Minister voor Rechtsbescherming
De heer S. Dekker
Postbus 20301
2500 EH Den Haag

Privacy
Management
Partners
Coöperatie UA
adres
Vondellaan 58
3521 GH Utrecht
telefoon
+31 85 401 38 66
e-mail
info@pmpartners.nl
website
www.pmpartners.nl
kvk
58176691

Utrecht, 14 juli 2020

Betreft Consultatie Verzamelwet gegevensbescherming
Uw Kenmerk 11059

Geachte heer Dekker,

Dank voor de gelegenheid om via de internetconsultatie te kunnen reageren op het wetsontwerp Verzamelwet gegevensbescherming. De Verzamelwet – zo maak ik op uit de beantwoording van de vragen in het tevens verstrekte integraal afwegingskader – verwoordt de meest wezenlijke uitkomsten van de evaluatie van de Uitvoeringswet AVG die u aan de Tweede Kamer had toegezegd.

Ik reageer als functionaris voor gegevensbescherming in de publieke en private sector, en werk vooral voor gemeenten. FG's zijn die andere toezichthouder waarin de AVG voorziet. FG's die voldoen aan de wettelijke kwaliteitseisen, zijn professionals die in onafhankelijkheid toezien op de naleving van het gegevensbeschermingsrecht op basis van hun wetsexpertise, praktijkdeskundigheid en beroepsvaardigheid.[1] Het zou prettig zijn wanneer u hiermee rekening wilt houden bij de weging van mijn input.

U heeft gelijk, zoals wordt aangegeven in het afwegingskader, dat er in de praktijk sterke behoefte bestaat aan voorlichting en uitleg. Maar dit hangt vooral samen met de manier waarop we in Nederland de AVG toepassen. De AVG zelf is een werkbare en heldere wet. Het zijn met name de FG's die de vertaalslag helpen maken van de wettekst naar de praktijk. Zie hierover ook onze praktijkhandreiking *Hoe ben je FG?*

Het probleem is dat we in Nederland beter zijn in het maken van privacyproblemen dan in het oplossen ervan. De discussies bij de aanvang van de ontwikkeling van de corona-app zijn illustratief. Maar bijvoorbeeld ook de klacht van burgemeester Aboutaleb dat privacy hem belemmert bij zijn uitoefening van taken. Of het rapport

[1] Artikel 37.5 AVG

van de Nationale Ombudsman 'Van wie is die privacy eigenlijk?'. Of de zwartgelakte dossiers van de Belastingdienst in de kinderopvangtoeslag-affaire.[2]

De AVG geldt voor ons allemaal. Privacy is daarmee minder vatbaar voor discussie dan we vaak denken. Het zegt iets over de kwaliteit van onze nationale privacybeleidsvoering dat in Nederland steeds opnieuw discussies kunnen oplaaien en de rechter eraan te pas moet komen om te oordelen. Toch zien we dat gebeuren, waarbij opvalt dat mensen slecht begrijpen wat het recht op gegevensbescherming eigenlijk inhoudt. Zie de recente rechtspraak over verkeerde uitoefening van AVG-rechten bij de gemeente Deventer,[3] rechtspraak over de rechtmatigheid van data-analyse voor fraudebestrijding in de SyRI-discussie,[4] en het oordeel van de rechter dat gebruik van surveillancesoftware bij thuisexamens geoorloofd is.[5]

Modernisering en verbetering van het gegevensbeschermingsrecht

Wat in Nederland nog teveel ontbreekt is evenwichtige normuitleg, management van verwachtingen en een heldere visie op gegevensbescherming. Maar dat biedt kansen. Tijdens de behandeling van het wetsvoorstel UAVG, gaf u aan dat u verdere modernisering en verbetering van het gegevensbeschermingsrecht nastreeft.

Met het wetsontwerp Verzamelwet gegevensbescherming, lost u die belofte nog niet in. De Verzamelwet bevat weliswaar nuttige reparaties, maar geen fundamentele verbeteringen. Waarschijnlijk is een verzamelwet daarvoor ook niet het geschikte instrument. Mijn eigen idee is dat modernisering en verbetering van het gegevensbeschermingsrecht vier actielijnen kent, wanneer ik ook de modernisering en verbetering van publieksvoorlichting meereken. Ik beperk mij hierna echter tot de tot de volgende drie actielijnen:

1. modernisering en verbetering van wet- en regelgeving;
2. modernisering en verbetering van de toepassingspraktijk;
3. modernisering en verbetering van toezicht en handhaving.

In de bijlage licht ik deze actielijnen toe, mede aan de hand van praktijkvoorbeelden. Ik hoop dat ik op die manier kan bijdragen aan de verdere optimalisering van de rechtsbescherming in Nederland.

Indien gewenst, ben ik beschikbaar voor nadere toelichting en uitwerking.

Met vriendelijke groet,

Sergej Katus

_____

Mr. S.H. Katus
Partner / FG

[2] NOS Nieuws 12 december 2019, Kamer neemt geen genoegen met zwartgelakte dossiers kinderopvangtoeslag

[3] Raad van State, 1 april 2020, ECLI:NL:RVS:2020:899

[4] Rechtbank Den Haag, 5 februari 2020, ECLI:NL:RBDHA:2020:865

[5] Rechtbank Amsterdam, 11 juni 2020, ECLI:NL:RBAMS:2020:2917

Bijlage

1 Modernisering en verbetering van wet- en regelgeving

Het streven naar modernisering en verbetering van het gegevensbeschermingsrecht verdient lof. Maar aangezien de AVG al modernisering en verbetering *is* en deze EU-verordening de komende jaren de norm is, liggen de mogelijkheden voorlopig alleen in nationaal beleid en wet- en regelgeving.

