Nederlandse Vereniging van Banken

Datum 13 juli 2020
Referentie BR4432

Betreft: consultatiereactie NVB verzamelwet gegevensbescherming

Geachte heer, mevrouw,

De Nederlandse Vereniging van Banken (NVB) maakt graag gebruik van de mogelijkheid om te reageren op de consultatie verzamelwet gegevensbescherming. U treft onze inbreng hierbij aan.

Algemeen:
Gegevensbescherming is belangrijk en heeft impact op iedereen. Banken gaan hier dagelijks op zorgvuldige wijze mee om. De NVB vindt het belangrijk dat de Uitvoeringswet Algemene Verordening Gegevensbescherming regelmatig wordt geëvalueerd zodat deze kan worden aangepast op basis van de ervaringen uit de praktijk, zowel binnen als buiten de financiële sector. De NVB heeft met belangstelling kennis genomen van het hieruit voortvloeiende voorstel van wet en wenst op een tweetal onderdelen input te geven. Het gaat hierbij om het gebruik van biometrische gegevens en de nieuw toegevoegde bepalingen in artikel 41 UAVG.

Leeswijzer: de opbouw van dit document volgt de artikelen en letters van het wetsvoorstel.

Opmerkingen en vragen:

ARTIKEL I. Uitvoeringswet Algemene verordening gegevensbescherming
Onderdeel L (artikel 29 UAVG)

Verzoek NVB:
De NVB verzoekt in de Memorie van Toelichting te verduidelijken/expliciteren dat het ook mogelijk kan zijn om gebruik te maken van biometrische gegevens voor financiële diensten.

Toelichting:
Er is een toenemende vraag naar het op afstand regelen van financiële zaken. Dat komt voort uit de digitalisering van onze maatschappij en door aanbieders die al dan niet uitsluitend digitaal financiële producten en diensten aanbieden. Tevens is sprake van een toenemende vraag van consumenten naar digitale dienstverlening. Voorts blijkt uit de recente mobiliteitsvraagstukken in relatie tot de Covid-19 dat de maatschappij behoefte heeft aan (en dat dit onder omstandigheden zelfs noodzakelijk is) een zo volledig mogelijke digitale dienstverlening.

Biometrie bij klantidentificatie
Banken zijn verplicht om klanten te identificeren om te voldoen aan de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Dit kan op afstand plaatsvinden. De Minister heeft eerder gezegd dat in dergelijke gevallen banken “meer inspanningen moeten verrichten om er zeker van te zijn dat de opgegeven identiteit correct is” (zie antwoord op Kamervragen)[1].

Bij de acceptatie van nieuwe klanten is het essentieel om de identiteit van de persoon met een grote mate van zekerheid vast te stellen. Op een kantoor gebeurt dit (o.a.) door middel van een check van de bankmedewerker om te verifiëren of de aanwezige persoon ook dezelfde persoon is als die op het identiteitsdocument. Veilige en betrouwbare alternatieven op deze traditionele wijze van identificatie en verificatie zijn noodzakelijk bij online acceptatie processen. Bij volledige online processen zal ook het gebruik van biometrie onvermijdelijk zijn.

Uitgangspunt van biometrie is dat de persoon niet te scheiden is van zijn lichaam. Het belangrijkste voordeel van een biometrische identificatiemethode is dan ook dat het niet afhangt van bezit (sleutelkaart) of kennis (pincode of een wachtwoord): het lichaam zelf bevat kenmerken die zo uniek zijn dat identificatie daarmee mogelijk is. In principe zijn lichaamskenmerken die in aanmerking komen voor biometrie niet makkelijk overdraagbaar op andere personen, zoals pasjes, sleutels en wachtwoorden dat wel zijn, en zijn ze ook niet fraudegevoelig, zoals foto's en handtekeningen.
De gangbare voorbeelden van biometrische gegevens zijn vingerafdrukken, iriskenmerken, het patroon van het netvlies, van de aders in de hand(palm) of vingers, het warmtepatroon van het gezicht en de spraak. Met behulp van goed functionerende sensoren (denk aan een camera en beeldanalysesoftware) kan met gezichtsherkenning de identiteit van een persoon ook op afstand worden gecontroleerd. Zo kunnen allerlei biometrische sensoren (irisscan, vingerafdruk ed.) dus worden ingezet om op afstand de identiteit van klanten (in het kader van de Wwft) te bepalen en verifiëren hetgeen een grote bijdrage levert aan het voorkomen van identiteitsfraude.

