



**Universiteit
Leiden**

The Netherlands

**Selfie-video bij Wwft identiteitsverificatie en de AVG:
Annotatie bij KiFiD Geschillencommissie Financiële
Dienstverlening 19 juli 2024, nr. 2024-0631
(Consumenten/LeasePlan Bank)**

Mekić, D.

Citation

Mekić, D. (2024). Selfie-video bij Wwft identiteitsverificatie en de AVG: Annotatie bij KiFiD Geschillencommissie Financiële Dienstverlening 19 juli 2024, nr. 2024-0631 (Consumenten/LeasePlan Bank). *Jurisprudentie Onderneming & Recht*, 2024(11), 2738-2744. Retrieved from <https://hdl.handle.net/1887/4109179>

Version: Publisher's Version

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/4109179>

Note: To cite this publication please use the final published version (if applicable).

264

Selfie-video bij Wwft identiteitsverificatie en AVG

Geschillencommissie Financiële Dienstverlening

19 juli 2024, nr. 2024-0631

(mr. dr. Bakkerus, mr. Ruinaard, mr. Van der Groen)

Noot mr. drs. D. Mekić

Verificatieplicht Wwft en AVG. Wel of geen verwerking biometrische persoonsgegevens bij verplichte selfie-video? Verantwoordingsplicht en verzwaarde motiveringsplicht verwerkingsverantwoordelijke. Belang van contractuele afspraken en redelijkheid en billijkheid.

[EU Handvest art. 7, 8; AVG art. 5, 9 lid 1; Wwft art. 3 lid 2 sub a, 11 lid 1]

De consumenten hebben online een spaarrekening bij de bank aangevraagd. Gedurende het identificatieproces werd hun gevraagd een verificatiefilmpje aan te leveren. De consumenten beklagen zich hierover, omdat de bank volgens hen daarmee biometrische persoonsgegevens van hen verwerkt en dat mag niet. Zij vorderen dat de bank hun persoonsgegevens verwijdert. De bank stelt dat de klacht niet behandelbaar is onder het reglement van Kifid. De bank stelt voorts dat met het verificatiefilmpje geen biometrische gegevens verwerkt worden zoals bedoeld in de AVG. De commissie is van oordeel dat zij de klacht wel kan behandelen. Niet is komen vast te staan dat de bank met het verificatiefilmpje biometrische gegevens verwerkt. Ook is niet komen vast te staan dat de bank nog persoonsgegevens van de consumenten heeft. De vorderingen van de consumenten worden afgewezen.

1. [Naam 1],

2. [naam 2],

consumenten,

tegen
LeasePlan Bank te Amsterdam.

(...; red.)

2. Het geschil

Wat is er gebeurd?

2.1. De bank biedt haar diensten alleen via internet aan. De consumenten hadden een online spaarrekening geopend bij de bank. Voordat zij die spaarrekening konden gaan gebruiken, dienden zij zich te identificeren. Hun poging om in dat identificatieproces een filmpje (hierna: het verificatiefilmpje) te uploaden, is mislukt.

2.2. Naast het verzochte verificatiefilmpje bestond het identificatieproces (onder meer) uit het uploaden van een foto van het paspoort van de consumenten en een overboeking van € 1,- vanaf een betaalrekening die op hun naam stond. Uiteindelijk is het identificatieproces geannuleerd en is de spaarrekening gesloten.

De klacht en vordering

2.3. De consumenten beklagen zich erover dat de bank tijdens het aanvraagproces voor de spaarrekening verlangt dat zij een verificatiefilmpje uploaden met een opname van henzelf.

De consumenten vinden dat de bank hen in dit geval niet mag verplichten om hun biometrische persoonsgegevens aan te leveren. Zij wijzen erop dat de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) de bank mogelijkheden biedt tot differentiatie voor een risico-georiënteerde benadering van cliëntenonderzoek. Volgens de consumenten is de bank niet verplicht om biometrische gegevens op te vragen voor het openen van een eenvoudige online privéspaarrekening, en is die eis van de bank te zwaar en niet proportioneel. De bank beschikt over hun paspoort, BSN, Nederlandse adres, e-mailadres en afschrift van een grootbank. Volgens de consumenten zijn er ongetwijfeld andere hen niet bekende mogelijkheden voor verificatie voorhanden die voldoende zijn. Zij bankieren bij een andere bank waar ze geïdentificeerd zijn, daar kan de bank ook navraag doen.

