RIVERWORKS
legal services

11 juli 2023

Betreft: Advies aan Kifid over wijze van identificatie en verificatie in het kader van de Wwft

---

1. Inleiding

1.1 Onderzoeksvraag Kifid

"De financiële dienstverlener, een onlinebank, vraagt voor de verificatie van de identiteit van nieuwe klanten naast onder meer een kopie van het identiteitsbewijs een video-opname op.
Is de door de financiële dienstverlener gehanteerde wijze van identificatie en verificatie gerechtvaardigd, in het licht van de AVG, met inachtneming van de verplichtingen onder de Wwft? Hoe verhoudt zich dit tot het beginsel van dataminimalisatie van de AVG? Kan opname van biometrische gegevens ter identificatie zondermeer verplicht worden?"

In dit advies beperk ik mij tot de Wwft aspecten van deze onderzoeksvraag. Ik zal mij daarbij richten op de volgende vragen, die in de navolgende hoofdstukken behandeld worden:

- Is de door de financiële dienstverlener gehanteerde wijze van identificatie gerechtvaardigd op grond van de verplichtingen uit hoofde van de Wwft regelgeving? (hoofdstuk 2)
- Geeft de Wwft aanwijzingen hoe in dit licht omgegaan moet worden met AVG aspecten? (hoofdstuk 3)
- Kan een video-opname met gebruik van biometrische gegevens op grond van de Wwft zonder meer verplicht worden? (hoofdstuk 4)

1.2 Uitgangspunten van dit advies

Niet alle gebruik van video-opnamen bij verificatie van de identiteit betekent dat er ook biometrische gegevens verwerkt worden. Alhoewel dat niet helemaal duidelijk blijkt uit de casus, ben ik er –mede gezien de vraagstelling- vanuit gegaan dat in dit geval inderdaad sprake is van verwerking van biometrische gegevens.

In het advies wordt in zijn algemeenheid ingegaan op de vraag of de gehanteerde vorm van identificatie en verificatie op grond van wet- en regelgeving mogelijk is en welke voorwaarden hieraan zijn verbonden. Een beoordeling van de betrouwbaarheid en passendheid van de gehanteerde technologie in deze casus valt buiten het kader van dit advies.

Voorts wordt in dit advies alleen ingegaan op de identificatie en verificatie die plaats vindt bij het aangaan van de zakelijke relatie. Bij een identificatie en verificatie die plaats vindt ná aangaan van de zakelijk relatie in het kader van artikel 38 Wwft, kunnen mogelijk ook andere overwegingen (zoals de algemene voorwaarden) een rol spelen.

Riverworks Legal Services **T** +31 (0) 6 242 05 809 **BTW** NL 01292864B2
Heemstede **E** ria@riverworkslegal.nl **KvK** 56581017

2. Is de wijze van identificatie gerechtvaardigd op grond van de Wwft ?

2.1 Verplicht cliëntenonderzoek

De verplichting tot identificatie en verificatie maakt onderdeel uit van het cliëntenonderzoek waartoe financiële dienstverleners op grond van artikel 2a lid 1 Wwft en art 3 lid 1 Wwft verplicht zijn. Het cliëntenonderzoek moet de financiële instelling -onder andere- in staat stellen de cliënt te identificeren en zijn identiteit te verifiëren. Zie art. 3 lid 2 sub a Wwft.

2.2 Open normen en risicogeoriënteerde benadering

De Wwft hanteert een stelsel van open normen. Dit betekent dat niet wordt voorgeschreven hoe het cliëntenonderzoek dient te worden verricht, maar alleen tot welk resultaat het onderzoek moet leiden. Door het te verrichten cliëntenonderzoek moeten financiële instellingen in staat zijn om te voldoen aan de eisen die gesteld worden in artikel 3 Wwft. Aangezien het de instelling vrij staat om te bepalen hoe tot het resultaat wordt gekomen, kan de wijze van uitvoering van cliëntenonderzoek in de praktijk sterk verschillen. Daarbij dient sprake te zijn van een risicogeoriënteerde benadering. Zie over het open normenstelsel en de risicogeoriënteerde benadering onder meer p. 6 en 7 van de MvT[1].

