Wwft en de Avg: Zijn instellingen verplicht om kopieën van legitimatiebewijzen te bewaren? Annotatie bij Gerechtshof Amsterdam, 30 april 2024, ECLI:NL:GHAMS:2024:1165 (Servicekosten Consultancy/International Card Services [ICS])

Mekić, D.

6. De afgelopen jaren is in de literatuur opgemerkt dat rechters bij beoordeling van de zorgplicht van een IT-leverancier niet schuw zijn om contractsbepalingen opzij te zetten ter interpretatie van de tussen partijen levende verwachtingen.[12] Na een kijk op de contracttekst, wordt buiten die tekst gezocht naar gebruikelijk- of feitelijkheden om uiteindelijk tot een conclusie te komen die de rechter redelijk of passend vindt. Voor de lezer van dit arrest, zonder beschikking over het hele dossier,[13] lijkt de door het Hof Amsterdam geformuleerde deskundigenopdracht te passen in deze trend. Nu wachten op de (publicatie van) verdere beoordeling.

Mrs. B.M. Dijkmans van Gunst & J. Koolhaas

Computerrecht 2024/218

HOF AMSTERDAM
30 april 2024, 200.324.736/01
(Mrs. M.C.H. Broesterhuizen, S.C.H. Molin en Y. Steeg-Tijms)
m.nt. D. Mekić[1]

(Art. 5 lid 3 VEU; art. 7 en 8 EU Handvest; art. 5, 6 AVG; art. 13 lid 1 sub a Richtlijn (EU) 2015/849 (4AMLD); art. 3, 5, 11, 33, 38 Wwft; art. 4 lid 1 Uitvoeringsregeling Wwft)

Module Privacy & AVG 2024/4409
ECLI:NL:GHAMS:2024:1165

Verificatieplicht en reconstructieplicht op grond van de Wwft en de Avg: recht op verstrekken beschreven kopie legitimatiebewijs? Zijn instellingen verplicht om kopieën van legitimatiebewijzen te bewaren? Mag een betrokkene zich daartegen verzetten?

Arrest (ingekort) in de zaak van
SERVICEKOSTEN CONSULTANCY V.O.F., gevestigd te Hoofddorp, 2. [appellant 2], wonende te [woonplaats], appellanten, advocaat: mr. B.O. Eschweiler te Amsterdam,
tegen
INTERNATIONAL CARD SERVICES B.V. gevestigd te Amsterdam, geïntimeerde, advocaat: mr. A.L. Bremmer te Amsterdam. Partijen worden hierna SKC, [appellant 2] (gezamenlijk: [appellanten]) en ICS genoemd.

1 **De zaak in het kort**

[appellanten] heeft sinds 2015 een zakelijke creditcard van ICS. In 2021 heeft ICS [appellanten] verzocht om zich online te identificeren. [appellanten] heeft bezwaren tegen de wijze waarop deze identificatie plaatsvindt en hoe zijn gegevens daarbij worden verwerkt, met name tegen het scannen van het identiteitsbewijs van [appellant 2] waarbij een kopie van het identiteitsbewijs wordt opgeslagen. [appellanten] wil zelf een gewaarmerkte kopie van het identiteitsbewijs kunnen aanleveren. Dit heeft ICS niet geaccepteerd. ICS heeft aangekondigd de creditcard te zullen blokkeren en mogelijk de overeenkomst te zullen opzeggen. De rechtbank heeft de vorderingen van [appellanten], waarmee hij dit beoogt te voorkomen, afgewezen.
[…]

3 **Feiten**

Het hof gaat uit van de volgende feiten.
3.1. SKC, waarvan [appellant 2] vennoot is, houdt sinds 2015 een zakelijke creditcard aan bij ICS, een dochtervennootschap van ABN AMRO Bank N.V. De creditcard is op naam gesteld van [appellant 2] Servicekosten Consultancy en wordt door [appellant 2] gebruikt voor zakelijke betalingen.
3.2. [appellant 2] houdt ook een privé creditcard aan bij ICS, waarvan hij en zijn echtgenote ieder kaarthouder zijn.
3.3. Op de overeenkomsten met [appellanten] zijn de Algemene Card-voorwaarden ICS van januari 2021 (hierna: de algemene voorwaarden) van toepassing.
3.4. In 2020 is ICS gestart met het (opnieuw) controleren van de identiteit van haar klanten. Bij e-mailbericht van 4 mei 2021 heeft ICS SKC verzocht de bedrijfsgegevens te controleren en aan te vullen. Nadat [appellant 2] de gegevens van SKC had aangevuld, ontving hij dezelfde dag een e-mailbericht van ICS met het verzoek zich online te identificeren.
[…]
3.5. Volgens de door ICS op haar website weergegeven uitleg houdt de online identificatie kort gezegd het volgende in. De klant downloadt de app “ICS Identificeren” op een smartphone. De klant vult zijn geboortedatum en de ontvangen persoonlijke validatiecode in. Vervolgens kiest de klant welk identiteitsbewijs hij wenst te gebruiken voor de identificatie. De klant maakt een foto van het originele identiteitsbewijs. Een foto van een foto of een kopie van het identiteitsbewijs wordt niet goedgekeurd. Het identiteitsbewijs dient onbeschreven te zijn. Daarnaast maakt de klant een foto van zichzelf met de smartphone (selfie). Ook hiervoor geldt dat een foto van een foto niet wordt goedgekeurd. Tot slot slaat de klant beide foto’s op in de app (uploaden).
3.6. Verder is op de website van ICS onder het kopje “veelgestelde vragen” over de online identificatie het volgende te lezen, voor zover hier relevant:

