Advies aan Kifid inzake wijze van identificatie en verificatie en de inzet van biometrie daarbij bezien vanuit de vereisten van de AVG

Prof. mr. A. Berlee
Hoogleraar gegevensbescherming en privacyrecht aan de Open Universiteit

d.d. 11 juli 2023

Inleiding

1. De onderzoeksvraag van Kifid is als volgt geformuleerd:

   "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 zonder meer verplicht worden?"

2. In dit advies wordt met name ingegaan op vereisten die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG), in het bijzonder de rechtmatigheid van de verwerking. Het bouwt daarvoor logischerwijs voort op hetgeen in het advies van *Riverworks Legal Services* is vastgesteld met betrekking tot de Wwft-verplichtingen.

3. In dit advies wordt dus enkel gekeken naar de mogelijke verwerking van biometrische gegevens in het kader van de identificatie- en verificatieverplichtingen die op een financiële dienstverlener rusten. De eisen die gesteld worden aan de mogelijke verdere verwerking van persoonsgegevens voor de vereiste bewaring van het bewijs van het naleven van de identificatie- en verificatieverplichtingen maken geen onderdeel uit van de onderzoeksvraag en worden derhalve niet nader uitgewerkt.

4. Dat betekent dat de volgende onderwerpen/vragen aan bod komen in dit advies:

   1) Het beginsel van minimale gegevensverwerking en de daaruit voortvloeiende vereisten.
   2) Is de verwerking in het kader van de verificatie aan de hand van een video-opname een verwerking van biometrische gegevens?
   3) Wanneer kan het verwerkingsverbod op de verwerking van biometrische gegevens worden doorbroken? Welke doorbrekingsgronden staan eventueel open voor de financiële dienstverlener, een onlinebank, die voor de identificatie en/of verificatie gebruik wil maken voor biometrische gegevens van de potentiële klant. Wat is de rol die alternatieven spelen hierin?
   4) Het belang van een DPIA.
   5) De vereiste grondslag voor de verwerking van biometrische gegevens.

Het beginsel van minimale gegevensverwerking en de daaruit voortvloeiende vereisten

5. De regels met betrekking tot de verwerking van persoonsgegevens zijn te vinden in de Algemene Verordening Gegevensbescherming (AVG). Deze legt verplichtingen op aan (met name) de verwerkingsverantwoordelijke,[1] in casu de financiële dienstverlener zijnde een onlinebank. In artikel 5 lid 1 AVG zijn de kernbeginselen opgenomen waar de verwerking van persoonsgegevens aan moet voldoen. Het gaat hier om de beginselen van rechtmatigheid, behoorlijkheid en transparantie,[2] doelbinding,[3] juistheid,[4] opslagbeperking[5] en de beginselen van integriteit en vertrouwelijkheid.[6] Daarnaast is een van de kernbeginselen het beginsel van minimale gegevensverwerking, ook wel dataminimalisatie genoemd, opgenomen in artikel 5 lid 1 sub c) AVG.

6. Het beginsel van minimale gegevensverwerking verplicht de verwerkingsverantwoordelijke dat de persoonsgegevens die worden verwerkt toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit brengt volgens de overwegingen van de AVG met name met zich mee dat ervoor wordt gezorgd dat de opslagperiode van de persoonsgegevens tot een strikt minimum wordt beperkt en dat persoonsgegevens alleen mogen worden verwerkt indien “het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt.”[7]

7. Het beginsel houdt dus drie elementen in zich die allen met elkaar verband houden. De persoonsgegevens moeten (i) ‘toereikend zijn’, (ii) ‘ter zake dienend’ en (iii) ‘beperkt tot wat noodzakelijk is voor de doeleinden’. Het gaat hier in wezen om de vraag of de persoonsgegevens die worden verwerkt voldoende zijn (toereikend zijn) om het gestelde doel op de juiste manier te kunnen vervullen; dat de persoonsgegevens ook daadwerkelijk relevant zijn in het kader van het doel (ter zake dienend) en dat voor het bereiken van het doel zo min mogelijk persoonsgegevens worden verwerkt. Ofwel, dat de hoeveelheid persoonsgegevens niet bovenmatig is (beperkt tot wat noodzakelijk is).

8. Belangrijk om te benadrukken in dit kader is dat dit beginsel, met name bezien in het licht van de rechtmatigheid van de verwerking,[8] echter niet met zich meebrengt dat iedere verwerking die de verwerkingsverantwoordelijke voorstaat tegengehouden kan worden omdat de verwerking mogelijk plaats kan vinden op een minder verregaande manier. Te allen tijde houdt dit een afweging van alternatieven en belangen in.[9]

9. In artikel 6 AVG wordt nader uitwerking gegeven aan het kernbeginsel dat de verwerking van persoonsgegevens rechtmatig plaats dient te vinden. In dit artikel worden limitatief de grondslagen gegeven waar een verwerking van persoonsgegevens op gestoeld kan zijn. Alle in de casus mogelijke grondslagen waarop de financiële dienstverlener de verwerking op kan baseren vereisen dat de verwerking noodzakelijk is.[10] Bij de beoordeling van de noodzakelijkheid van de verwerking speelt ook het beginsel van minimale gegevensverwerking een rol.

10. De noodzaak van een verwerking van persoonsgegevens is namelijk pas aangetoond wanneer het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een

[1] Kortgezegd degene die het doel en middelen van de verwerking bepaalt.
[2] Artikel 5 lid 1 sub a) AVG.
[3] Artikel 5 lid 1 sub b) AVG.
[4] Artikel 5 lid 1 sub d) AVG.
[5] Artikel 5 lid 1 sub e) AVG.
[6] Artikel 5 lid 1 sub f) AVG.
[7] Overweging 39 bij de AVG.
[8] Waaraan in artikel 6 AVG uitvoering is gegeven.
[9] Zie in deze zin ook ABRvS 30 juni 2021, 201906880/1/A3, ECLI:NL:RVS:2021:1420 (*Afvalpas*), r.o. 14.
[10] HvJ EU 16 december 2008, C-524/06, ECLI:EU:C:2008:724 (*Heinz Huber tegen Bundesrepublik Deutschland*). In deze zaak had het HvJ EU vastgesteld dat het begrip “noodzakelijk” een EU autonoom begrip is.

andere, voor de bij de verwerking van persoonsgegevens betrokken personen minder nadelige wijze kan worden verwezenlijkt.[11]

11. Voor de bepaling van de rechtmatigheid van een verwerking maakt het voorts uit of er sprake is van een verwerking van biometrische gegevens. Bij de verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon gelden additionele eisen op grond van de AVG naast de vereiste grondslag voor de verwerking. Biometrische persoonsgegevens worden op grond van artikel 9 lid 1 AVG aangemerkt als een bijzondere categorie van persoonsgegevens.

12. Het verwerken van bijzondere categorieën van persoonsgegevens is in beginsel verboden. Het gaat hier namelijk om persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, en daarom verdienen zij specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden.[12] De Autoriteit Persoonsgegevens (AP) wijst in het geval van de verwerking van biometrische gegevens ook op 'een ernstig risico voor de gegevensbescherming van betrokkenen'. Met name wanneer deze gegevens in verkeerde handen komen kan dit risico zich verwezenlijken, op dat moment 'kan dit gegeven immers niet worden gewijzigd (in tegenstelling tot een wachtwoord) en daarom is de impact ook groter'.[13]

13. Dit verbod kan maar zeer beperkt doorbroken worden. Daarop wordt hierna ingegaan nadat eerst de vraag beantwoord wordt of daadwerkelijk sprake is van de verwerking van biometrische gegevens.

Is er sprake van een verwerking van biometrische gegevens?