Risicofactoren die bij de risicogeoriënteerde aanpak een rol kunnen spelen zijn onder andere het type cliënt, het geografisch gebied, het leveringskanaal en de aard van het product of de dienst. De instelling moet de risico's die voor haar gelden vaststellen en beoordelen. De resultaten van de risicobeoordeling moeten worden vastgelegd. De instelling moet voorts beschikken over gedragsregels, maatregelen en procedures om de risico's te beperken en te beheersen. De te nemen maatregelen kunnen zijn afgestemd op de aard en omvang van de instelling (zie art. 2b en 2c Wwft).

2.3 Richtsnoeren ML/TF Risicofactoren

In 2021 heeft de EBA richtsnoeren uitgevaardigd waarin de risicogeoriënteerde benadering nader wordt uitgewerkt (Richtsnoeren ML/TF Risicofactoren van 1 maart 2021, hierna "Richtsnoeren 2021/02[2]).

In de Richtsnoeren 2101/02 is een sectorale Richtsnoer voor retailbanken opgenomen vanaf p 61. Daarin worden onder §9.2 de specifieke risico's van deze sector als volgt verwoord:

> *"Door de aard van de aangeboden producten en diensten, de relatief gemakkelijke toegang en het vaak grote aantal transacties en zakelijke relaties, is retailbanking kwetsbaar voor terrorismefinanciering en voor alle fasen van het witwasproces. Tegelijkertijd kan de hoeveelheid zakelijke relaties en transacties die verband houden met retailbanking, het erg lastig maken om het aan afzonderlijke relaties verbonden ML/TF-risico te identificeren en verdachte transacties op te merken".*

Het is dus niet zo, dat het feit dat het om een relatief eenvoudig product gaat per definitie betekent dat er sprake is van een relatief laag risico.

2.4 Potentieel verhoogd risico bij identificatie op afstand

Vóór de implementatie van de gewijzigde vierde anti-witwasrichtlijn (op 25 juli 2018) werd elke vorm van identificatie en verificatie zonder fysieke aanwezigheid van de cliënt gezien als een verhoogd

---

[1] Kmst. II 2007-2008, 31238 nr. 3 p. 6 en 7

[2] EBA/GL/2021/02 Richtsnoeren ML/TF-risicofactoren, 1 maart 2021 p. 35 (deze Richtsnoeren zijn momenteel onder revisie in verband met een toegevoegd hoofdstuk voor NPO's. In het kader van dit advies is deze revisie echter niet relevant)

risico, waarbij maatregelen verplicht waren om dit verhoogde risico te compenseren (art. 8 lid 2 Wwft (oud)).

Omdat er inmiddels ook elektronische identificatiemiddelen bestaan die voldoende betrouwbaar kunnen zijn, wordt dit In het huidige art. 8 lid 2 Wwft niet meer zo absoluut gesteld. In de huidige tekst wordt verwezen naar de risicofactoren in bijlage III van de Richtlijn (EU) 2015/849 (hierna "de Richtlijn"[3]),. In deze bijlage wordt onder punt 2 sub c als potentiele risicofactor genoemd:

> *"zakelijke relaties op afstand of transacties op afstand, zonder bepaalde garanties, zoals elektronische identificatiemiddelen of relevante vertrouwensdiensten zoals gedefinieerd in Verordening (EU) nr. 910/2014 of ieder andere identificatieproces dat veilig is, op afstand of langs elektronische weg plaatsvindt en door de relevante nationale autoriteiten is gereglementeerd, erkend, goedgekeurd of aanvaard"*

Dit betekent, dat als er geen sprake is van bepaalde gegarandeerde identificatiemiddelen (onder de Wwft: identificatiemiddelen die voldoen aan het betrouwbaarheidsniveau "substantieel" of "hoog" als bedoeld in de eIDAS verordening, zie hierna onder 2.5), de identificatie op afstand kan bijdragen aan een verhoogd risico in de zin van art. 8 Wwft waardoor een verscherpt cliëntenonderzoek noodzakelijk zou zijn.

Dit hoeft niet zo te zijn als andere maatregelen binnen het identificatieproces het risico van de niet fysieke aanwezigheid van de cliënt voldoende mitigeren. Bij de beoordeling of er sprake is van een relatie met een verhoogd risico zal de instelling dit aspect van fysieke afwezigheid in ieder geval mee moeten nemen. Daar komt bij dat, als er in het identificatieproces gebruik wordt gemaakt van nieuwe technologieën die zich nog onvoldoende bewezen hebben, dit op zich ook een potentiele risicofactor is (zie bijlage III van de Richtlijn onder punt 2 sub e).

