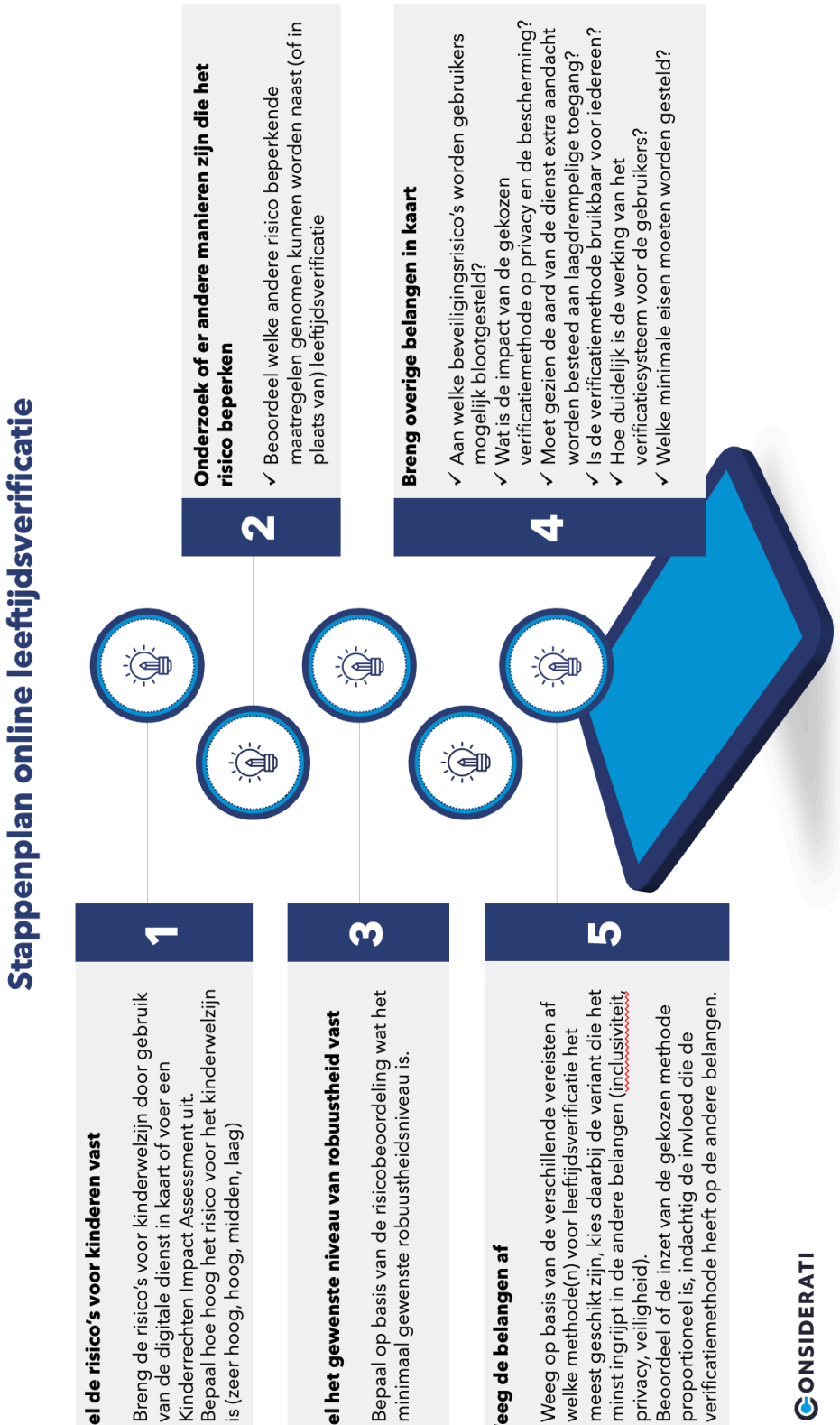
Het verwerken van een digitale identiteit kan mogelijk een robuust en privacy-vriendelijk alternatief opleveren voor de elektronische verwerking van het paspoort. Bij verschillende digital identity solutions wordt er lokaal op de randapparatuur van een gebruiker, zoals op een smartphone, een digitale kopie van een paspoort of een ander identificatiemiddel opgeslagen. In deze zogenaamde ‘wallet’ kunnen wettelijke identificatie documenten zoals paspoorten of identiteitskaarten worden opgeslagen. De gebruiker kan diens identiteit verifiëren door het maken van een biometrische match tussen de foto op het paspoort en een live gezichtsopname. De gebruiker beslist vervolgens welke attributen van diens identiteit (met uitzondering van het BSN) er worden gedeeld met de aanbieder van het online platform. De gebruiker behoudt in dit geval de controle over diens persoonsgegevens.