2.4. De consumenten vorderen dat het de bank verboden wordt om bij de aanvraagprocedure biometrische gegevens op te vragen. De consumenten willen een spaarrekening kunnen openen zonder dat de bank biometrische gegevens van hen verlangt. Ook vorderen zij dat de bank de eventueel door hen geüploade informatie verwijdert.

Het verweer

2.5. De bank voert verweer tegen de stellingen van de consumenten. Voor zover relevant zal de commissie bij de beoordeling daarop ingaan.

*3. De beoordeling**Inleiding*

3.1. Aan de commissie is ter beoordeling voorgelegd of de bank voor het openen van een online spaarrekening een verificatiefilmpje mocht verlangen van de consumenten. Eerst dient de commissie echter te beoordelen of zij bevoegd is om de klacht te behandelen.

De commissie kan de klacht behandelen

3.2. De bank stelt dat de commissie de klacht niet kan behandelen, omdat de bank de persoonsgegevens van de consumenten niet ontvangen heeft. De consumenten hebben het verificatiefilmpje en de foto van het legitimatiebewijs namelijk niet geüpload.

3.3. De overboeking van € 1,- van een tegenrekening hebben zij wel gedaan, maar niet vanaf een tegenrekening met de juiste tenaamstelling. De consumenten hebben dus zelf niet alle stappen gezet om de identificatie te voltooien en zij wilden uiteindelijk geen klant worden. Zij hebben volgens de bank daarom geen individueel belang bij de klacht.

3.4. De consumenten hebben hierop gereageerd dat zij de bedoeling hadden om de identificatieprocedure volledig te doorlopen, maar dat niet gedaan hebben omdat hen gevraagd werd biometrische gegevens af te geven. Zij zijn er wel mee begonnen: zij hebben inderdaad de overboeking vanaf de tegenrekening uitgevoerd. Bovendien hebben zij een foto van hun paspoort(en) gemaakt. De volgende fase was die van het verificatiefilmpje. Dat lukte technisch niet en zij wilden dat eigenlijk niet. Toen kregen zij bericht dat de overboeking vanaf de tegenrekening niet akkoord was, in verband met de tenaamstelling. De tegenrekening was van de consumenten samen, maar dat bleek niet uit de tenaamstelling. Zij hebben daarom contact opgenomen met de bank van de tegenrekening, maar het duurde lang voordat de tenaamstelling aangepast was. Toen hebben de consumenten geuit dat zij bezwaar hadden tegen de verwerking van biometrische gegevens, wat resulteerde in deze klachtenprocedure.

3.5. De commissie oordeelt als volgt. Volgens haar reglement is de commissie, naast de behandeling van klachten over financiële diensten die de klager afneemt, ook bevoegd om privacyklachten te behandelen.¹

Het reglement vermeldt dat met een privacyklacht wordt bedoeld:

“Klachten over het verwerken van persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming (AVG).”

3.6. Vast staat dat er een online spaarrekening was geopend en dat voor daadwerkelijk gebruik een identificatieproces doorlopen moest worden. Het is naar het oordeel van de commissie niet komen vast te staan dat de bank het bestreden verificatiefilmpje en de foto van het legitimatiebewijs daadwerkelijk ontvangen heeft. En dit betekent dat de bank geen gegevens van de consumenten heeft verwerkt. Nu de klacht van de consumenten inhoudt dat de bank tijdens het identificatieproces eisen stelt die een ongeoorloofde inbreuk op hun privacy impliceren, kan de commissie die klacht wel behandelen. Anders zouden de consumenten dat identificatieproces eerst moeten afronden voordat zij een klacht kunnen indienen. Omdat de consumenten menen dat een onderdeel van het identificatieproces ongeoorloofd is, kan dat in het onderhavige geval niet van hen verlangd worden.