Of er nu wel of niet sprake is van een verhoogd risico in de zin van art. 8 Wwft doet overigens niets af aan de eis dat de verificatie van de identiteit plaats dient te vinden aan de hand van betrouwbare en onafhankelijke bronnen, zoals vastgelegd is in art. 11. Wwft. In alle gevallen zal ten minste een betrouwbare vorm van identificatie plaats moeten vinden (Richtsnoeren 2021/02, § 1.24 op p.12[4]).

2.5 Betrouwbare en onafhankelijke bron

Verificatie van de identiteit van natuurlijke personen dient plaats te vinden aan de hand van documenten, gegevens of inlichtingen uit betrouwbare en onafhankelijke bron (art 11 lid 1 Wwft).

Art 11 wordt nader uitgewerkt in artikel 4 lid 1 van de "Uitvoeringsregeling Wet te voorkoming van witwassen en financiering van terrorisme" (hierna "Uitvoeringsregeling"), waarbij documenten worden aangewezen die (in ieder geval) voldoen aan de kwalificatie "betrouwbare en onafhankelijke bron". Het gaat hier om een niet-limitatieve opsomming (zie p. 10 MvT onder iii[5]). Zie ook de toelichting op art 4 lid 1 van de Uitvoeringsregeling[6]:

> *"Deze opsomming is niet-limitatief zodat verificatie ook kan plaatsvinden aan de hand van andere documenten, gegevens of inlichtingen uit onafhankelijke bron. Dit houdt verband met de principle*

---

[3] Richtlijn (EU) 2015/849 van het Europees parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, zoals gewijzigd bij Richtlijnen (EU)2018/843 en 2019/2177 (geconsolideerde tekst)

[4] EBA/GL/2021/02 Richtsnoeren ML/TF-risicofactoren, 1 maart 2021 p.12

[5] Kmst. II 2007-2008, 31238 nr. 3 p.10

[6] Stcrt 2008/142/ pag 8 p.3

based benadering van de wet: voorgeschreven is tot welk resultaat het cliëntenonderzoek moet leiden maar niet hoe het onderzoek dient te worden uitgevoerd. Voordeel is dat deze formulering aan instellingen de mogelijkheid biedt om gebruik te maken van eventuele technologische ontwikkelingen waarmee een efficiëntiewinst behaald kan worden."

In 2020 is de Uitvoeringsregeling gewijzigd bij de implementatie van de gewijzigde vierde anti-witwasrichtlijn. De wijziging is op 22 mei 2020 in werking getreden. Vóór 22 mei 2020 waren in art. 4 lid 1 alleen de punten a t/m g opgenomen, die allen betrekking hebben op identificatiedocumenten. Per genoemde datum is als punt h toegevoegd: "een voldoende betrouwbaar identificatiemiddel". Bedoeling was om hiermee meer expliciet aan te geven dat ook andere (elektronische) identificatiemiddelen een voldoende betrouwbare bron kunnen zijn in de zin van art. 11 Wwft.

Uit de Toelichting[7] op deze wijziging blijkt dat in ieder geval elektronische identificatiemiddelen die voldoen aan het betrouwbaarheidsniveau 'substantieel' of 'hoog' als bedoeld in de eIDAS verordening[8] als betrouwbare en onafhankelijke bron worden gezien. Wordt gebruik gemaakt van andere identificatiemiddelen dan is het de verantwoordelijkheid van de financiële dienstverlener om aan te tonen dat het gebruikte identificatieproces -op basis van een risicogeoriënteerde benadering- voldoende betrouwbaar is en voldoet aan art. 11 Wwft.

2.6 Welke identificatie of verificatiemiddelen op afstand kunnen gehanteerd worden?

Uit de wetshistorie zoals boven beschreven blijkt dat een financiële dienstverlener bij het identificatieproces gebruik kan maken van nieuwe technologische ontwikkelingen. Ook in de Leidraad Wwft en Sw van DNB[9] (hierna "Leidraad DNB ") blijkt dat DNB er van uit gaat dat het mogelijk is om gebruik te maken van innovatieve technologische oplossingen bij identificatie en verificatie op afstand. Zie p.49 waar het voorbeeld wordt genoemd van video-identificatie en –verificatie.

