

# 242. Financiële zorgplichten vs. privacyregels: een botsing of geen reden tot zorg?

MR. DRS. M. JANSEN EN MR. C.H.D.W. VAN DEN BORNE-VERHEIJEN

Sinds de jaren negentig zijn zowel de (bijzondere) zorgplicht bij financiële dienstverlening als privacywetgeving geïntroduceerd en geëvolueerd. In dit artikel wordt het juridisch kader toegelicht en aan de hand van praktische voorbeelden ingegaan op het snijvlak tussen deze twee. Tevens worden aanbevelingen gedaan.

## Inleiding

Sinds de jaren negentig<sup>1</sup> zijn op financiële ondernemingen (bijzondere) zorgplichten van toepassing die verschillen per product en type dienstverlening en die afhankelijk zijn van de omstandigheden van het geval.<sup>2</sup> Vanaf omstreeks diezelfde tijd<sup>3</sup> moeten financiële ondernemingen tevens privacyregels in acht nemen. Zowel de (bijzondere) zorgplichten als de privacywetgeving zijn de afgelopen jaren sterk geëvolueerd. Dit leidt met name in de retailpraktijk tot praktische en juridische afbakeningsvraagstukken, bijvoorbeeld als het gaat om de identificatieplicht, kredietwaardigheidstoetsen, BKR-registraties of gegevensverwerking bij incassotrajecten. In dit artikel staan we stil bij de vraag in hoeverre privacyregels bij retailproducten (zoals consumptief krediet en hypotheek), in de weg kunnen staan aan de naleving van de verplichtingen die op financiële ondernemingen rusten uit hoofde van de (bijzondere) zorgplichten. We schetsen hiertoe eerst het privacyrechtelijke kader (par. 1) en vervolgens de (bijzondere) zorgplichten die in dit kader relevant zijn (par. 2). Daarna werken we aan de hand van enkele praktijkvoorbeelden uit tot welke spanningsvelden toepassing van beide rechtsgebieden kan

leiden (par. 3). We sluiten vervolgens af met een conclusie met daarin enige aanbevelingen (par. 4).

## 1. Privacyrecht

Het juridisch kader rondom privacy is verspreid over diverse wetten. We zullen de kern van de belangrijkste wetgeving hierna uitlichten, te weten de (U)AVG en de onderliggende grondrechten. Ook in vele andere wetgeving staan privacyregels (uiteenlopend van het strafrecht tot het medezeggenschapsrecht), maar die privacyregels gaan het kader van dit artikel te buiten.

### 1.1 AVG en UAVG

#### 1.1.1 Algemene privacywetgeving

De belangrijkste privacyregels worden sinds 25 mei 2018 gegeven door de combinatie van Europese AVG (Verordening (EU) 2016/679<sup>4</sup>) en de Nederlandse Uitvoeringswet AVG (UAVG). Deze zijn in Nederland zowel binnen als buiten de werkingssfeer van het Unierecht van toepassing.<sup>5</sup>

#### 1.1.2 Breed toepassingsbereik

De (U)AVG hebben een zeer breed toepassingsbereik. Ze zijn van toepassing op iedere ‘verwerking’ van ‘persoonsgegevens’, mits die verwerking geautomatiseerd plaatsvindt of de persoonsgegevens in een bestand zijn opgenomen of bestemd zijn in een bestand te zijn opgenomen.<sup>6</sup> Persoonsgegevens zijn alle gegevens die al dan niet met enige moeite<sup>7</sup>

1 HR 23 mei 1997 (*Rabobank/Everaars*), NJ 1998/192; HR 26 juni 1998 (*Van de Klundert/Rabobank*), NJ 1998/660; HR 11 juli 2003 (*Van Zuylen/Rabobank*), NJ 2005/103.

2 O.a.: HR 5 juni 2009, ECLI:NL:HR:2009:BH2822.

3 Van 1 juli 1989 tot 1 september 2001 was de Wet persoonsregistraties van kracht. Deze werd op 1 september 2001 vervangen door de Wet bescherming persoonsgegevens (Wbp). De Wbp vloeide voort uit de Richtlijn (EG) nr. 1995/46. Deze richtlijn is per 25 mei 2018 vervangen door de Algemene Verordening Gegevensbescherming (AVG), waarover verderop in dit artikel meer. Begrippen uit de AVG en Wbp moeten in beginsel hetzelfde worden uitgelegd, zie daarover o.a. HvJ EU 17 juni 2021, zaak C-597/19, ECLI:EU:C:2021:492, r.o. 107 (*M.I.C.M.*). Overigens vloeien de materiele normen ter zake de verwerking van persoonsgegevens voor een belangrijk deel voort uit het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens d.d. 28 januari 1981 (*Tfb.* 1988, nr. 7).

4 Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

5 Art. 3 lid 2 jo. lid 1 sub a UAVG.

6 Art. 2 lid 1 AVG.

7 HvJ EU 19 oktober 2016, ECLI:EU:C:2016:779, r.o. 48.

naar een persoon herleid kunnen worden.<sup>8</sup> Het begrip ‘verwerken’ is zo breed gedefinieerd dat hiervoor ook gelezen kan worden: ieder werkwoord dat voor de woorden ‘van persoonsgegevens’ kan staan.<sup>9</sup> Dus bijvoorbeeld het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden of op andere wijze ter beschikking stellen van persoonsgegevens, maar ook het combineren, afschermen, wissen of vernietigen daarvan. Van een bestand is reeds sprake wanneer de persoonsgegevens ‘zijn gestructureerd volgens specifieke criteria die het in de praktijk mogelijk maken deze gegevens gemakkelijk terug te vinden voor een later gebruik ervan’.<sup>10</sup> Dit brede toepassingsbereik maakt in de praktijk dat nagenoeg iedere handeling van een financiële instelling met persoonsgegevens onderworpen is aan de (U)AVG.

### 1.1.3 Verwerkingsbeginselen

De kern van de AVG en de UAVG is dat bij de verwerking van persoonsgegevens de beginselen van art. 5 AVG in acht worden genomen. Dit zijn de beginselen van rechtmatigheid, eerlijkheid, doelbinding, minimale gegevensverwerking, juistheid en relevantie, beperkte opslagduur en integriteit en vertrouwelijkheid. Het zijn beginselen die – behoudens een enkele uitzondering – met een zekere ‘soepelheid’ worden ingevuld waarbij in de concrete toepassing ‘een juist evenwicht tussen de betrokken rechten en belangen moet worden gevonden’.<sup>11</sup> Dat maakt dat de wetgeving aan veel interpretatie onderhevig is. Onder de AVG is daarom voorzien in het Europees Comité voor Gegevensbescherming<sup>12</sup> dat onder andere tot taak heeft het ‘uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken om te bevorderen dat deze verordening consequent wordt toegepast’.<sup>13</sup>

### 1.1.4 Grondslagen

Verder mogen gegevens alleen worden verwerkt indien daarvoor één (of meer) van de zes rechtsgronden uit art. 6 AVG aanwezig is: toestemming, uitvoering overeenkomst, voldoen aan een wettelijke plicht, behartigen van een vitaal belang van betrokkene of een derde, het vervullen van een overheidstaak of het behartigen van een gerechtvaardigd belang. Zoals we hierna nader zullen toelichten zijn in het kader van de naleving van de zorgplichten vooral de gronden ‘wettelijke verplichting’<sup>14</sup> en het ‘gerechtvaardigd belang’<sup>15</sup> van belang.

De wettelijke verplichting in voornoemde zin moet zijn vastgesteld bij Unierecht of lidstatelijk recht.<sup>16</sup> Die wetge-

ving moet bovendien ‘beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel’.<sup>17</sup> Een door de privacytoezichthouders onderschreven voorbeeld van een wettelijke plicht is de identificatieplicht die onder omstandigheden op banken rust op grond van de know your customer verplichtingen en op grond van anti-witwasregelgeving.<sup>18</sup>

## Bijzondere zorgplichten van financiële dienstverleners botsen op diverse vlakken met privacywetgeving, hier volgt een uiteenzetting van het wettelijk kader en toelichting aan de hand van praktijkvoorbeelden

Uit de memorie van toelichting bij de UAVG volgt dat de wettelijke plicht niet expliciet hoeft te zien op het verwerken van persoonsgegevens, doch dat deze ook kan voortvloeien uit ‘een ruimer geformuleerde zorgplicht of wettelijke verplichting’.<sup>19</sup> Volgens de wetgever is de kernvraag of zonder verwerking van de gegevens het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk is. De Autoriteit Persoonsgegevens (AP) lijkt dit toch iets strenger te zien. Zo haalt de AP in het recente boetebesluit inzake Wifi-tracking bij de gemeente Enschede<sup>20</sup> weliswaar dit leerstuk omtrent een ruimere zorgplicht aan, doch wijst er anderzijds ook op dat de wet zo moet zijn geformuleerd dat de burger ‘met voldoende precisie kan opmaken welke op zijn privéleven betrekking hebbende gegevens’ kunnen worden verwerkt.<sup>21</sup> Ook het Hof van Justitie van de EU (‘HvJ EU’) lijkt, in lijn met het EHRM, te eisen dat een wettelijke plicht tot verwerking voldoende nauwkeurig is geformuleerd.<sup>22</sup> Hier is het laatste woord dus nog niet over gezegd, zie ook hierna over BKR-registraties.

