Verzoek aan De Nederlandsche Bank en de minister van Financiën inzake identificatie bij financiële instellingen

Identiteitsfraude achtervolgt een mens de rest van zijn leven en moet met alle mogelijke middelen voorkomen worden

aan	DNB en de Minister van Financiën
kopie	vaste commissies Financiën, Digitale Zaken en Justitie en Veiligheid van de Tweede Kamer; de Autoriteit Persoonsgegevens
datum	12 september 2024
onderwerp	Risico's verbonden aan verificatie van de identiteit op grond van de Wwft

Ons verzoek

Zoals hierna wordt toegelicht is sprake van grote risico's verbonden aan de verificatie van de identiteit van mensen door financiële instellingen. Daarom verzoeken wij De Nederlandsche Bank (DNB) en het ministerie van Financiën om zo spoedig mogelijk maatregelen te (laten) nemen om de risico's verbonden aan verificatie van de identiteit van burgers door financiële instellingen te mitigeren.

Wij sturen dit stuk ter informatie aan de commissies Financiën, Digitale Zaken en Justitie en Veiligheid van de Tweede Kamer, met het verzoek er aandacht aan te besteden. Wij zullen ook een aantal andere relevante partijen informeren.

Stichting Privacy First
Nieuwe Herengracht 49
1011 RN Amsterdam

https://privacyfirst.nl
info@privacyfirst.nl
+31 20 810 0279

KvK 34298157
ANBI erkend

Samenvatting

Vanwege de digitale ontwikkelingen, onder meer op het gebied van kunstmatige intelligentie, nemen de risico's rondom identiteitsfraude sterk toe. Privacy First heeft de afgelopen jaren geconstateerd dat met name bij financiële instellingen (FI's) riskante praktijken zijn ontstaan op het gebied van identificatie van hun cliënten die gevaar opleveren voor burgers. FI's beroepen zich bij hun identificatiepraktijken op de antiwitwaswet, de *Wet ter voorkoming van witwassen en financieren van terrorisme* (Wwft) en op andere financiële regelgeving.

In dit verzoek komen wij onder meer tot de volgende opmerkingen en aanbevelingen:

- De Wwft biedt geen grondslag voor het langdurig bewaren van kopieën van identiteitsbewijzen.
- Het maken van selfies en video-opnamen wordt evenmin door de Wwft voorgeschreven en ook een grondslag voor het bewaren ontbreekt. Het gebruik ervan is alleen toegestaan als sprake is van een adequate onderbouwing.
- Het langdurig bewaren van kopieën van identiteitsbewijzen, selfies en video-opnamen leidt tot verhoogde risico's op identiteitsmisbruik. Als er een aantoonbare noodzaak tot bewaren zou zijn, dient dat zo kort mogelijk te duren, ter voldoening aan het dataminimalisatiebeginsel van de AVG. De kopieën van identiteitsbewijzen en de beelden dienen alsdan zo spoedig mogelijk te worden verwijderd.
- Op grond van de Wwft en de AVG dienen de identificatiemaatregelen van Wwft-plichtige ondernemingen aantoonbaar proportioneel te zijn en niet verder te gaan dan nodig voor het beoogde doel. Dat betekent dat de risico's van identiteitsmisbruik zo goed mogelijk gemitigeerd moeten worden en FI's dit ook aan de burger kunnen aantonen.
- FI's vervullen een maatschappelijk essentiële functie en zijn digitale ondernemingen zonder fysieke kantoren geworden. Dat heeft riskante identificatiepraktijken in de hand gewerkt. Wij menen dat van de FI's mag worden verwacht dat zij laagdrempelige fysieke identificatiemogelijkheden bieden, zodat riskante digitale handelingen worden voorkomen.
- Het is nodig de aanpak bij verificatie van de identiteit op grond van de Wwft ingrijpend aan te passen, zodat wordt voorkomen dat andere Wwft-plichtige ondernemingen het slechte voorbeeld van de financiële sector volgen.

PRIVACY FIRST

Inhoud

1. Inleiding: rumoer rond identificatie door financiële instellingen

Sinds 2020 is er rumoer rondom het door financiële instellingen (FI's) identificeren van hun klanten, officieel wordt dit 'verificatie van de identiteit' genoemd. Met name creditcard-maatschappij International Card Services (ICS) is daarmee bekend geworden. Rond die tijd zijn een aantal FI's gestart met 'heridentificatie' van hun klanten, vermoedelijk in opdracht van DNB. DNB heeft niet openbaar gemaakt wat de instructie exact inhield en was tot nu toe niet bereid om vragen te beantwoorden.

Ongeruste klanten van FI's lazen de informatie over het kopiëren van identiteitsbewijzen op de site van de Autoriteit Persoonsgegevens en vroegen zich af waarom ze als bestaande klant geheridentificeerd zouden moeten worden en waarom ze kopieën van hun identiteitsbewijs zouden moeten (laten) maken en soms uploaden. De verificatie van de identiteit bij aanvang van de relatie leverde ook vragen op.

Mensen zijn bezorgd over identiteitsfraude en over andere risico's verbonden aan de verspreiding van kopieën van hun identiteitsbewijs. Ook aspecten van het identificeren door FI's riepen vragen op, zoals het inschakelen van het gespecialiseerde bedrijf (AMP), waarvan de medewerkers zichzelf niet kunnen/willen identificeren en die met een onduidelijk apparaat de echtheid van het identiteitsbewijs zeggen te controleren en er een kopie van maken.

De bezorgdheid van burgers leidde tot een groot aantal procedures bij de *Geschillencommissie Financiële Dienstverlening* van het Kifid (hierna: 'Kifid'), waarin het Kifid het standpunt van de FI's volgt.

Er is ook geprocedeerd over identificatie bij de onafhankelijke rechter, wat wisselende uitspraken heeft opgeleverd. Het oordeel van het *College van Beroep voor het bedrijfsleven* (CBb) van 29 mei 2018 is hier van groot belang, een oordeel waar het Kifid en sommige rechters in latere uitspraken geen acht op hebben geslagen.

Datalekken komen ook bij financiële instellingen voor, zo leren diverse affaires.[1] Overigens hoeven financiële instellingen datalekken niet aan klanten te melden, op grond van artikel

[1] Recente voorbeelden: bij bunq kunnen medewerkers allerlei persoonsgegevens inzien, zie het artikel in het NRC van 26 juni 2024, https://www.nrc.nl/nieuws/2024/06/26/bunq-werknemers-keken-stiekem-in-klantrekeningen-het-was-te-verleidelijk-a4857800.

ABN Amro kreeg te maken met een datalek vanwege een leverancier, https://www.abnamro.com/nl/nieuws/leverancier-abn-amro-geraakt-door-gijzelsoftware.

42 UAVG. Daardoor is onbekend in welke omvang datalekken bij financiële instellingen voorkomen en kunnen betrokkenen geen maatregelen nemen.

Standpunt Privacy First

Een zorgvuldige omgang met persoonsgegevens behoort tot de kernwaarden van Nederland en de EU en vloeit onder andere voort uit het Europese Handvest (de relevante artikelen staan aan het begin van het Handvest [2]) en diverse internationale verdragen. Zorgvuldige omgang met de identiteit en de gegevens waar die identiteit uit blijkt (identiteitsbewijs en beelden van de persoon) is dus van essentieel belang.

Privacy First is van mening dat de onzekerheid rondom identificatie door financiële instellingen ongewenst is en dat zowel acht moet worden geslagen op de voorschriften van de *Wet ter voorkoming van witwassen en financieren van terrorisme* (Wwft), op grond waarvan FI's hun cliënten moeten identificeren (in de terminologie van de Wwft: de identiteit moeten vastleggen en deze verifiëren), als op de *Algemene Verordening Gegevensbescherming* (AVG), die onder andere dataminimalisatie en passende veiligheidsmaatregelen voorschrijft.

Privacy First heeft in november 2023 meegedaan aan een consultatie van De Nederlandsche Bank (DNB) over de 'Consultatieversie DNB 'Q&As' en 'Good Practices' Wwft' [3] en heeft daarin de identificatieproblematiek bij DNB aangekaart. Helaas heeft DNB vrijwel niets gedaan met onze suggesties.

Daarom hebben wij besloten de problematiek door middel van dit verzoek aan te kaarten. In de huidige tijd groeien de risico's op identiteitsfraude exponentieel. Als er niet tijdig wordt ingegrepen is het leed niet te overzien. In de digitale wereld betekent eenmaal gelekt dat gegevens voor eeuwig gecompromitteerd zijn.