Alhoewel hier niet expliciet wordt gesproken over het gebruik van biometrische gegevens, verwijst de Leidraad DNB wel naar een opinie van de European Supervisory Authorities (ESA)[10] die in 2018 is verschenen (hierna "de Opinie"). In deze Opinie wordt beoogd om bepaalde standaarden te stellen voor de toepassing van innovatieve oplossingen bij het cliëntenonderzoek. Deze Opinie gaat er van uit dat ook biometrische gegevens van de cliënt een rol kunnen spelen (zie bijvoorbeeld hoofdstuk 19 p. 14 van de Opinie, waar gesproken wordt over biometrische gezichtsherkenning bij video-opnamen).

De Leidraad Wwft en Sanctiewet van de AFM[11] (hierna "Leidraad AFM") wijkt in dit opzicht niet af van de Leidraad DNB (zie p. 26/27). Na het verschijnen van de Leidraden van DNB en AFM heeft de EBA nog twee richtsnoeren uitgevaardigd die in dit verband relevant zijn. De richtsnoeren zijn gericht tot zowel de toezichthouder als tot de kredietinstellingen en financiële instellingen. Het gaat om de volgende twee Richtsnoeren:

---

[7] Stcrt 2020 nr. 27198 onder B

[8] Verordening (EU) nr. 910/2014 van het Europees parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257)

[9] Leidraad Wwft en Sw versie december 2020, De Nederlandsche Bank, p.49

[10] JC 2017 81 ESA: Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process, 23 januari 2018 p.14

[11] Leidraad Wwft en Sanctiewet AFM 19 oktober 2020 p.26-27

- De eerdergenoemde Richtsnoeren ML/TF Risicofactoren van 1 maart 2021[12] (Richtsnoeren 2021/02)
- Richtsnoeren voor het gebruik van oplossingen voor de acceptatie van cliënten op afstand van 22 november 2022[13] (hierna Richtsnoeren 2022/15)

In de Richtsnoeren 2021/02 wordt op p. 34-36 aandacht gegeven aan situaties op afstand. In §4.32 wordt aangegeven dat instellingen, vanwege het technologie neutrale karakter van Richtlijn kunnen kiezen voor het gebruik van elektronische of schriftelijke middelen of een combinatie daarvan, om de identiteit van hun cliënten te verifiëren

Ten aanzien van het gebruik van innovatieve technologische oplossingen wordt aangegeven dat de instelling onder meer aandacht moet schenken aan de volgende risico's (§4.33):

- ICT- en veiligheidsrisico's;
- het risico dat de mate van identiteitsverificatie die de technologische oplossing biedt niet in verhouding staat tot het aan de zakelijke relatie verbonden ML/TF-risiconiveau;
- het risico dat de aanbieder van de technologische oplossing niet voldoet aan de geldende wetgeving inzake gegevensbescherming;
- risico's op gebruik van valse identiteiten en identiteitsfraude.

De instelling moet ten overstaan van de bevoegde autoriteit aan tonen dat het gebruik van de innovatieve oplossing passend is (§4.36). Voorts verwijst deze richtsnoer ten aanzien van het gebruik van innovatieve technologische identificatiemiddelen , evenals de Leidraad DNB en de Leidraad AFM, naar de eerdere Opinie van de ESA (zie §4.37 p. 36).

De Richtsnoeren 2022/15 zijn vrij recent verschenen. Uiterste ingangsdatum is 2 oktober 2023. DNB heeft aangegeven per 30 mei 2023 aan deze richtsnoeren te voldoen. De laatste richtsnoeren zijn volledig gewijd aan het gebruik van innovatieve oplossingen voor identificatie en verificatie op afstand. In deze richtsnoeren wordt expliciet aandacht geschonken aan het gebruik van biometrische gegevens (zie p. 13 en 14, met name de punten 39 en 41). Dat deze Richtsnoeren nog niet in werking zijn getreden doet niets af aan het feit dat het gaat om richtsnoeren voor reeds bestaande regelgeving.