Het is zelfs mogelijk met ‘*zero knowledge proof*’ te werken, waarbij de aanbieder van het online platform uitsluitend de melding krijgt dat de leeftijd akkoord bevonden of niet akkoord bevonden is. Dit is met het oog op dataminimalisatie en een verantwoorde verwerking van persoonsgegevens mogelijk een oplossing. Verder onderzoek is nodig om te bezien of deze technologie kan bijdragen aan het invullen van de eisen.

Mogelijke afweging bij toegang tot social media

Waar bij online alcoholverkoop een zeer robuuste vorm van leeftijdsverificatie gewenst is, kan de afweging bij bijvoorbeeld de toegang tot social media platformen heel anders zijn. In deze context kan de waarde toegankelijkheid en inclusiviteit zwaarwegender zijn dan in het voorgaande voorbeeld. Bij het (onterecht) buitensluiten van gebruikers op social media kunnen de gevolgen groot zijn. Mensen halen steeds meer informatie van sociale media. In hoofdstuk 3.1.1 is uitgelegd dat het beperken van online vrijheid van kinderen hun zelfexpressie, persoonlijke ontwikkeling en persoonlijke autonomie kan belemmeren. Ook de sociale contacten tussen mensen vinden in toenemende mate online plaats. Het kan dan ook aanzienlijke gevolgen hebben voor mensen om buitengesloten te worden. Immers, het instellen van een systeem van online leeftijdsverificatie heeft impact op alle gebruikers, niet alleen op minderjarigen. Om te voorkomen dat kinderen worden blootgesteld aan bijvoorbeeld schadelijke content is het in dit geval wenselijk om risico's zoveel mogelijk op andere manieren te mitigeren.

Als de waarde toegankelijkheid zwaarwegend is, dan is het mogelijk problematisch om te kiezen voor een systeem dat (alleen) afhankelijk is van directe identificatie. Ook systemen gebaseerd op AI en bijvoorbeeld gezichtsherkenning kunnen problematisch zijn (zie hoofdstuk 8.2.4).


Stappenplan online leeftijdsverificatie
1
Stel de risico's voor kinderen vast
✓ Breng de risico's voor kinderwelzijn door gebruik van de digitale dienst in kaart of voer een Kinderrechten Impact Assessment uit.
✓ Bepaal hoe hoog het risico voor het kinderwelzijn is (zeer hoog, hoog, midden, laag)
2
Onderzoek of er andere manieren zijn die het risico beperken
✓ Beoordeel welke andere risico beperkende maatregelen genomen kunnen worden naast (of in plaats van) leeftijdsverificatie
3
Stel het gewenste niveau van robuustheid vast
✓ Bepaal op basis van de risicobeoordeling wat het minimaal gewenste robuustheidsniveau is.
4
Breng overige belangen in kaart
✓ Aan welke beveiligingsrisico's worden gebruikers mogelijk blootgesteld?
✓ Wat is de impact van de gekozen verificatiemethode op privacy en de bescherming?
✓ Moet gezien de aard van de dienst extra aandacht worden besteed aan laagdrempelige toegang?
✓ Is de verificatiemethode bruikbaar voor iedereen?
✓ Hoe duidelijk is de werking van het verificatiesysteem voor de gebruikers?
✓ Welke minimale eisen moeten worden gesteld?
5
Weeg de belangen af
✓ Weeg op basis van de verschillende vereisten af welke methode(n) voor leeftijdsverificatie het meest geschikt zijn, kies daarbij de variant die het minst ingrijpt in de andere belangen (inclusiviteit, privacy, veiligheid).
✓ Beoordeel of de inzet van de gekozen methode proportioneel is, indachtig de invloed die de verificatiemethode heeft op de andere belangen.
CONSIDERATI

CONSIDERATI

LEGAL | PUBLIC AFFAIRS | RESPONSIBLE TECH

Technologie en data bieden kansen voor elke organisatie. De toepassing hiervan is voorpaginanieuws geworden. Maar deze vernieuwing wringt. Organisaties lopen tegen juridische vraagstukken en maatschappelijke belangen aan. En als organisatie wilt u hierin de regie behouden.

Considerati is het juridisch en public affairs adviesbureau voor de digitale wereld, met kantoren in Amsterdam en Den Haag. Wij helpen organisaties maatschappelijk verantwoord te innoveren met digitale technologie en data. Dit doen we met drie gespecialiseerde teams:

Legal: voor een datastrategie die compliant is met privacyregelgeving

Responsible Tech: voor een ethisch kompas bij innoveren met data en algoritme

Public Affairs: voor maatschappelijk en politiek draagvlak voor innovaties

En dit doen we al meer dan 15 jaar voor zowel grote bedrijven en overheden als groeiende organisaties.

Contact

Neem contact met ons op via **info@considerati** of bel naar 020 73 70 069. Voor meer informatie kunt u ook kijken op onze website via **www.considerati.nl**.