8 Art. 4 sub 1 AVG.

9 Art. 4 sub 2 AVG.

10 HvJ EU 10 juli 2018, ECLI:EU:C:2018:551, r.o. 62.

11 HvJ EU 6 november 2003, r.o. 83-85 (*Lindqvist*).

12 Beter bekend onder de Engelse afkorting EDPB.

13 Art. 70 lid 1 sub e AVG.

14 Art. 6 lid 1 sub c AVG.

15 Art. 6 lid 1 sub f AVG.

16 Art. 6 lid 3 AVG.

17 Art. 6 lid 3 slotzin AVG. De eis die de AVG op dit punt aan wetgeving stelt is overigens in lijn met de eisen die op grond van het Europees Verdrag voor de Rechten van de Mens (EVRM) aan een inbreuk op de persoonlijke levenssfeer worden gesteld.

18 EDPB, Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van art. 6 lid 1 onder b van de AVG in het kader van de verlening van onlinediensten aan betrokkenen, voorbeeld 6, [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines-art\\_6-1-b-adopted\\_after\\_public\\_consultation\\_nl.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_nl.pdf)

19 *Kamerstukken II* 2017/18, 34851, nr. 3, p. 35.

20 Zie [https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit\\_ap\\_gemeente\\_enschede.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf)

21 Die overweging wordt gegeven in het kader van een beroep op de grondslag ‘publiekrechtelijke taak’, maar de onderbouwing verwijst naar overwegingen in de AVG die zien op wetgeving in algemene zin.

22 Vgl. HvJ EU 20 mei 2003, zaak C-465/00 (*Rechnungshof v. Österreichischer Rundfunk*), r.o. 77, en de verwijzing daar naar EHRM 20 mei 1999, arrest-*Rekvényi/Hongarije*. Of vergelijk, heel recent, HvJ EU 22 juni 2021, ECLI:EU:C:2021:504, r.o. 105: ‘(...) de regeling die inbreuk maakt op de betreffende grondrechten, moet duidelijke en nauwkeurige regels bevatten over de draagwijdte en de toepassing van de maatregel in kwestie.’

De grondslag gerechtvaardigd belang is wetshistorisch gezien een bewust breed geformuleerde grondslag.<sup>23</sup> De Europese Commissie sprak destijds over een clausule die *'is likely to concern very different kinds of processing'*. Op grond van deze grondslag mogen persoonsgegevens worden verwerkt als dat noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke, tenzij de belangen van de betrokkene zwaarder wegen. Het is vaste rechtspraak van het Hof van Justitie dat de grondslag van het gerechtvaardigd belang een open norm is, die van geval tot geval moet worden toegepast.<sup>24</sup> In de rechtspraak van het HvJ EU is een driestappentoezicht ontwikkeld: (i) gerechtvaardigd belang, (ii) noodzaak en (iii) geen prevalentie belangen betrokkene.<sup>25</sup>

In november 2019 publiceerde de AP een 'normuitleg gerechtvaardigd belang'.<sup>26</sup> In dit document stelde de AP dat een belang alleen gerechtvaardigd is als de verwerkingsverantwoordelijke zich op een geschreven of ongeschreven rechtsregel kan beroepen. Zo zou het volgens de AP wel gerechtvaardigd zijn om 'zorgplichten na te komen voor werknemers en/of klanten', maar niet "het zonder gerechtvaardigd belang volgen van het gedrag van werknemers of het (koop)gedrag van (potentiële) klanten".<sup>27</sup> Het is maar zeer de vraag of deze normuitleg standhoudt. De AP had een boete opgelegd aan VoetbalTV op grond van dezelfde uitleg van het gerechtvaardigd belang. Die boete is, onder expliciete verwerping van deze interpretatie van het begrip gerechtvaardigd belang, door de rechtbank Midden-Nederland vernietigd.<sup>28</sup> Het lijkt veeleer wachten op Europese uitleg door de EPDB over het begrip. Tot die tijd lijkt de oude opinie van de Artikel 29 werkgroep ter zake nog steeds relevant.<sup>29</sup>

De discussie over grondslagen lijkt wellicht wat theoretisch, maar heeft een directe weerslag op de praktijk, zoals bijvoorbeeld blijkt uit de jurisprudentie over BKR-registraties. Daarover meer verderop in het artikel.

### 1.1.5 Bijzondere persoonsgegevens

Rondom bijzondere persoonsgegevens geldt een strenger regime. De verwerking van deze gegevens is verboden,

behoudens wettelijke uitzonderingen of de toestemming van betrokkene.

Onder bijzondere persoonsgegevens worden verstaan persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, alsmede genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.<sup>30</sup>

Voor financiële instellingen is met name de categorie 'gegevens over gezondheid' mogelijk relevant. Hieronder worden verstaan 'persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven'.<sup>31</sup> Uit overweging 35 volgt dat hieronder 'alle gegevens die betrekking hebben op de gezondheidstoestand' dienen te vallen. Dat is zeer ruim. Illustratief is dat in de memorie van toelichting bij de Wbp<sup>32</sup> stond vermeld dat het enkele feit dat iemand ziek is al een gezondheidsgegeven vormt.<sup>33</sup> Gelijk zo is in de *Lindqvist*-kwesitie geoordeeld dat het feit dat iemand zijn voet bezeerd heeft en met gedeeltelijk verlos is, een gezondheidsgegeven is.<sup>34</sup> Niets wijst erop dat het begrip onder de AVG enger zou moeten worden geïnterpreteerd.<sup>35</sup>

In art. 30 UAVG zijn enkele uitzonderingen op het verbod om gezondheidsgegevens te verwerken opgenomen. Zo mogen gezondheidsgegevens onder meer worden verwerkt door werkgevers indien dat noodzakelijk is voor de re-integratie of begeleiding van werknemers bij ziekte.<sup>36</sup> Voor verzekeraars,<sup>37</sup> scholen en reclasseringsinstellingen<sup>38</sup> gelden vergelijkbare beperkte uitzonderingen op het verbod. En uiteraard mogen hulpverleners in de gezondheidszorg gezondheidsgegevens verwerken, maar ook slechts voor zover noodzakelijk voor hun taak.<sup>39</sup> Er is echter geen ruimte voor financiële instellingen om bijzondere persoonsgegevens te verwerken. Ook de Wft bevat hiervoor geen uitzonderingen.

Dit betekent dat financiële instellingen alleen bijzondere persoonsgegevens van klanten mogen verwerken als aan één of meer uitzonderingen uit art. 9 lid 2 AVG is voldaan. Dat is het geval als de betrokkene uitdrukkelijke toestem-

23 Zie over die wethistorie bijv. uitvoeriger: M. Jansen, 'KNLTB-boete: wie kaatst kan de bal verwachten of toch een misslag?', *Computerrecht* 2020/180.

24 Vgl. o.a. HvJ EU 24 november 2011, zaak C-468/10, ECLI:EU:C:2011:777 (ASNEF); HvJ EU 19 oktober 2016, zaak C-582/14, ECLI:EU:C:2016:779, r.o. 62 (Breyer); HvJ EU 4 mei 2017, zaak C-13/16, ECLI:EU:C:2017:336 (Rigas).

25 Zie o.a. HvJ EU 4 mei 2017, zaak C-13/16, ECLI:EU:C:2017:336, r.o. 28 (Rigas); HvJ EU 29 juli 2019, zaak C-40/17, ECLI:EU:C:2019:629, r.o. 95 (Fashion ID); HvJ EU 17 juni 2021, zaak C-597/19, ECLI:EU:C:2021:492, r.o. 106 (M.I.C.M.).

26 [https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg\\_gerechtvaardigd\\_belang.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf)

27 Dit laatste is uiteraard een cirkelredenering.

28 Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111.

29 Nog terug te vinden via [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index\\_en.htm](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm)

30 Art. 9 AVG.

31 Art. 4 sub 15 AVG.

32 De Wbp staat voor de Wet bescherming persoonsgegevens, de voorganger van de AVG. Zie hierover uitgebreid voetnoot 3.

33 *Kamerstukken II* 1997/98, 25892, nr. 3, p. 102.