In oktober 2023 werd een groot datalek bij BNP Paribas Real Estate Netherlands bekend, zie het bericht in het FD, https://fd.nl/bedrijfsleven/1492402/groot-datalek-bij-nederlandse-vastgoedtak-bnp-paribas en security.nl https://www.security.nl/posting/814659/Datalek+bij+BNP+Paribas+Real+Estate+Netherlands.

[2] Zie artikelen 1 en 3 die waarborgen creëren ter bescherming van de menselijke waardigheid en integriteit. Artikelen 6, 7, 8 en verder doen dat ter bescherming van vrijheid, veiligheid, privéleven en persoonsgegevens.

[3] Meer informatie in de aankondiging van de consultatie door DNB: https://www.dnb.nl/nieuws-voor-de-sector/oud/toezicht-2023/dnb-legt-nieuwe-aanpak-witwassen-voor-aan-financiele-sector/, de consultatiereactie Privacy First: https://www.dnb.nl/media/gukbb4y0/consultatiereactie-privacy-first.pdf en het bericht van DNB over de uitkomsten van de consultatie: https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2024/resultaten-consultatie-qas-en-good-practices-wwft/.

2. Het belang: identiteitsfraude is een groeiend probleem

De identificatiepraktijken van FI's leveren grote zorgen op omdat identiteitsfraude een groeiend probleem is in de Nederlandse samenleving. Steeds vaker vindt identificatie op afstand plaats doordat steeds meer bedrijven geen fysieke kantoren meer hebben waar mensen zich in persoon met een origineel identiteitsbewijs kunnen identificeren. Uit de *Monitor Identiteit* van de Nederlandse overheid blijkt dat nu al op grote schaal identiteitsfraude wordt gepleegd door middel van een kopie van het identiteitsbewijs.[4]

Vanwege de technische ontwikkelingen, zoals *artificial intelligence* (kunstmatige intelligentie) zullen de risico's op identiteitsfraude steeds verder toenemen. Daarbij speelt een rol dat het gebruik van biometrische gegevens bij identificatie riskant is omdat wij allen deze kenmerken verspreiden door ons in het maatschappelijk verkeer te begeven (bijvoorbeeld vanwege het grootschalig opnemen van camerabeelden in winkels, benzinestations en elders), wat misbruik vergemakkelijkt.

Aan de verspreiding van biometrische gegevens is niet te ontkomen. Biometrische kenmerken kunnen als deze misbruikt worden niet worden vervangen. Omdat Privacy First ziet dat FI's in toenemende mate gebruik maken van biometrische gegevens en dat zij zich onvoldoende verdiepen in de risico's daarvan voor burgers, is er aanleiding de problematiek aan de orde te stellen, vóórdat er grote ongelukken gebeuren. Dit gaat iedere Nederlander aan!

Financiële instellingen hebben steeds minder fysieke kantoren en proberen de communicatie met de klant op digitale wijze af te wikkelen, omdat dit goedkoper zou zijn. Identiteitsfraude ligt dan op de loer.[5] Privacy First constateert dat er in de digitale communicatie tussen financiële instellingen en hun klanten het nodige mis gaat. Voorbeeld daarvan is onder meer de grootbank die aan klanten vraagt om identiteitsgegevens en

---

[4] Volgens de *Monitor Identiteit 2023*, aankondiging, monitor, tabel 57, in 2023 werd in 55% van de gevallen identiteitsfraude gepleegd met een kopie van het identiteitsbewijs.

In de monitor wordt gemeld dat identiteitsfraude bij uitstek een delict is dat plaatsvindt met accounts in het digitale domein. Uit onderzoek blijkt dat een groot deel van de identiteitsfraude plaatsvindt met als doel toegang te krijgen tot de bankrekening (tabellen 43 en 44). Uit tabel 56 blijkt dat het aantal meldingen bij het *Centraal Meldpunt Identiteitsfraude* (CMI) groeit, in 2023 waren er 7.115 meldingen, terwijl er in 2010 maar 152 meldingen waren.

[5] In algemene zin over identiteitsfraude in de financiële sector het proefschrift van N. S. van der Meulen, *Fertile grounds: The facilitation of financial identity theft in the United States and the Netherlands* (2010), te downloaden via https://research.tilburguniversity.edu/en/publications/fertile-grounds-the-facilitation-of-financial-identity-theft-in-t.

andere vertrouwelijke gegeven per e-mail op te sturen, terwijl die bank er mee bekend is dat e-mail een onveilig communicatiemiddel is.

Het is daarom van groot belang dat inzake het onderwerp identificatie (verificatie van de identiteit) juridische duidelijkheid komt over de vraag hoe FI's moeten handelen. Daarbij kunnen niet alleen de wensen van de witwasbestrijdingstoezichthouder, zoals bij FI's De Nederlandsche Bank (DNB), leidend zijn, aangezien DNB behoeften kan hebben die strijdig zijn met de gegevensbeschermingsbelangen van burgers en gebruikers van bankrekeningen en creditkaarten.

Hierna zal allereerst de identificatieplicht op grond van de Wwft worden besproken.

3. De regels: identificatie op grond van de Wwft ('verificatie van de identiteit')

Al lange tijd is een hoofdregel van de witwasbestrijdingsregelgeving dat een cliënt zich bij de financiële instellingen dient te identificeren. Overigens is dat iets wat ook privaatrechtelijk nodig is, aangezien de FI anders niet weet wie de wederpartij is.

De juridische context van identificatie op grond van de Wwft is in **bijlage 1** beschreven.

De Wwft biedt voor ondernemingen die zich aan die wet moeten houden (Wwft-plichtigen) een grondslag als bedoeld in artikel 6 lid 1 sub c) AVG om bepaalde persoonsgegevens te verwerken. Dat betekent echter niet dat er een ongelimiteerde vrijheid is voor de Wwft-plichtige of voor de Wwft-toezichthouders.

Zowel voor de FI, als voor de wetgever, als voor de Wwft-toezichthouders (zoals DNB en AFM) geldt dat zij bij de interpretatie van de Wwft rekening dienen te houden met de eisen die de AVG en internationale afspraken stellen aan de verwerking van persoonsgegevens. Hierna wordt gefocust op de AVG, waarvan de relevante bepalingen in **bijlage 2** zijn vermeld.

De bepalingen in de Wwft inzake identificatie dienen aan de norm van artikel 6 lid 3 AVG te voldoen. Dat artikel schrijft onder andere voor dat het Unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en evenredig dient te zijn met het nagestreefde gerechtvaardigde doel. Daarnaast blijven de beginselen van artikel 5 AVG relevant, onder meer het principe van dataminimalisatie van artikel 5 lid 1 sub c) AVG en dient rekening te worden gehouden met het verbod op verwerking van biometrische gegevens.

4. Identificatieproblematiek

Bij de verificatie van de identiteit op grond van de Wwft spelen de volgende problemen:

- de gang van zaken bij het maken van kopieën van het identiteitsbewijs ('kopie-ID');
- de wijze waarop de identiteit wordt geverifieerd;
- het maken of laten maken van bestanden met biometrische kenmerken, zoals selfies en video's;
- de wijze van bewaren van kopie-ID's en bestanden met biometrische kenmerken;
- de bewaartermijn;
- de onafhankelijke controle op naleving van de AVG door FI's.

Kopie-ID

Opvallend aan de identificatieproblematiek is dat veel FI's lijken te veronderstellen dat het maken van een kopie van het identiteitsbewijs verplicht is, terwijl de Wwft daartoe niet verplicht (en evenmin tot het langdurig bewaren daarvan). Voor een toelichting op artikel 33 Wwft verwijzen we naar bijlage 1.

Dat een dergelijke verplichting er niet is wordt bevestigd door twee juristen die verantwoordelijk waren voor het wetsvoorstel tot samenvoeging van de *Wet identificatie bij dienstverlening* (WID) en de *Wet melding ongebruikelijke transacties* (Wet MOT) tot de Wwft [6], Eric Ligthart en Martine Suijkerbuijk. Zij schreven in hun artikel over de Wwft [7] dat de nieuwe identificatieregels een verlichting voor de banken opleveren. Op de tweede pagina van het artikel wordt als een van de nieuwe elementen van de Wwft genoemd: "*afschaffen kopietje paspoort*".

Op de vierde pagina wordt dit nader toegelicht en schrijven de twee auteurs:

> *Op grond van de WWFT geldt dat de gegevens aan de hand waarvan de identificatie en verificatie heeft plaatsgevonden, moeten worden vastgelegd. [27] Het bewaren van een afschrift van het document is geen vereiste. Ook op grond van de WID was het overigens niet verplicht om een afschrift van het desbetreffende document te bewaren. (...)*
> *Met het afschaffen van het zogenoemde 'kopietje paspoort' is een bron van ergernis bij financiële ondernemingen weggenomen.*

[6] In werking getreden op 1 augustus 2008.