Op grond van het bovenstaande kan worden geconcludeerd dat de regelgeving ruimte biedt voor innovatieve technologische oplossingen voor identificatie op afstand, waaronder ook het gebruik van biometrische gegevens. De instelling is verplicht de keuze voor de gehanteerde identificatiemethode waarbij technologische oplossingen worden gehanteerd, vooraf te onderbouwen en te documenteren. Daarbij moeten zij aantonen dat de gehanteerde oplossing passend is. Zie § 4.36 van de Richtlijnen 2021/02[14] en ook punt 16 op p.7 van de Richtsnoeren 2022/15[15]

[12] EBA/GL/2021/02 Richtsnoeren ML/TF-risicofactoren, 1 maart 2021 p.34-36
[13] EBA/GL/2022/15, Richtsnoeren voor het gebruik van oplossingen voor de acceptatie op afstand, 22 november 2022 p13-14
[14] EBA/GL/2021/02 Richtsnoeren ML/TF-risicofactoren, 1 maart 2021 p.36
[15] EBA/GL/2022/15, Richtsnoeren voor het gebruik van oplossingen voor de acceptatie op afstand, 22 november 2022 p.7

3. Geeft de Wwft aanwijzingen hoe omgegaan moet worden met AVG aspecten?

(Aangezien er een apart advies wordt opgesteld vanuit de optiek van de bescherming persoonsgegevens is in dit advies vooral gekeken naar wat de Wwft regelgeving aangeeft over de bescherming van persoonsgegevens)

3.1 Bepalingen Richtlijn en Wwft over verwerking persoonsgegevens

In de Richtlijn wordt in art. 41 bepaald dat de verwerking van persoonsgegeven op grond van de Richtlijn onderworpen is aan de AVG.

In art 34a Wwft is ter implementatie van artikel 41 van de Richtlijn een apart artikel over gegevensbescherming opgenomen. Art. 34a Wwft regelt het volgende:

- doelbinding (gegevens mogen alleen worden verwerkt voor zover noodzakelijk met het oog op het voorkomen van witwassen en financieren van terrorisme),
- verplichting tot precontractuele informatieverschaffing (transparantie)
- de verplichting de gegevens te vernietigen na het verstrijken van de bewaartermijn.

Dit artikel geeft dus een aantal waarborgen hoe omgegaan moet worden persoonsgegevens die verzamelt zijn in het kader van de Wwft verplichtingen.

In de MvT[16] wordt er van uitgegaan dat de verwerking van persoonsgegevens in het kader van de Wwft, verwerkingen zijn op grond van een wettelijke verplichting in de zin van art. 6, eerste lid, onderdeel c, AVG. In art. 43 van de Richtlijn wordt bovendien bepaald dat de verwerking van persoonsgegevens in het kader van de Richtlijn wordt beschouwd als een taak van algemeen belang in de zin van de AVG. Op grond daarvan kunnen deze verwerkingen mogelijk ook worden gezien als verwerkingen in de zin van art. 6 eerste lid, onderdeel e, AVG .

3.2 Is in de Wwft iets geregeld over de verwerking van biometrische gegevens?

Momenteel wordt in de Wwft geen onderscheid gemaakt naar de aard van de te verwerken persoonsgegevens. De enige beperking in art 34a Wwft is dat persoonsgegevens alleen mogen worden verwerkt voor zover noodzakelijk met het oog op het voorkomen van witwassen en financieren van terrorisme. Dit roept de vraag op hoe dit zich verhoudt tot het verbod op het verwerken van bijzondere categorieën van persoonsgegevens op grond van art. 9 lid 1 AVG. Eén van die bijzondere categorieën is het verwerken van "biometrische gegevens met het oog op de unieke identificatie van een persoon". Op het verbod wordt echter in lid 2 sub g een uitzondering gemaakt als de verwerking noodzakelijk is om redenen van "zwaarwegend algemeen belang" op grond van Unierecht of lidstatelijk recht.

Of er bij het verwerken van gegevens op grond van de Wwft verplichtingen sprake is van een zwaarwegend algemeen belang als bedoeld in de AVG blijkt niet uit de Richtlijn zelf. Wél wordt in de overwegingen (nr 42) aangegeven dat bestrijding van witwassen en terrorismefinanciering door alle lidstaten wordt erkend als een zwaarwegend algemeen belang.