34 HvJ EU 6 november 2003, ECLI:EU:C:2003:596.

35 Sterker nog, het Hof van Justitie bevestigde recent nog dat rechtspraak over de Privacyrichtlijn in beginsel ook van toepassing is op de Privacyverordening: HvJ EU 17 juni 2021, zaak C-597/19, ECLI:EU:C:2021:492, r.o. 107 (M.I.C.M.).

36 Art. 30 lid 1 sub b UAVG.

37 Art. 30 lid 3 sub b UAVG.

38 Art. 30 lid 2 sub a en sub b UAVG.

39 Art. 30 lid 3 sub a UAVG.

ming heeft gegeven<sup>40</sup> en/of als er een noodzaak voor de instelling is in het kader van de uitoefening of onderbouwing van een rechtsvordering.<sup>41</sup> Toestemming ligt echter vanwege onder meer de afhankelijkheidsrelatie bepaald niet voor de hand.<sup>42</sup> En wat precies onder een rechtsvordering is te verstaan is nog onduidelijk. De rechtbank Rotterdam heeft reeds geoordeeld dat dit artikel niet van toepassing is op de buitengerechtelijke fase van geschilafhandeling.<sup>43</sup> En het is gelet op deze uitspraak de vraag of deze uitzondering van toepassing is in KiFiD zaken. Hoewel het privacyrecht dus niet aan bewijsvoering in procedures in de weg staat, kan het – indien de leer van de rechtbank Rotterdam de bestendige leer wordt – in de weg staan en mogelijk van invloed zijn op de voorbereiding (en dossiervorming) van gerechtelijke procedures en op KiFiD zaken.

#### 1.1.6 Strafrechtelijke persoonsgegevens

Van de bijzondere persoonsgegevens te onderscheiden zijn de gegevens betreffende ‘*strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen*’. De verwerking daarvan is op grond van art. 10 AVG voor niet-overheden verboden, tenzij nationale wetgeving verwerking toestaat. Daarnaast bepaalt art. 10 AVG dat registers van veroordelingen alleen onder toezicht van de overheid mogen worden bijgehouden.

Het HvJ EU heeft in een recent arrest benadrukt dat het begrip in de gehele Europese Unie autonoom en uniform moet worden uitgelegd.<sup>44</sup> Er moet worden gekeken naar de kwalificatie van het feit naar nationaal recht,<sup>45</sup> naar de aard van het feit en de zwaarte van de daaraan verbonden sanctie.<sup>46</sup> Het komt erop neer dat alle feiten waaraan een (enigszins substantiële) sanctie is verbonden en bovendien die sanctie een repressief doel dient, de daarmee verband houdende gegevens al snel zullen kwalificeren als strafrechtelijk van aard. Verkeersovertredingen worden door het EHRM in ieder geval in algemene zin als strafrechtelijk gezien<sup>47</sup> en het HvJ EU ziet verkeersovertredingen waarvoor strafpunten worden toegekend in ieder geval als zodanig.<sup>48</sup>

Die grens ligt dus (veel) lager dan tot op heden in Nederlands rechtspraak werd aangenomen. Naar Nederlands recht werd immers onder strafrechtelijke gegevens veelal verstaan ‘*zodanig concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring (...) kunnen dragen*’.<sup>49</sup>

40 Art. 9 lid 1 sub a AVG.

41 Art. 9 lid 1 sub f AVG.

42 Vgl. overweging 32 AVG.

43 Rb. Rotterdam 10 april 2020, ECLI:NL:RBROT:2020:3430, r.o. 4.8.

44 HvJ EU 22 juni 2021, ECLI:EU:C:2021:504, r.o. 85.

45 Met de kanttekening dat de kwalificatie die een lidstaat aan een strafbaar feit geeft niet bepalend is (r.o. 85, slot) en dat ook juist feiten die volgens lidstaten niet strafrechtelijk van aard zijn, dat gelet op de aard van het feit en de zwaarte van de sanctie in Europeesrechtelijke zin wel kunnen zijn (r.o. 88).

46 R.o. 87.

47 R.o. 91.

48 R.o. 92.

49 Vgl. HR 29 mei 2009, ECLI:NL:HR:2009:BH4720.

De nationale wetgeving laat weinig ruimte voor het verwerken van strafrechtelijke persoonsgegevens. Strafrechtelijke gegevens mogen alleen voor intern gebruik worden verwerkt voor, vrij vertaald, eigen zwarte lijsten of in het kader van bewijsvoering van feiten die (dreigen te worden) gepleegd jegens de organisatie of het personeel.<sup>50</sup> Daarbij geldt bovendien dat voor zover personeelsgegevens worden verwerkt, dit moet geschieden overeenkomstig een door de ondernemingsraad goedgekeurd procedé.<sup>51</sup> Strafrechtelijke persoonsgegevens mogen niet met derde partijen worden gedeeld, tenzij de derde tot de groep behoort of er voor het delen een vergunning is verleend.<sup>52</sup> Een voorbeeld van een dergelijke vergunning is overigens het recent door de AP goedgekeurde Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021.<sup>53</sup>

Over hoe deze regels in de praktijk uit kunnen pakken meer bij de casusposities zoals besproken in hoofdstuk 3.

Opmerkelijk is verder dat Nederland het verbod een ruimer toepassingsbereik heeft gegeven. Niet alleen de gegevens als bedoeld in art. 10 AVG mogen niet worden verwerkt, ook de ‘*persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag*’.<sup>54</sup> Dit is gedaan om de regels daaromtrent uit de Wbp te behouden. De regering stelt in de memorie van toelichting bij de UAVG dat de AVG hiertoe ruimte zou bieden.<sup>55</sup> De vraag is of dit standpunt vol te houden is; uitgangspunt is immers dat de AVG leidt tot uniformering van het privacyrecht en nationale afwijkingen slechts mogelijk zijn voor zover de AVG die ruimte biedt.<sup>56</sup>

#### 1.1.7 Procedurevoorschriften

De AVG schrijft verder voor dat organisaties allerlei procedurevoorschriften dienen na te leven. Die zien veelal op het borgen van een rechtmatige verwerking van persoonsgegevens (uitvoeren DPIA, aanstellen F-G, het privacy-statement etc.). Deze werken we hier verder niet uit, maar die komen mogelijk zijdelings aan bod in het vervolg.

50 Dit is vrij vertaald de samenvatting van art. 33 lid 2 UAVG. Dit artikel luidt als volgt: ‘*Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt door de verwerkingsverantwoordelijke die deze gegevens ten eigen behoeve verwerkt:*

*a. ter beoordeling van een verzoek van betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren; of*

*b. ter bescherming van zijn belangen, voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn.’*

51 Art. 33 lid 3 UAVG.

52 Art. 33 lid 5 UAVG.

53 Zie het nieuwsbericht en het goedkeuringsbesluit <https://autoriteitpersoonsgegevens.nl/nl/nieuws/vergunning-voor-financi%C3%ABle-instellingen-om-info-over-fraude-te-delen>. Dit is overigens een herziening van het eerder in 2011 en 2013 goedgekeurde PIFI.

54 Zie de verruimde definitie van ‘persoonsgegevens van strafrechtelijke aard’ in art. 1 UAVG, gelezen in samenhang met art. 31 UAVG dat verwerking alleen toestaat op dezelfde gronden als verwerking van gegevens als bedoeld in art. 10 AVG in Nederland is toegestaan.

55 *Kamerstukken II* 2017/18, 34851, nr. 3, p. 90.

56 Vgl. o.m. AVG considerans 10.

### 1.1.8 Rechten betrokkene

De AVG kent de betrokkene diverse rechten toe. Het betreft het recht van inzage,<sup>57</sup> het recht op rectificatie en vervollediging,<sup>58</sup> het recht op gegevenswisseling,<sup>59</sup> het recht op beperking,<sup>60</sup> het recht op overdraagbaarheid van persoonsgegevens<sup>61</sup> en het recht van bezwaar tegen bepaalde verwerkingen van persoonsgegevens.<sup>62</sup> Betrokkene kan al deze rechten kosteloos uitoefenen, tenzij de verzoeken buitensporig zijn in bijvoorbeeld hun frequentie.<sup>63</sup> Bij twijfel over de identiteit van de betrokkene mag (sterker nog: dat is heel verstandig<sup>64</sup>) om aanvullende identificerende informatie worden gevraagd.<sup>65</sup>

## Privacywetgeving: het toepassingsbereik, de verwerkingsbeginselen, grondslagen, rechten van betrokkenen en handhaving

Daarnaast zijn er in het hoofdstuk ‘rechten van de betrokkene’ enkele aanverwante verplichtingen in de AVG opgenomen, zoals de plichten om het uitoefenen van de rechten te faciliteren,<sup>66</sup> tot transparantie,<sup>67</sup> tot het treffen van maatregelen zodat betrokkene die informatie ook ontvangt,<sup>68</sup> tot kennisgeving aan derde-ontvangers<sup>69</sup> en het verbod om betrokkene te onderwerpen aan uitsluitend geautomatiseerde besluitvorming.<sup>70</sup>

Indien een verzoek van betrokkene niet wordt gehonoreerd, of niet (tijdig) wordt beantwoord, kan betrokkene zich binnen zes weken met een verzoekschrift tot de rechtbank wenden met het verzoek de verwerkingsverantwoordelijke te bevelen het verzoek alsnog te honoreren.<sup>71, 72</sup> Over het overschrijden van die termijn van zes weken wordt in de praktijk verschillend geoordeeld: in de regel wordt betrokkene niet-ontvankelijk verklaard of worden zijn vorderingen afgewezen, doch soms wordt de kwestie inhoudelijk beoordeeld.