[7] E.Y.C. Ligthart en M.E.M. Suijkerbuijk, *De nieuwe antiwitwaswet: oude wijn in nieuwe zakken?* Tijdschrift voor Compliance 2008, nr. 5, pagina 199-203.

[27] *Zie art. 33 WWFT.*

In dat licht moet de problematiek rondom identificatie door FI's worden beoordeeld.

Het is daarom onbegrijpelijk dat FI's zich op het standpunt stellen dat zij hun cliënten kunnen verplichten om een kopie of scan van hun identiteitsbewijs te (laten) maken. Het is ons niet bekend op welke juridische basis dit is gestoeld. Een en ander is in strijd met het dataminimalisatiebeginsel van de AVG en is ongewenst omdat daarmee het risico op identiteitsfraude wordt verhoogd.

Hierna zal ook rechtspraak worden besproken waarin voornoemd uitgangspunt wordt bevestigd.

De wijze waarop de identiteit wordt geverifieerd

Privacy First constateert dat - los van het hiervoor opgemerkte over het kopie-identiteitsbewijs - ook op de wijze van identificatie (verificatie van de identiteit) het nodige is aan te merken. De klassieke manier van identificatie - het je bij een fysiek kantoor van de FI vervoegen en je originele identiteitsbewijs tonen - komt nog weinig voor omdat FI's op grote schaal hun fysieke kantoren hebben gesloten en digitale dienstverleners zijn geworden.

Er waren de afgelopen jaren FI's die aan hun klant vroegen om zelf een kopie van het identiteitsbewijs te maken en per post of zelfs per e-mail op te sturen. Dit is natuurlijk onacceptabel vanwege de mogelijkheid tot het plegen van identiteitsfraude, immers de FI is dan niet zeker of de kopie wel door de klant is opgestuurd en de kopie kan onderweg worden onderschept en worden misbruikt.

Een aantal FI's laten tegenwoordig hun klant met de eigen app op de smartphone een kopie van het identiteitsbewijs maken of het identiteitsbewijs uitlezen (met de NFC-chip) en soms vragen ze dan ook om met diezelfde app een foto of zelfs een video van zichzelf te maken. Bij deze aanpak is allereerst essentieel of de app van de FI wel digitaal veilig is. Vervolgens is de vraag of de FI de gegevensbeschermingsrisico's beheerst, wat de klant niet kan controleren.

Een andere aanpak is dat de FI het gespecialiseerde bedrijf AMP langs stuurt. Een medewerker (die zich niet wil identificeren, zo is ons bekend) scant dan het identiteitsbewijs met een apparaat waarvan de klant niet kan vaststellen wat de eigenschappen zijn. Hoewel het gebruik van een apparaat logisch lijkt, immers daarmee kunnen de kenmerken waaraan een origineel identiteitsbewijs kunnen herkend worden afgelezen, is het voor de klant niet te verifiëren wat het apparaat doet en hoe de gegevens met de FI worden gedeeld.

Een variant daarop is dat de identiteit wordt geverifieerd door een notaris, die gebruik maakt van een gelijksoortig apparaat als AMP. Het voordeel van een notaris is dat deze het verifiëren van de identiteit als professie heeft en onder toezicht staat, al is het Privacy First niet bekend of de technische omgeving waarvan notarissen gebruik maken onafhankelijk geaudit wordt.

Punt van aandacht is verder dat veel FI's niet toestaan dat de foto en het BSN door betrokkenen worden afgedekt, terwijl de Wwft geen wettelijke grondslag voor de verwerking van die persoonsgegevens bevat (zie ook bijlagen 1 en 2).

Standpunt Privacy First

Het is belangrijk dat er een vaste veilige structuur gaat ontstaan in de verificatiepraktijken van FI's en dat de AVG correct wordt nageleefd. Naar de mening van Privacy First betekent dat voor de wijze van verificatie van de identiteit onder meer:

- Geen kopieën van identiteitsbewijzen per post of e-mail.
- Het identiteitsbewijs wordt bij de aanvang van de relatie geverifieerd en alleen dan wordt door FI's die het BSN mogen verwerken het BSN vastgesteld. Herhaling van de verificatie vindt alleen plaats als daartoe aantoonbaar redelijkerwijs aanleiding is. De veronderstelling van sommige FI's dat er om de zoveel jaar op grond van de Wwft verificatie van de identiteit moet plaatsvinden, is onjuist.[8]
- Verificatie vindt plaats op een fysiek kantoor van een FI, dan wel met een apparaat/app die een gegevensbeschermingsaudit heeft ondergaan, in beide gevallen zonder een kopie te maken.
- Indien de verificatie met technische middelen (bijvoorbeeld een apparaat of een app op een smartphone) plaats vindt, wordt de persoon in de gelegenheid gesteld te verifiëren of dat middel aan alle gegevensbeschermingseisen voldoet.
- Mensen die daar prijs op stellen krijgen altijd de mogelijkheid om op een fysiek kantoor van een FI of notaris in persoon de verificatie van de identiteit uit te voeren.
- Vergelijking van het identiteitsbewijs met een foto of video vindt alleen plaats als er geen andere extra maatregelen kunnen worden genomen.
- Als er secundaire financiële producten worden afgenomen (zoals een spaarrekening) moet er een systeem komen dat de spaarbank gebruik mag maken van de identiteitsverificatie van de FI in Nederland bij wie de klant een gewone betaalrekening heeft. (Dus een aparte regeling die los staat van het huidige systeem in de Wwft van uitbesteding.)

[8] Dit volgt ook uit het risicogebaseerdheidsbeginsel van artikel 3 Wwft.

- Als de verificatie door middel van een bedrijf plaats vindt, dient de medewerker zich te kunnen identificeren en dient de klant zekerheid te kunnen verkrijgen over het gebruikte apparaat en over de wijze van gegevensuitwisseling met de FI.

Gebruikmaking van biometrische kenmerken, zoals selfies en video's

In toenemende mate maken FI's bij identificatie gebruik van biometrische kenmerken.

Dat thema kwam recent aan de orde in een uitspraak van de Geschillencommissie van het *Klachteninstituut Financiële Dienstverlening* (Kifid) in een zaak tegen de LeasePlan Bank. Deze bank eiste een verificatiefilmpje van de aanvragers van een spaarrekening. De uitspraak zal hierna worden besproken.

Het gebruik van biometrische kenmerken bij verificatie van de identiteit is zeer riskant omdat deze kenmerken kunnen worden gekopieerd en nagemaakt, bijvoorbeeld door middel van deepfakes. Biometrische gegevens van mensen worden op allerlei manieren digitaal geoogst en verspreid, wat identiteitsfraude makkelijk maakt.

De Autoriteit Persoonsgegevens meldt op de website [9] dat de risico's bij gezichtsherkenning groot zijn:

> *Het is erg belangrijk dat organisaties zulke gegevens goed beschermen. Dat staat ook in de wet. Doen zij dat niet, dan kan dat grote gevolgen hebben voor mensen. Een wachtwoord kunt u veranderen als dit is gelekt, maar uw gezicht niet. Daarom kunnen de gevolgen bij het lekken van bijzondere persoonsgegevens groter zijn. Een korrelige foto is genoeg om uw gezicht overal te kunnen herkennen en van alles over u te weten te komen: uw adres, salaris, zoekgeschiedenis en nog veel meer. U zou zo op grote schaal kunnen worden 'gevolgd'.*
> *Omdat de risico's zo groot zijn, mogen organisaties alleen in zeldzame situaties gezichtsherkenning gebruiken.*

en niet voor niets heeft de AP recent een boete uitgedeeld aan het Amerikaanse bedrijf Clearview AI.[10]

[9] https://autoriteitpersoonsgegevens.nl/themas/identificatie/biometrie/krijgt-u-te-maken-met-gezichtsherkenning-dit-moet-u-weten

[10] Zie https://autoriteitpersoonsgegevens.nl/actueel/ap-legt-clearview-boete-op-voor-illegale-dataverzameling-voor-gezichtsherkenning.

Die risico's zijn al lang bekend, zo schreef de Privacy Company in 2016 over de vier belangrijke gevaren van biometrische authenticatie.[11]

Het *Maatschappelijk Overleg Betalingsverkeer* (MOB) publiceerde in mei 2017 een rapport over biometrie in het betalingsverkeer [12], waarin wordt aangegeven dat aan het gebruik van biometrie de nodige risico's zijn verbonden. Bezwaar is onder meer dat:

- de techniek een 'black box' is, bedrijfsgeheim van leveranciers als Apple en Samsung;
- de techniek niet onafhankelijk gecontroleerd en gecertificeerd is;
- de kwaliteit van de biometrische authenticatie wisselend is (soms gewoon slecht!), zo is gezichtsherkenning zeer wisselend in betrouwbaarheid;
- vervanging van een uitgelekte pincode of wachtwoord mogelijk is, wat niet geldt voor een biometrisch authenticatiemiddel zoals de vingerafdruk of het gezicht;
- verwarring kan ontstaan als meerdere authenticatiemethoden gebruikt worden voor gelijksoortige toepassingen;
- biometrische gegevens eenvoudig door kwaadwillenden geoogst kunnen worden voor malafide gebruik, want biometrische gegevens zijn niet geheim.