12 Ontwikkelingen rechtspraak IT-wanprestatie – papier versus praktijk’, *Computerrecht* 2023/211, p. 359.
13 Helaas ook, is de zaak in eerste aanleg niet gepubliceerd: Rb. Noord-Holland 16 maart 2022, ECLI:NL:RBNHO:2022:2868.
1 Danny Mekić is promovendus bij eLaw, Centrum voor Recht en Digitale Technologie, Universiteit Leiden en de Eindhoven University of Technology. Hij dankt prof. dr. G.-J. Zwenne voor het meelezen en zijn waardevolle opmerkingen.

"Waarvoor gebruiken jullie de foto van mijn identiteitsbewijs?

We gebruiken de foto van uw identiteitsbewijs voor de identificatie en de controle van uw gegevens. Via de foto controleren we of uw identiteitsbewijs echt is, en of het echt van u is. We bewaren de foto daarna als bewijs van uw identificatie. We gaan zorgvuldig om met de foto's die u maakt bij de online identificatie, en met de andere gegevens die u met ons deelt. Meer hierover leest u in ons Privacy Statement.

Goed om te weten: de foto die u van het identiteitsbewijs maakt, en wij bewaren, krijgt een watermerk. Zodat het document echt alleen gebruikt kan worden voor uw online identificatie bij ICS. Het watermerk ziet er zo uit (…)

"Hoelang bewaren jullie mijn identificatie?

De foto van uzelf en de foto van uw identiteitsbewijs met het watermerk, bewaren wij in onze systemen zolang u klant bij ons bent. Daarna bewaren we de foto's nog eens 7 jaar. Dat is omdat wij, net als andere bedrijven, verplicht zijn om onze administratie 7 jaar te bewaren (…)"

3.7. Bij e-mailbericht van 25 mei 2021 heeft ICS een herinnering verstuurd aan SKC, waarin ICS haar verzoek tot online identificatie heeft herhaald. Hierin heeft ICS verder geschreven, voor zover relevant:

"(…) Voorkom dat de Card(s) worden geblokkeerd

Om de Card(s) van uw bedrijf te kunnen blijven gebruiken, is het belangrijk dat de identificatie gebeurt vóór 03 juni 2021. Daarna moeten wij de Card(s) van uw bedrijf helaas blokkeren en mogelijk onze overeenkomst met u opzeggen. (…)"

3.8. [appellant 2] heeft zich niet voor 3 juni 2021 online geïdentificeerd. [appellant 2] heeft bij ICS zijn bezwaren geuit tegen het uploaden van een onbeschreven kopie van zijn identiteitsbewijs. Ter onderbouwing hiervan heeft [appellant 2] verwezen naar de website van de Autoriteit Persoonsgegevens (hierna: AP), met name de volgende passages:

"Mag ik iets op een kopie van mijn identiteitsbewijs schrijven?

Ja, dat mag. U heeft altijd het recht om een tekst door de kopie van uw identiteitsbewijs heen te schrijven. Zo beschermt u de kopie tegen identiteitsfraude.

In sommige gevallen heeft een organisatie of bedrijf een wettelijke grondslag om een volledige kopie van uw identiteitsbewijs te verwerken voor een specifiek doel.

Bijvoorbeeld wanneer u als werknemer in dienst treedt bij een bedrijf. Uw werkgever moet dan een kopie van uw identiteitsbewijs bewaren.

Maar ook in die gevallen heeft u altijd het recht om een tekst door de kopie van uw identiteitsbewijs heen te schrijven. Bijvoorbeeld: 'Kopie voor [naam werkgever] van [datum]'.

Zo beschermt u de kopie tegen identiteitsfraude, want de volledige kopie zal niet zomaar voor een ander doel gebruikt kunnen worden.