57 Art. 15 AVG.

58 Art. 16 AVG.

59 Art. 17 AVG.

60 Art. 18 AVG.

61 Art. 20 AVG.

62 Art. 21 AVG.

63 Art. 12 lid 5 AVG.

64 Het verstrekken van persoonsgegevens aan de onjuiste persoon zal immers al snel kwalificeren als ‘datalek’ dat vervolgens, afhankelijk van het risico, mogelijk moet worden gemeld bij toezichthouder en/of de getroffen betrokkene(n).

65 Art. 12 lid 6 AVG.

66 Art. 12 lid 2 AVG.

67 Art. 13 en 14 AVG.

68 Art. 12 lid 1 AVG.

69 Art. 19 AVG.

70 Art. 22 AVG.

71 Art. 35 UAVG.

72 Art. 35 lid 2 UAVG.

### 1.1.9 Handhaving

De AVG bevat ten slotte een uitgebreide regeling omtrent handhaving. Bij nationale kwesties is de lokale toezichthouder bevoegd, terwijl bij grensoverschrijdende kwesties het coördinatie- en coherentiemechanisme moet worden gevolgd door de toezichthouders. De toezichthouders kunnen allerlei maatregelen treffen, waaronder het opleggen van boetes tot € 20.000.000 of 4% van de wereldwijde omzet. Overigens heeft de AP boetebeleidsregels gepubliceerd op grond waarvan in veel gevallen het boetemaximum in beginsel tot € 1.000.000 beperkt is.<sup>73</sup>

### 1.1.10 Uitleg tegen het licht van grondrechten

Het is vaste rechtspraak dat de AVG en UAVG moeten worden uitgelegd tegen het licht van grondrechten, waaronder het grondrecht op de bescherming van de relationele privacy.<sup>74</sup> Daarbij kan uit verschillende grondrechtencatalogi worden geput; het HvJ EU heeft reeds geoordeeld dat de rechten die in het EU Handvest worden toegekend op gelijke wijze moeten worden uitgelegd als de vergelijkbare rechten die in het EVRM staan.<sup>75</sup>

### 1.2 Grondrechten

Het meest in het oog springende grondrecht in dit kader is art. 8 van het Europees Verdrag voor de Rechten van de Mensen (EVRM). Op grond van dit artikel heeft eenieder het recht op ‘*respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie*’. Het Europees Hof voor de Rechten van de Mens interpreteert het begrip privéleven breed.<sup>76</sup> In de Nederlandse praktijk wordt, ook in privacy zaken, veelvuldig een beroep gedaan op art. 8 EVRM en de op grond daarvan door het EHRM gewezen rechtspraak.

## 2. De achtergronden van (bijzondere) zorgplichten

Op financiële ondernemingen rusten (bijzondere) zorgplichten. De achtergrond hiervan is dat dergelijke professionele aanbieders en adviseurs van financiële producten een maatschappelijke functie en deskundigheid hebben ten opzichte van hun klanten. Deze zorgplichten zijn zowel van civielrechtelijke aard als publiekrechtelijk gegrond.

De civielrechtelijke zorgplicht kent zijn basis in de relatie tussen een financiële onderneming en haar klanten. Deze is meestal te kwalificeren als een overeenkomst van opdracht (art. 7:400 BW e.v.). De Algemene Bankvoorwaarden (‘ABV’) maken veelal deel uit van die overeenkomst van opdracht. Op grond van art. 7:401 BW en art. 2 lid 1 ABV moeten financiële ondernemingen de zorg van een goed

73 *Stcrt.* 2019, 14586.

74 Zie o.m. AVG-considerans overweging 1, 4, 10; HR 9 september 2011, ECLI:NL:HR:2011:BQ8097; HvJ EU 20 mei 2003, ECLI:EU:C:2003:294, r.o. 68-69.

75 HvJ EU 9 november 2010, ECLI:EU:C:2010:662, r.o. 52.

76 EHRM 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. and Marper v. The United Kingdom*).

opdrachtnemer in acht nemen en zoveel mogelijk rekening houden met de belangen van de klant (cliënt). Op grond van de jurisprudentie is de maatstaf die in acht genomen moet worden die van een ‘redelijk bekwaam en redelijk handelend opdrachtnemer’.<sup>77</sup> Wat dit precies inhoudt is afhankelijk van de omstandigheden van het geval.

Hoe financiële ondernemingen jegens hun klanten moeten handelen, wordt eveneens ingevuld door publiekrechtelijke gedragsnormen. In afdeling 4.2.3 van de Wet op het financieel toezicht (‘Wft’) en aanvullende bepalingen in het Besluit Gedragtoezicht financiële ondernemingen Wft (‘BGfo’) zijn publiekrechtelijke regels van zorgvuldige dienstverlening geformuleerd waar financiële ondernemingen zich jegens hun klanten in de contractuele en precontractuele fase aan moeten houden.

De publiekrechtelijke gedragsnormen werken (direct) door in de civielrechtelijke verhouding tussen de financiële onderneming en de klant (cliënt), althans zij geven een nadere invulling van de normen van art. 7:401 BW dan wel 6:162 BW.

Daarnaast wordt de civielrechtelijke (bijzondere) zorgplicht ingekleurd door jurisprudentie. Deze civielrechtelijke bijzondere zorgplicht gaat verder dan de zorgplicht op basis van publiekrechtelijke wetgeving. Volgens vaste rechtspraak van de Hoge Raad *‘rust op de bank als professionele en bij uitstek deskundige dienstverlener een bijzondere zorgplicht bij beleggingsadviesrelaties met particuliere beleggers. Die zorgplicht strekt mede ter bescherming van de cliënt tegen het gevaar van een gebrek aan kunde en inzicht of van eigen lichtvaardigheid.* De reikwijdte van deze bijzondere zorgplicht is afhankelijk van de omstandigheden van het geval, waaronder de mate van deskundigheid en relevante ervaring van de betrokken wederpartij, de ingewikkeldheid van het product en de daaraan verbonden risico’s. Zie HR 28 juni 2019, ECLI:NL:HR:2019:1046 (*rentederivaat ABN AMRO*), r.o. 3.5.2-3.5.5, en HR 5 juni 2009, ECLI:NL:HR:2009:BH2815 (*De T./Dexia*), r.o. 4.4.4, 4.4.5 en 4.8.4.

De (bijzondere) zorgplichten die op financiële ondernemingen rusten, kunnen bij dienstverlening aan consumenten (retailproducten) in de knel komen als gevolg van privacywetgeving. Dit illustreren we hierna aan de hand van een aantal voorbeelden. Het spanningsveld tussen privacywetgeving en zorgplicht is overigens niet beperkt tot deze voorbeelden, maar is breed te zien bij financiële dienstverlening aan consumenten.

### 2.1 De zorgplicht bij kredietverstrekking aan consumenten

Bij het verstrekken van (hypothecair) krediet aan consumenten zijn de zogenaamde *‘Know Your Customer’*-verplichtingen van toepassing. Op grond van art. 4:23 lid 1 sub a Wft moet een financiële onderneming die een

consument adviseert, informatie inwinnen over de financiële positie, kennis, ervaring, doelstellingen en risicobereidheid, voor zover dat redelijkerwijs relevant is voor het advies. De financiële onderneming die adviseert, draagt er op grond van art. 4:23 lid 1 sub b Wft zorg voor dat het advies mede is gebaseerd op de informatie die op grond van sub a vergaard is. De financiële onderneming die zonder advies een financiële dienst verleent (*execution only*), moet op grond van art. 4:24 Wft een passendheidstoets uitvoeren waarbij informatie van de consument wordt ingewonnen om na te gaan of het betreffende financiële product of de dienst passend is voor die consument. Deze bepalingen zijn verder uitgewerkt in Afdeling 8.2 van het Besluit Gedragtoezicht financiële ondernemingen Wft (de ‘Bgfo’).