De rapporteurs concluderen dat biometrie weliswaar gebruikersgemak kan opleveren maar dat de mate van veiligheid sterk afhankelijk is van de kwaliteit van de implementatie, waarbij riskant is dat er geen onafhankelijke certificatie beschikbaar is.

In 2020 publiceerde de European Data Protection Supervisor (EDPS) op de site een document over de misverstanden rondom biometrische identificatie en authenticatie.[13] Daarin wordt gewezen op de beperkingen en de risico's. Onder meer wordt gemeld:

> *If no measures are taken to reduce the risk of unauthorised use of biometric data, their use would be equivalent to writing our access codes on our forehead*

en:

> *It could have the same effect as using the same password on many different systems, so the scale in biometric deployment is a problem in itself. Moreover, unlike password-based systems, once biometric information has been compromised it cannot be modified or cancelled.*

---

[11] https://www.privacycompany.eu/nl/blog/vier-belangrijke-gevaren-van-biometrische-authenticatie

[12] https://www.dnb.nl/media/h2dpz3ia/biometrie-in-betalingsverkeer-mob-eindrapport.pdf

[13] https://www.edps.europa.eu/sites/edp/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_auuthentication_en.pdf

Standpunt Privacy First

Privacy First is van mening dat biometrische identificatie/identiteitsverificatie alleen mag worden gebruikt als er geen alternatief is, er een adequate wettelijke basis is en er afdoende waarborgen zijn.

De wijze van bewaren van kopie-ID's en bestanden met biometrische kenmerken

Als er al biometrische gegevens en kopie-ID's zouden mogen worden verwerkt, is het essentieel dat aan zeer hoge verifieerbare veiligheidsstandaarden wordt voldaan, zowel technisch als organisatorisch. Hoewel FI's van huis uit veel moeten doen aan beveiliging, is er op dit moment onvoldoende bewustzijn van de risico's die burgers lopen.

Dat blijkt onder meer uit de boete die ICS van de Autoriteit Persoonsgegevens kreeg vanwege het niet naleven van veiligheidsvoorschriften, zie het bericht van 15 januari 2024, *Boete voor creditcardbedrijf ICS na ontbrekende risicoanalyse*.[14] Recent kwam in het nieuws dat uit een door de Europese Centrale Bank (ECB) uitgevoerde stresstest is gekomen dat er bij banken nog veel moet worden verbeterd.[15]

Nu financiële instellingen een essentiële rol in het maatschappelijk verkeer spelen, is het essentieel dat alle financiële instellingen aan hoge eisen voldoen op het gebied van gegevensbescherming.

Problematisch is dat het voor klanten van FI's niet is te controleren of de betreffende FI de veiligheidsmaatregelen op orde heeft. Voorts reageren sommige FI's negatief tegen hun klant als er vragen worden gesteld over de wettelijke basis voor het opvragen van kopieën van identiteitsbewijzen en beelden en over de beveiliging, terwijl die vragen van klanten legitiem zijn en op grote schaal leven (zoals onder meer uit de vele Kifid zaken blijkt die hierna worden besproken).

[14] https://autoriteitpersoonsgegevens.nl/actueel/boete-voor-creditcardbedrijf-ics-na-ontbrekende-risicoanalyse

[15] Artikel door een lid van de raad van toezicht van ECB: Enhancing banks 'resilience against cyber threats – a key priority for the ECB, https://www.bankingsupervision.europa.eu/press/blog/2024/html/ssm.blog240726~7bfb4e2267.en.html.

Standpunt Privacy First

Vooralsnog gaat Privacy First er van uit dat er geen noodzaak is om een kopie-ID en biometrische gegevens (zoals een foto) in de administratie op te nemen, terwijl er ook geen wettelijke verplichting daartoe bestaat.

Als het aantoonbaar noodzakelijk zou zijn dat FI's kopieën van ID's en biometrische gegevens zouden moeten verwerken, is daar een wettelijke basis voor nodig, alsmede strenge extra maatregelen, onder meer beperking in de bewaartermijn (zie hierna) en onafhankelijke privacy-audits.

De bewaartermijn

Een belangrijk punt van aandacht is de bewaartermijn. De Wwft bevat slechts voorschriften over bepaalde gegevens over de identiteit die geregistreerd moeten worden gedurende de periode dat iemand klant is van een FI en gedurende vijf jaar na afloop daarvan.[16]

De Wwft zegt niets over het langdurig bewaren van kopie-ID's, wat wordt veroorzaakt door het feit dat de Wwft geen verplichting kent om een kopie-identiteitsbewijs (of beelden van betrokkene) op te nemen in de administratie.

De relaties met FI's kunnen zeer langdurig zijn, wat tot gevolg kan hebben - als FI's denken dat ze om de paar jaar de identiteit moeten verifiëren - dat er een zeer riskante verzameling van persoonsgegevens ontstaat, terwijl er geen wettelijke grondslag is om kopieën en beelden te (laten) maken en evenmin om ze langdurig te bewaren.

Uit een hierna te bespreken Kifid-uitspraak blijkt dat de FI zich beroept op een niet openbaar gemaakt standpunt van DNB, dat de kopieën van identiteitsbewijzen nodig zouden zijn voor de controle door DNB. Voor dat standpunt is geen wettelijke grondslag. Het is niet de bevoegdheid van DNB om extra regels te creëren. Het behoort voldoende te zijn dat DNB de processen bij de FI's controleert.

Standpunt Privacy First

Privacy First is van mening dat de controle door een FI van het identiteitsbewijs zich dient te beperken tot het inzien van een origineel identiteitsbewijs, waarna uitsluitend de wettelijk

[16] Artikel 33 lid 3 Wwft. Zie nader in bijlage 1.

vereiste gegevens worden geregistreerd (dus geen opslag van kopieën van identiteitsbewijzen).

Het standpunt van DNB over verificatie van de identiteit zoals via een Kifid-uitspraak bekend is geworden, is niet openbaar en ook niet getoetst aan de AVG. Gezien de grote gegevensbeschermingsrisico's verbonden aan verificatie van de identiteit is ongewenst dat DNB buiten de wetgever om beleid heeft (= regels maakt) die het risico van identiteitsfraude verhogen. Privacy First nodigt DNB uit haar beleid inzake verificatie van de identiteit openbaar te maken, de noodzaak daarvan te onderbouwen en aan te geven welke maatregelen worden voorgeschreven om het risico op identiteitsfraude te mitigeren.

Samenvattend: als er een controle-noodzaak zou zijn, meent Privacy First dat de minister van Financiën dan wel DNB die noodzaak dient toe te lichten en aan te geven op welk manier de risico's op identiteitsfraude kunnen worden beperkt.

Onafhankelijke controle op naleving van de AVG door FI's

FI's beschikken vanwege hun rol in het betalingsverkeer over zeer veel financiële persoonsgegevens. Vanwege de toenemende digitalisering nemen de risico's voor burgers in hoog tempo toe. In welke mate FI's de gegevensbeschermingsrisico's voldoende onder controle hebben, is voor de klanten niet na te gaan. Er ontbreekt een structurele onafhankelijke toetsing van de naleving van gegevensbeschermingsvoorschriften. Die is niet alleen nodig vanwege eventuele kopieën van identiteitsbewijzen en biometrische gegevens, maar ook vanwege alle andere financiële persoonsgegevens die FI's verwerken.

De huidige controles zijn ad hoc, niet systematisch en onvoldoende gericht op gegevensbescherming. Immers, de Autoriteit Persoonsgegevens reageert alleen op incidenten en de checks van DNB en ECB zijn onvoldoende gericht op de gegevensbeschermingsbelangen van klanten.[17] De burger staat er alleen voor in het debat met de FI, die uit angst voor de hoge Wwft-boetes de neiging heeft om de gegevensbeschermingsbelangen van die burger te verwaarlozen. Daarbij speelt dat FI's soms buitengewoon negatief reageren (op het intimiderende af) als klanten vragen stellen over gegevensbescherming, terwijl de zorgen van klanten over identiteitsfraude legitiem zijn.

Vanwege de toenemende gegevensbeschermingsrisico's is het essentieel dat er streng toezicht wordt gehouden op de door FI's genomen gegevensbeschermingsmaatregelen.