Let op: alle persoonsgegevens (zoals de foto en het BSN) op de beschreven kopie moeten leesbaar zijn. Ook de foto moet voldoende zichtbaar zijn om u te kunnen identificeren.

Wat u op de kopie schrijft, mag dus geen afbreuk doen aan de identificerende functie van de kopie. (…)"

"Mag een organisatie een beschreven kopie van mijn identiteitsbewijs weigeren?

Nee, dat mag niet. Wanneer die organisatie een wettelijke grondslag heeft om een volledig kopie van het identiteitsbewijs te verwerken, dan is een beschreven kopie hiervoor genoeg.

U kunt er dus voor kiezen om op de kopie te schrijven. Dat is ook aan te raden, want zo beschermt u de kopie tegen identiteitsfraude. (…)"

3.9. Naar aanleiding van de bezwaren van [appellant 2] heeft ICS in haar e-mailberichten van 15 en 16 juni 2021 [appellant 2] onder andere uitgelegd waarom het nodig is dat hij zich online identificeert en waarom hij het identiteitsbewijs niet mag beschrijven:

"Waarom kunt u het identiteitsbewijs niet beschrijven?

U kunt het identiteitsbewijs niet beschrijven. Zoals eerder aangegeven kunnen we alleen digitaal identificeren. Bij de identificatie moet het identiteitsbewijs op echtheid worden gecontroleerd. Schrijft u iets op het document dan zorgt dit ervoor dat de echtheid van het document niet kan worden vastgesteld. (…)"

3.10. Bij e-mailbericht van 22 juni 2021 heeft ICS twee alternatieven voor het online identificeren voorgedragen, namelijk identificatie aan huis of identificatie bij de notaris. Bij de eerste variant komt een medewerker van het door ICS ingeschakelde bedrijf AMP bij de klant langs om hem te identificeren. De medewerker gebruikt hiervoor dezelfde software als bij de online identificatie (via de app). Bij de tweede variant kan de klant zich bij de notaris identificeren, die daarvan een akte opmaakt. In beide gevallen wordt het identiteitsbewijs op echtheid gecontroleerd door middel van een scanner. [appellant 2] heeft op dezelfde dag in een e-mail gereageerd en kort gezegd te kennen gegeven dat de door ICS aangeboden alternatieven niet bespreekbaar zijn.

3.11. Na afwijzing van zijn klacht heeft [appellant 2] zijn rechtsbijstandverzekeraar DAS ingeschakeld. Naar aanleiding van een brief van DAS van 30 juli 2021 heeft ICS bij e-mailbericht van 11 augustus 2021 aangegeven in afwach-

ting van een inhoudelijke reactie van DAS zowel de creditcard als de privé creditcard vooralsnog niet te blokkeren.
3.12. Bij e-mailbericht van 24 september 2021 heeft DAS namens [appellant 2] als volgt bericht:

> "(…) Gelet op het voorgaande verzoek ik u binnen twee weken na heden aan mij te bevestigen dat u de creditcard(s) van cliënt niet zult blokkeren en dat u genoegen neemt met een beschreven kopie van het identiteitsbewijs van cliënt (nadat een fysieke identificatie van client en controle van de echtheid van het identiteitsbewijs hebben plaatsgevonden bij hem thuis, bij u op kantoor of op een kantoor van ABN AMRO in de regio Hoofddorp/Amsterdam). (…)"

3.13. In reactie daarop heeft ICS op dezelfde dag te kennen gegeven geen andere alternatieven te accepteren dan de identificatie aan huis door een AMP medewerker of de identificatie bij de notaris zoals hiervoor onder 3.10 beschreven en heeft de klacht van [appellant 2] wederom afgewezen.
3.14 De website van de AP vermeldt het volgende over identificatie bij een bank:

> *"Kopie identiteitsbewijs bij identificatie*
> Bij het cliëntenonderzoek moet de financiële onderneming of dienstverlener een aantal gegevens van u vastleggen. In de Wwft staat dat dit mag door een kopie, scan of foto (hierna noemen we dit 'kopie') van uw identiteitsbewijs te maken. Hiermee kan de financiële onderneming of dienstverlener bewijzen dat uw identiteit is vastgesteld."

4 Eerste aanleg

4.1. [appellanten] heeft in eerste aanleg gevorderd dat de rechtbank bij vonnis, uitvoerbaar bij voorraad:
I. voor recht verklaart dat ICS niet van [appellanten] kan eisen zich op de wijze zoals door ICS wordt voorgeschreven te doen identificeren;
II. voor recht verklaart dat [appellant 2] gerechtigd is een (fysieke) identificatie te eisen, in het kader waarvan een kopie en/of scan van het originele identiteitsbewijs, zonder dat deze is gewaarmerkt, achterwege blijft;
III. voor recht verklaart dat [appellant 2] gerechtigd is zelf een waarmerk aan te brengen op een kopie van het identiteitsbewijs welke voor ICS tot opslag ex artikel 33 Wwft dient;
IV. ICS verbiedt de creditcard te blokkeren en de rechtsverhouding tussen partijen te doen beëindigen, enkel en alleen vanwege de omstandigheid dat [appellanten] zich aan de door ICS voorgeschreven identiteitsprocedure niet wenst te conformeren;
V. ICS veroordeelt in de kosten van de procedure.