Bij consumentenkrediet hebben deze bepalingen tevens hun weerslag gekregen in de VFN-Gedragscode en de NVB-Gedragscode Consumptief Krediet (‘NVB-Gedragscode’). Deze Gedragscodes zijn door de sector opgestelde gedragscodes die van toepassing zijn op alle krediet aan consumenten anders dan (kort gezegd) hypothecaire leningen. Op grond van art. 3 a lid 3 en 4 van de VFN-Gedragscode moeten financiële ondernemingen algemeen bekende voorzienbare ontwikkelingen zoals pensioen, meenemen in de advisering. Tevens wordt consumenten gevraagd naar overige voorzienbare ontwikkelingen die van belang kunnen zijn voor het advies. Om aan te kunnen tonen dat deze van belang zijnde factoren meegenomen zijn bij de advisering, ligt het voor de hand om deze gegevens in het klantdossier op te nemen.

### 2.2 De zorgplicht ten aanzien van goed kredietgeverschap

Art. 4:34 lid 1 Wft bepaalt dat de aanbieder van krediet aan een consument voor de totstandkoming van een kredietovereenkomst of een belangrijke verhoging van de kredietlimiet in het belang van de consument informatie moet inwinnen over diens financiële positie en ter voorkoming van overkreditering moet beoordelen of het aangaan van de overeenkomst of de belangrijke verhoging verantwoord is. Dit wordt ook wel de kredietwaardigheidstoets genoemd. Deze kredietwaardigheidstoets is bedoeld om overkreditering tegen te gaan.

Op grond van art. 113 lid 1 Bgfo is de kredietaanbieder verplicht om te beschikken over voldoende schriftelijke, of op een andere duurzame drager vastgelegde informatie aangaande de financiële positie van de consument, om te kunnen beoordelen of het aangaan van het krediet verantwoord is. De norm van ‘goed kredietgeverschap’ die in art. 4:34 Wft juncto 113 Bgfo is vastgelegd, is een open norm.<sup>78</sup> De wetgever heeft het aan de sector overgelaten om de normen voor verantwoorde kredietverstrekking nader uit te werken. De VFN-Gedragscode en de (grotendeels vergelijkbare) NVB-Gedragscode vormen een belangrijke leidraad voor zorgvuldige kredietverstrekking bij

77 O.a. HR 9 juni 2000, NJ 2000/460.

78 M.H.P. Claassen & J.L. Sijnders, ‘Overkreditering bij consumentenkrediet’, MvV 2014, nr. 7/8, p. 3.

consumptief en hypothecair krediet.<sup>79</sup> Voor een uitgebreide uiteenzetting van de kredietwaardigheidstoets bij consumentenkrediet wordt verwezen naar het artikel van Pronk en Bosselaar in het tijdschrift *TvFR* van 23 februari 2021.<sup>80</sup> Om tot een juiste vaststelling van de kredietwaardigheid te komen, heeft de kredietaanbieder veel informatie van de consument nodig. Naast de salarisgegevens zijn er ook nog allerlei andere gegevens nodig. In art. 5 van de VFN-Gedragscode is bepaald om welke gegevens dat kan gaan. Dat kunnen bijvoorbeeld ook alimentatiegegevens, extra ziektekosten, hoge energielasten, kinderopvang of pensioenverplichtingen zijn. Het is volgens de toelichting op de VFN-Gedragscode aan de aanbieder om daar invulling aan te geven.

### (Bijzondere) zorgplichten nopen tot bewaren van persoonsgegevens

Ten aanzien van hypothecair krediet is in art. 2 van de Tijdelijke regeling hypothecair krediet een basisbepaling opgenomen waar de hypotheekverstrekker rekening mee moet houden voor de vaststelling van het toetsinkomen dat de basis vormt voor de bepaling van de kredietwaardigheid. De inkomsten die de hypotheekverstrekker betreft in de vaststelling van het toetsinkomen kunnen zijn: vaste inkomsten, of – als deze ontbreken – de gemiddelde inkomsten van de consument over de laatste drie kalenderjaren, maar ook toekomstige beschikbare inkomsten uit vrij beschikbaar vermogen die redelijkerwijs te verwachten zijn en te verwachten structurele inkomensstijgingen binnen een redelijke termijn. Op grond van art. 4.1 van de Gedragscode Hypothecaire Financieringen die door de NVB in samenwerking met het Verbond van Verzekeraars is opgesteld, mag ook rekening gehouden worden met andere bronnen van inkomsten, zoals vermogen in de vorm van bijvoorbeeld spaargeld of effecten.

Als de kredietwaardigheid niet zorgvuldig wordt vastgesteld en er sprake blijkt te zijn van overkreditering, dan is de kredietaanbieder aansprakelijk. Op de kredietaanbieder rust in dit kader bovendien een zelfstandige onderzoeksplicht, waarbij deze niet zondermeer mag afgaan op door tussenpersonen aangeleverde gegevens, maar deze in voorkomende gevallen door de kredietaanbieder zelf geverifieerd moeten worden. Dat betekent dat in het geval er een tussenpersoon bij de financiële dienstverlening betrokken is, zowel door de tussenpersoon als door de kredietaanbieder de benodigde gegevens van de consument moeten worden vergaard en bewaard. Wordt niet voldaan aan deze bijzondere zorgplicht, dan kunnen zowel de tussenpersoon als de kredietaanbieder aansprakelijk zijn.<sup>81</sup>

79 *Kamerstukken II* 1986/87, 19785, nr. 3, p. 44.

80 W.M.A. Pronk & M.J. Bosselaar, 'De kredietwaardigheidstoets bij consumentenkrediet', *TvFR* 2021, nr. 3, p. 88-96.

81 HR 14 december 2018, ECLI:NL:HR:2018:2298.

Dit alles betekent dat zowel kredietaanbieders, hypotheekverstrekkers als tussenpersonen bij het aangaan van krediet en hypotheek om vele gegevens en inlichtingen van de consument moeten vragen om te voldoen aan de open norm van de kredietwaardigheid. Rechters toetsen ambtshalve of de betreffende financiële ondernemingen deze zorgplicht in acht genomen hebben.<sup>82</sup>

### 2.3 Nazorgplichten van aanbieders en tussenpersonen

Krachtens art. 4:20, lid 1 en 6 Wft is een financiële onderneming gehouden om aan de cliënt informatie te verstrekken *voorafgaand* aan de totstandkoming van een overeenkomst inzake een financieel product (lid 1) zodat de cliënt in staat is om het financiële product of de financiële dienst adequaat te beoordelen. In art. 4:20 lid 3 Wft is de nazorgplicht opgenomen: de financiële dienstverlener moet de cliënt ook *gedurende de looptijd* van de overeenkomst informeren over wezenlijke, voor de cliënt relevante wijzigingen in de informatie die op grond van het eerste lid is verstrekt en eventuele andere, krachtens algemene maatregel van bestuur aan te wijzen onderwerpen. Deze nazorgplicht rust in beginsel op de aanbieder van het financiële product, maar kan op grond van art. 4:21 Wft eveneens op de tussenpersoon (of bemiddelaar) rusten. Hoever deze nazorgplicht gaat, is niet bepaald en is onderwerp van jurisprudentie.<sup>83</sup> De nazorgplicht is (deels) verder uitgewerkt in Afdeling 8.1.6 Bgfo.

Om naar behoren invulling te kunnen geven aan de nazorgplicht is het van belang dat de financiële onderneming over de benodigde informatie van de consument beschikt.

## 3. Enkele casusposities

### Casus 1: Privacywetgeving en de identificatieplicht

Financiële dienstverleners zijn wettelijk verplicht om de identiteit van nieuwe en bestaande klanten te controleren. Dit gebeurt door een geautomatiseerde controle van de echtheidskenmerken van het ID-bewijs. Hiervoor is een onbewerkt ID-bewijs noodzakelijk; bij een bewerkt ID-bewijs zijn de echtheidskenmerken niet goed leesbaar. De Geschillencommissie heeft zich recentelijk uitgelaten over bezwaren die een consument maakte tegen het bewaren van een onbewerkt ID-bewijs. Op grond van het 'noodzakelijkheids criterium' van de AVG heeft de Geschillencommissie geoordeeld dat de bank weliswaar het onbewerkte ID-bewijs moet opvragen om te voldoen aan de identificatieplicht, maar dat uit de Wet ter voorkoming van witwassen en financieren van terrorisme (de Wwft) niet volgt dat het noodzakelijk is om de pasfoto vast te leggen en te bewaren. De bank moet de pasfoto daarom afschermen op de kopie van het ID-bewijs en een watermerk aanbrengen om

82 Voor meer achtergronden over de ambtshalve toetsing wordt verwezen naar C.H.D.W. van den Borne-Verheijen & R.J.M. Sanders, 'Ambtshalve toetsing bij consumentenkrediet', *TvFR*, nr. 7, 24 juli 2021.