14. In de onderzoeksvraag wordt expliciet gevraagd naar de rechtmatigheid van de verwerking van *biometrische* gegevens met het oog op de unieke identificatie van een persoon in het kader van de identificatie- en verificatieprocedure. Uit het procesdossier blijkt echter niet expliciet dat er sprake is van de verwerking van *biometrische* gegevens bij de identificatie en verificatie van de identiteit van de potentiële klant.

15. Het is namelijk niet zo dat iedere video-opname die wordt gebruikt om de identiteit te verifiëren, leidt tot een verwerking van biometrische gegevens in de zin van de AVG.

16. In artikel 4 punt 14) AVG worden biometrische gegevens gedefinieerd als zijnde:

> *"persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;"*

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:

---

[11] Zie ABRvS 30 juni 2021, 201906880/1/A3, ECLI:NL:RVS:2021:1420 (Afvalpas), r.o. 11.
[12] Overweging 51 bij de AVG.
[13] Autoriteit Persoonsgegevens, *Brief aan Centraal Bureau Levensmiddelenhandel inzake Voorlichting – regels voor gezichtsherkenning in supermarkten*, 1 mei 2020 z2020-02082, blz. 3.
[14] Zie ook EDPB, Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur, versie 2.0 d.d. 29 januari 2020, punt 74, waarin staat: "De video-opnamen van een persoon kunnen echter op zichzelf niet als biometrische gegevens in de zin van artikel 9 worden beschouwd als deze niet met bepaalde technische middelen zijn verwerkt met het oog op diens identificatie." Zie eveneens *Kamerstukken II* 2017/18, 34 851, nr. 3 (MvT *Uitvoeringswet Algemene verordening gegevensbescherming*), blz. 40-41.

"[…] 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. […]"

18. Dit in tegenstelling tot de uitspraak van de Commissie van Beroep in zaak nr. 2023-0004, waarin ten onrechte werd overwogen dat uit artikel 4 punt 14) AVG "blijkt dat een foto moet worden beschouwd als een biometrisch gegeven (…) wanneer verwerking gebeurt met het oog op identificatie."[15] De Commissie van Beroep ziet daarmee een belangrijk punt over het hoofd.

19. Overweging 51 bij de AVG stelt namelijk, net als de definitie in artikel 4 punt 14) AVG, dat er enkel sprake is van een verwerking van biometrische gegevens wanneer er bij foto's – maar dit geldt eveneens voor video-opnames – (i) sprake is van een verwerking van fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon,[16] waarbij (ii) een specifieke technische verwerking ervoor zorgt dat (iii) de unieke identificatie of authenticatie van een natuurlijk persoon mogelijk wordt gemaakt. 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.

20. Om onder de AVG als biometrische gegevens aangemerkt te worden, moet de verwerking van ruwe gegevens, zoals de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon, dus gepaard gaan met een meting van deze kenmerken.[17] Voorbeelden van dit soort technische middelen zijn bijvoorbeeld het gebruik van gezichtsherkenningssoftware of de vergelijking van vingerafdrukken.

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 gezichtsherkenningssoftware die bepaalde punten op het gezicht gebruikt en de afstand daartussen meet om deze te vergelijken met een database met templates van gezichten.

22. Uit het procesdossier zelf blijkt niet direct *hoe* de video-opnames worden gebruikt voor de verificatie. De klager heeft het consequent over de verwerking van biometrie en de verwerende partij beroept zich op enig moment ook op de uitzonderingsgrond in artikel 29 Uitvoeringswet AVG (UAVG) die specifiek gericht is op de verwerking van biometrische gegevens met het oog op de unieke identificatie. Desalniettemin wordt in datzelfde stuk enkel gesproken over een video-opname en een 'korte selfie video opname' zodat 'de foto op het

[15] Commissie van Beroep Financiële Dienstverlening 8 februari 2023, nr. 2023-0004, punt 5.25-5.27.
[16] Het gaat hierbij om fysieke kenmerken zoals het aangezicht, maar ook iemands stem, wijze van lopen, en zelfs de analyse van de manier van typen op een toetsenbord kan hieronder worden verstaan. Zie bijvoorbeeld C. Wendehorst & Y. Duller, *Biometric Recognition and Behavioural Detection* (rapportage ten behoeve van het EU parlement, PE 696.968), Brussel: Europese Unie 2021, blz. 12. Bij de invoering van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), werd expliciet gewezen op de verwerking van 'vingerafdrukken, gezichtsherkenning of irisscans', *Kamerstukken II* 2017/18, 34 851, nr. 3, blz. 108.
[17] EDPB, Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur, versie 2.0 d.d. 29 januari 2020, punt 74.
[18] Bijvoorbeeld relevant met het oog op de *liveness* check die plaats dient te vinden.

copy ID vergeleken kan worden met de selfie video opname'. Daaruit blijkt niet direct de verwerking van biometrische gegevens. Tevens biedt de derde partij die de financiële dienstverlener inzet bij de identificatie en/of verificatie, verschillende producten aan die gebruik maken van video-opnamen, die niet allemaal eveneens de inzet van biometrie inhouden.

23. Het is derhalve van het grootste belang dat bij zaken die aan het Kifid worden voorgelegd, zoals de onderhavige, steeds de voorvraag beantwoord wordt of daadwerkelijk sprake is van de verwerking van biometrische gegevens.

24. Gelet op de onderzoeksvraag wordt er in het vervolg daarom – zonder dat dit ook daadwerkelijk is vastgesteld – aangenomen dat er sprake is van een verwerking van biometrische gegevens in de zin van artikel 4 punt 14) AVG die eveneens leidt tot een verwerking die op grond van artikel 9 lid 1 AVG in beginsel verboden is.

Doorbreking van het verwerkingsverbod op de verwerking van biometrische gegevens met het oog op de unieke identificatie

25. Het verbod op de verwerking van biometrische gegevens is echter niet absoluut. Zo biedt het tweede lid van artikel 9 AVG de mogelijke gronden op basis waarvan het verwerkingsverbod in het eerste lid doorbroken kan worden. Het gaat hier bijvoorbeeld om uitdrukkelijke toestemming van de betrokkene voor de verwerking van deze bijzondere persoonsgegevens, of het feit dat de verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene (zo moet een medisch hulpverlener gegevens over gezondheid ook kunnen verwerken wanneer de betrokkene bewusteloos is).[19]

26. In het kader van de adviesaanvraag is met name de uitzondering in artikel 9 lid 2 sub g) AVG relevant. Daarin is opgenomen dat het verwerkingsverbod ook niet geldt indien de verwerking "*noodzakelijk [is] om redenen van zwaarwegend algemeen belang, op grond van […] lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene*".

27. De Nederlandse wetgever heeft op grond van artikel 9 lid 2 sub g) AVG de mogelijkheid om in de wet een uitzondering op het verwerkingsverbod neer te leggen. Dat kan op twee wijzen gebeuren, (i) via een algemene of specifieke bepaling in de UAVG, of (ii) via een specifiek in sectorale wetgeving opgenomen uitzonderingen op het verwerkingsverbod. Beide opties worden hieronder besproken.

Een uitzondering op het verwerkingsverbod in sectorale wetgeving?

28. In de Wwft is op dit moment niet een expliciete wettelijke bepaling opgenomen waarin staat dat het verwerkingsverbod voor bijzondere categorieën van persoonsgegevens in het algemeen, en biometrische gegevens in het bijzonder, wordt doorbroken. Om de daaruit ontstane onduidelijkheid[20] voor instellingen maar ook voor betrokkenen weg te nemen is er een wijziging voorgesteld van de Wwft.