4.2. Bij verstekvonnis van 20 april 2022 zijn de vorderingen van [appellanten] integraal toegewezen en is ICS veroordeeld in de proceskosten.
4.3. Na verzet van ICS heeft de rechtbank in het bestreden vonnis het verstekvonnis vernietigd en de vorderingen van [appellanten] afgewezen, met veroordeling van [appellanten] in de proceskosten van de verzetprocedure.

5 Beoordeling

5.1. [appellanten] heeft in hoger beroep vijf grieven aangevoerd. [appellanten] heeft geconcludeerd tot het vernietigen van het bestreden vonnis en, zo begrijpt het hof, tot het bekrachtigen van het verstekvonnis, met veroordeling – uitvoerbaar bij voorraad – van ICS in de proceskosten met rente.
5.2. ICS heeft geconcludeerd tot bekrachtiging van het bestreden vonnis, met veroordeling – uitvoerbaar bij voorraad – van [appellanten] in de proceskosten.
5.3. Gelet op wat [appellanten] met grief I aanvoert over de inhoud van de e-mail van zijn gemachtigde van 24 september 2021 heeft het hof de beschrijving daarvan aangepast in 3.12. Deze grief kan echter niet tot vernietiging van het bestreden vonnis leiden, gelet op de hierna volgende beoordeling.
5.4. Met grieven II en III voert [appellanten] aan dat de bepalingen van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) niet verplichten tot de door ICS gehanteerde identificatie- en verificatieprocedure die online plaatsvindt en/of waarbij elektronische identificatiemiddelen worden gebruikt, zodat de verwerking van de persoonsgegevens van [appellant 2] die daarbij plaatsvindt niet noodzakelijk is om te voldoen aan een wettelijke verplichting, in de zin van artikel 6 lid 1 onder c van de Algemene Verordening Gegevensbescherming (AVG). Deze verwerking is daarom niet rechtmatig, en dus mocht [appellanten] zijn medewerking daaraan weigeren, aldus [appellanten] Met grief III betoogt [appellanten] daarnaast, zo begrijpt het hof, dat het gebruik van een scanner voor de verificatie van het identiteitsbewijs niet in overeenstemming is met het proportionaliteitsbeginsel dat bij toepassing van de Wwft in acht moet worden genomen. Met grief IV voert [appellanten] aan dat artikel 33 Wwft ICS niet verplicht om een kopie van het identiteitsbewijs van [appellant 2] op te slaan. Verder bestrijdt [appellanten] met deze grief het oordeel van de rechtbank dat [appellanten] zijn stelling dat hij niet kan controleren of ICS een watermerk aanbrengt op de kopie van het identiteitsbewijs en dat hij ook niet kan controleren of de door ICS gebruikte software het aangebrachte watermerk weer ongedaan kan maken, onvoldoende heeft onderbouwd. [appellanten] betoogt ten slotte, met grief V, dat de informatie gepubliceerd op de website van de AP steun biedt voor zijn stelling dat hij kan volstaan met het aanleveren van een door hem zelf gewaarmerkte kopie van het identiteitsbewijs. Deze grieven lenen zich voor gezamenlijke behandeling.
5.5. Het hof stelt voorop dat tussen partijen vaststaat dat ICS op grond van de artikelen 3 en 38 Wwft verplicht is een cliëntenonderzoek te verrichten naar [appellanten], en dat dit onderzoek ICS in staat moet stellen om [appellant 2] te identificeren en zijn identiteit te verifiëren. Ook

staat tussen partijen vast dat de rechtmatigheid van de gegevensverwerking door ICS moet worden getoetst aan artikel 6 lid 1 onder c AVG, zodat het hof ook daarvan zal uitgaan. De Wwft schrijft niet (per geval) voor hoe een instelling als ICS het cliëntenonderzoek moet verrichten; de Wwft bepaalt slechts tot welk resultaat het onderzoek moet leiden. Indien een instelling niet kan voldoen aan haar verplichting tot identificatie en verificatie, moet zij de relatie met de cliënt beëindigen (artikel 5 lid 3 Wwft). Verder is van belang dat uit de Wwft of de AVG niet een recht op fysieke identificatie voortvloeit.