Het verificatiefilmpje is noodzakelijk in het kader van identificatie en verificatie op afstand

3.7. Tussen partijen staat vast dat de bank uit hoofde van de Wwft verplicht is om bij het aangaan van een nieuwe relatie de identiteit van de aanvrager te vragen en diens identiteit ook te verifiëren. De consumenten stellen dat de bank ook zonder het verificatiefilmpje voldoende informatie heeft om aan haar verplichtingen uit de Wwft te voldoen. De bank betwist dat en stelt dat zij zonder dit filmpje de identiteit van de aanvrager niet deugdelijk kan verifiëren. Zij heeft geen goede alternatieven. De bank biedt haar diensten alleen online aan via gestandaardiseerde processen, dus niet ook via kantoren. Dat is een bewuste keuze en maakt het mogelijk een relatief aantrekkelijke spaarrente te bieden. De aanstaande klan-

1 Vraag 1 van het Reglement Geschillencommissie Kifid (vanaf 1 april 2022 tot 1 oktober 2023), te vinden op www.kifid.nl/reglementen-en-statuten.

ten moeten invullen wie zij zijn en de bank moet vervolgens aan de hand van een legitimatiebewijs vaststellen of de opgegeven identiteit juist is. Vanwege de bedrijfsvoering van de bank is fysieke controle niet mogelijk. Daardoor kan de bank de echtheidskenmerken van het legitimatiebewijs niet controleren zoals dat bij fysiek contact wel gebeurt. Daarom heeft zij gekozen voor het opvragen van een foto van het ID-bewijs en een korte selfie video-opname, zodat de foto van het ID-bewijs kan worden vergeleken met die video-opname. De bank kan zelf bepalen op welke wijze invulling wordt gegeven aan de verplichting tot identificatie en verificatie van nieuwe klanten. De Nederlandsche Bank heeft in zijn DNB Leidraad uit 2020² voor identificatie en verificatie op afstand het verificatiefilmpje ook nadrukkelijk als voorbeeld aangedragen.

3.8. Volstaan met een afgeleide identificatie door de overboeking vanaf een rekening bij een andere bank als enige identificatiemiddel is volgens de bank niet mogelijk. De overboeking is namelijk niet voldoende voor verificatie van de identiteit. En om te kunnen vertrouwen op het cliëntenonderzoek van een andere bank waar de consumenten bankieren, is de bank op grond van genoemde DNB Leidraad gehouden de procedure van die bank voor een betrouwbaar identificatie- en verificatieproces op te vragen en te beoordelen. Dat is niet werkbaar.

3.9. De commissie is van oordeel dat de bank hiermee voldoende heeft onderbouwd dat een verificatiefilmpje noodzakelijk is om de identiteit van de rekeningaanvragers te verifiëren (artikel 5 AVG, zie de bijlage). Gelet op de online bedrijfsvoering van de bank kan de bank volstaan met deze werkwijze.

Het verificatiefilmpje kwalificeert niet als biometrische gegevens

3.10. Volgens de consumenten mag de bank geen verificatiefilmpje opvragen, omdat zij met een dergelijk filmpje biometrische gegevens verwerkt. Verwerking van “biometrische gegevens met het oog op de unieke identificatie van een persoon” is verboden op grond van artikel 9 AVG (zie de bijlage).

3.11. De bank betwist dat bij de uitvoering van het aanvraagproces biometrische gegevens verwerkt

worden zoals bedoeld in artikel 9 AVG. Tijdens het verificatiefilmpje moet de aanvrager in de camera kijken, enkele getoonde cijfers hardop zeggen en enkele acties uitvoeren zoals het hoofd draaien. Daarmee wordt gecontroleerd of sprake is van een levende persoon in plaats van bijvoorbeeld een foto van iemand. Die toets wordt een *liveness check* genoemd. Daarnaast wordt aan de hand van identificatiepunten bepaald of de persoon in het identiteitsbewijs dezelfde is als de persoon in de verificatievideo. Die stappen zijn volgens de bank noodzakelijk om de identiteit van de aanvrager te verifiëren.