De Wet plan van aanpak witwassen

[19] Zie voor alle uitzonderingsgronden artikel 9 lid 2 AVG.
[20] Hetgeen ook door de Autoriteit Persoonsgegevens is opgemerkt, met name in relatie tot transactiemonitoring, in haar advisering op het conceptwetsvoorstel Wet plan van aanpak witwassen, zie Autoriteit Persoonsgegevens, *Advies consultatieversie voorstel voor de wet plan van aanpak witwassen*, 12 maart 2020 *z*2019-27972.

29. In het wetsvoorstel Wet plan van aanpak witwassen is een wijziging voorgesteld van artikel 34a Wwft waarbij een nieuw eerste lid wordt ingevoegd:

> *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*.

30. In de Memorie van Toelichting wordt in dit kader ook stilgestaan bij de verwerking van bijzondere categorieën van persoonsgegeven in het kader van het cliëntenonderzoek.

31. Belangrijk in dit kader is dat de voorbeelden die worden gegeven waarbij het noodzakelijk is dat de instellingen bijzondere categorieën van persoonsgegevens moeten kunnen verwerken met name zien op de verwerking van bijzondere persoonsgegevens die blijken uit transactiegegevens.[21] Denk aan de verwerking van gezondheidsgegevens in het kader van een transactie aan een zorginstelling, seksuele gerichtheid die blijkt uit een betaling aan een seksclub, of lidmaatschap van een vakbond of politieke partij, dan wel een levensbeschouwelijke of religieuze overtuiging die blijkt uit een contributiebetaling. Deze voorbeelden zijn dus met name gericht op informatie die blijkt uit transactiegegevens. Daarnaast worden ook enkele voorbeelden gegeven die zien op vereisten uit hoofde van het cliëntonderzoek (los van de transacties), zoals het bepalen of een persoon een politiek prominente functie bekleedt hetgeen een verwerking van politieke overtuiging met zich meebrengt.

32. In het kader van de vereiste identificatieplicht wordt in de Memorie van Toelichting enkel het voorbeeld gegeven van de mogelijke verwerking van bijzondere persoonsgegevens in het kader van een afschrift van een identiteitsbewijs.

> *Daarnaast zijn instellingen altijd verplicht om een cliënt te identificeren en doen dit middels een afschrift van een identiteitsbewijs. Het vastleggen van dit afschrift komt reeds neer op het verwerken van persoonsgegevens waaruit iemands ras of etnische afkomst kan worden afgeleid.[22] Dit is ook het geval bij het vastleggen van camerabeelden bij pintransactie bij geldautomaten. Hierbij kan sprake zijn van verwerking van biometrische persoonsgegevens, zoals gezichtsafbeeldingen.[23]*

33. De Memorie van Toelichting biedt daarmee maar beperkte duidelijkheid voor de beantwoording van de casus die aanleiding is voor dit advies. Zo wordt er niet gesproken over de verwerking van biometrische persoonsgegevens in relatie tot de verplichting om de identiteit vast te stellen. Alleen in het kader van het vastleggen van camerabeelden bij pintransacties wordt hierover gesproken,[24] maar dat ziet niet op de identificatie of verificatie zoals bedoeld in het kader van het eerste clientonderzoek bij het openen van een (spaar)rekening.

---

[21] *Kamerstukken II* 2022/23, 36 228, nr. 3, blz. 16-17.
[22] Hierbij lijkt te worden aangesloten bij de opmerking van de Autoriteit Persoonsgegevens zoals deze op haar website blijkt (link). Zie kopje 'Bijzondere persoonsgegevens'. Hiermee wijkt de AP dus af van het standpunt van de EDPB richtsnoeren EDPB, Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur, versie 2.0 d.d. 29 januari 2020, punt 74.
[23] *Kamerstukken II* 2022/23, 36 228, nr. 3, blz. 16.
[24] Daarnaast is het ook hier de vraag of er inderdaad biometrische persoonsgegevens worden verwerkt. Het enkel vastleggen van camerabeelden bij pintransacties brengt zoals eerder aangegeven namelijk niet zonder meer een verwerking van biometrische persoonsgegevens met het oog op de unieke identificatie met zich mee.

34. Ook is de verwerking van biometrische gegevens met het oog op de unieke identificatie geen verwerking die kan worden afgeleid, maar vereist deze verwerking juist een actieve handeling die gericht is op de unieke identificatie. Dat laat enige onduidelijkheid of de wetgever ook heeft beoogd om biometrische persoonsgegevens onderdeel van de voorgenomen brede uitzonderingsgrond zoals vormgegeven in artikel 34a Wwft te laten zijn.

35. Daartegenin kan worden gebracht dat de wetgever wél biometrische gegevens expliciet noemt in de Memorie van Toelichting, ware het niet in het kader van het vastleggen van camerabeelden bij pintransacties. Ofwel de wetgever lijkt de verwerking van biometrische gegevens met het oog op de unieke identificatie niet uit te sluiten.

36. Zelfs wanneer we ervan uitgaan dat met de invoering van het nieuwe eerste lid van artikel 34a Wwft de wettelijke mogelijkheid wordt geboden om biometrische gegevens met het oog op de unieke identificatie te kunnen gebruiken in het kader van het vaststellen van de identiteit en verificatie voorafgaand aan het openen van een (spaar)rekening, is de inzet van dit middel alleen mogelijk indien dit daadwerkelijk *noodzakelijk* is. De doorbreking is immers geclausuleerd voor die verwerkingen van bijzondere persoonsgegevens die noodzakelijk zijn. Daar komen we dadelijk op terug.

De UAVG

37. In de Wwft zelf is dus (nog) niet een expliciete uitzondering op het verwerkingsverbod opgenomen. De Nederlandse wetgever heeft echter in de UAVG ook enkele algemene uitzonderingsgronden en een specifieke uitzonderingsgrond opgenomen.

38. De algemene uitzonderingsgronden die voor alle bijzondere categorieën van persoonsgegevens gelden zijn in artikel 22 lid 2 UAVG opgenomen en betreffen hoofdzakelijk een herhaling van de bepalingen in artikel 9 lid 2 sub a), en c) t/m f) AVG. Het gaat hier allemaal om uitzonderingen die overduidelijk niet van toepassing zijn in de onderhavige casus en daarom geen verdere bespreking behoeven.[25]

39. Artikel 29 UAVG geeft een specifieke uitzonderingsgrond voor de verwerking van biometrische gegevens en luidt:

> *"Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden."*

40. De inzet van biometrie moet dus *noodzakelijk* zijn voor bijvoorbeeld authenticatiedoeleinden. Deze vereiste noodzakelijkheid van de verwerking van biometrische gegevens houdt in dat de verwerking moet voldoen aan de vereisten van subsidiariteit en proportionaliteit, waarbij het beginsel van minimale gegevensverwerking zoals eerder aangegeven ook een rol speelt.

41. Dit werpt dus de vraag op of in deze specifieke situatie (het betrouwbaar kunnen identificeren van klanten door een onlinebank) er ook gebruik gemaakt kan worden van andere, voor de betrokkene minder ingrijpende methoden om te kunnen voldoen aan de vereiste identificatie en/of verificatie die de Wwft met zich meebrengt (subsidiariteit). Zijn deze aanwezig dan kan een beroep op de uitzondering van artikel 29 UAVG niet slagen. Evenmin staat een beroep

[25] De uitzonderingsgrond van de uitdrukkelijke toestemming komt mogelijk in beeld wanneer de verwerking van biometrische gegevens als alternatief wordt geboden naast bijvoorbeeld identificatie of verificatie in persoon op locatie. Ook aan het geven van toestemming zijn echter voorwaarden verbonden, waar in dit advies niet nader op wordt ingegaan, nu de financiële dienstverlener zich niet op deze grondslag noch doorbrekingsgrond beroept.

op de uitzonderingsgrond open wanneer de hoeveelheid gegevens die wordt verwerkt niet in verhouding staat tot het doel en als bovenmatig kan worden aangemerkt (proportionaliteit).