5.6. Op grond van artikel 11 lid 1 Wwft dient de identiteit van [appellant 2] te worden geverifieerd aan de hand van de in artikel 4 lid 1 van de Uitvoeringsregeling genoemde documenten, zoals een paspoort, Nederlandse identiteitskaart of Nederlands rijbewijs. Gelet op het bepaalde in artikel 13 lid 1 sub a van Richtlijn (EU) 2015/849 (de Vierde anti-witwasrichtlijn), zoals gewijzigd bij Richtlijn (EU) 2018/843, is het ICS toegestaan om bij de identificatie en verificatie elektronische identificatiemiddelen te gebruiken. ICS heeft gemotiveerd uiteengezet dat de elektronische techniek die bij het scannen van het identiteitsbewijs wordt gebruikt op dit moment op het gebied van echtheidscontrole de hoogste betrouwbaarheid heeft, en dat de inzet van deze techniek haar beter in staat stelt om hoogwaardige vervalsingen van identiteitsbewijzen te herkennen dan met de inzet van personen die hiervoor getraind en opgeleid zijn. [appellanten] heeft dit niet, althans onvoldoende, gemotiveerd betwist. Gelet op de mate van vrijheid die ICS toekomt bij de invulling van haar verplichting tot identificatie en verificatie onder de Wwft, en de toegevoegde waarde van het gebruik van de door haar gekozen elektronische techniek van het scannen van het identiteitsbewijs boven andere vormen van echtheidscontrole zoals een fysieke controle door een persoon, kan dit gebruik worden beschouwd als noodzakelijk in de zin van artikel 6 lid 1 sub c AVG om te voldoen aan haar verplichting tot het uitvoeren van een cliëntenonderzoek op grond van de Wwft. Het hof neemt hierbij in aanmerking dat ICS, gelet op het grote aantal cliënten voor wie een dergelijk onderzoek moet worden uitgevoerd en de noodzaak om daarover verantwoording te kunnen afleggen aan de toezichthouder, er een gerechtvaardigd belang bij heeft om de identificatie- en verificatieprocedure zoveel mogelijk uniform in te richten. Dat de identificatie- en verificatieprocedure van ICS eventueel anders ingericht had kunnen worden, betekent nog niet dat de procedure die ICS heeft gekozen, niet voldoet aan dit noodzakelijkheidsvereiste.

5.7. Op grond van artikel 33 lid 1 Wwft is ICS verplicht om op opvraagbare wijze de documenten en gegevens vast te leggen die zijn gebruikt voor de naleving van de verplichting tot het doen van een cliëntenonderzoek. Dit betekent dat ICS een afschrift dient te bewaren van het identiteitsbewijs waarvan zij met behulp van de scanner de echtheid heeft gecontroleerd en waarmee zij de identiteit van de cliënt heeft vastgesteld. ICS heeft er belang bij dit afschrift zelf te maken door het afschrift tegelijkertijd met het scannen en het controleren van het identiteitsbewijs op echtheid te maken en op te slaan, omdat daarmee gewaarborgd is dat het afschrift dat ICS bewaart daadwerkelijk het afschrift is van het identiteitsbewijs dat ICS heeft gebruikt voor de identificatie en verificatie. Van ICS kan niet worden verlangd dat zij, zoals [appellanten] voorstelt, een door [appellanten] gewaarmerkt afschrift van het identiteitsbewijs accepteert. ICS zou dan een extra (handmatige) controle moeten uitvoeren om vast te stellen of dit daadwerkelijk een afschrift is van het identiteitsbewijs dat [appellanten] heeft getoond voor de identificatie en verificatie. Dit laat ruimte voor fouten, die kunnen worden voorkomen door het maken van een afschrift bij het scannen van het identiteitsbewijs. De door ICS gebruikte methode kan daarom worden beschouwd als noodzakelijk in de zin van artikel 6 lid 1 onder c AVG om te voldoen aan haar verplichting tot het bewaren van bewijsstukken met betrekking tot het uitgevoerde cliëntenonderzoek op grond van de Wwft. ICS dient er wel voor te zorgen dat zij dit afschrift van het identiteitsbewijs veilig opslaat (EBA Richtsnoeren voor het gebruik van oplossingen voor de acceptatie van cliënten op afstand overeenkomstig artikel 13, lid 1, van Richtlijn (EU) 2015/849, par. 26). ICS heeft toegelicht dat het afschrift veilig wordt opgeslagen door het aanbrengen van een watermerk en dat [appellanten] dit kan controleren door gebruik te maken van zijn inzagerecht onder de AVG. [appellanten] heeft dit onvoldoende gemotiveerd bestreden. Zijn suggestie dat het door ICS aangebrachte watermerk met software mogelijk kan worden verwijderd, acht het hof in dit verband niet voldoende. Bovendien geldt dat ook voor een waarmerk dat [appellanten] zelf zou aanbrengen op een kopie van het identiteitsbewijs.