[17] DNB heeft een sterkte focus op bestrijding van financieel-economische criminaliteit en speelt een rol op het gebied van financiële stabiliteit. Ook de AFM houdt toezicht op grond van de Wwft en heeft diverse andere taken. Privacy First heeft het beeld dat gegevensbescherming in het kader van de Wwft zeer weinig aandacht krijgt van deze financiële toezichthouders.

Daarvan deel dient uit te maken dat er periodiek onafhankelijke integrale AVG-audits van de systemen van FI's zullen plaatsvinden, zowel technisch als organisatorisch.

Standpunt Privacy First

Het is hoog tijd dat krachtig toezicht op de gegevensbeschermingsmaatregelen en structurele gegevensbeschermingstoetsing van de systemen van FI's gaat plaatsvinden. De uitkomsten daarvan dienen ook bekend te worden gemaakt, zodat klanten de maatregelen die de verschillende FI's nemen kunnen vergelijken en zelf de afweging kunnen maken of zij bepaalde risico's accepteren.

5. Tegenstrijdige beslissingen rechtspraak en Kifid

Privacy First constateert dat er tegenstrijdige beslissingen zijn gegeven door geschilbeslechtende instanties. Deze worden hierna besproken.

Geen kopie identiteitsbewijs nodig

College van Beroep voor het bedrijfsleven 29 mei 2018

De bestuursrechter heeft in diverse zaken beslist dat registratie van de op grond van artikel 33 Wwft genoemde gegevens voldoende is en dat de wet niet eist dat kopieën van identiteitsbewijzen worden bewaard. Dat is in lijn met wat Ligthart en Suijkerbuijk schreven over artikel 33 Wwft.

De hoogste rechter in economisch bestuursrecht zaken, het College van Beroep voor het bedrijfsleven (Cbb) oordeelde in de uitspraak van 29 mei 2018, ECLI:NL:CBB:2018:233 [18], dat de Wwft niet verplicht tot het kopiëren van een identiteitsbewijs. Het Cbb overweegt (4.6):

> *Nu uit het onderzoek dat door BFT is verricht volgt dat appellant in de door BFT onderzochte dossiers geen kopie van het identiteitsbewijs heeft bewaard en de verificatiegegevens ten aanzien van de identiteit van de (uiteindelijk belanghebbende van de) cliënten ook niet op andere wijze heeft vastgelegd, is niet gebleken dat appellant deze personen heeft geïdentificeerd en hun identiteit heeft geverifieerd zoals vereist op grond van de Wwft.*

Hieruit volgt dat een Wwft-plichtige de keuze heeft tussen het maken van een kopie of het vastleggen van de op grond van de Wwft vereiste gegevens. Deze uitspraak, gewezen onder een oudere versie van de Wwft en de voorganger van de AVG, is nog steeds relevant.

Rechtbank Noord-Holland 27 oktober 2021

De Rechtbank Noord-Holland oordeelde in de uitspraak van 27 oktober 2021, ECLI:NL:RBNHO:2021:9542 dat kan worden volstaan met het vastleggen van bepaalde gegevens:

[18] In gelijke zin andere uitspraken, onder meer rechtbank Rotterdam 23 juni 2016, ECLI:NL:RBROT:2016:4630 en 29 juni 2017, ECLI:NL:RBROT:2017:4911.

4.12.1. [eiser] heeft zich echter verzet tegen de toezending van een kopie van zijn paspoort, zoals door Srlev verlangd. Hij heeft gelijk dat die verplichting niet volgt uit de Wwft. Het is wel een van de mogelijkheden die wordt genoemd, art. 33 lid 2, sub a, onder 1o, maar onder 2o wordt vermeld dat dat ook kan door vastlegging van "de aard, het nummer en de datum en plaats van uitgifte van het document met behulp waarvan de identiteit is geverifieerd".

Rechtbank Rotterdam 20 april 2023

In de uitspraak van de Rotterdamse rechtbank van 20 april 2023, ECLI:NL:RBROT:2023:3301, wordt overwogen dat de Wwft niet verplicht tot het maken van een kopie van het identiteitsbewijs:

3.5. (...) Zoals [eiseres] terecht heeft opgemerkt, bestaat geen wettelijke verplichting om bij een cliëntenonderzoek een kopie van het identiteitsbewijs van de klant te maken. Wel is een instelling die een persoon heeft geïdentificeerd en zijn identiteit heeft geverifieerd op grond van artikel 33 van de Wwft verplicht dit op opvraagbare wijze vast te leggen (om op een efficiënte wijze te voldoen aan de verplichting tot het vastleggen van gegevens wordt in dit artikel de mogelijkheid geboden een afschrift vast te leggen van het document aan de hand waarvan de identificatie heeft plaatsgevonden; TK, 2007-2008, 31 238, nr. 3, blz. 35).
Dit betekent dat pas als uit onderzoek is gebleken dat de instelling geen kopie van het identiteitsbewijs heeft bewaard en de verificatiegegevens ten aanzien van de identiteit van de klant ook niet op andere wijze heeft vastgelegd, grond bestaat voor de conclusie dat de instelling deze klant niet heeft geïdentificeerd en diens identiteit niet heeft geverifieerd en dus heeft nagelaten een (toereikend) cliëntenonderzoek te verrichten (vergelijk de uitspraken van het College van Beroep voor het bedrijfsleven (CBb) van 29 juni 2017, ECLI:NL:CBB:2017:235, en 29 mei 2018, ECLI:NL:CBB:2018:233).

Wel kopie-identiteitsbewijs nodig

Rechtbank Gelderland 1 november 2022 (Mollie)

In de uitspraak van Rechtbank Gelderland van 1 november 2022, ECLI:NL:RBGEL:2022:6145 (Mollie), komt verificatie zijdelings aan bod. In overweging 5.5 wordt door de rechtbank ten onrechte overwogen dat een betaaldienstverlener een nieuwe kopie van het identiteitsbewijs zou moeten opvragen als het eerder door de UBO getoonde kopie is verlopen. De rechtbank was er kennelijk niet van op de hoogte dat de Wwft geen voorschrift bevat dat een Wwft-plichtige een kopie-identiteitsbewijs moet opslaan; ook is er geen bepaling dat er permanent een kopie van een geldig identiteitsbewijs in het dossier moet zitten.[19]

Rechtbank Amsterdam 11 januari 2023 (ICS)

In de uitspraak van 11 januari 2023, ECLI:NL:RBAMS:2023:145 beslist de Rechtbank Amsterdam in een geschil tussen ICS en haar klant dat ICS de klant kan verplichten mee te werken aan de door ICS gekozen vorm van digitale verificatie van de identiteit, waarna een kopie van het identiteitsbewijs in de systemen van ICS wordt opgeslagen.
De rechtbank overweegt onder andere (4.4):

> *Op welke wijze deze documenten moeten worden geverifieerd, is niet neergelegd in de Wwft, maar is, zoals door partijen ook onderkend, aan de instellingen zelf overgelaten. Dat een identificatie op afstand of langs elektronische weg kan plaatsvinden, vindt zijn grondslag in artikel 13 van de gewijzigde vierde Europese anti-witwasrichtlijn (Richtlijn (EU) 2018/843) en artikel 4 lid 1 sub h van de Uitvoeringsregeling.*

en in overweging 4.5:

[19] De rechtbank overwoog ten onrechte: "*Ook daarna is de betaaldienstverlener op grond van de Wwft verplicht om ervoor te zorgen dat zij over voldoende gegevens van de UBO beschikt en bijvoorbeeld een nieuwe kopie van een identiteitsbewijs opvraagt indien een dergelijk bewijs is verlopen.*"

De actualiseringsplicht inzake de UBO houdt met name in dat wordt nagegaan of betrokkene nog steeds die hoedanigheid heeft, bijvoorbeeld door aandeelhouderschap. De identiteit verandert niet, dus de actualiseringsplicht in de Wwft heeft daar geen betrekking op.

Hieruit volgt dat het instellingen vrij staat om innovatieve oplossingen te bedenken voor de verificatie van de identiteit van cliënten.