Onze Nederlandse wetgever heeft meerdere malen aangegeven de gegevensverwerking op grond van de Wwft te beschouwen als een zwaarwegend algemeen belang in de zin van de AVG. Bijvoorbeeld bij de implementatie van de vierde anti-witwasrichtlijn, zie MvT § 4.1, p. 13[17] en ook bij de latere implementatiewet wijziging vierde anti-witwasrichtlijn, zie MvT § 6 p.21[18] . Echter dit bleek tot nu alleen uit de toelichting en niet uit de Wwft zelf. Daardoor kon discussie ontstaan of dit onderdeel vormt van het "lidstatelijke recht". Momenteel is een wijzigingsvoorstel in behandeling bij

[16] Kmst II 2017–2018, 34 808, nr. 3 p.12
[17] Kmst II 2017–2018, 34 808, nr. 3 p.13
[18] Kmst II 2018–2019, 35 245, nr. 3 p.21

de Tweede Kamer (Wet Plan van Aanpak Witwassen) dat eventuele onduidelijkheid op dit punt moet wegnemen.

Als dit voorstel wordt aangenomen zal aan art 34a Wwft een nieuw lid 1 worden toegevoegd waarin uitdrukkelijk bepaald wordt, dat de uitzondering van art. 9 lid 2 sub g AVG (zwaarwegend algemeen belang) van toepassing is op het moment dat er bijzondere categorieën van persoonsgegevens worden verwerkt op grond van verplichtingen uit de Wwft[19]. De tekst zou als volgt komen te luiden:

> *"1. Voor zover noodzakelijk om aan de verplichtingen te voldoen gesteld bij of krachtens deze wet zijn instellingen bevoegd om persoonsgegevens te verwerken, waaronder bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard als bedoeld in artikel 1 van de Uitvoeringswet Algemene verordening gegevensbescherming. Gelet op artikel 9, tweede lid, onderdeel g, van de Algemene verordening gegevensbescherming is het verbod om bijzondere categorieën van persoonsgegevens respectievelijk persoonsgegevens van strafrechtelijke aard te verwerken in dat geval niet van toepassing."*

Dat de wetgever dit nu ook als geldend recht beschouwt, blijkt uit het feit dat de wijziging een verduidelijking wordt genoemd (zie ook de MvT onder § 2.3 p. 14[20]).

3.3 Biometrische gegevens voor authenticatie of beveiligingsdoeleinden

De tekst van het voorgestelde nieuwe artikel 34aWwft is zodanig breed geformuleerd dat ook het verwerken van biometrische gegevens bij het identificatieproces daaronder valt.

Voor deze biometrische gegevens zou op dit moment ook een beroep kunnen worden gedaan op art. 29 van de Uitvoeringswet AVG (UAVG). Op grond van artikel 29 UAVG is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken, namelijk niet van toepassing indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Als het wijzigingsvoorstel voor het nieuwe artikel 34a Wwft wordt aangenomen zal een beroep op art 29 UAVG echter niet meer nodig zijn.

3.4 Noodzakelijkheidsvereiste

Bij de totstandkoming van de Richtlijn is uitdrukkelijk overwogen dat het verwerken van persoonsgegevens beperkt dient te blijven tot hetgeen noodzakelijk is met het oog op voorkomen van witwassen en financieren van terrorisme. Dit is geïmplementeerd in art. 34a lid 1 Wwft.

Over de noodzaak van goede identificatie en verificatie zegt de MvT[21] het volgende (p.16):

> *"Een goede identificatie is noodzakelijk omdat het gedurende de relatie nodig kan blijken om een melding van een ongebruikelijke transactie te doen. De identiteitsgegevens moeten ook beschikbaar zijn voor eventueel onderzoek van nationale of buitenlandse opsporingsautoriteiten. In bepaalde gevallen wordt het noodzakelijk geacht verder te gaan dan het vaststellen en verifiëren van de identiteit van de betrokkene. De risico inschatting van de instelling speelt hierbij een belangrijke rol. "*

Het cliëntenonderzoek is naast de meldingsplicht één van de twee kernverplichtingen van de anti-witwasregelgeving. De verplichting tot identificatie en verificatie vormt hiervan een belangrijke

[19] Kmst II 2022–2023, 36 228, nr. 2 p.4-5
[20] Kmst II 2022–2023, 36 228, nr. 3 p.14
[21] Kmst. II 2007-2008, 31238 nr. 3 p.16

onderdeel. Zonder goede identificatie vervalt immers de grondslag onder het cliëntenonderzoek (zie MvT §4.1, p. 13[22]):