Identificatie en verificatie zoals bedoeld in de Wwft vinden niet plaats en dienen ook niet plaats te vinden op basis van toestemming. De grondslag voor de verwerking van deze persoonsgegevens is “noodzakelijk om te voldoen aan wettelijke verplichting waaraan de verwerkingsverantwoordelijke moet voldoen”. In dit kader is deze wettelijke verplichting de Wwft. Het toestaan van het gebruik van biometrie bij online acceptatieprocessen slechts op basis van toestemming van de klant strookt dan niet met deze wettelijke verplichting.

Toegang hebben tot financiële diensten is een algemeen zwaarwegend belang. Deze toegang moet worden gegarandeerd ook wanneer het lastig is om naar een kantoor te gaan. Dit is niet vanzelfsprekend, bijvoorbeeld bij lock down maatregelen als gevolg van Covid-19- of wanneer financiële instellingen over geen of een steeds kleiner kantorenetwerk beschikken. Banken moeten ook in deze gevallen voldoen aan de strenge identificatieregels die uit de Wwft voortvloeien. Zoals

[1] https://zoek.officielebekendmakingen.nl/ah-tk-20182019-1737.html
‘Het is mogelijk en toegestaan om het cliëntenonderzoek niet in persoon maar op afstand te verrichten. In deze gevallen geldt eveneens dat verificatie plaats dient te vinden aan de hand van documenten, gegevens of inlichtingen uit betrouwbare en onafhankelijke bron. Het cliëntenonderzoek op afstand brengt meer risico’s met zich dan een cliëntenonderzoek in persoon. De bank is verplicht om deze risico’s te mitigeren. Dit betekent dat de bank meer inspanningen moet verrichten om er zeker van te zijn dat de opgegeven identiteit correct is, bijvoorbeeld door gebruik te maken van aanvullende gegevens uit betrouwbare en onafhankelijke bron. Cliëntenonderzoek op afstand kan bijvoorbeeld plaatsvinden doordat degene die een bankrekening wil openen zijn paspoort of identiteitskaart inscant, waarna er identificatie en verificatie van de identiteit kan plaatsvinden met behulp van een (live) videoverbinding. ‘

aangegeven verwacht de minister dat ook. Biometrie vormt daarbij een alternatief. Daarom is het van belang dat banken een beroep kunnen doen op art. 29 van de UAVG.

Biometrie bij betalingsverkeer
PSD2 stimuleert het gebruik van biometrie bij het toepassen van “sterke clientauthenticatie”. Dit is authenticatie met gebruikmaking van twee of meer factoren die worden aangemerkt als kennis (iets wat alleen de gebruiker weet, bijvoorbeeld een wachtwoord of PIN5), bezit (iets wat alleen de gebruiker heeft, bijvoorbeeld een telefoon) en een inherente eigenschap (iets wat de gebruiker is, bijvoorbeeld biometrie) en die onderling onafhankelijk zijn, in de zin dat het compromitteren van één ervan geen afbreuk doet aan de betrouwbaarheid van de andere en die zodanig is opgezet dat de vertrouwelijkheid van de authenticatiegegevens wordt beschermd. Biometrie is een van de hiervoor genoemde factoren.

Een wachtwoord of een PIN5 kan worden vergeten. Het kan ook zijn dat door phishing deze in verkeerde handen vallen met alle gevolgen van dien. Organisaties moeten kunnen kiezen, afhankelijk van de beschikbare technologie voor de opties die zij het meest passend vinden. Als een organisatie ervoor kiest om biometrie te gebruiken als een van deze factoren, nadat alle checks en balances hebben plaatsgevonden, dan moet ze in de praktijk dit ook kunnen toepassen. De verantwoordelijkheid voor de afweging over welke van deze factoren de betreffende organisatie besluit toe te passen, kan niet bij de klant worden neergelegd. Toestemming van de klant past daar niet bij. In dergelijke gevallen moet de klant kunnen vertrouwen op de keuze die de bank heeft gemaakt ten aanzien van de authenticatiefactoren bij cruciale processen, zoals zich online toegang verschaffen tot zijn betaalrekening of bij het initiëren van een elektronische betalingstransactie.