ICS bood aan de klant de mogelijkheid om bij een notaris te identificeren of via de gespecialiseerde dienstverlener AMP. Beiden maken gebruik van een scanner om de echtheid van het identiteitsbewijs te verifiëren. Het door de klant geboden alternatief dat hij een door hemzelf gewaarmerkte kopie verschaft, hoeft ICS volgens de rechtbank niet te accepteren. De rechtbank verwerpt het argument dat ICS geen kopie van het identiteitsbewijs zou mogen bewaren en overwoog:

> *4.10 Ten aanzien van de bewaarplicht geldt het volgende. Artikel 33 Wwft bepaalt dat een instelling gegevens met betrekking tot het cliëntenonderzoek op opvraagbare wijze moet vastleggen en bewaren. Lid 1 onder a schrijft onder meer voor dat het dient te gaan om een afschrift van het document dat een persoon identificerend nummer bevat en aan de hand waarvan de verificatie van de identiteit heeft plaatsgevonden. Met een beroep op dit artikel en artikel 3 Wwft voert ICS terecht aan dat het identiteitsbewijs op echtheid moet worden gecontroleerd en van dit gecontroleerde, op echtheid gecontroleerde identiteitsbewijs een afschrift moet worden opgeslagen. Dit is van belang voor ICS zodat zij kan bewijzen dat zij de Wwft heeft nageleefd. Om deze reden kan niet van ICS worden verlangd dat zij een door [eiser 2] gewaarmerkte of beschreven kopie van het identiteitsbewijs accepteert. Zoals eerder overwogen en door ICS tijdens de zitting uitvoerig is toegelicht, kan van een beschreven kopie van het identiteitsbewijs de echtheid niet worden vastgesteld, omdat de echtheidskenmerken daardoor (gedeeltelijk) onleesbaar zijn geworden. De stelling van SCK en [eiser 2] dat deze vorm van bewaarplicht in strijd is met de AVG omdat een wettelijke grondslag ontbreekt, gaat derhalve niet op. Artikel 6 AVG eist een wettelijke basis voor verwerking van persoonsgegevens en die is gegeven in de artikelen 3 en 33 Wwft.*

De overweging van de rechtbank dat een kopie van het identiteitsbewijs zou moeten worden opgeslagen om bewijs te leveren (waarschijnlijk aan DNB) is in tegenspraak met de hiervoor genoemde rechtspraak en met het genoemde artikel van Ligthart en Suijkerbuijk, en volgt ook niet uit de Wwft.

Uit de uitspraak blijkt dat ICS overleg heeft gevoerd met de Autoriteit Persoonsgegevens (AP) en dat deze "*op de online identificatiemethode niets aan te merken had. AP is derhalve op de hoogte van deze methode van ICS en heeft gebruikmaking daarvan kennelijk niet verboden*". Privacy First is teleurgesteld dat de AP zich kennelijk onvoldoende in het wettelijk kader heeft verdiept.

Diverse belangrijke aspecten van het onderwerp komen in deze uitspraak niet of onvoldoende aan de orde:

- ICS eist van de klant dat hij een selfie maakt, waar de Wwft niets over voorschrijft en dat in de uitspraak niet verder aan de orde komt, de vraag is waarom de selfie nodig zou zijn en als er een goede reden voor zou zijn, hoe lang de selfie bewaard mag worden;
- de lange duur van bewaren van het kopie-identiteitsbewijs is in deze uitspraak niet aan de orde geweest, terwijl uit de uitspraak blijkt dat ICS de persoonsgegevens zelfs langer bewaart dan de bewaartermijn van de Wwft toe staat [20].

In hoger beroep heeft het Gerechtshof Amsterdam bij uitspraak van 30 april 2024, ECLI:NL:GHAMS:2024:1165 het bestreden vonnis bekrachtigd. Privacy First vindt dat zeer teleurstellend omdat het Hof geen blijk er van geeft op de hoogte te zijn van de keuzemogelijkheid die artikel 33 Wwft biedt. Er staat immers 'of'. Als er 'of' staat, betekent het dat er geen verplichting bestaat om een kopie van het ID-bewijs vast te leggen.

Privacy First is het niet eens met deze uitspraken, om meerdere redenen.

Uitspraken Klachteninstituut Financiële Dienstverlening (Kifid)

De problematiek van identificatie door financiële instellingen is aan de orde geweest in diverse uitspraken van de *Geschillencommissie Financiële Dienstverlening* van het Kifid en ook in een uitspraak van de *Commissie van Beroep Financiële Dienstverlening* van het Kifid. Ook op deze uitspraken heeft Privacy First grote kritiek.

Hierna volgt informatie inzake enige van deze uitspraken.

Commissie van Beroep Financiële Dienstverlening 8 februari 2023, zaak 2023-0004 ABN Amro. Hoger beroep van Geschillencommissie 10 januari 2022, zaak 2022-0013.

Samenvatting van Kifid:

> *Cliëntenonderzoek bij bestaande relatie. De consument houdt een betaalrekening aan bij de bank. Op enig moment is zij door de bank verzocht zich online te identificeren. Volgens de consument neemt de bank ten onrechte geen genoegen met een door haar bewerkt identiteitsdocument. De bank heeft aangevoerd dat zij*

[20] Overweging 2.6: "*De foto van uzelf en de foto van uw identiteitsbewijs met het watermerk, bewaren wij in onze systemen zolang u klant bij ons bent. Daarna bewaren we de foto's nog eens 7 jaar. Dat is omdat wij, net als andere bedrijven, verplicht zijn om onze administratie 7 jaar te bewaren*". Dat is onjuist, nu de Wwft bepaalt dat gegevens worden bewaard tot vijf jaar na het eindigen van de zakelijke relatie.

> *alleen aan haar verplichtingen op grond van de Wwft kan voldoen door identificatie en verificatie aan de hand van een foto of scan van een onbewerkt identiteitsdocument en het vastleggen en bewaren van een volledige kopie daarvan. De Commissie van Beroep oordeelt dat de bank in het kader van haar verplichtingen op grond van de Wwft bevoegd (en verplicht) is om een foto of scan van een onbewerkt identiteitsdocument op te vragen voor het identificeren en verifiëren van de identiteit van de consument. Anders dan de Geschillencommissie is de Commissie van Beroep van oordeel dat de bank in het kader van haar verplichtingen op grond van de Wwft ook bevoegd is om deze zelfde, dus onbewerkte, gegevens in haar administratie te bewaren. Noch het opvragen noch het bewaren van een kopie of scan van het onbewerkte identiteitsdocument is in strijd met de AVG. De klacht van de consument is dus alsnog (volledig) ongegrond.*

Privacy First is van mening dat deze uitspraak veel onjuiste elementen bevat en dat de werkwijze gegevensbeschermingsrisico's voor klanten van financiële instellingen en andere Wwft-plichtige ondernemingen oplevert, onder meer om de volgende redenen:

- Ten onrechte wordt geoordeeld dat de bewaarplicht van artikel 33 Wwft het bewaren van een kopie van een identiteitsbewijs met herkenbare pasfoto omvat.
- Ten onrechte wordt acht geslagen op het belang van DNB, die in de gelegenheid is gesteld om haar standpunt inzake verificatie van de identiteit te geven, waarbij de gegevensbeschermingsbelangen van klanten het onderspit delven. DNB wenst een oneindige 'audittrail' met alle risico's voor burgers van dien.
- Ten onrechte worden de verplichtingen op grond van de Wwft (verificatie van de identiteit) verward met de cybersecurity maatregelen die een financiële instelling ook moet nemen [21], maar die niet inhouden dat persoonsgegevens langdurig hoeven te worden bewaard.
- Ten onrechte worden de AVG-aspecten onvoldoende aan de orde gesteld, waaronder de gevolgen van de dataminimalisatievereisten voor de bewaarplicht.

Geschillencommissie Kifid 1 juli 2021, zaak 2021-0606

In diverse uitspraken noemt de Geschillencommissie deze uitspraak een richtinggevende uitspraak. Samenvatting Kifid:

> *Cliëntenonderzoek bij bestaande relatie. De consument houdt een creditcard aan bij ICS. Op enig moment is zij door ICS verzocht zich online te identificeren. De*

[21] Zie bijvoorbeeld het citaat uit de tekst van DNB: "*DNB kan ook bevestigen dat het bewaren van de identiteitsbewijzen inclusief pasfoto ook is noodzakelijk om fraude en mogelijk onjuist gebruik van een rekening tegen te gaan, bijvoorbeeld bij het identificeren op afstand of online*." Dit is niet gebaseerd op de Wwft.

consument heeft daar niet binnen de door ICS gestelde termijn aan meegewerkt, waarna ICS heeft aangegeven de creditcard te zullen blokkeren en de overeenkomst op te zeggen. Volgens de consument verplicht ICS haar ten onrechte zich opnieuw te laten identificeren. De wet biedt geen grondslag voor heridentificatie bij bestaande klanten zonder dat daar aanleiding voor is. Daarnaast heeft zij bezwaar tegen online heridentificatie. De commissie oordeelt dat ICS op grond van de Wwft verplicht is de consument te heridentificeren. Het staat ICS bovendien vrij om bij het identificeren van cliënten te kiezen voor een online methode. De vordering wordt afgewezen.

De eerder genoemde kritiekpunten gelden ook hier.