> *"Het verwerven van kennis en informatie over de identiteit van de cliënt, diens UBO en het doel en de aard van een zakelijke relatie of incidentele transactie is onmisbaar om signalen die kunnen duiden op witwassen, daaraan ten grondslag liggende basisdelicten, of terrorismefinanciering vroegtijdig te kunnen herkennen. Ook voor het functioneren van de opsporingsautoriteiten is deze informatie essentieel. Het voorkomen van witwassen en financieren van terrorisme wordt aangemerkt als een zwaarwegend algemeen belang"*

Een betrouwbaar identificatieproces ter voorkoming van identiteitsfraude is op grond van de Wwft verplichtingen dus onontbeerlijk. De instelling moet te allen tijden de noodzakelijke maatregelen nemen om er zeker van te zijn dat de potentiele cliënt de persoon is voor wie hij zich uitgeeft.

Dat het, bij bepaalde vormen van identificatie op afstand, noodzakelijk kan zijn om gebruik te maken video-opnamen lijkt onvermijdelijk. Bij identificatie op afstand is de cliënt niet fysiek aanwezig. Instellingen dienen daarom rekening te houden met het risico dat de persoon geen werkelijke persoon is. Video-opnamen kunnen dan de fysieke afwezigheid compenseren. Wanneer er sprake is van een identificatieproces zonder menselijke tussenkomst, zal daarbij ook het gebruik van biometrische gegevens noodzakelijk kunnen zijn. Zie bijv. punt 39 en 41 op p 13 en 14 van Richtsnoeren 2022/15[23].

De risico gebaseerde aanpak laat ruimte voor een op de aard en omvang van een organisatie afgestemd identificatieproces. Het identificatieproces moet bovendien zodanig worden ingericht dat de instelling de gesignaleerde risico's op een adequate manier kan beheersen. Zo zal bij een online-organisatie, die niet is ingericht op fysieke contacten met de cliënt, een online-identificatieproces eerder voor de hand liggen. Maar er zijn zoals in hoofdstuk 2 is aangegeven meerdere factoren die van belang zijn bij de risicoanalyse en het daarop gebaseerde identificatieproces.

Omdat instellingen zelf hun risico's identificeren en daarop hun identificatieproces aanpassen, dienen zij daarbij ook zelfstandig te beoordelen in welke mate daarbij gegevensverwerking noodzakelijk is om hun verplichtingen op grond van de Wwft te voldoen. Dit wordt nog eens bevestigd in de MvT bij het wetsvoorstel voor het nieuwe art. 34a Wwft[24]:

> *"Uit het bovenstaande volgt dat het voor instellingen alleen is toegestaan om bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard te verwerken indien dat noodzakelijk is om aan de verplichtingen te voldoen, gesteld bij of krachtens deze wet. Instellingen dienen zelfstandig te beoordelen in welke mate gegevensverwerking noodzakelijk is om aan die verplichtingen te voldoen."*

Het enkele feit dat er vormen van identificatie en verificatie bestaan waarbij geen of minder biometrische gegevens worden verwerkt (zoals een fysiek identificatie), betekent naar mijn mening niet dat de instelling verplicht is deze andere vormen ook aan te bieden. Ook al zijn deze vormen van identificatie mogelijk minder bezwaarlijk voor de cliënt in het kader van privacy. Dit zou in strijd zijn met de in de Wwft voorgeschreven risico-gebaseerde aanpak.

---

[22] Kmst II 2017–2018, 34 808, nr. 3 p.13
[23] EBA/GL/2022/15, Richtsnoeren voor het gebruik van oplossingen voor de acceptatie op afstand, 22 november 2022 p.13,14
[24] Kmst II 2022–2023, 36 228, nr. 3 p.52

Het noodzakelijksvereiste op grond van de Wwft wordt dus mede ingekleurd door het antwoord op de vraag in hoeverre een identificatieproces passend is in het licht van de geïdentificeerde risico's. De uiteindelijke inrichting van het identificatieproces is daarmee een resultante van een afwegings- en beoordelingsproces waarbij vele factoren een rol spelen. Zoals in hoofdstuk 2.7 is aangegeven is het aan de instelling om de gemaakte keuzes te onderbouwen.