42. Uit de parlementaire geschiedenis blijkt dat de wetgever deze uitzondering strikt hanteert en alleen toelaat als sprake is van een uitzonderlijke situatie:[26]

> *" […] Er dient wel een afweging te worden gemaakt of identificatie met biometrische gegevens noodzakelijk is voor authenticatie of beveiligingsdoeleinden. De werkgever zal dan moeten afwegen of de gebouwen en informatiesystemen zodanig beveiligd moeten zijn dat dit met biometrie dient plaats te vinden. Dit zal het geval zijn als de toegang beperkt dient te zijn tot bepaalde personen die daartoe geautoriseerd zijn, zoals bij een kerncentrale. Het verwerken van biometrische gegevens dient ook proportioneel te zijn. Als het om de toegang tot een garage van een reparatiebedrijf gaat, zal de noodzaak van de beveiliging niet zodanig zijn dat werknemers alleen met biometrie toegang kunnen krijgen en daartoe deze gegevens worden vastgelegd om de toegangscontrole uit te oefenen. Aan de andere kant kan biometrie soms juist een belangrijke vorm van beveiliging zijn voor bijvoorbeeld informatiesystemen, die zelf veel persoonsgegevens bevatten, waarbij onrechtmatige toegang, ook van werknemers, moet worden voorkomen [...]."*

43. Tussen de beveiliging van een kerncentrale en een garage van een reparatiebedrijf zit echter nog wel veel licht. Dit leidde in de praktijk dan ook tot veel onduidelijkheid over wanneer nu wel en niet een beroep op deze uitzondering kon worden gedaan. De AP legde aan een niet nader bekend bedrijf een boete van EUR 725.000,- op voor het inzetten van vingerafdrukscans voor tijdsregistratie terwijl daarvoor de noodzakelijkheidstoets niet kon worden gehaald,[27] en ook schoenenwinkel Manfield mocht van de Rechtbank Amsterdam geen gebruik maken van een kassasysteem dat gebruik maakt van een vingerafdrukscan, aangezien de noodzaak hiervoor niet kon worden aangetoond.[28] Er was onvoldoende onderzocht of er alternatieven bestonden, en daarnaast waren er in het filiaal verder ook geen enkele andere beveiligingsmaatregelen genomen, wat gevolgen had voor de proportionaliteit.[29] De voorbeelden bij andere toezichthouders binnen de EU richten zich ook met name op de inzet van biometrie in de werkgever/werknemer relatie en geven daarmee maar zeer beperkt nadere duiding over wanneer nu wel en niet het verwerken van biometrische gegevens noodzakelijk kan zijn.[30]

Nadere uitleg in komend recht

44. De wetgever heeft mede in het licht van deze onduidelijkheid een aanpassing van artikel 29 UAVG voorgesteld en in de toelichting op deze wijziging nadere uitleg verschaft over de doeleinden waarvoor biometrische gegevens verwerkt mogen worden.

45. In het momenteel aanhangig zijnde wetsvoorstel Verzamelwet gegevensbescherming wordt artikel 29 UAVG gewijzigd in de volgende bepaling:[31]

> *"Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of omwille van beveiligingsdoeleinden en slechts voor zover dit noodzakelijk is vanwege een*

[26] Kamerstukken 2017/18, 34 851, nr. 3 (MvT), blz. 109.
[27] Autoriteit Persoonsgegevens, Besluit tot het opleggen van een bestuurlijke boete (link), 4 december 2019.
[28] Rechtbank Amsterdam 12 augustus 2019, ECLI:NL:RBAMS:2019:6005.
[29] *Idem*, r.o.24-26.
[30] State Data Protection Inspectorate (Litouwen), 21 juni 2021 in het kader van werknemers van een sportclub (link). De Italiaanse toezichthouder heeft ook een boete opgelegd voor de inzet van biometrie bij werknemers van een fitnessclub in 10 november 2021 (link). Ook de werkgever die haar werknemers middels vingerafdrukscan liet inklokken werd door de Spaanse toezichthouder beboet op 26 oktober 2021 (link).
[31] *Kamerstukken II* 2022/23, 36 264, nr. 2 (*Voorstel van wet*), Artikel I, onderdeel K.

zwaarwegend algemeen belang van rechtmatige toegang tot bepaalde plaatsen, gebouwen, diensten, producten, informatiesystemen of werkprocessystemen."

46. Ofwel er wordt een dubbele noodzakelijkheidstoets ingevoerd. Het verbod kan alleen worden doorbroken indien (i) de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden, én (ii) slechts voor zover dit noodzakelijk is vanwege een zwaarwegend algemeen belang van rechtmatige toegang tot bijvoorbeeld bepaalde diensten/producten.

47. Hiermee beoogt de wetgever te voorzien in een extra waarborg nu het noodzakelijk is:

> *"[…] ook nog in het concrete geval te toetsen aan het bedoelde zwaarwegend algemeen belang. […] In de rechtspraktijk zal een verwerkingsverantwoordelijke nu telkens zelf actief moeten toetsen of ook in het specifieke geval wel aan het vereiste «noodzakelijk voor een zwaarwegend algemeen belang» is voldaan, voordat een beroep op de uitzondering kan worden gedaan. Deze afweging zal vervolgens door de AP en uiteindelijk ook door de rechter kunnen worden beoordeeld*."[32]

48. Vervolgens geeft de wetgever aan welke gevallen in aanmerking komen voor een dergelijk zwaarwegend algemeen belang (onderstreping AB):[33]

> *"In de toelichting bij dit artikel bij de invoering van de UAVG, werd reeds als voorbeeld van een zwaarwegend algemeen belang de toegang tot een kerncentrale gegeven in tegenstelling tot de toegang van een garage van een reparatiebedrijf. De beveiliging van een kerncentrale is natuurlijk een aansprekend voorbeeld van een zwaarwegend algemeen belang. Maar ook het beschermen van de volksgezondheid, het voorkomen van milieuschade of het beveiligen van vitale processen kunnen redenen zijn waarmee aan de eis van zwaarwegend algemeen belang wordt voldaan. Naast het reeds genoemde voorbeeld van een kerncentrale, kan bij controle op toegangsbevoegdheden op vitale, gevoelige of gevaarlijke locaties, gedacht worden aan bedrijven en/of diensten uit de vitale infrastructuur (zoals telecomcentrum, beheercentrum energie-infra), aanbieders van essentiële diensten en voor digitale dienstverleners (NIS-Richtlijn), bedrijven of gebieden met veiligheidsrisico's zoals bedrijven met veel risico's op zware ongevallen door de aanwezigheid van grote hoeveelheden gevaarlijke stoffen die onder het Besluit risico's zware ongevallen vallen en lucht- en zeehavens. Voor de goede orde wordt opgemerkt dat het niet alleen gaat om toegang tot gebouwen maar ook om toegangsbeveiliging van randapparatuur (laptop, telefoon e.d.) voor authenticatiedoeleinden ter beveiliging van systemen en netwerken. Er zal in ieder geval een belang gediend moeten worden dat uitstijgt boven louter reguliere bedrijfs- of organisatiebelangen (als efficiëntie of kostenbesparing), wil een verwerkingsverantwoordelijke een beroep op deze uitzondering kunnen doen."*

49. Hoewel de voorbeelden met name zien op de inzet van biometrie bij de *beveiliging* van plaatsen en randapparatuur, gelden deze overwegingen eveneens voor authenticatiedoeleinden voor rechtmatige toegang tot diensten en producten, waaronder ook de financiële dienstverlening geschaard kan worden.