83 O.a. is dit voor assurantietussenpersonen aan de orde geweest in het *Bralis/Octant*-arrest, HR 10 januari 2003, «JOR» 2003/76, in Conclusie A-G Wissink 13 oktober 2017, ECLI:NL:PHR:2017:3055, onder 3.6.1 en 3.8, en in diverse KiFiD uitspraken (GC 2018-339, GC 2019-623 en GC 2019-625).

misbruik te voorkomen. Het Burgerservicenummer mag wel opgevraagd, vastgelegd en bewaard worden.<sup>84</sup>

**Casus 2: Privacywetgeving en de kredietwaardigheidsstoets**  
Zoals hiervoor toegelicht is, moeten financiële ondernemingen in het kader van de *Know Your Customer*-verplichtingen en bij de beoordeling van de kredietwaardigheid beschikken over veel persoonsgegevens van consumenten. Op zich zal deze gegevensverwerking te kwalificeren zijn als een wettelijke verplichting, dan wel met zich brengen dat de financiële onderneming een gerechtvaardigd belang heeft om de gegevens te verwerken.<sup>85</sup> Maar deels betreft het de invulling van open normen die door financiële ondernemingen (via gedragscodes of eigen interpretaties) zelf nader moeten worden ingevuld en die in de tijd (mede als gevolg van jurisprudentie) kunnen wijzigen. Financiële ondernemingen zullen deze gegevens bovendien gedurende lange periodes willen bewaren. Er kunnen immers in gerechtelijke procedures vele jaren na die dienstverlening of het aangaan van het product, nog (ambtshalve) toetsingen plaatsvinden over de vraag of voldaan is aan de zorgplichten. Zo moet ten aanzien van de kredietwaardigheidsstoets op grond van jurisprudentie van het HvJ EU aan de hand van toereikende informatie en bewijsstukken door de kredietverstrekker worden aangetoond in hoeverre aan die zorgplicht voldaan is.<sup>86</sup> Maar ook ten aanzien van de passendheid van het advies, kan het voorkomen dat een financiële onderneming jaren na het verstrekte advies in een gerechtelijke procedure moet aantonen dat aan die zorgplicht voldaan is. Het is de vraag hoe deze gegevensverwerkingen van persoonsgegevens vanwege de (bijzondere) zorgplichten zich verhouden tot de privacywetgeving.

Vanuit privacyrechtelijke optiek bezien is het uitgangspunt dat er niet meer gegevens dan noodzakelijk worden verwerkt. Die noodzakelijkheidseis geldt zowel bij de initiële verzameling<sup>87</sup> van de persoonsgegevens als bij de verdere verwerking.<sup>88</sup> Het HvJ EU wijst er in rechtspraak herhaaldelijk op dat het begrip ‘noodzakelijk’ eng moet worden geïnterpreteerd<sup>89</sup> en dat steeds moet worden getoetst of hetzelfde doel niet met minder ingrijpende middelen kan worden bereikt.<sup>90</sup> Bovendien zal, naast de noodzakelijkheidsvraag, steeds moeten worden getoetst of de belangen

van de betrokkene in het concrete geval niet prevaleren.<sup>91</sup> Een dergelijke belangenafweging hangt volgens het HvJ EU altijd af van de specifieke omstandigheden van het geval.<sup>92</sup> Daarbij komt dat het aan de verwerkingsverantwoordelijke (de financiële onderneming) is om op ieder moment te kunnen verantwoorden waarom deze (nog steeds) over de persoonsgegevens beschikt.<sup>93</sup>

Het voorgaande zal in de praktijk niet altijd eenvoudig zijn. Tegelijkertijd kan het wel eenvoudig worden samengevat. De financieelrechtelijke zorgplichten enerzijds en de privacyrechtelijke verplichtingen anderzijds kunnen in de kern worden gezien als twee zijden van dezelfde medaille: indien vaststaat dat de verwerking van persoonsgegevens noodzakelijk is om de zorgplicht na te leven, dan zal die verwerking *in beginsel* vanuit privacyrechtelijke optiek gerechtvaardigd zijn,<sup>94</sup> tenzij het privacybelang van de betrokkene, gelet op de specifieke omstandigheden van het geval, prevaleert. De andere kant van de medaille is echter dat indien niet vaststaat dat de gegevensverwerking noodzakelijk is om de zorgplicht na te leven, de verwerking van persoonsgegevens alleen rechtmatig is als er een andere rechtvaardiging voor die verwerking is aan te wijzen.

Dat roept de vervolgvraag op of alle gegevens die op grond van de zorgplicht worden verzameld daadwerkelijk daarvoor noodzakelijk zijn. Zoals hiervoor uitgewerkt is noodzakelijkheid een strenge toets. Het enkele feit dat het ‘handig’ is om gegevens te hebben zal niet aan dit strenge criterium voldoen. De vraag die bij alle verwerkte persoonsgegevens steeds gesteld moet worden is of de financiële onderneming niet zonder die gegevens aan zijn zorgplicht kan voldoen. Kan niet overtuigend worden beargumenteerd waarom de instelling niet zonder die persoonsgegevens kan, dan zullen de persoonsgegevens (vanuit privacyrechtelijke optiek bezien) moeten worden verwijderd of moeten worden geanonimiseerd.<sup>95</sup>

### Casus 3: Privacywetgeving bij BKR-registraties

Aanbieders van krediet zijn verplicht deel te nemen aan een generiek toegankelijk stelsel van kredietregistratie.<sup>96</sup> Dit stelsel dient onder andere om overkreditering te voorkomen (zie daarover ook hetgeen hiervoor over het toetsen van kredietwaardigheid is vermeld). De Stichting Bureau

84 KiFiD 12 januari 2022, GC 2022-0013.

85 Over het verschil tussen de grondslagen gerechtvaardigd belang en wettelijke verplichting hierna meer uitgebreid bij bespreking van de BKR-registraties.

86 HvJ EU 18 december 2014, zaak C-449/13 (*Bakkaus*).

87 De noodzakelijkheidseis staat immers in alle grondslagen behoudens toestemming als genoemd in art. 6 AVG.

88 Gegevens mogen immers niet langer worden bewaard dan noodzakelijk voor de oorspronkelijke of latere verwerkingsdoeleinden, zie art. 5 lid 1 sub e AVG.

89 Vgl. recent HvJ EU 17 juni 2021, zaak C-597/19, ECLI:EU:C:2021:492, r.o. 110 (*M.I.C.M.*).

90 Vgl. recent HvJ EU 22 juni 2021, zaak C-439/19, ECLI:EU:C:2021:504 (*Puntenrijbewijs*), r.o. 110.

91 Vgl. hierover bijv. HR 9 september 2011, ECLI:NL:HR:2011:BQ8097 (*Santander*).

92 Vgl. o.m. HvJ EU 4 mei 2017, zaak C-13/16 (*Rigas*), r.o. 31.

93 Er geldt immers een verantwoordingsplicht, zie zowel art. 5 lid 2 AVG als art. 24 lid 1 AVG.

94 Ervan uitgaande dat de overige verplichtingen van de privacywetgeving worden nageleefd.

95 Hierbij zij direct aangetekend dat anonimiseren in relatie tot de zorgplicht geen logische route lijkt. Anonimiseren veronderstelt immers het niet-herleidbaar wegnemen van alle identificerende gegevens, terwijl de zorgplicht nu juist ziet op de vraag of ten aanzien van een bepaalde, identificeerbare, klant de juiste zorg in acht is genomen. Na anonimisering zijn de gegevens dus in relatie tot de zorgplicht waardeloos.

96 Art. 4:32 Wft.

Kredietregistratie ('BKR') is de uitvoerder van het enige kredietregistratiesysteem (CKI) in Nederland.

In de praktijk vechten betrokkenen hun BKR-registratie regelmatig aan; wie op [rechtspraak.nl](https://rechtspraak.nl) zoekt op 'BKR' krijgt meer dan 1300 treffers.

Rondom de grondslag is de vraag of alle verwerkingen van persoonsgegevens die verband houden met de kredietregistratie vallen onder de grondslag wettelijke plicht van de AVG (sub c) of gerechtvaardigd belang (sub f). Dat onderscheid is om twee redenen van belang. Vooropstaat dat indien sprake is van een wettelijke plicht, de rechtmatigheid van de verwerking *a priori* is gegeven. Bij de gerechtvaardigdbelanggrondslag zal de verwerkingsverantwoordelijke moeten aantonen dat hij daadwerkelijk een gerechtvaardigd belang heeft. Een andere reden dat de twee grondslagen zoveel aandacht krijgen is dat het recht op gegevenswisseling niet van toepassing is op een wettelijk verplichte verwerking,<sup>97</sup> terwijl gegevenswisseling juist verplicht is wanneer de verwerkingsverantwoordelijke na bezwaar zijn gerechtvaardigd belang bij (verdere) verwerking niet kan aantonen.<sup>98</sup> Dat het stelsel van kredietregistratie een legitiem doel dient is overigens al regelmatig geoordeeld,<sup>99</sup> zij het dat dit enkele feit volgens sommige rechtbanken op zichzelf nog niet de registratie rechtvaardigt.<sup>100</sup> Het verschil in grondslag maakt in zoverre met name verschil voor de bewijspositie van de financiële instellingen.