In de specifieke gevallen waar een bank, nadat de juiste afwegingen hebben plaatsgevonden, voor biometrie kiest als een van de sterke clientauthenticatie factoren in het kader van betalingsverkeer, belemmert het stellen van toestemming als voorwaarde de implementatie ervan. Daarom moeten banken ook hiervoor een beroep kunnen doen op de uitzondering van art. 29 van de UAVG.

Het gebruik van biometrie - zowel bij clientidentificatie als bij clientauthenticatie bij betalingsverkeer - zijn belangen die uitstijgen boven louter reguliere bedrijfs- of organisatiebelangen en kan niet alleen worden gezien als efficiëntie of kostenbesparing.

Bij de opsomming van doeleinden in het wetsvoorstel staan “diensten” genoemd. Het zou de duidelijkheid ten goede komen als in de MvT nader toegelicht wordt dat financiële diensten daar tevens worden inbegrepen.

ARTIKEL I. Uitvoeringswet Algemene verordening gegevensbescherming
Onderdeel P (artikel 41 UAVG)

<u>Artikel 41 lid 1 UAVG onderdeel P</u>
De NVB begrijpt de voorgestelde aanpassingen bij de eerste lid van artikel 41 UAVG en steunt deze. Aansluiting bij de formulering van de AVG is wenselijk. We delen de mening van de Minister dat deze aanpassing geen afbreuk doet aan het beoogde doel van artikel 23 van de AVG.

<u>Artikel 41 nieuw lid 3 UAVG: Onduidelijke toevoeging</u>

Verzoek NVB: nieuw lid 3 schrappen. In onze ogen is dit overbodig en kan dit tot verwarring leiden.

Toelichting:
De NVB vraagt zich af wat het doel van deze toevoeging is. In de Memorie van Toelichting (MvT) bij

de UAVG werd de vangnetwerking van artikel 23 al duidelijk toegelicht. In de MvT is opgenomen dat sprake is van een gelaagdheid van wetgeving. Daarbij wordt genoemd dat in sectorspecifieke regelgeving specifieke bepalingen kunnen worden opgenomen op grond waarvan de rechten kunnen worden beperkt. Maar – zoals ook aangegeven in dezelfde MvT – zijn sectorspecifieke bepalingen alleen mogelijk in een situatie waarin voorzienbaar is dat een afwijking noodzakelijk is. Hierom is het 'noodzakelijk om een generieke regeling op te nemen in de Uitvoeringswet, die ruimte biedt aan de praktijk om in de toekomst hierin een belangenafweging te maken.' In deze toelichting is de vangnetwerking van artikel 23 AVG/41 UAVG al voldoende verduidelijkt.

Zo wordt in de tekst van de UAVG nu al erkend dat het soms niet mogelijk is om invulling te geven aan de rechten van de betrokkene. Dit is bijvoorbeeld te zien bij artikel 12 lid 4, artikel 14 lid 5, artikel 15 lid 4 of artikel 16 lid 4. Maar ook in sectorspecifieke wetgeving zijn bepalingen opgenomen die de rechten van betrokkenen beperken. Zo geldt voor banken het tipping of verbod (aan de betrokkene) bij de melding van ongebruikelijke transacties aan de FIU. Artikel 23 AVG bepaalt in aanvulling daarop dat in sommige gevallen deze rechten nader beperkt kunnen worden en geeft een aantal redenen die eventuele beperkingen kunnen rechtvaardigen. De verhouding tussen art. 23 AVG / art. 41 UAVG en de andere artikelen lijkt helder te zijn zonder te toevoeging van lid 3. Daarom stelt de NVB voor om dit lid te schrappen. In onze ogen is dit overbodig en kan dit tot verwarring leiden.

<u>Artikel 41 nieuw lid 4 en lid 5</u>
Verzoek NVB:
De NVB stelt voor om de nieuw toegevoegde leden 4 en 5 te schrappen.

Toelichting:
Het voorgestelde lid 4 verplicht de verwerkingsverantwoordelijke tot de verstrekking van informatie over de beperking van de rechten bedoeld in artikel 23 AVG/41 UAVG aan de betrokkene en aan de AP. De ruimte die artikel 23 AVG aan de lidstaten biedt om door middel van wetgeving de reikwijdte van de verplichtingen en rechten als bedoeld in art 12 t/m 22 en 34 AVG te beperken is gelimiteerd. Artikel 23 lid 2 AVG stelt zelfs met welke aspecten in ieder geval eventueel lidstatelijk recht rekening zou moeten houden bij de beperking van de rechten bedoeld in artikel 23 AVG. Aanvullende verplichtingen – zoals nu voorgesteld in lid 2 van artikel 23 lijken daar niet bij te horen.