50. Ofwel, de financiële dienstverlener dient te hebben aangetoond dat voor het identificeren en verifiëren van een (potentiële) klant op een wijze die voldoet aan de Wwft verplichtingen de verwerking van biometrische gegevens niet redelijkerwijs op een andere minder ingrijpende wijze kan plaatsvinden en dat de inzet van biometrie proportioneel is. Daarbij kan de financiële dienstverlener zich niet enkel beroepen op het louter reguliere bedrijfs- of organisatiebelang zoals efficiëntie of kostenbesparing. Het belang dat wordt gediend bij de wijze van

[32] *Kamerstukken II* 2022/23, 36 264, nr. 3 (MvT), blz. 22-23.
[33] *Kamerstukken II* 2022/23, 36 264, nr. 3 (MvT), blz. 23.

identificatie/verificatie aan de hand van biometrische gegevens moet worden gekwalificeerd als zijnde *zwaarwegend*.

51. In het advies van *Riverworks* is al naar voren gekomen dat in overweging 42 AMLD4 expliciet is opgenomen dat de bestrijding van witwassen en terrorismefinanciering door alle lidstaten wordt erkend als een zwaarwegend algemeen belang. Dit is ook in Nederland het geval. Daarnaast is in de parlementaire geschiedenis uiteengezet dat het cliëntenonderzoek, met inbegrip van de vereiste identificatie en verificatieverplichtingen, een van de twee kernverplichtingen betreft van deze anti-witwasregelgeving.[34] Hiermee lijkt in het algemeen aangetoond dat de inzet van biometrie een zwaarwegend algemeen belang kan dienen. Vereist is dan nog wel dat de drempel van de noodzaak in het *specifieke* geval moet worden beoordeeld.

Toepassen op de casus

52. Ofwel, vereist de specifieke situatie dat er identificatie en/of verificatie op basis van biometrische gegevens met het oog op de unieke identificatie plaats dient te vinden?

53. Zoals blijkt uit het advies van *Riverworks* wordt de beoordeling van de noodzakelijkheid van de verwerking, net als de wijze van uitvoering van het cliëntenonderzoek overgelaten aan de financiële instelling zelf. Zoals uiteen wordt gezet in de *Richtsnoeren ML/TF-risicofactoren* van de EBA wordt hierover gezegd dat "*bij het identificeren van de ML/TF-risico's verbonden aan een zakelijke relatie of occasionele transactie dienen ondernemingen relevante risicofactoren in overweging te nemen, met inbegrip van wie hun cliënt is, de landen of geografische gebieden waarin deze actief is, de specifieke producten, diensten en transacties die de cliënt verlangt, en de kanalen die de onderneming gebruikt om deze producten, diensten en transacties te leveren*". In de zaak waar het advies op ziet bestaat er een algemeen risico-verhogende factor gelegen in het feit dat de relatie op afstand wordt onderhouden, het gaat hier om een zogenoemd leveringskanaalgebonden risicofactor. Deze factor is echter niet doorslaggevend, er dient te worden gekeken naar het totaalbeeld.[35] Ik zal hier niet herhalen van wat er door *Riverworks* hierover al is gezegd en verwijs naar dat advies voor de uitwerking van de vereiste risicobepaling door de financiële instelling.

54. Hieruit kan voortvloeien dat bij bepaalde vormen van identificatie op afstand het noodzakelijk zijn om gebruik te maken van video-opnamen (zonder de verwerking van biometrische gegevens). Indien de cliënt niet fysiek aanwezig is kan het gebruik van video-opnamen de fysieke afwezigheid compenseren. Dit sluit aan bij de *Leidraad Wwft en Sw* waarin ook wordt gesproken over *'(een combinatie van) video-identificatie en verificatie, het uitlezen van de chip op het identiteitsdocument, het toepassen van een liveness-check en het gebruik van een eID-middel met een adequaat betrouwbaarheidsniveau'*.[36]

Alternatieven

55. In de *Leidraad Wwft en Sw* noch in de *EBA Richtsnoeren ML/TF-risicofactoren*[37] wordt echter expliciet verwezen naar de inzet van biometrische gegevensverwerking als een middel waar de financiële dienstverlener gebruik van kan maken. Met dien verstande dat het 'uitlezen van de chip op het identiteitsdocument' wel in veel gevallen ook een verwerking van biometrische

[34] *Kamerstukken II* 2017-2018, 34 808, nr. 3 (MvT), blz. 13, zie ook Kamerstukken II 2018-2019, 35 245, nr. 3, blz. 21.
[35] European Banking Authority, Richtsnoeren krachtens artikel 17 en artikel 18, lid 4, van Richtlijn (EU) 2015/849 betreffende cliëntenonderzoek en de factoren die kredietinstellingen en financiële instellingen in overweging dienen te nemen wanneer zij het aan afzonderlijke zakelijke relaties en occasionele transacties verbonden witwasrisico en risico van terrorismefinanciering beoordelen (hierna "de richtsnoeren ML/TF-risicofactoren" genoemd), tot intrekking en vervanging van Richtsnoeren JC/2017/37, EBA/GL/2021/02 van 1 maart 2021, punten 3.2-3.3.
[36] DNB, Leidraad Wwft en Sw, versie december 2020, blz. 49.
[37] Zie voetnoot 35.

gegevens met zich mee zal brengen wanneer hierin bijvoorbeeld vingerafdrukken zijn opgenomen.[38]

56. ESA[39]-opinie waaraan ook in het advies van *Riverworks* naar wordt verwezen en waar ook de *Leidraad Wwft en Sw* en de EBA Richtsnoeren ML/TF-risicofactoren naar verwijzen lijkt wel de inzet van gezichtsherkenningssoftware te accepteren als middel om het risico dat er met het videobeeld is geknoeid te voorkomen of verlagen.[40] Andere robuuste methoden die ook worden genoemd in dit kader zijn het (al dan niet in combinatie te gebruiken) live chatten met een gespecialiseerde werknemer, het adequaat belichten van het beeld, automatische herkenning van of er is geknoeid met het beeld zelf aan de hand van pixelatie of vervaging etc.

57. Als robuuste methoden voor het bewerkstelligen van zekerheid met betrekking tot de identiteit van de klant, en daarmee het risico dat iemand zich voordoet als een ander te voorkomen of verkleinen, wordt gewezen op onder andere de mogelijkheid om op alle vereiste documentatie een gekwalificeerde elektronische handtekening te vereisen.[41] Niet onbelangrijk zijn hier ook de overige wijzen waarop verificatie plaats kan vinden of 'de betrouwbaarheid van het verificatieproces te vergroten' zoals opgesomd in de *EBA Richtsnoeren voor het gebruik van oplossingen voor de acceptatie van cliënten op afstand overeenkomstig artikel 13, lid 1, van Richtlijn (EU) 2015/849*.[42]

58. Daarnaast kan ook hier gewezen worden op de elektronische identificatiemiddelen die voldoen aan het betrouwbaarheidsniveau 'substantieel' of 'hoog' als bedoeld in de eIDAS verordening.[43] Wordt gebruik gemaakt van een van deze middelen dan worden deze ook als een betrouwbare en onafhankelijke bron gezien die kan worden ingezet voor de verificatie van de identiteit van natuurlijke personen.[44]

59. Deze – hier maar beperkt aangegeven – lijst met (potentiële) alternatieven is relevant in het kader van de vraag of de inzet van biometrische gegevens voldoet aan de vereiste noodzakelijkheid, in het bijzonder de daaronder begrepen vereiste subsidiariteit. Wanneer naar de beoordeling van de financiële dienstverlener – of in voorkomend geval het Kifid – een dergelijke maatregel of combinatie van maatregelen getroffen kan worden die (in samenhang) *een redelijk alternatief* vormt dat gepaard gaat met een minder vergaande inbreuk op de persoonlijke levenssfeer van de betrokkene, is immers de verwerking van biometrische gegevens voor de identificatie/verificatie niet noodzakelijk.