5.8. Uit de door [appellanten] aangehaalde passages van de website van de AP volgt, mede gelet op de door ICS aangehaalde passages (zie 3.14), niet zonder meer dat [appellanten] kan volstaan met het aanleveren van een door hem gewaarmerkt afschrift van het identiteitsbewijs van [appellant 2] ten behoeve van de opslag en bewaring door ICS. Bovendien kan wat [appellanten] aanvoert met betrekking tot de AP niet afdoen aan de rechtmatigheid van de identificatie- en verificatieprocedure jegens [appellanten] zoals uit voorgaande beoordeling volgt. Hetzelfde geldt voor het feit dat ICS, volgens het besluit van de AP van 18 december 2023, voorafgaand aan haar identificatie- en verificatieproces heeft nagelaten een gegevensbeschermingseffectbeoordeling in de zin van artikel 35 AVG uit te voeren.

5.9. Gelet op het voorgaande voldoet ICS met het door haar geboden alternatief waarbij een medewerker van het door ICS ingeschakelde bedrijf AMP bij de klant langs komt om hem te identificeren, aan de relevante bepalingen van de Wwft en AVG. Daarmee falen de grieven, zodat het bestreden vonnis zal worden bekrachtigd. Het algemene bewijsaanbod van [appellanten] heeft geen betrekking op stellingen die, indien bewezen, tot een ander oordeel zullen leiden. [appellanten] is in het hoger beroep in het ongelijk gesteld en zal daarom worden veroordeeld in de proceskosten in hoger beroep.

[…]

6 **Beslissing**

Het hof:
bekrachtigt het bestreden vonnis;
[…]

Noot

1. In deze zaak staan twee vragen centraal. Enerzijds, op welke wijze moet [appellant 2], de vennoot van SKC die sinds 2015 een zakelijke creditcard heeft bij ICS, een dochteronderneming van ABN AMRO Bank N.V., zijn identiteit laten verifiëren in het kader van de *verificatieplicht* op grond van art. 11 Wwft? En anderzijds, kan, mag of moet en, zo ja, op welke wijze dient een kopie van het bij de identiteitsverificatie gebruikte legitimatiebewijs te worden bewaard door ICS op grond van de *reconstructieplicht* van art. 33 Wwft?

2. De partijen denken hier verschillend over, en halen tegenstrijdige teksten aan van de Autoriteit Persoonsgegevens (AP) in r.o. 3.8 en 3.14. Zoals elders opgemerkt, verschenen er met de lancering van de nieuwe AP-website medio 2023 zonder aanwijsbare reden nieuwe teksten op de AP-website.[2] Dat ook andere Wwft-toezichthouders tegenstrijdige standpunten innemen over de reikwijdte van de verificatieplicht en reconstructieplicht, draagt niet bij aan duidelijkheid.[3]

3. Appellant 2 lijkt wel mee te willen werken aan het opnieuw verifiëren van zijn identiteit, maar wil dat er een door hem zelf beschreven kopie van zijn identiteitsbewijs in de administratie van ICS wordt opgenomen. ICS biedt ook wel alternatieven aan voor een online identiteitsverificatie (aan huis), maar houdt vast aan de bewaring van een kopie van [Appellant 2]'s identiteitsbewijs, dat wel van een watermerk wordt voorzien. Behalve als [Appellant 2] zijn identiteit laat controleren bij de notaris, dan neemt ICS genoegen met een notariële akte. De wensen van partijen rondom de *verificatieplicht* (origineel tonen, beschreven kopie) en *reconstructieplicht* (notariële akte of door betrokkene/ICS gewatermerkte scan/kopie) lopen dus uit elkaar en door elkaar heen. Dit werkt door in de uitspraak.

4. Het Hof oordeelt dat ICS verplicht is om 'op opvraagbare wijze de documenten en gegevens vast te leggen die zijn gebruikt voor de naleving van de verplichting tot het doen van een cliëntenonderzoek' (de *reconstructieplicht*), en, mede verwijzend naar de tegenstrijdige teksten van de AP, dat [Appellant 2] 'niet zonder meer (…) kan volstaan met het aanleveren van een door hem gewaarmerkt afschrift van het identiteitsbewijs', wat verwijst naar de *verificatieplicht*, en vervolgens: 'ten behoeve van de opslag en bewaring door ICS', wat weer verwijst naar de *reconstructieplicht* (r.o. 5.8). En dat ICS met het geboden alternatief voor een thuisbezoek voldoet aan de relevante bepalingen van de Wwft en AVG (r.o. 5.9), wat hoofdzakelijk verwijst naar de *verificatieplicht*. Het bestreden gelijkluidende vonnis van de rechtbank wordt bekrachtigd: SKC wordt in het ongelijk gesteld. Als SKC een duidelijker onderscheid had aangebracht tussen de verificatieplicht en de reconstructieplicht, had de zaak mogelijk een andere uitkomst gekend.