3.12. De commissie stelt vast dat de bank het verificatiefilmpje niet zelf maakt. De bank laat dit door een ander bedrijf doen. Desgevraagd heeft de bank geweigerd de commissie inzage te geven in de verwerkersovereenkomst tussen de bank en dat andere bedrijf. In het navolgende gaat de commissie ervan uit dat niet dat bedrijf, maar de bank de verwerkingsverantwoordelijke is van de persoonsgegevens die verwerkt worden voor de rekeningaanvraag (zoals bedoeld in artikel 4 AVG, zie de bijlage). In het kader van de leesbaarheid wordt hierna de bank genoemd als verantwoordelijke voor het verificatiefilmpje.

3.13. De commissie heeft in deze klachtenprocedure twee deskundigen gevraagd om advies te geven over de onderzoeksvraag: “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 Wvft? Hoe verhoudt zich dit tot het beginsel van dataminimalisatie van de AVG? Kan opname van biometrische gegevens ter identificatie zondermeer verplicht worden?”.

Riverworks Legal Services heeft deze vraag besproken vanuit het oogpunt van de Wvft en prof. mr. A. Berlee heeft dat gedaan vanuit het oogpunt van de AVG. De adviezen worden als separate bijlagen bij deze uitspraak gepubliceerd.

3.14. In beide adviezen is benadrukt dat het van belang is om vast te stellen of sprake is van de

2 DNB Leidraad Wvft en Sanctiewet december 2020.

verwerking van biometrische gegevens. In het advies van prof. mr. A. Berlee³ is opgenomen:

“17. Het is dus niet zo dat een video-opname vanzelfsprekend de verwerking van biometrische gegevens met zich meebrengt.¹⁴ In dit kader is overweging 51 bij de AVG ook relevant waarin staat dat:

‘[...] de verwerking van foto’s mag niet systematisch worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, aangezien foto’s alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken. [...]’

(...) De verwerking moet dus niet enkel het doel hebben de unieke identificatie of authenticatie mogelijk te maken, maar dit dient tevens het gevolg te zijn van een specifieke technische verwerking.

(...)

21. Er is evenwel géén sprake van de verwerking van biometrische gegevens wanneer bijvoorbeeld een potentiële klant wordt gevraagd om in een video-opname bepaalde handelingen uit te voeren zoals het heen en weer bewegen van het hoofd,¹⁸ of dat op afstand een video-opname wordt gebruikt om door iemand (in opdracht) van de financiële dienstverlener vervolgens te worden beoordeeld of deze persoon overeenkomt met de foto op het al eerder aangeleverde kopie identiteitsbewijs of het identiteitsbewijs dat werd getoond in de video-opname. In deze voorgaande gevallen wordt de video-opname gebruikt voor de unieke identificatie, maar is er geen sprake van dat het de technische middelen zijn die tot deze unieke identificatie of authenticatie te komen. Dit is anders bij bijvoorbeeld het softwarematig vergelijken van een vingerafdruk met een vingerafdruk opgeslagen in het paspoort, of de inzet van gezichtsherkenningsoftware die bepaalde punten op het gezicht gebruikt en de afstand daartussen meet om deze te vergelijken met een database met templates van gezichten.”

Ook in het advies van Riverworks Legal Services⁴ is vermeld:

“1.2 Niet alle gebruik van video-opnamen bij verificatie van de identiteit betekent dat er ook biometrische gegevens verwerkt worden.”

3.15. De commissie stelt vast dat de uiteenzetting van de bank van de aard van het verificatiefilmpje aansluit bij de weergave uit het advies van prof. mr. A. Berlee. Met het uitvoeren van handelingen zoals in de camera kijken, enkele cijfers hardop zeggen en het hoofd bewegen voert de bank een *liveness check* uit. Het enkele feit dat een verificatiefilmpje moet worden aangeleverd maakt nog niet dat biometrische gegevens moeten worden verstrekt. Tegenover deze gemotiveerde betwisting van de bank hebben de consumenten niet nader onderbouwd dat de bank wel biometrische gegevens verwerkt. Er is dan ook niet komen vast te staan dat de bank met het verificatiefilmpje biometrische gegevens verwerkt. Waar de commissie bij het formuleren van de onderzoeksvraag is uitgegaan van een verificatiefilmpje dat biometrische gegevens bevat, kan de commissie, met name gelet op de inhoud van de uitgebrachte adviezen, nu niet anders dan tot de vaststelling komen dat daarvan in dit geval geen sprake is geweest. Om die reden kan dan ook niet worden geconcludeerd dat de bank ongeoorloofd handelt door van de consumenten te verlangen dat zij een verificatiefilmpje verstrekken. De vordering om de bank te verbieden biometrische gegevens op te vragen voor het openen van een spaarrekening zal dan ook worden afgewezen.