60. In dit kader is het ook van belang dat de klagende partij als alternatief aanbood om zich fysiek te komen identificeren, maar dat deze onlinebank geen fysieke kantoren heeft die open zijn voor het publiek. Hiervoor verwijs ik net als *Riverworks* naar de uitspraak van de Rechtbank Amsterdam in januari.[45]

---

[38] Zie over de verenigbaarheid van het opslaan van biometrische gegevens in paspoorten en reisdocumenten, HvJ EU 17 oktober 2013, C-291/12, ECLI:EU:C:213:670 (*Schwarz* tegen *Stadt Bochum)*.
[39] De ESA is de afkorting van de Joint Committee of the European Supervision Authorities bestaande uit de European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) en de European Securities and Markets Authority (ESMA). ESA, Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process, JC 2017 81 van 23 januari 2018 (link).
[40] *Idem*, blz. 13-15.
[41] Joint Committee of the European Supervisory Authorities (ESA), Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process, 23 januari 2018, JC 2017 81, blz. 16.
[42] EBA Richtsnoeren voor het gebruik van oplossingen voor de acceptatie van cliënten op afstand overeenkomstig artikel 13, lid 1, van Richtlijn (EU) 2015/849, EBA/GL/2022/15, 22 november 2022.
[43] 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).
[44] In de zin van artikel 11 lid 1 Wwft. Zie ook EBA Richtsnoeren voor het gebruik van oplossingen voor de acceptatie van cliënten op afstand overeenkomstig artikel 13, lid 1, van Richtlijn (EU) 2015/849, EBA/GL/2022/15, 22 november 2022, punt 45.
[45] Rechtbank Amsterdam 11 januari 2023, ECLI:NL:RBAMS:2023:145.

Het belang van een DPIA

61. Zoals blijkt uit artikel 41 AMLD4 is de verwerking van persoonsgegevens op grond van de richtlijn onderworpen aan de AVG. Dit betekent in dit geval ook dat de financiële dienstverlener een gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, ofwel DPIA) dient uit te voeren. Artikel 35 AVG bepaalt immers dat wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen dit met zich meebrengt dat de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uitvoert van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Dit is een DPIA.

62. De AP heeft aangegeven dat grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren, met zich meebrengt dat een verwerkingsverantwoordelijke verplicht is een DPIA uit te voeren.[46]

63. Een dergelijke DPIA bevat ten minste a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd; b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden; c) een beoordeling van de bedoelde risico's voor de rechten en vrijheden van betrokkenen zoals hiervoor omschreven; en d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan de AVG is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.[47]

64. Ofwel, voorafgaand aan het inzetten van biometrie voor de vereiste verificatie van haar potentiële klanten heeft de financiële dienstverlener als het goed is een dergelijke DPIA opgesteld waarin expliciet is ingegaan op de vraag waarom de inzet van biometrie in dit geval noodzakelijk is en hoe de subsidiariteit en proportionaliteit gewaarborgd zijn. Let wel, een verwerkingsverantwoordelijke is niet verplicht op grond van de AVG om een dergelijke DPIA te publiceren. Men hoeft deze dus niet te verwachten op de website van de dienstverlener bijvoorbeeld.

De vereiste grondslag voor de verwerking van biometrische gegevens

65. Naast de vereiste doorbreking van het verwerkingsverbod dient de financiële dienstverlener ook een grondslag voor de verwerking van biometrische gegevens te hebben, wil de verwerking rechtmatig zijn in de zin van de AVG.

66. Zoals eerder aangegeven zijn er zes limitatief opgesomde grondslagen voor de verwerking van persoonsgegevens opgenomen in artikel 6 lid 1 AVG. Er komen meerdere grondslagen mogelijk in aanmerking voor de verwerking van persoonsgegevens op grond van de verplichtingen uit hoofde van AMLD4 en de Wwft, zie in dit kader ook het advies van Riverworks. Hieruit blijkt ook dat de Nederlandse wetgever bij de implementatie van AMLD4 ervan uit is gegaan dat de verwerkingen die daarmee gepaard gaan voor de betrokken instellingen gebaseerd kunnen worden op artikel 6 lid 1 sub c) AVG.[48] De Uniewetgever heeft

[46] Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens, *Stcrt*. 2019, nr. 64418, punt 17.
[47] Artikel 35 lid 7 AVG.
[48] Dit werd destijds ook voorgesteld als de voor de hand liggende grondslag door de Europese Toezichthouder voor gegevensbescherming (EDPS) in haar wetgevingsadvies. Opinion of the European Data Protection Supervisor

in AMLD4 daarentegen gesteld dat de grondslag artikel 6 lid 1 sub e) AVG is. Beiden worden hieronder besproken.

Noodzakelijk om te voldoen aan een wettelijke verplichting

67. Artikel 6 lid 1 sub c) AVG geeft aan dat als grondslag voor de verwerking kan dienen dat de verwerking van persoonsgegevens 'noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust'.

68. De wettelijke bepaling moet op grond van artikel 6 lid 3 AVG en toegelicht in overweging 41 bij de AVG voorts voldoende duidelijk en nauwkeurig zijn, en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is.[49] Dit brengt volgens de Hoge Raad in het *BKR*-arrest ook met zich mee dat uit de wettelijke bepaling moet blijken *welke* persoonsgegevens gebruikt mogen worden.[50]

69. Het is *in casu* zo dat de onlinebank (de verwerkingsverantwoordelijke) wettelijk verplicht is om de natuurlijk persoon die een (spaar)rekening bij hem wenst te openen te identificeren. Het is inherent daaraan dat persoonsgegevens moeten worden verwerkt. Dat ligt immers besloten in het feit dat het hier gaat om identificeren en hetgeen daaromtrent is vastgelegd in artikel 11 Wwft jo artikel 4 Uitvoeringsregeling Wwft waarin de bronnen aan de hand waarvan deze identificatie plaats kan vinden zijn vastgelegd.

70. Het is vervolgens de vraag of daaruit eveneens volgt dat een verwerking van de extra beschermde biometrische persoonsgegevens kan volgen. Artikel 11 Wwft jo. artikel 4 lid 1 sub h) Uitvoeringsregeling Wwft, spreekt in dit kader enkel van 'een voldoende betrouwbaar identificatiemiddel'. Daarop is de verwerking van biometrie met het oog op de unieke identificatie gestoeld. Echter, totdat de voorgestelde wijziging van artikel 34a Wwft wordt ingevoerd is onvoldoende voorzienbaar dat uit hoofde van artikel 11 Wwft jo. 4 lid 1 sub h) Uitvoeringsregeling Wwft volgt dat bijzondere persoonsgegevens zoals biometrische gegevens vallen onder wettelijke verplichting die op de verwerkingsverantwoordelijke rust. Ter onderbouwing daarvan verwijs ik naar wat hier eerder over is gezegd in dit advies.

71. De Europese Toezichthouder voor gegevensbescherming (EDPS) gaf in haar wetgevingsadvies (let wel: uit 2013)[51] op het voorstel voor AMLD4 aan dat het noodzakelijk is om de Richtlijn te verduidelijken en daarin aan te geven of bijzondere persoonsgegevens verwerkt zouden mogen worden of niet. Totdat die duidelijkheid er was leek de EDPS de verwerking van bijzondere persoonsgegevens op deze grond af te wijzen.[52]

---

on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds, 4 juli 2013, blz. 8.