4. Kan een video-opname met gebruik van biometrische gegevens zonder meer verplicht worden?

Mits het identificatieproces passend/noodzakelijk is in het kader van de uitvoering van de Wwft verplichtingen, kan een instelling een beroep doen op de uitzonderingsbepaling van art. 9 lid 2 sub g AVG om gebruik te kunnen maken van biometrische gegevens bij de identificatie en verificatie. Uitdrukkelijke toestemming van de cliënt op grond van art.9 lid 2 sub a is dan geen vereiste.
Dat betekent dat een instelling bij het aangaan van de relatie de cliënt verplicht kan stellen het identificatieproces, zoals dat door de instelling gehanteerd wordt, te doorlopen.

Daartegenover staat dat de potentiele cliënt de vrijheid heeft om op grond daarvan van de relatie af te zien. In de fase van het aangaan van de relatie heeft de cliënt immers een reële keuzevrijheid. Hij kan het gehanteerde identificatieproces mee laten wegen bij de keuze van een aanbieder.

De vraag of een instelling verplicht is om een alternatief te bieden doet zich voor in situaties waarin de uitdrukkelijke toestemming vereist is. Om er zeker van te zijn dat de toestemming in vrijheid wordt gegeven (met name in een afhankelijkheidsrelatie zoals tussen werkgever-werknemer) is het belangrijk dat er sprake is van een keuzemogelijkheid. Deze situatie doet zich hier niet voor.

Er is in deze casus dan ook geen reden om aan te nemen dat de instelling verplicht zou zijn om een alternatief te bieden aan cliënten die bezwaar maken tegen de gehanteerde identificatiemethode. De Rechtbank Amsterdam[25] heeft onlangs een uitspraak gedaan in een casus waarin sprake was van (her)identificatie binnen een bestaande relatie. Daarin werd geoordeeld dat de cliënt geen recht had op fysieke identificatie.

Als een instelling, naast het proces waarbij gebruik wordt gemaakt van biometrie, wél een alternatief aan zou bieden, dan zal zij er rekening mee moeten houden dat dit alternatief van gelijkwaardige betrouwbaarheid moet zijn. Bovendien kan het hanteren van een niet-eenduidig identificatiesysteem mogelijk de beheersbaarheid van het proces beïnvloeden. Alternatieve vormen van identificatie kunnen daarom door een cliënt niet worden afgedwongen.

5. Conclusies

5.1 Is de wijze van identificatie gerechtvaardigd op grond van de Wwft ?

De Wwft biedt in principe ruimte voor vormen van innovatieve technologische oplossingen voor identificatie en verificatie op afstand. Oók als daarbij sprake is van verwerking van biometrische gegevens. Of de specifieke oplossing in een bepaald geval op grond van de Wwft gerechtvaardigd is, hangt af van de aard en omvang van de instelling en haar risicoanalyse en beoordeling.
Hieraan gerelateerd moet het identificatieproces passend zijn, dat wil zeggen voldoende betrouwbaar en beheersbaar. De instelling is verplicht de keuze voor de gehanteerde

[25] ECLI:NL:RBAMS:2023:145, Rechtbank Amsterdam, C/13/718627 / HA ZA 22-458 (rechtspraak.nl)

identificatiemethode vooraf te onderbouwen en te documenteren en moet ten overstaan van de bevoegde autoriteit aan kunnen tonen dat het gebruik van een bepaalde innovatieve oplossing passend is.

5.2 Geeft de Wwft aanwijzingen hoe omgegaan moet worden met AVG aspecten?

De Wwft maakt (nog) geen onderscheid tussen bijzondere categorieën persoonsgegevens en "gewone" persoonsgegevens. De enige eis die de Wwft stelt, is dat de verwerking van (biometrische) persoonsgegevens noodzakelijk moet zijn om aan de Wwft verplichtingen te voldoen. De instelling dient zelfstandig te beoordelen in welke mate gegevensverwerking noodzakelijk is voor de identificatie en verificatie van haar cliënten. Het noodzakelijksvereiste wordt mede ingekleurd door het antwoord op de vraag in hoeverre het identificatieproces passend is in het licht van de geïdentificeerde risico's.

5.3 Kan een video-opname met gebruik van biometrische gegevens zonder meer verplicht worden?

Een instelling kan bij het aangaan van een relatie de cliënt verplichten om het door haar gehanteerde identificatieproces te doorlopen. Daartegenover staat de keuzevrijheid van de cliënt om wel of niet voor deze aanbieder te kiezen. Er is geen aanleiding om aan te nemen dat de instelling verplicht kan worden om een alternatief identificatieproces aan te bieden.

Riverworks Legal Services
11 juli 2023