Verwijdering gegevens

3.16. De consumenten vorderen ook dat de bank hun persoonsgegevens verwijderd. De bank heeft aanvankelijk gesteld dat zij de persoonsgegevens van de consumenten heeft verwijderd. Tijdens de mondelinge behandeling heeft de bank aangegeven dat de consumenten het verificatiefilmpje en de foto van het legitimatiebewijs niet hebben geupload, dat de bank dit dus niet heeft ontvangen zodat zij dit niet kan verwijderen. Gelet op dit verweer van de bank is niet komen vast te staan dat de bank nog persoonsgegevens van de consu-

3 Advies aan Kifid inzake wijze van identificatie en verificatie en de inzet van biometrie daarbij bezien vanuit de vereisten van de AVG van 11 juli 2023 van prof. mr. A. Berlee, hoogleraar gegevensbescherming en privacyrecht aan de Open Universiteit.

4 Advies aan Kifid inzake wijze van identificatie en verificatie en in het kader van de Wvft van 11 juli 2023 van Riverworks Legal Services.

menten heeft. De commissie kan de vordering van de consument daarom niet toewijzen.

4. De beslissing

De commissie wijst de vorderingen af.

NOOT

1. De Geschillencommissie van het KiFiD (Klachteninstituut Financiële Dienstverlening, hierna: GC) heeft een bindend advies uitgebracht over de vraag of een financiële instelling, in dit geval LeasePlan Bank (hierna: LPB), van cliënten mag verlangen dat zij een selfie-video maken en verstrekken waarop zij bepaalde handelingen verrichten (bijvoorbeeld het draaien van hun hoofd). Dit in het kader van een identiteitsverificatie op grond van art. 3 lid 2 sub a jo. art. 11 lid 1 Wwft.

2. KiFiD kwalificeert dit bindend advies op haar website als “een belangrijke uitspraak” die in de media betrekkelijk veel aandacht heeft gekregen. Het persbericht kopt: “Bank mag voor identificeren klant vragen om een filmpje”. De strekking van de berichtgeving is duidelijk, zoals De Telegraaf het in een artikel van 23 juli 2024 zegt: “Online bank mag selfie-video eisen bij opening rekening”.

3. De klacht van de consumenten ging echter niet alleen over de vraag of een bank een filmpje mag vragen, maar ook of de bank *bijzondere persoonsgegevens met het oog op de unieke identificatie van een persoon* mag verwerken op grond van de AVG. De GC wees de klacht af omdat niet vast is komen te staan of er sprake is van de verwerking van biometrische gegevens door LPB.

4. De casus roept meteen al een aantal vragen op. Bijvoorbeeld *waarom* in dit geval niet kan worden volstaan met een minder vergaande identiteitsverificatie zonder additionele privacyinbreuk in de vorm van een selfie-video, zoals LPB stelt in r.o. 3.7. De verificatieplicht uit de Wwft vormt immers de implementatie van Unierecht, en vormt een inperking op het recht op privacy en gegevensbescherming (art. 7 en 8 EU Handvest). Daarom moet uit verschillende geschikte identificatiemethodes de minst inbreukmakende gekozen worden (het subsidiariteitsvereiste).