5. De *verificatieplicht* verplicht ICS om de door de cliënt opgegeven identiteit te verifiëren 'aan de hand van documenten, gegevens of inlichtingen uit betrouwbare en onafhankelijke bron', zoals een identiteitsbewijs. Als aangebrachte watermerken op een kopie door de echtheidskenmerken heen gaan doet dit, zoals ICS terecht opgemerkt heeft in r.o. 3.9, afbreuk aan de betrouwbaarheid van een dergelijke kopie. Maar [Appellant 2] heeft ook aangeboden om zijn identiteitsbewijs fysiek op kantoor te tonen, wat net als de door de ICS aangeboden identificatie aan huis of bij de notaris geschikte manieren zijn om aan deze verplichting te voldoen.

6. De *reconstructieplicht* bevat echter géén verplichting voor Wwft-instellingen om een kopie legitimatiebewijs in hun administratie te bewaren. Wat volstaat, is het noteren van de art. 33 lid 2 Wwft opgesomde gegevens.[4] Dat in plaats ('of') van die gegevens ook een kopie van het legitimatiebewijs bewaard kan worden, was volgens de minister in 2007 bij de invoering van die mogelijkheid een 'efficiënt' alternatief, een 'mogelijkheid'.[5] Later is de reconstructieplicht verruimd zodat instellingen ook documenten kunnen bewaren over de uiteindelijke belanghebbenden (UBO) van juridische identiteiten. Die verruiming zag volgens de MvT echter niet op de identiteitsverificatie van natuurlijke personen: 'Het voorgestelde artikel 33 voorziet niet in een wijziging van de documenten en gegevens die van [natuurlijke personen, niet zijnde een UBO, maar de cliënt van de instelling] moeten worden vastgelegd en bewaard.'[6]

7. Hoewel de Wwft geen grondslag biedt voor het bewaren van foto's van cliënten, zoals ICS in deze zaak heeft aangegeven wel te doen (r.o. 3.6, maar waar het beroep niet op zag),[7] kunnen kopieën van legitimatiebewij-

2 Voetnoot 16 in: D. Mekić, 'Het opslaan van kopieën van legitimatiebewijzen, foto's en video's van cliënten: de grenzen van de Wwft-reconstructieplicht in het licht van fundamentele rechten', *Privacy & Informatie* 2024/1. Vgl. Autoriteit Persoonsgegevens, Financiële ondernemingen, www.perma.cc/998Z-NJBX 23 mei 2023 en Autoriteit Persoonsgegevens, Financiële ondernemingen, www.perma.cc/LE5G-V7H8 30 december 2023. Voor een uitgebreide bespreking biedt deze noot geen ruimte, maar de nieuwe teksten lijken niet in overeenstemming te zijn met de wet.

3 Mekić 2024, p. 3.

4 *Kamerstukken II* 2007/08, 31238, p. 35; Rb. Noord-Holland 27 oktober 2021, ECLI:NL:RBNHO:2021:9542, r.o. 4.12.1; Rb. Rotterdam 20 april 2023, ECLI:NL:RBROT:2023:3301, r.o. 3.5; Autoriteit Financiële Markten, *Hoe moet u zich identificeren bij een financiële onderneming?*, www.perma.cc/HK3F-V5WK 30 december 2023; Rijksoverheid, '*Moet een bank een kopie van mijn paspoort maken en bewaren?*', www.perma.cc/9C4P-PKCM 24 maart 2023.

5 *Kamerstukken II* 2007/08, 31238, p. 35.

6 *Kamerstukken II* 2017/18, 34808, nr. 3, p. 79-80.

7 Zie ook M. Laan, 'Bank verzamelt ten onrechte foto van klant', *Het Parool* 9 augustus 2006, Tweakers, '*Vraagtekens bij opslag id-bewijzen door banken*', www.tweakers.net, 9 augustus 2006 en Mekić 2024, p. 6 e.v.

zen dus wel worden bewaard,[8] maar *enkel* als alternatief ('of', zie art. 33 lid 2 sub a onder 1 Wwft) voor de losse bewaring van de in de Wwft vermelde gegevens. Dat moet dus niet. Wanneer mag dat dan wel?