In artikel 23 lid 2 AVG is daarnaast al het recht van betrokkenen om van een beperking op de hoogte te worden gesteld opgenomen. Anders dan het voorgestelde lid 4 is dit geen verplichting, maar een recht. De Europese wetgever realiseert zich dat dit recht, zelfs in het kader van art. 23 AVG niet ongelimiteerd kan zijn. Het recht om geïnformeerd te worden over de beperking geldt "tenzij dit afbreuk kan doen aan het doel van de beperking" (zie art. 23 lid 2 AVG). Bijvoorbeeld: in de bancaire sector is het verplicht om onderzoek te doen naar fraude. Het verplicht informeren van de betrokkene dat een onderzoek naar fraude loopt kan leiden tot het vernietigen van bewijs en kan het onderzoek ernstig hinderen.
In deze gevallen doet het moeten informeren dat aan de informatieplicht niet kan worden voldaan duidelijk afbreuk aan het doel van de beperking van deze informatieplicht. De verplichting uit het voorgestelde lid 4 houdt hier -anders dan in de AVG- geen rekening mee.

Maar ook in het kader van het inzage- en correctierecht en bij een beroep op de andere rechten uit de AVG kan dit leiden tot situaties waarbij banken in het kader van het onderzoek bepaalde verwerkingen/doorgiftes niet mogen/kunnen verstrekken aan betrokkenen in het kader van samenwerkingen/onderzoek door politie en justitie. Ook zijn banken gebonden aan expliciete geheimhoudingsverplichtingen.

De NVB stelt voor om – gezien het voorgaande - deze verplichting te schrappen.

Een bijkomend gevolg als lid 4 wordt toegevoegd is dat - gelet op de hoeveelheid van transacties die dagelijks plaatsvinden en waarover op verschillende gronden onderzoek moet worden gedaan - banken vaak de AP zullen moeten informeren dat niet voldaan kan worden aan de informatieplicht op basis van artikel 23 AVG. Op basis van het aantal meldingen aan de AP kan de onjuiste indruk worden gewekt dat banken structureel gebruik maken van het inperken van rechten van betrokkenen, terwijl dit gelet op de verhouding tussen het aantal transacties en onderzoeken die plaats moeten vinden, een vertekend beeld geeft van de realiteit. Daarenboven bestaat het risico dat door de mogelijke WOB baarheid van deze meldingen – deze informatie –alsnog bij betrokkenen terecht komt.

In lid 4 en 5 van het wetgevingsvoorstel wordt aan de toezichthouder een nieuwe taak toegekend. Daarbij wordt verwezen naar artikel 6 lid 3 UAVG. In dit artikel is opgenomen dat ‘ter uitvoering van een bindende EU-rechtshandeling’… ‘bij regeling van onze Minister aan de Autoriteit Persoonsgegevens taken worden opgedragen’. In de MvT bij de UAVG wordt als voorbeeld genoemd ‘adequaatsheidsbesluiten van de EC’. Een dergelijke aanvullende taak als nu wordt voorgesteld in lid 5 past niet bij het bepaalde in overweging 129 van de AVG. Daar wordt duidelijk gemaakt dat “de toezichthoudende autoriteiten in alle lidstaten dezelfde taken en feitelijke bevoegdheden hebben”. De NVB stelt voor lid 5 te schrappen, omdat een dergelijke aanvullende taak van de nationale toezichthouder niet past bij overweging 129 van de AVG.

ARTIKEL VII. Wet op het financieel toezicht
De NVB onderschrijft de toevoeging aan artikel 3:17 van de Wet op het financieel toezicht die zien op het onder voorwaarden geautomatiseerd besluiten om betalingstransacties die zijn gekoppeld aan een financieel product te blokkeren of op te schorten.

Tot slot
We hopen nadrukkelijk dat u bij de vervolgstappen in het kader van dit wetsvoorstel rekening houdt met de door ons genoemde vragen en verzoeken. We zijn vanzelfsprekend graag beschikbaar voor eventuele vragen en een nadere toelichting.

Met vriendelijke groet,

Eelco Dubbeling
Directeur Nederlandse Vereniging van Banken