5. Volgens De Nederlandsche Bank (*Leidraad Wwft en Sw*, december 2020, p. 28) volstaat *enkel* een afgeleide identificatiestorting van 1 cent vanaf een tegenrekening op naam niet, zoals LPB

in r.o. 3.8 terecht stelt. Echter, zo een identificatiestorting *in combinatie met* het tonen of overleggen van een kopie van het legitimatiebewijs, eventueel in combinatie met iDIN, zou bij een zgn. laagrisicoproduct (zoals een spaarrekening met vaste tegenrekening) wél voldoende kunnen zijn. Dus zonder extra privacyinbreuk in de vorm van een selfie-filmpje. Waar LPB gelet op het subsidiariteitsbeginsel, indien mogelijk, ook voor zou moeten kiezen. Waarom een ernstigere privacyinbreuk in de vorm van een selfie-video in dat licht noodzakelijk zou zijn wordt door LPB niet onderbouwd, maar door de GC wel aangenomen (r.o. 3.9).

6. De omgekeerde vraag geldt evenzeer. Als er géén sprake zou zijn van een laag risico op witwassen en terrorismefinanciering, moet de gebruikte verificatiemethode betrouwbaar genoeg zijn. Dit volgt mede uit het Unierechtelijk beginsel van *geschiktheid*, dat net als het subsidiariteitsvereiste onderdeel uitmaakt van het evenredigheidsbeginsel vastgelegd in art. 5 lid 4 VEU. De Duitse privacytoezichthouder, *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, heeft in 2021 in het Jaarbericht 2020 (*Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit 2020*, p. 77-78) geconcludeerd dat videoverificaties “onder geen enkele omstandigheid” kunnen worden gebruikt voor identiteitsverificaties met een hoog risico. Dan is een selfie-filmpje dus ook niet geschikt.

7. In deze noot richt ik mij op twee andere aspecten van dit GC-advies, namelijk (1) wie de bewijslast draagt of er sprake is van de verwerking van bijzondere persoonsgegevens, en (2) of de GC wellicht op andere gronden tot de conclusie had kunnen komen dat LPB geen selfie-video had mogen “eisen”.

8. GC heeft twee deskundigen geraadpleegd: mr. A. Berlee, hoogleraar privacyrecht aan de OU, en Riverworks Legal Services. Volgens Berlee leidt niet iedere gebruikte video-opname tot een verwerking van *biometrische gegevens met het oog op de unieke identificatie van een persoon* in de zin van art. 9 lid 1 AVG, waarvoor in beginsel een verwerkingsverbod geldt. Daar is meer voor nodig, namelijk een *specifieke technische verwerking* die als doel en gevolg heeft dat de identificatie of authenticatie van een natuurlijk persoon mogelijk wordt gemaakt (overweging 51 AVG). Daarvan is sprake wanneer de cliënt wordt gevraagd bepaalde handelingen uit te voeren in

een video, zoals het heen en weer bewegen van het hoofd (een “*liveness check*”) én identificatie of authenticatie, het bevestigen van de identiteit van de persoon in de video, plaatsvindt middels minimaal één specifieke technische verwerking (zie Autoriteit Persoonsgegevens, *Antwoord op vragen over verwerkingen van persoonsgegevens bij de inzet van gezichtsherkenning*, 2 mei 2024, p. 8 en 10). Daarvan is geen sprake wanneer een *medewerker* de persoon in het filmpje volledig (zonder specifieke technische verwerking) handmatig vergelijkt met de pasfoto op het paspoort, of als de instelling helemaal niet controleert *wie* er op het filmpje te zien is – maar enkel of het een levend persoon is (beide zullen in de praktijk niet vaak voorkomen).

9. Volgens de GC is er (1) sprake van een *liveness check*, en (2) het vergelijken van de foto op het identiteitsbewijs met de persoon in de video-opname (r.o. 3.7) en het “*aan de hand van identificatiepunten [bepalen] of de persoon in het identiteitsbewijs dezelfde is als de persoon in de verificatievideo*” (r.o. 3.11). De uitspraak maakt niet duidelijk of dit volledig handmatig door mensen gebeurt, of (ook) met specifieke technische verwerkingen. De GC komt tot het oordeel dat niet is komen vast te staan dat er sprake is van de verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon: “Het enkele feit dat een verificatiefilmpje moet worden aangeleverd maakt nog niet dat biometrische gegevens moeten worden verstrekt” (r.o. 3.15).