[49] Overweging bij de 41 AVG. Hierbij wordt aangesloten bij rechtspraak van het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens.

[50] In die situatie ging het om artikelen 4:32 lid 1 Wft en 4:34 lid 1 Wft, zoals nader uitgewerkt in artikel 114 BGfo. De Hoge Raad overwoog dat deze bepalingen "kredietaanbieders weliswaar [verplichten] tot deelname aan en raadpleging van een stelsel van kredietregistratie, maar deze wettelijke bepalingen zijn niet voldoende duidelijk en nauwkeurig en de toepassing ervan is niet voldoende voorspelbaar voor degenen op wie deze wettelijke bepalingen van toepassing zijn, zoals art. 6 lid 3 AVG eist (zie hiervoor in 3.1.5). Uit die wettelijke bepalingen blijkt immers niet welke persoonsgegevens in het CKI geregistreerd moeten of mogen worden, wat de voorwaarden voor een dergelijke registratie zijn en onder welke voorwaarden en binnen welke termijnen tot verwijdering van persoonsgegevens moet worden overgegaan. Een en ander wordt wel geregeld in het CKI-reglement, maar dat reglement berust niet op een wettelijke grondslag; de registratie van persoonsgegevens in het CKI vindt plaats op grond van een overeenkomst tussen het BKR en kredietaanbieders (zie hiervoor in 3.1.8)." HR 3 december 2021, ECLI:NL:HR:2021:1814, r.o. 3.1.9.

[51] Het advies ziet dan ook op de verenigbaarheid van de voorgestelde AMLD4 tekst en de Richtlijn 95/46/EG en niet de AVG. Pas met de AVG is de verwerking van biometrische persoonsgegevens expliciet opgenomen als een bijzondere categorie van persoonsgegevens.

[52] EDPS, Opinion of the European Data Protection Supervisor on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds, 13 juli 2013, blz. 17-18.

72. Gelet op een en ander is daarom niet aannemelijk dat de financiële dienstverlener in casu zich kan beroepen op de grondslag van artikel 6 lid 1 sub c) AVG voor de verwerking van biometrische gegevens met het oog op de unieke identificatie om te voldoen aan de wettelijke verplichting die voortvloeit uit artikel 11 Wwft.

73. Indien de wettelijke verplichting wél zo ver kan reiken, dan vereist artikel 6 lid 1 sub c) AVG voorts dat de verwerking van persoonsgegevens *noodzakelijk* moet zijn om aan de wettelijke verplichting te voldoen. Uit de Memorie van Toelichting bij de UAVG blijkt dat de Nederlandse wetgever de eis van noodzakelijkheid zo heeft opgevat dat daaraan is voldaan als zonder verwerking van de persoonsgegevens het uitvoeren van een wettelijke verplichting die op de verwerkingsverantwoordelijke rust, redelijkerwijs niet goed mogelijk is.[53]

74. Als we ervan uitgaan dat het verwerkingsverbod allereerst is doorbroken voordat we de vereiste grondslag gaan toetsen, dan is de onderbouwing van het doorbreken van het verwerkingsverbod op grond van artikel 29 UAVG ook relevant in het aannemen van de noodzakelijkheid in het kader van de grondslag. Immers, de identificatie in de zin van de (wettelijke) Wwft verplichting en de noodzakelijkheid om voor het 'authenticatie'-doeleinde in de zin van artikel 29 UAVG biometrische gegevens te verwerken zijn zeer nauw verbonden aan elkaar.

Noodzakelijk voor de uitvoering van een taak van algemeen belang

75. De zojuist besproken grondslag 'wettelijke verplichting' laat relatief weinig ruimte aan de financiële dienstverlener voor de invulling daarvan. Meer ruimte heeft de verwerkingsverantwoordelijke die een taak van algemeen belang moet vervullen en daarvoor noodzakelijkerwijs persoonsgegevens verwerkt. Het is in beginsel aan de verwerkingsverantwoordelijke om dan te bepalen welke persoonsgegevens hiervoor, met inachtneming van het beginsel van minimale gegevensverwerking, nodig zijn. De verwerkingsverantwoordelijke beroept zich dan op de grondslag zoals vastgelegd in artikel 6 lid 1 sub e) AVG.

76. De Uniewetgever heeft in artikel 43 AMLD4 vastgelegd dat de verwerking van persoonsgegevens op basis van de richtlijn met het oog op het voorkomen van witwassen en terrorismefinanciering "wordt beschouwd als een taak van algemeen belang" in de zin van de AVG. Daaruit vloeit dus de mogelijkheid voort dat de onlinebank zich kan beroepen op de grondslag artikel 6 lid 1 sub e) AVG, ook voor de verwerking van persoonsgegevens in het kader van de identificatie en verificatieverplichtingen.

77. Deze conclusie is echter niet onomstreden.

78. In de regel worden *overheidsorganisaties* met een dergelijke taak van algemeen belang belast en niet private partijen zoals een (online) bank. Het is wel mogelijk, gelet op de overwegingen van de AVG,[54] dat ook een private partij, een taak van algemeen opgedragen krijgt en zich vervolgens op deze grondslag kan beroepen, maar A-G Pikamäe in de *SCHUFA*-zaak die momenteel voorligt bij het HvJ EU concludeerde in dit verband dat:[55]

> *"De verhouding met de „uitoefening van openbaar gezag" en de overwegingen 45, 55 en 56 AVG wijzen er eerder op dat deze bepaling in de eerste plaats gericht is op overheidsinstanties in strikte zin, alsook op rechtspersonen met een taak van openbaar gezag, en in de tweede plaats op privaatrechtelijke rechtspersonen die verwerkingen uitvoeren in het kader van de openbare dienstverlening, bijvoorbeeld op het gebied van „volksgezondheid", „sociale bescherming" en „het beheer van gezondheidszorgdiensten",*

[53] *Kamerstukken II* 2017/18, 34 851, nr. 3, blz. 35.
[54] In het bijzonder overwegingen 45, 55 en 56 bij de AVG.
[55] Conclusie van Advocaat-Generaal Pikamäe 16 maart 2023, C-634/21, ECLI:EU:C:2023:220 (*SCHUFA*), punt 76.

die uitdrukkelijk zijn vermeld in overweging 45. Deze bepaling heeft met andere woorden betrekking op de traditionele taken van de staat."

79. Het standpunt van de A-G krijgt bijval van de EDPB, die kritiek heeft geuit op het gebruik van deze grondslag in het kader van de strijd tegen witwassen.[56] In het bijzonder aan de orde was de verwerking van persoonsgegevens door middel van transactiemonitoring waarbij de opsporing van witwassen en terrorismefinanciering centraal staat. Dat zou volgens de EDPB een overheidstaak zijn die maar *zeer* restrictief belegd zou moeten worden bij private partijen zoals banken.[57] Het Hof van Justitie EU heeft zich evenwel nog niet hierover uitgelaten.

80. Hoewel ik mij kan vinden in deze overwegingen van de EDPB en A-G Pikamäe is er ook wat voor te zeggen dat de beschreven transactiemonitoring en de verwerking van persoonsgegevens die daarmee gepaard gaat (of zal gaan) primair het doel van de *opsporing* van witwassen en terrorismefinanciering dient, en dat deze daarom te onderscheiden is van de verwerking van persoonsgegevens in het kader van de *voorkoming* van witwassen en terrorismefinanciering.

81. De vereiste identificatie en verificatie die de onlinebank voorafgaand aan het openen van een spaarrekening moet uitvoeren ziet volgens mij in beginsel niet op het *opsporen* van witwassen of terrorismefinanciering, maar juist op de *voorkoming* daarvan. De financiële dienstverlener vervult hier een klassieke poortwachtersfunctie. In dat kader is het aannemelijk dat deze taak wel belegd kan zijn bij een private partij zoals een bank, in tegenstelling tot de daaropvolgende transactiemonitoring.