### Aanbeveling: schep duidelijkheid via een specifieke, sectorale gedragscode of leidraad

De AP wees in de brief van 14 november 2019 de minister van Financiën erop dat de huidige wetgeving inzake het BKR voor kredietaanbieders tekortschiet.<sup>101</sup> De wet bepaalt immers slechts dat de kredietaanbieder moet deelnemen aan een stelsel voor kredietregistratie, maar de wet zelf bevat niet de nadere waarborgen en grenzen die daarbij in acht moeten worden genomen. Dit maakt, volgens de AP, dat kredietaanbieders zich louter op de grondslag gerechtvaardigd belang kunnen beroepen, hetgeen een afweging van geval tot geval vergt. Het hof Den Haag was het eens met de AP dat de grondslag gerechtvaardigd belang, de juiste

grondslag is voor de gegevensverwerking van persoonsgegevens in de AVG. Naar het oordeel van het hof leverde art. 6 lid 1 onder f AVG in elk geval een grondslag op voor de gegevensverwerking door het BKR van de gegevens van de consument. Dat de gegevensverwerking daarnaast noodzakelijk is om te voldoen aan een wettelijke verplichting die op de kredietaanbieder als verwerkingsverantwoordelijke rust, vond het hof niet aannemelijk. De door de kredietaanbieder in dit verband genoemde verplichting is immers de verplichting om deel te nemen aan een stelsel van kredietregistratie. Niet gezegd kon worden dat de kredietaanbieder niet aan die deelnemingsverplichting voldeed als zij de verwerking van de gegevens van de kredietnemer in het CKI staakt.<sup>102</sup>

Het gerechtshof 's-Hertogenbosch was het daar – uitvoerig gemotiveerd – niet mee eens.<sup>103</sup> Volgens het hof was de wettelijke plicht tot deelname aan een stelsel van kredietregistratie een verplichting die *'volstrekt voldoet aan de c-grond als duidelijke en nauwkeurige rechtsgrond'* en was het niet logisch, werkbaar, noch om privacyredenen noodzakelijk om vervolgens onderscheid te maken tussen die verplichting als zodanig en de daaruit voortvloeiende verwerkingen van persoonsgegevens.<sup>104</sup> Het hof wijst er in het kader van dat laatste op dat betrokkene immers altijd, gelet op de *Santander*-rechtspraak,<sup>105</sup> kan stellen dat de verwerking niet voldoet aan de eisen van proportionaliteit en subsidiariteit.<sup>106</sup> Enkele maanden later schaarde het gerechtshof Arnhem-Leeuwarden zich ook achter dit oordeel.<sup>107</sup>

Weer enkele maanden later oordeelde het hof Amsterdam min of meer vergelijkbaar aan het hof Den Haag.<sup>108</sup> De gerechtshoven waren dus verdeeld over de grondslag voor de gegevensverwerking van persoonsgegevens. Moet de gegevensverwerking van het BKR nu gezien worden als een wettelijke verplichting in de zin van art. 6 lid 1 onder c AVG, ofwel als een gegevensverwerking die noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke in de zin van art. 6 lid 1 sub f AVG?

Om daarover uitsluitsel te krijgen, stelde de rechtbank Amsterdam prejudiciële vragen aan de Hoge Raad.<sup>109</sup> Daarbij is niet alleen de vraag gesteld welke grondslag of grond-

97 Art. 17 lid 3 sub b AVG.

98 Art. 17 lid 1 sub c AVG jo. art. 21 lid 2 AVG.

99 Zie o.a. rb. Overijssel 28 mei 2021, ECLI:NL:RBOVE:2021:2147; hof Arnhem-Leeuwarden 7 januari 2020, ECLI:NL:GHARL:2020:126; rb. Midden-Nederland 12 mei 2021, ECLI:NL:RBMNE:2021:3109.

100 Vgl. rb. Amsterdam 22 april 2021, ECLI:NL:RBAMS:2021:3161; rb. Midden-Nederland 6 februari 2018, ECLI:NL:RBMNE:2018:1030; rb. Den Haag 13 december 2019, ECLI:NL:RBDHA:2019:13444; hof Den Haag 18 mei 2021, ECLI:NL:GHDHA:2021:912 (ietwat atypisch wellicht wegens het refereren aan het oordeel van het Hof); rb. Amsterdam 4 maart 2021, ECLI:NL:RBAMS:2021:1721.

101 Autoriteit Persoonsgegevens, brief d.d. 14 november 2019, kenmerk Z2019-19579, [https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies\\_kredietregistratie.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_kredietregistratie.pdf)

102 Hof Den Haag 10 november 2020, ECLI:NL:GHDHA:2020:2068.

103 Hof 's-Hertogenbosch 6 augustus 2020, ECLI:NL:GHSHE:2020:2536.

104 R.o. 3.5.14.

105 HR 9 september 2011, ECLI:NL:HR:2011:BQ8097. De Hoge Raad heeft in die kwestie immers geoordeeld dat *iedere* verwerking van persoonsgegevens, ongeacht grondslag, moet voldoen aan eisen van noodzakelijkheid, proportionaliteit en subsidiariteit en dat de verwerkingsverantwoordelijke desgevraagd een heroverweging zal moeten maken van de belangen in kwestie.

106 R.o. 3.5.15.

107 Hof Arnhem-Leeuwarden 17 december 2020, ECLI:NL:GHARL:2020:10564.

108 Hof Amsterdam 9 februari 2021, ECLI:NL:GHAMS:2021:459.

109 Rb. Amsterdam 21 januari 2021, ECLI:NL:RBAMS:2021:174.

slagen van toepassing zijn, maar ook wat dit betekent voor het recht op gegevenswisseling of het recht van bezwaar. Naar aanleiding van die prejudiciële vragen heeft de Hoge Raad (in navolging van de Procureur-Generaal in zijn conclusie) recent geantwoord dat de grondslag voor de gegevensverwerking gelegen is in het gerechtvaardigd belang.<sup>110</sup> De Wft en Bgfo zijn volgens de Hoge Raad onvoldoende concreet en specifiek om te kunnen concluderen dat sprake is van een wettelijke verplichting tot gegevensverwerking in de zin van art. 6 lid 1 sub c AVG. Gelet op die grondslag is de Hoge Raad van mening dat aan betrokkene het recht van bezwaar toekomt (tweede prejudiciële vraag). Kortom, bij een klacht zal de kredietaanbieder de BKR-gegevens moeten verwijderen, tenzij er goede redenen zijn voor handhaving. De bewijslast ligt aan de zijde van de bank.

#### Casus 4: Privacywetgeving bij nazorgplicht

Zoals hiervoor uiteengezet is, zijn de nazorgplichten die financiële ondernemingen op grond van art. 20 lid 3 Wft hebben, nog niet geheel uitgekristalliseerd. Financiële ondernemingen zullen dus gedurende de hele looptijd van het betreffende financiële product moeten kunnen beschikken over de benodigde persoonsgegevens van cliënten, om (zo nodig) adequaat invulling te kunnen geven aan de nazorgplicht. Hiervoor geldt eveneens de noodzakelijkheidseis die in casus 1 uiteengezet is. Lastig blijft dat er geen sprake is van vaste bakens, maar van een organische invulling van de zorgplichten die in de tijd nogal eens wijzigen als gevolg van jurisprudentie.

Een heel ander vraagstuk is hoe om te gaan met gegevensverwerking bij incassotrajecten. Indien een consument gedurende de looptijd van het krediet in gebreke blijft om te voldoen aan de kredietverplichtingen, wordt door de kredietverstrekker een incassotraject gestart, waarbij (uiteraard) persoonsgegevens verwerkt worden. Stel dat de kredietnemer met wie in het kader van het incassotraject contact opgenomen wordt, meldt dat hij vanwege ziekte of een strafrechtelijke situatie niet langer aan de kredietverplichtingen kan voldoen, dan is de kredietverstrekker mede op grond van de zorgplicht (en bij consumentenkrediet op grond van art. 12 van de VFN-Gedragscode) verplicht om de kredietsituatie te actualiseren, zodat voorkomen wordt dat er een problematische schuldsituatie ontstaat. De kredietverstrekker zal de redenen van de achterstand en de actualisatie van de kredietsituatie vanzelfsprekend willen vastleggen in het kredietdossier. Tegelijkertijd mag de kredietverstrekker deze zeer relevante gegevens van de consument niet verwerken omdat er sprake is van bijzondere persoonsgegevens.