10. De GC gaat daarmee echter voorbij aan het tweede aspect van de verwerking van het verificatiefilmpje, namelijk het “*aan de hand van identificatiepunten [bepalen] of de persoon in het identiteitsbewijs dezelfde is als de persoon in de verificatievideo*” (r.o. 3.11). Indien dat proces namelijk gedeeltelijk of volledig geautomatiseerd plaatsvindt, kwalificeert dat wel als een specifieke technische verwerking met als doel en gevolg de unieke identificatie of authenticatie van de natuurlijke persoon die de *liveness check* ondergaat. En dus is er, anders dan de GC heeft geoordeeld, in dat geval wel sprake van de verwerking van biometrische gegevens die mogelijk raakt aan het verwerkingsverbod van bijzondere persoonsgegevens.

11. Zowel Riverworks als Berlee hebben opgemerkt dat uit het procesdossier niet blijkt hoe LPB de video-opnames gebruikt voor de identi-

teitsverificatie. De GC had LPB gevraagd om de verwerkingsovereenkomst met softwareleverancier Onfido te overleggen, die volgens haar website “AI-powered digital identity solutions” aanbiedt. Maar LPB heeft dat geweigerd (r.o. 3.12). Ook LPB’s Privacyverklaring d.d. 5 mei 2021 vermeldt niet dat van (toekomstige) cliënten een video-opname wordt verwerkt, laat staan hoe dat gebeurt (handmatig of met een technische verwerking).

12. Opmerkelijk is daarom dat de GC, ondanks de weigering om deze overeenkomst te overleggen, in haar advies spreekt van een “gemotiveerde betwisting” van LPB dat sprake is van de verwerking van biometrische gegevens (r.o. 3.15). En even opmerkelijk is dat de GC oordeelt dat *de consumenten* onvoldoende hebben onderbouwd dat de bank wél biometrische gegevens verwerkt. Het is niet duidelijk wat die gemotiveerde betwisting inhoudt, noch hoe een consument kan onderbouwen dat er sprake is van de verwerking van biometrische gegevens als de verwerkingsverantwoordelijke daarover geen openheid geeft.

13. De Rechtbank Amsterdam (15 maart 2023, «JOR» 2023/225, m.nt. Van der Kooij en Reus, r.o. 11.20) en het Hof Amsterdam (4 april 2023, ECLI:NL:GHAMS:2023:793, r.o. 3.20) hebben overwogen dat de AVG afwijkende bewijsregels bevat (de verantwoordingsplicht, zie ook De Vries, in *T&C Privacy- en gegevensbeschermingsrecht*, art. 5 AVG, aantek. 2). De *verwerkingsverantwoordelijke* moet bewijzen dat een gegevensverwerking rechtmatig is. Als informatie zich grotendeels in het domein van de verwerkingsverantwoordelijke bevindt, geldt ook een verzwaarde motiveringsplicht. Op grond van art. 35 lid 6 UAVG zijn partijen bovendien verplicht om inlichtingen en onder hen berustende stukken te verstrekken.

14. Gelet op het voorgaande volstaat een betwisting van LPB dat LPB biometrische gegevens verwerkt dus niet in het licht van twee deskundigen die opmerken dat uit het procesdossier niet blijkt hoe LPB de selfie-video’s dan wel verwerkt, en had LPB minimaal de door de GC gevraagde verwerkingsovereenkomst met Onfido moeten verstrekken. Als een verwerkingsverantwoordelijke echter niet transparant wil zijn, kan dit ook geen rechtmatige gegevensverwerking opleveren, wat reeds voldoende grond op zou kunnen leveren om de klacht van de consumenten toe te wijzen.

15. Er is nog een andere reden waarom de consumenten in het gelijk gesteld hadden kunnen worden. In art. 2.2 van de Voorwaarden Online Spaarrekening van LPB d.d. 1 februari 2019 staat dat de identiteit van de cliënt wordt gecontroleerd aan de hand van een identificatiestorting van € 1 en dat LPB de cliënt kan benaderen "voor aanvullende informatie." Net als in de Privacyverklaring wordt daarin de geëiste verificatievideo niet genoemd. Nieuwe cliënten die niet eerst de website doorzoeken, worden hier pas mee geconfronteerd nadat het aanvraagproces is aangevangen.