Geschillencommissie Kifid 19 juli 2024, LeasePlan Bank, zaak 2024-0631 [22]

Twee consumenten hadden bezwaar tegen het aanleveren van een verificatiefilmpje tijdens het identificatieproces. Het identificatieproces bestond onder meer uit het uploaden van een foto van het paspoort, overboeking van 1 euro vanaf een betaalrekening en het filmpje. Het uploaden van het filmpje lukte niet. Uiteindelijk is het identificatieproces geannuleerd en is de spaarrekening gesloten.

Volgens de uitspraak stellen de consumenten dat de bank niet verplicht is 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 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.

De bank beweert dat fysieke controle vanwege de bedrijfsvoering niet mogelijk zou zijn en dat - nu de bank de echtheidskenmerken van het legitimatiebewijs niet zou kunnen controleren zoals dat bij fysiek contact wel gebeurt - heeft 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 beroept zich op DNB die in een leidraad het gebruik van een filmpje als voorbeeld heeft genoemd. Opvallend is dat de bank stelt dat zij niet van de identificatie door een andere bank gebruik kan maken omdat ze alsdan de procedure van die andere bank voor een betrouwbaar identificatie- en verificatieproces moet opvragen en beoordelen en dat dat niet werkbaar zou zijn. Volgens de Geschillencommissie heeft de bank daarmee voldoende onderbouwd dat een verificatiefilmpje noodzakelijk is.

[22] Uitspraak van 23 juli 2024, https://www.kifid.nl/wp-content/uploads/2024/07/Uitspraak-2024-0631-Bindend.pdf.

De Geschillencommissie oordeelt dat de bank verantwoordelijke is in de zin van de AVG en heeft deskundigenadvies gevraagd aan Riverworks Legal Services en aan prof. mr. A. Berlee. Beide deskundigen menen dat het gebruik van de video om te zien of iemand in leven is en of hij/zij overeenkomt met een foto van het identiteitsbewijs geen verwerking van biometrische gegevens in de zin van de AVG zou inhouden.

In deze uitspraak komt niet aan de orde of aan de veiligheidseisen van de AVG wordt voldaan, voldoening aan het dataminimalisatiebeginsel van de AVG en hoe het zit met het bewaren van de gegevens.

Literatuur: artikel Mekić over het opslaan van kopieën van legitimatiebewijzen, foto's en video's van cliënten door FI's

Lees in dit verband het artikel *Het opslaan van kopieën van legitimatiebewijzen, foto's en video's van cliënten: de grenzen van de Wwft-reconstructieplicht in het licht van fundamentele rechten* van promovendus Danny Mekić in P&I van februari 2024.

Mekić concludeert dat praktijk van het kopiëren van identiteitsbewijzen grote risico's voor burgers oplevert en dat het bewaren daarvan niet nodig is op grond van de witwasbestrijdingsregelgeving:

> *Jaarlijks worden honderdduizenden Nederlandse ingezetenen slachtoffer van identiteitsfraude waarbij misbruik wordt gemaakt van een kopie van hun legitimatiebewijs. Instellingen die vallen onder de reikwijdte van de Wwft bewaren het vaakst op grote schaal kopieën van legitimatiebewijzen. (…)*
>
> *Uit een rechtshistorische analyse van de Wwft blijkt, in lijn met de vaste rechtspraak, dat het bewaren van een kopie van het legitimatiebewijs van cliënten niet verplicht is, wel kan maar niet altijd mag, en dat de Wwft geen grondslag biedt, laat staan een verplichting bevat, om foto's en audio- en video opnamen van cliënten te bewaren.*
>
> *Het bewaren van een kopie van een legitimatiebewijs vormt een ernstigere inperking van het fundamentele recht op privacy en gegevensbescherming dan het enkel bewaren van losse identiteitsgegevens, omdat een kopie legitimatiebewijs een groter en ernstiger risico op misbruik met zich meebrengt dan de bewaring van losse identiteitsgegevens. Nu op grond van de Wwft blijkt dat het (enkel) bewaren van identiteitsgegevens volstaat, schrijft het subsidiariteitsvereiste voor dat instellingen daar indien mogelijk ook voor moeten kiezen, in plaats van voor het (ook) bewaren van een kopie van het legitimatiebewijs van de cliënt. Het*

subsidiariteitsvereiste staat er in de context van de reconstructieplicht van de Wwft om dezelfde reden aan in de weg om een kopie legitimatiebewijs te bewaren waar ook andere gegevens (foto, handtekening, burgerservicenummer) op zichtbaar zijn. (…)

Instellingen die naast identiteitsgegevens ook (volledige) kopieën van legitimatiebewijzen, foto's en audio en video-opnamen van hun cliënten willen bewaren, kunnen zich wat betreft de grondslag niet beroepen op de reconstructieplicht uit de Wwft. Dit sluit echter niet uit dat er andere grondslagen zijn om zulks alsnog te doen. Ook die zullen dan moeten voldoen aan het vereiste van voorzienbaarheid en evenredigheid (geschiktheid, subsidiariteit en proportionaliteit) om een rechtmatige inbreuk op het fundamentele recht op privacy en gegevensbescherming te vormen.

Slotopmerking

De hiervoor behandelde beslissingen zijn teleurstellend omdat de identificatieproblematiek onvolledig en soms onjuist aan de orde komt en de AVG-aspecten onvoldoende tot hun recht komen.

Er moet iets gebeuren!

Vanwege de groeiende risico's is Privacy First van mening dat het nodig is dat de werkwijze rondom de verificatie van de identiteit door financiële instellingen wordt aangepast, zodat zij aan de AVG voldoen en de risico's op identiteitsfraude beperken. Daarbij is van belang dat zij een maatschappelijke voorbeeldfunctie hebben en essentiële diensten leveren.

Wij zouden graag zien dat de problematiek van verificatie van de identiteit door financiële instellingen structureel wordt aangepakt in lijn met de Wwft en de AVG, zoals in het voorgaande is voorgesteld.

Hierbij nodigen wij u uit om zo spoedig mogelijk maatregelen te nemen.

Bijlage 1 - Verificatie van de identiteit van natuurlijke personen op grond van de Wwft

In de terminologie van de huidige tekst van de Wwft (artikel 1) wordt onder 'identificeren' verstaan: opgave van de identiteit laten doen. Datzelfde artikel definieert 'verifiëren' als: vaststellen dat de opgegeven identiteit overeenkomt met de werkelijke identiteit.

Artikel 3 Wwft verplicht tot cliëntenonderzoek. Daarvan maakt onder meer deel uit dat bepaalde personen geïdentificeerd en hun identiteit geverifieerd dienen te worden, onder andere de cliënt en de uiteindelijk belanghebbende (UBO). Dat dient te gebeuren op het moment van aangaan van de relatie. Er is geen verplichting om periodiek te identificeren, tenzij er twijfel bestaat aan de identiteit, wat ook volgt uit het risicogebaseerde karakter van het cliëntenonderzoek op grond van de Wwft.

In de Wwft is niet opgenomen dat de verificatie van de identiteit moet plaats vinden volgens bepaalde technische normen. Alleen het notariaat kent op dat punt specifieke voorschriften. In het *Reglement gebruik WID-scanner* dat op 1 oktober 2021 in werking is getreden [23] is opgenomen dat als een persoon voor het eerst voor een notaris verschijnt, de notaris de identiteit verifieert met een gespecialiseerde scanner die aan een groot aantal eisen voldoet. Dientengevolge kunnen Wwft-plichtigen volstaan met een vorm van verificatie die passend is gelet op de risico's. Normaliter is het fysiek inzien van een identiteitsbewijs en het noteren van de relevante gegevens voldoende.

Bij de cliënt dient de identiteit altijd te worden geverifieerd bij het aangaan van de zakelijke relatie. De eisen bij de uiteindelijk belanghebbende zijn minder strikt, daarover staat in artikel 3 dat de Wwft-plichtige verplicht is om "*redelijke maatregelen te nemen om zijn identiteit te verifiëren*". Een Wwft-plichtige mag alleen een zakelijke relatie aangaan of transactie uitvoeren als zij beschikt over alle identificatie- en verificatiegegevens en overige gegevens inzake de identiteit van de cliënt en andere in artikel 3, tweede, derde en vierde lid Wwft bedoelde personen (artikel 5 lid 1 Wwft).

In artikel 11 Wwft is aangegeven welke documenten voor de verificatie van de identiteit gebruikt kunnen worden, waarbij wordt verwezen naar een ministeriële regeling [24]. Voor natuurlijke personen betreft dit onder andere een paspoort, een Nederlandse identiteitskaart en een Nederlands rijbewijs, die geldig zijn op het moment van verificatie.