82. Daarnaast is te verdedigen dat de Uniewetgever juist ook het beroep op deze grondslag mogelijk heeft willen maken voor financiële dienstverleners zoals een onlinebank. Namelijk door het opnemen van artikel 43 AMLD4.

83. Dat de onlinebank zich kan beroepen op de grondslag van artikel 6 lid 1 sub e) AVG lijkt mij daarom verdedigbaar, gelet op zowel een tekstuele als contextuele benadering van artikel 43 AMLD4.

84. Wanneer inderdaad wordt aangenomen dat de onlinebank in dit geval zich kan beroepen op deze taak van algemeen belang, dan vereist artikel 6 lid 1 sub e) AVG voorts dat de verwerking van persoonsgegevens *noodzakelijk* moet zijn om aan deze taak van algemeen belang te voldoen.

85. Ook hier geldt dan dat, als we ervan uitgaan dat het verwerkingsverbod allereerst is doorbroken voordat we de vereiste grondslag gaan toetsen, de onderbouwing van het doorbreken van het verwerkingsverbod op grond van artikel 29 UAVG ook relevant is in het aannemen van de noodzakelijkheid in het kader van de grondslag.

Conclusie

86. De onderzoeksvraag gaat ervan uit dat er sprake is van een verwerking van biometrische gegevens, maar dit is niet vast te stellen op basis van het procesdossier. Er wordt gesproken over een video-opname, maar daarmee staat geenszins vast dat er sprake is van een verwerking van biometrische gegevens in de zin van de AVG. Het is derhalve van het grootste belang dat bij zaken die aan het Kifid worden voorgelegd, zoals de onderhavige, steeds de voorvraag beantwoord wordt of daadwerkelijk sprake is van de verwerking van biometrische gegevens.

[56] EDPB van 28 maart 2023, EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations, blz. 3.
[57] *Idem*.

87. De aan te leggen toets voor de vraag of de verwerking rechtmatig is hangt namelijk af van de beantwoording van deze voorvraag. Indien géén biometrische gegevens worden verwerkt bij of aan de hand van de video-opname dan moet de verwerkingsverantwoordelijke een grondslag voor de verwerking van de persoonsgegevens hebben wil deze rechtmatig zijn. Is er echter wel sprake van een verwerking van biometrische gegevens dan is naast de vereiste grondslag ook een doorbreking van het verwerkingsverbod vereist wil de verwerking rechtmatig zijn.

88. Het verwerken van biometrische gegevens met het oog op de unieke identificatie is namelijk in beginsel verboden. De financiële dienstverlener kan dit verwerkingsverbod alleen in bepaalde uitzonderlijke gevallen doorbreken. Hiervoor moet de onlinebank, aantonen dat een succesvol beroep open staat op de doorbrekingsgrond van artikel 9 lid 2 sub g) jo artikel 29 UAVG. Deze uitzonderingsgrond vereist echter dat de onlinebank onderbouwd, op grond het specifieke geval, dat de vereiste authenticatie noodzakelijk is.

89. De vraag of de verwerking noodzakelijk is, mede in het licht van het beginsel van minimale gegevensverwerking, vereist allereerst dat de financiële dienstverlener aantoont dat de identificatie en/of verificatie van haar potentiële klant die een spaarrekening wil openen bij haar op geen enkele andere redelijke wijze plaats kan vinden die een minder verregaande impact heeft op de persoonlijke levenssfeer van de potentiële klant(en). Of daar sprake van is, kan niet op basis van het procesdossier worden vastgesteld.

90. Deze beoordeling brengt namelijk een complexe weging van veel verschillende factoren met zich mee. Zo dient onder meer in kaart te worden gebracht wat de risico's zijn die geassocieerd kunnen worden met het specifieke product en de (potentiële) klant. Dit heeft de onlinebank op grond van de verplichtingen uit hoofde van de Wwft al gedaan in de risicobeoordeling en staat als het goed is ook in de verplichte DPIA. Andere relevante factoren zijn weer gelieerd aan de aanbieder zelf, in dit kader het feit dat het gaat om een onlinebank zonder eigen vestigingen, wat bijvoorbeeld de mogelijkheid tot het fysieke komen identificeren bemoeilijkt zo niet onmogelijk maakt.

91. Belangrijk is ook dat de onlinebank is nagegaan dat de andere, in de wet vastgelegde of in de praktijk gangbare wijzen van identificeren en verifiëren die een minder verregaande impact op de persoonlijke levenssfeer hebben, geen redelijk alternatief vormen.

92. De vereiste proportionaliteit brengt voort met zich mee dat de onlinebank onder meer de omvang van de verwerking van biometrische gegevens beoordeeld, denk daarbij bijvoorbeeld aan de specificaties met betrekking tot de ingezette technologie en het aantal meetpunten dat wordt gebruikt.

93. Het is voor mij niet mogelijk op dit moment te beoordelen of de onlinebank zich kan beroepen op een doorbrekingsgrond gelet op de verschillende factoren. Dit is beginsel aan de onlinebank zelf. Die dit goed gedocumenteerd zal hebben.

94. Wanneer de onlinebank zich met succes kan beroepen op de doorbrekingsgrond dient zoals aangegeven, voor de beoordeling van de rechtmatigheid van de verwerking, ook nog afzonderlijk te worden beoordeeld of de onlinebank een grondslag heeft voor deze verwerking van biometrische gegevens.[58]

95. Naar mijn mening is het verdedigbaar dat de onlinebank zich in dat specifieke geval zou kunnen beroepen op de grondslag dat de verwerking noodzakelijk is ter vervulling van een taak van algemeen belang opgelegd aan de onlinebank. Aanleiding voor dat standpunt is te vinden in artikel 43 AMLD4. De onderbouwing dat het voor deze onlinebank noodzakelijk is

[58] De AVG schrijft niet voor dat eerst het verwerkingsverbod doorbroken zou moeten worden en daarna pas de grondslag moet worden aangegeven. Het mag ook andersom. Het zijn cumulatieve vereisten.

om ter vervulling van deze taak van algemeen belang ook biometrische gegevens te verwerken is dan al grotendeels gegeven in relatie tot het doorbreken van het verwerkingsverbod van artikel 9 lid 1 AVG, gelet op het feit dat deze doelen zo dicht bij elkaar liggen.

96. Concluderend kunnen we dus stellen dat de rechtmatigheid van de verwerking van biometrische gegevens met het oog op de unieke identificatie die wordt vereist van een potentiële klant de een online spaarrekening wil openen bij een onlinebank niet zonder meer kan worden vastgesteld. De AVG verbiedt in beginsel de verwerking van dit soort gegevens, maar biedt eveneens een mogelijkheid om dit verbod te doorbreken, een mogelijkheid die eventueel openstaat voor de onlinebank.

97. Of de onlinebank een succesvol beroep kan doen op deze doorbrekingsgrond hangt af van een nauwkeurige en gedetailleerde afweging van de risico's die de aanbieding van *dit* product door *deze* aanbieder met zich meebrengen, voor *deze soort klanten* en het al dan niet bestaan van *redelijke alternatieven* voor het identificeren en verifiëren van de identiteit van een potentiële klant.

98. Of de verwerking van biometrische gegevens voorts in overeenstemming is met de AVG hangt ook af van de wijze waarop de financiële dienstverlener voldoet aan de *overige* vereisten met betrekking tot de verwerking van persoonsgegevens, zoals transparantie met betrekking tot de verwerking en de informatiebeveiligingsmaatregelen die genomen zijn.

***