16. De Rechtbank Noord-Holland 27 oktober 2021, ECLI:NL:RBNHO:2021:9542, overwoog in r.o. 4.14 dat voor zover geen contractuele afspraken zijn gemaakt over de wijze van identificatie, partijen zich jegens elkaar dienen te gedragen naar de eisen van redelijkheid en billijkheid. Hoewel ook dan de gekozen verificatiemethode nog steeds aan de vereisten van de Wvft moet voldoen, kan dit ertoe leiden dat de instelling rekening moet houden met de voorkeur van de cliënt om bijvoorbeeld thuis, op kantoor of (volgens de ktr.) via een persoonlijk FaceTime-gesprek geverifieerd te worden. Ook op grond hiervan had de GC kunnen oordelen dat LPB de consumenten op kantoor had moeten verwelkomen.

17. Anders dan de mediaberichtgeving doet vermoeden, is met deze uitspraak niet vast komen te staan dat banken selfie-video's "voor [het] identificeren [van] klant[en]" mogen "eisen". Dit omdat deze video's in de praktijk doorgaans wel aan automatische identiteitsverificaties worden onderworpen mét verwerking van biometrische gegevens om de persoon op de video te identificeren of authenticeren. En zoals blijkt uit de lezenswaardige adviezen van Berlee en Riverworks, is het nog lang geen uitgemaakte zaak of banken daarvoor selfie-video's mogen eisen.

18. Een laatste vraag, die volgens mij dringend beantwoord moet worden, is waarom er (nog) geen privacyvriendelijke identiteitsverificatiemethode is voor Wvft-instellingen. DigiD kan daarvoor geschikt worden gemaakt. Net als in andere lidstaten kan dit ook betrekkelijk eenvoudig via postkantoren worden georganiseerd. Daar toont de klant een QR-code of voucher van de instelling die de identiteitsverificatie nodig heeft, en toont fysiek zijn of haar paspoort aan een balie-medewerker die het paspoortnummer noteert en digitaal doorstuurt naar de instelling. Hiervoor is

geen foto of video nodig. En het is sneller dan een onlineverificatie.

mr. drs. D. Mekic
promovendus te Leiden en Eindhoven

Financiering, zekerheden en insolventie

265

Profijtbeginsel draagplicht concernfinanciering

Rechtbank Noord-Nederland zp Assen
27 december 2023, rolnr. HA ZA 20-112,
ECLI:NL:RBNNE:2023:5607
(mr. Van Baalen)
Noot mr. dr. C.H.A. van Oostrum

Hoofdelijke aansprakelijkheid voor concernfinanciering. Vaststelling onderlinge draagplicht. (Indirect) profijt van belang voor bepaling van onderlinge draagplicht.
Verwijzing naar HR 18 april 2003, «JOR» 2003/160, m.nt. Bartman (Rivier de Lek/Van de Wetering). Vervolg op Rb. Noord-Holland 15 december 2021 en 15 juni 2022, «JOR» 2023/45, m.nt. Heesterbeek en HR 24 februari 2023, «JOR» 2023/166, m.nt. Wessels.

[BW art. 6:6, 6:10]

Failliet heeft indirect geprofiteerd van (een deel van) het krediet dat aan gedaagde (in conventie) verleend is, te weten het krediet dat is verkregen en aangewend voor het pand in X. Door dit krediet kon gedaagde het betreffende pand aankopen en kamers aanbieden aan zorgbehoevende mensen. Deze zorg konden de mensen vervolgens desgewenst afnemen bij een aan gedaagde gelieerde vennootschap: failliet. Indien gedaagde het pand niet op deze wijze had geëxploiteerd, had failliet geen zorg verleend aan deze geconcentreerde hoeveelheid mensen op deze locatie, maar mogelijk aan minder mensen of aan dezelfde hoeveelheid mensen, maar dan verspreid door