[23] Zie https://www.wet-en-regelgeving-notariaat.nl/overige-regelgeving/reglement-gebruik-wid-scanner. De tekst is niet openbaar.

[24] Artikel 4 Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme.

Te registreren gegevens (artikel 33 leden 1 en 2 Wwft)

In de Wwft is geen bepaling te vinden die voorschrijft dat Wwft-plichtigen kopieën moeten maken van identiteitsbewijzen. Er staat slechts dat bepaalde gegevens moeten worden geregistreerd.

Uit artikel 33 leden 1 en 2 Wwft is op te maken welke gegevens de Wwft-plichtige in verband met de verificatie van de identiteit van een natuurlijke persoon dient te registreren:

> *1. Een instelling die op grond van deze wet cliëntenonderzoek heeft verricht, of bij wie een cliënt is geïntroduceerd conform de procedure van artikel 5, legt op opvraagbare wijze de documenten en gegevens vast die zijn gebruikt voor de naleving van het bepaalde in artikel 3, tweede tot en met vierde lid, artikel 3a, eerste lid, artikel 6, eerste en tweede lid, artikel 7, tweede lid, en artikel 8, derde tot en met zesde en achtste lid.*
>
> *2. Onder de documenten en gegevens, bedoeld in het eerste lid, zijn ten minste begrepen:*
> *a. van natuurlijke personen, niet zijnde uiteindelijk belanghebbenden als bedoeld in artikel 1, eerste lid:*
>
> *1°. de geslachtsnaam, de voornamen, de geboortedatum, het adres en de woonplaats, dan wel de plaats van vestiging van de cliënt alsmede van degene die namens die natuurlijke persoon optreedt, of een afschrift van het document dat een persoonidentificerend nummer bevat en aan de hand waarvan de verificatie van de identiteit heeft plaatsgevonden;*
> *2°. de aard, het nummer en de datum en plaats van uitgifte van het document met behulp waarvan de identiteit is geverifieerd;*
>
> *b. van natuurlijke personen, zijnde uiteindelijk belanghebbenden als bedoeld in artikel 1, eerste lid:*
> *1°. de identiteit, waaronder ten minste de geslachtsnaam en voornamen van de uiteindelijk belanghebbende; en*
> *2°. de gegevens en documenten die zijn vergaard op basis van de redelijke maatregelen die zijn genomen om de identiteit van de uiteindelijk belanghebbende te verifiëren; (…)*
> *3°. van degenen die voor de vennootschap of juridische entiteit bij de instelling optreden: de geslachtsnaam, de voornamen en de geboortedatum. (…)*

Let op het gebruik van het woord 'of' in lid 2 sub 1° van artikel 33 Wwft.[25] Dat woord geeft aan dat er geen verplichting is om een kopie van het identiteitsbewijs vast te leggen. Uit dit artikel vloeit niet voort dat er beelden (biometrische gegevens) moeten worden opgeslagen.

Nu er een keuze is, dient de FI op grond van het dataminimalisatiebeginsel van de AVG de verplichting van artikel 33 Wwft op zodanige wijze na te leven dat de identiteitsfrauderisico's voor burgers zo veel mogelijk worden gemitigeerd. Dat betekent dat er geen kopieën worden opgeslagen, tenzij er een aantoonbare en goed onderbouwde noodzaak is en passende veiligheidsmaatregelen zijn genomen.

Bewaarplicht (artikel 33 lid 3 Wwft)

Het derde lid van artikel 33 Wwft geeft aan dat de Wwft-plichtige de gegevens van het cliëntenonderzoek, onder meer de verificatiegegevens, langdurig dient te bewaren, te weten gedurende vijf jaar na het tijdstip van het beëindigen van de zakelijke relatie of gedurende vijf jaar na het uitvoeren van de transactie. De gegevens moeten na afloop van deze termijn worden vernietigd (artikel 34a lid 3 Wwft).

Bij FI's komen langdurige zakelijke relaties voor, wat betekent dat de verificatiegegevens zeer lange tijd moeten worden bewaard.

Gegevensbescherming

In artikel 34a Wwft is bepaald dat persoonsgegevens alleen mogen worden verwerkt met het oog op het voorkomen van witwassen en financieren van terrorisme en worden niet verder verwerkt voor commerciële doeleinden of andere doeleinden die niet verenigbaar zijn met dat doel.

Lid 2 van artikel 34a schrijft voor dat een Wwft-plichtige alvorens een zakelijke relatie aan te gaan of een incidentele transactie te verrichten, informatie aan een cliënt verschaft over de krachtens de Wwft geldende verplichtingen ter zake van de verwerking van persoonsgegevens met het oog op het voorkomen van witwassen en financieren van terrorisme. Voor het overige is de AVG onverkort op de activiteiten van Wwft-plichtigen van

[25] In het citaat hierna is het woord 'of' dik gedrukt: "*de geslachtsnaam, de voornamen, de geboortedatum, het adres en de woonplaats, dan wel de plaats van vestiging van de cliënt alsmede van degene die namens die natuurlijke persoon optreedt,* ***of*** *een afschrift van het document dat een persoonidentificerend nummer bevat en aan de hand waarvan de verificatie van de identiteit heeft plaatsgevonden*".

toepassing, wat onder meer betekent dat als de cliënt geen natuurlijke persoon is, de FI ten aanzien van de betrokkenen in de zin van de AVG waarvan op grond van de Wwft persoonsgegevens worden verwerkt, de voorschriften van artikel 14 AVG (informatieplicht) dient na te leven.

Bijlage 2 - Identificatieplicht en de AVG

De Wwft biedt voor Wwft-plichtigen zoals FI's een grondslag als bedoeld in artikel 6 lid 1 sub c) AVG om persoonsgegevens te verwerken. Dat betekent echter niet dat er een ongelimiteerde vrijheid is voor FI's. Ook voor de wetgever en de toezichthouders (zoals DNB en AFM) geldt dat zij bij de interpretatie van de Wwft rekening dienen te houden met de eisen die de AVG stelt aan de verwerking van persoonsgegevens.

Grondslag

Artikel 6 lid 3 AVG stelt de eis dat de verwerking is voorgeschreven bij Unierecht of nationaal recht ('rechtsgrond') en bepaalt:

> *Het doel van de verwerking wordt in die rechtsgrond vastgesteld of is met betrekking tot de in lid 1, punt e), bedoelde verwerking noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend. Die rechtsgrond kan specifieke bepalingen bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verwerkingsverantwoordelijke; de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslagperioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking, zoals die voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX. Het Unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel.*

De bepalingen in de Wwft inzake identificatie dienen aan de norm van artikel 6 lid 3 AVG te voldoen.

Beginselen artikel 5 AVG

Daarnaast blijven de beginselen van de AVG, zoals artikel 5 AVG, relevant. Lid 1 van artikel 5 bepaalt dat persoonsgegevens moeten:

> *a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie");*

b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding");
c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking")
d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren („juistheid");
e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen („opslagbeperking");
f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").

Biometrische gegevens

De hoofdregel van artikel 9 lid 1 AVG is dat het verboden is de navolgende persoonsgegevens te verwerken:

- persoonsgegevens waaruit ras of etnische afkomst blijken;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon.

In lid 2 van artikel 9 AVG is aangegeven wanneer daarop uitzondering mag worden gemaakt, onder meer als aan de volgende voorwaarde is voldaan: [26]

g) de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het

[26] Het verlenen van toestemming is hier geen relevante uitzondering.

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;

In de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) is in artikel 25 bepaald dat verwerking van persoonsgegevens waaruit ras of etnische afkomst blijkt is toegestaan indien de verwerking geschiedt met het oog op de identificatie van de betrokkene, en slechts voor zover de verwerking voor dat doel onvermijdelijk is.

In artikel 29 UAVG staat dat het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing is, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.

Overige bepalingen UAVG: geen meldplicht datalekken, verwerking BSN

Op grond van artikel 42 UAVG geldt artikel 34 AVG (melding van datalekken [27]) niet voor financiële ondernemingen. Dit is een zeer ruime groep ondernemingen, waar onder meer FI's onder vallen. Gevolg hiervan is dat banken betrokkenen niet hoeven te informeren als zij risico lopen op identiteitsfraude. De Autoriteit Persoonsgegevens heeft er recent weer op gewezen dat het voor betrokkenen belangrijk is dat datalekken gemeld worden en dat wordt aangegeven welke maatregelen betrokkenen tegen identiteitsfraude kunnen nemen.

In artikel 46 UAVG is geregeld dat verwerking van het nationaal identificatienummer (BSN) uitsluitend is toegestaan als dat wettelijk is bepaald, ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald.

[27] Zie de tekst van het artikel, dat bepaalt dat wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee deelt.