Dit is geen louter theoretisch risico. Illustratief is bijvoorbeeld de last onder dwangsom die in 2019 aan Menzis is opgelegd.<sup>111</sup> De AP had geconstateerd dat marketingmedewerkers in theorie toegang zouden kunnen hebben gehad tot medische gegevens. Dat ging kennelijk niet om de medische dossiers of iets dergelijks, maar om de door de klant zelf gemelde informatie bij het geven van feedback over een zorgverzekering.<sup>112</sup> Menzis nam dan ook het standpunt in dat dit geen medische informatie is, omdat deze informatie voor een heel ander doel wordt gebruikt (namelijk productverbetering).<sup>113</sup> De AP verwerpt dit uitdrukkelijk door te overwegen *'dat ook het enkele gegeven dat iemand ziek is een gegeven omtrent gezondheid is, hoewel dat gegeven op zichzelf nog niets zegt over de aard van de aandoening'*.<sup>114</sup>

Voor financiële ondernemingen geldt waarschijnlijk hetzelfde. Zij mogen geen persoonsgegevens van cliënten verwerken die enigszins verband houden met de gezondheidstoestand van betrokkene. Hetzelfde geldt voor het verwerken van strafrechtelijke persoonsgegevens. Gelet op de ruime uitleg die het HvJ EU aan dat begrip geeft in de kwestie over het puntenrijbewijs, lijkt informatie die verband houdt met enige punitieve sanctie hier al snel onder te vallen. Mocht een betrokkene zich melden met de mededeling dat er betalingsonmacht bestaat wegens opgelegde boetes of een gevangenisstraf, dan lijkt het aldus niet toegestaan dat gegeven te administreren. Hoewel we het privacybelang van die regel zien, schuurt dit wel met de administratie- en zorgplicht die op de financiële onderneming rust. Het lijkt aldus wenselijk dat op dit punt aanvullende wetgeving komt die, onder strikte voorwaarden, financiële ondernemingen de ruimte biedt dergelijke gegevens wel te verwerken.

#### Casus 5: Verbod op geautomatiseerde besluitvorming vs. verplichting tot steeds grootschaliger controles

Tot slot signaleren wij nog dat financiële ondernemingen er niet aan ontkomen om de dienstverlening steeds verdergaand te automatiseren, hetgeen meer en meer zal gaan leiden tot geautomatiseerde besluitvorming.

De AVG verbiedt echter in beginsel geautomatiseerde besluitvorming, tenzij deze noodzakelijk is, bij wet is toegestaan of de betrokkene daarvoor zijn toestemming geeft.<sup>115</sup> Indien de verwerking op de wet is gebaseerd, moet de wet ook aanvullende kaders bieden ter bescherming van de privacy.<sup>116</sup> In andere gevallen zal de verwerkingsverantwoorde-

111 Zie <https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/sancties-voorzorgmenzis-en-vgz-voor-overtreding-van-de-privacywet>

112 Het eigenlijke dwangsombesluit is door anonimisering niet altijd goed te lezen. Uit het invorderingsbesluit blijkt waar de kwestie eigenlijk over ging, namelijk van klanten ontvangen feedback waarin mogelijk terloops medische gegevens stonden. Het staat niet ter discussie dat er geen toegang was tot de medische dossiers.

113 Zie p. 6/7 van het invorderingsbesluit.

114 Invorderingsbesluit, p. 10.

115 Art. 22 AVG.

116 Art. 22 lid 2 sub b AVG.

110 HR 3 december 2021, ECLI:NL:HR:2021:1814 en Conclusie P-G 15 september 2021, ECLI:NL:PHR:2021:831.

lijke, naast het onderbouwen van de noodzakelijkheid,<sup>117</sup> zelf passende maatregelen moeten treffen, waaronder in ieder geval begrepen het recht op menselijke tussenkomst, het recht om het standpunt kenbaar te maken en het recht het besluit aan te vechten.<sup>118</sup> Er mogen, behoudens toestemming, in die niet wettelijk geregelde gevallen bovendien geen bijzondere persoonsgegevens worden verwerkt bij geautomatiseerde besluitvorming.<sup>119</sup>

Opmerkelijk in dat kader is dat in de in internetconsultatie gegeven Verzamelwet gegevensbescherming<sup>120</sup> weliswaar voorzien is in een wijziging van art. 3:17 Wft in het kader van het geautomatiseerd monitoren en blokkeren van betalingstransacties, doch dat hierbij *niet* voorzien is in een uitzondering op het verbod om bijzondere persoonsgegevens te verwerken.<sup>121</sup> Dit lijkt een gemiste kans.

Gelijk zo zou juist deze wet aangegrepen kunnen worden om vast te leggen dat, en onder welke voorwaarden, financiële ondernemingen gerechtigd zijn bijzondere persoonsgegevens (al dan niet via geautomatiseerde besluitvorming) te verwerken. Veel van de hiervoor beschreven onduidelijkheden zouden zodoende weggenomen kunnen worden. Het lijkt op dit punt echter wachten op een nieuwe regering; het wetsvoorstel staat al een behoorlijke tijd stil.<sup>122</sup>

#### 4. Aanbeveling

De hiervoor weergegeven voorbeelden laten zien dat er nog veel onduidelijk is op het grensvlak tussen privacywetgeving en (bijzondere) zorgplicht. Het is onwenselijk dat financiële ondernemingen op dit vlak steeds zelf het wiel moeten uitvinden. De AVG voorziet in de mogelijkheid om gedragscodes op te stellen en deze door de toezichthouder te laten goedkeuren.<sup>123</sup> Tot op heden is in Nederland alleen de 'Data Pro Code' van NLdigital goedgekeurd.<sup>124</sup> Het lijkt

aldus wenselijk dat, in dialoog met toezichthouder AFM, er voor de financiële sector een gedragscode wordt opgesteld die meer concreet invulling geeft aan de vraag welke (categorieën van) persoonsgegevens noodzakelijk zijn voor de invulling van de zorgplicht en hoe in voorkomend geval voor andersoortige persoonsgegevens te rechtvaardigen is dat deze niettemin in het kader van de zorgplicht worden verwerkt. Een dergelijke gedragscode zou vermoedelijk vele hoofdbreken schelen.

#### 5. Conclusie

Privacywetgeving en de (bijzondere) zorgplichten kunnen op onderdelen met elkaar wringen. Een afbakening is lastig wettelijk vast te stellen omdat de invulling van de (bijzondere) zorgplichten met name via open normen en jurisprudentie vorm wordt gegeven. Wel biedt de AVG met de route van gedragscodes mogelijk een vorm om, in samenspraak met alle relevante actoren, tot breed gedragen uitgangspunten te komen. Daar ligt voor de sector een goede kans om de open normen uit de privacywet zelf nader inkleuring te geven. Mocht het niet tot gedragscodes in formele zin kunnen komen, dan zouden in samenspraak tussen AFM en AP vastgestelde en na consultatie van de sector opgestelde leidraden zeer welkom kunnen zijn.

*Dit artikel is afgesloten op 25 januari 2022.*

##### Over de auteurs

**Mr. drs. M. (Mark) Jansen**

Advocaat te Arnhem bij Dirkzwager.

**Mr. C.H.D.W. (Chantal) van den Borne-Verheijen**

Advocaat te Arnhem bij Dirkzwager.

117 In opinie WP251rev01 van de Artikel 29 werkgroep erkennen de privacytoezichthouders dat 'menselijke tussenkomst kan soms eenvoudigweg door de hoeveelheid verwerkte gegevens onpraktisch of onmogelijk zijn', maar ze benadrukken tegelijkertijd wel dat de bewijslast dat een privacyvriendelijker alternatief ontbreekt steeds bij de verwerkingsverantwoordelijke blijft rusten.

118 Art. 22 lid 2 sub 3 AVG.

119 Art. 22 lid 4 AVG.

120 Zie <https://www.internetconsultatie.nl/verzamelwetgegevensbescherming>

121 Terwijl bijv. transacties met religieuze of levensbeschouwelijke instellingen (die kunnen getuigen van levensbeschouwelijke opvattingen, een bijzonder persoonsgegevens) wellicht wel als indicator in dergelijke risicoanalyses worden gebruikt.

122 Zie <https://wetgevingskalender.overheid.nl/Regeling/WGK011059>

123 Art. 40 AVG.

124 Zie [https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011\\_en](https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en) voor een actueel overzicht van in de hele EU goedgekeurde gedragscodes. Het recent goedgekeurde Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021 is geen dergelijke gedragscode; deze vergde goedkeuring vanwege de verwerking van strafrechtelijke gegevens.