8. Nu de reconstructieplicht voortvloeit uit Uniewetgeving, moet de uitvoering voldoen aan de eisen voor een rechtmatige inperking van het fundamentele recht op privacy en gegevensbescherming (art. 7 en 8 EU Handvest), en het subsidiariteitsvereiste (art. 5 lid 3 VEU), en dus niet verder mag gaan dan strikt noodzakelijk. Aangezien op grote schaal fraude wordt gepleegd met kopieën van legitimatiebewijzen, vormt het bewaren van die kopieën een ernstigere privacyinbreuk dan het noteren van losse gegevens.[9]

9. Nu uit de wettekst en wetsgeschiedenis van de Wwft volgt dat het bewaren van een kopie van het legitimatiebewijs niet noodzakelijk is, mag daar enkel voor worden gekozen wanneer er geen andere reële minder inbreukmakende mogelijkheid bestaat, zoals in het begin van deze eeuw toen sommige financiële instellingen handmatig miljoenen identiteitsverificaties moesten verrichten zonder moderne computersystemen. Een, in de woorden van de minister, 'efficiënt' kopietje doet dan wonderen. Anno 2024 is echter niet snel meer sprake van een dergelijke situatie. Zeker bij financiële instellingen, die ook een renseigneringsplicht hebben waarvoor zij losse gegevens moeten bewaren, biedt de Wwft dus geen rechtsgeldige grondslag om óók een kopie van het legitimatiebewijs te bewaren.[10] Dit volgt ook uit het beginsel van minimale gegevensverwerking van art. 5 lid 1 onder c AVG, gelezen in samenhang met overweging 4.

10. Als SKC scherper had gevaren op de reconstructieplicht dan had de zaak mogelijk een andere uitkomst gehad. ICS mag een identiteitsdocument op grond van de verificatieplicht immers wel op betrouwbaarheid controleren. De Wwft biedt echter geen verplichting en, gelet op het voorgaande, dus geen grondslag om die scan of een kopie van legitimatiebewijzen vervolgens ook te bewaren.

11. Een laatste vraag die resteert is: waarom is er anno 2024 geen betrouwbaar, privacyvriendelijk alternatief voor identiteitsverificaties? Als DigiD daar geschikt voor wordt gemaakt, dan hoeven geen (kopietjes van) fysieke identiteitsbewijzen meer gebruikt te worden. En hoeven betrokkenen, die zich in het licht van een toenemend aantal datalekken terecht zorgen maken om hun privacy, dit soort zaken niet aan te spannen.

D. Mekić

8 Ingevolge het subsidiariteitsbeginsel en het beginsel van minimale gegevensverwerking dienen overbodige gegevens dan wel onleesbaar te worden gemaakt en de kopie van een permanent watermerk worden voorzien, zie hierna.

9 Centraal Bureau voor de Statistiek (CBS), *Veiligheidsmonitor 2022* 11 mei 2023 en G. Bummelkamp e.a., *Monitor Identiteit 2021*, maart 2022, p. 21 en 57.

10 Een andere reden zou kunnen zijn omdat de reconstructiebepaling in de huidige formulering een zgn. 'free text' bepaling is die niet aan het voorzienbaarheidsvereiste voldoet en dus ongeldig is. Overweging 41 AVG stelt dat een verwerkingsgrondslag, overeenkomstig de vereisten van het EHRM en het HvJ EU, 'duidelijk en nauwkeurig [moet] zijn, en de toepassing daarvan moet voorspelbaar [moet] zijn voor degenen op wie deze van toepassing is'. Vgl concl. A-G G. Pitruzzella 20 januari 2022, gev. zaken C-37/20 en C-601/20, ECLI:EU:C:2022:43, par. 114 (*Commissie/Luxembourg Business Registers*). Zie verder: HvJ EU 26 juli 2017, advies 1/15, ECLI:EU:C:2017:592 (*PNR-overeenkomst EU-Canada*), r.o. 160. Ditzelfde kan gelden voor de aankomende reconstructieplicht in art. 77 van de eerder dit jaar aangenomen Verordening (EU) 2024/1624 van het Europees Parlement en de Raad van 31 mei 2024 tot voorkoming van het gebruik van het financiële stelsel voor witwassen of terrorismefinanciering (AMLR) die over drie jaar de Wwft zal vervangen. Zie verder over de AMLD, waar de Wwft op is gebaseerd, in relatie tot privacyrechten: J. Milaj & C. Kaiser, 'Retention of data in the new Anti-money Laundering Directive—"need to know" vs "nice to know"', *International Data Privacy Law* 2017/7, afl. 2, p. 115-125; C. Kaiser, *Privacy and Identity Issues in Financial Transactions* (diss.), Rijksuniversiteit Groningen 2018 en A. Bertrand, W. Maxwell & X. Vamparys, 'Do AI-based anti-money laundering (AML) systems violate European fundamental rights?', *International Data Privacy Law* 2021/11, afl. 3, p. 276-293.