Om te beginnen, is het belangrijk om te herhalen dat de AVG de uitwerking is van het recht op bescherming van persoonsgegevens in de zin van artikel 10 Grondwet en artikel 8 EU Handvest Grondrechten. In de AVG gebeurt dat aan de hand van de universele beginselen voor maatschappelijk verantwoord omgaan met persoonsgegevens.[6] Deze beginselen zijn ook herkenbaar in de ethische richtsnoeren van de EU voor kunstmatige intelligentie.[7]

De AVG kun je het beste beginnen te lezen bij artikel 24. Vanaf hier wordt duidelijk hoe het recht op gegevensbescherming precies moet worden gewaarborgd. Via open normen reikt de EU kaders en praktische handvatten aan. Er is alle ruimte voor flexibiliteit en eigen inkleuring. Gegevensverwerking wordt niet verboden of beperkt, maar het gaat er wel om dat dit voortduren met passende waarborgen is omkleed, om personen te beschermen tegen de keerzijden van digitalisering.[8]

Naar analogie met het klimaatbeleid, gaat het in de AVG welbeschouwd óók over duurzaamheid. Verwerking van persoonsgegevens is geen inbreuk op de privacy maar behoort 'klimaatneutraal' plaats te vinden, door middel van het bieden van passende waarborgen waarmee de risico's voor personen worden gemitigeerd. De manier waarop de corona-app momenteel wordt ontwikkeld, is een uitstekend voorbeeld van hoe het wel moet.[9]

De kinderopvangtoeslag-affaire is een voorbeeld van hoe het *niet* moet. Dit niet zozeer omdat gegevens over herkomst worden verwerkt en dit meteen al een privacyprobleem zou zijn. Maar omdat de aanpak krakkemikkig is, waardoor risico's werden gecreëerd voor mensen met een dubbele nationaliteit, die hierdoor schade lijden. Op zich staat artikel 9 AVG toe om gegevens over herkomst te verwerken als dat nodig is. Daarnaast verduidelijkt artikel 22 AVG dat data-analyse en *profiling* geoorloofd zijn, maar niet zonder passende beschermingsmaatregelen waaronder nadrukkelijk 'menselijke tussenkomst'.[10]

De kunst is om de AVG te nemen zoals zij is en Nederlandse wet- en regelgeving in dat licht te bekijken. Daar zijn we nog niet goed in. Met name het AVG-risicobegrip vergt omdenken. Volgens de AVG mogen we alleen van een (privacy)risico spreken wanneer dat blijkt uit objectieve beoordeling.[11] Pas door risico's van gegevens-verwerking te doorgronden, wordt het mogelijk om te voorzien in passende

[6] Artikel 5 en hoofdstuk III en IV AVG zijn uitwerkingen van de duurzaamheidsprincipes in de OECD Privacy Guidelines uit 1980 (revisie 2013) en Convention 108 van de Raad van Europa (revisie 2018)

[7] EU Witboek over kunstmatige intelligentie, 19 februari 2020, COM (2020) 65 final

[8] Artikel 1 AVG

[9] 'Veilige en nuttige corona-app: kan dat?', Tweakers 11 juli 2020

[10] Volgens dezelfde lijnen redeneert de rechter in de SyRI-zaak, aangehaald in voetnoot 4.

[11] Overweging 76 AVG

maatregelen om die risico's tegen te gaan (wie het probleem niet begrijpt, begrijpt ook de oplossingen niet).

Ons nationale gegevensbeschermingsrecht is op een andere leest geschoeid. We zijn gewend om op principiële gronden discussies over privacy te voeren.[12] Als reactie hierop hebben we vanaf de jaren '80 een steeds ingewikkelder systeem gecreëerd van regels, procedures en juridische toetsen – vooral grondslagentoetsen.[13] Wie ervaart dat privacy juridisch complex is of niets zou mogen van de AVG, ervaart waarschijnlijk het oude systeem in een AVG-jasje.[14]

Het AVG-risicobegrip noodzaakt echter om kritischer te zijn en vragen te stellen, zoals: wat zijn precies de voor- en nadelen van gegevensverwerking? Welke omstandigheden veroorzaken de nadelen? Hoe realistisch is het dat die omstandigheden zich voordoen?

Op die manier noodzaakt de AVG om onderscheid te maken tussen reële risico's en theoretische risico's. Met theoretische risico's hoeven we geen rekening te houden. Maar voor de reële risico's hebben we in passende oplossingen te voorzien, zodat de voorziene problemen zich normaal gesproken niet kunnen voordoen.

Modernisering en verbetering van het gegevensbeschermingsrecht begint met het doorlichten van bestaande en voorgenomen wet- en regelgeving op wérkelijke oplossingsgerichtheid – dus een data protectie assessment *van* wet- en regelgeving.[15] Vermoedelijk komen we er achter dat veel rechtsregels zijn gebaseerd op theoretische risico's in plaats van reële risico's. Waarschijnlijk zullen we ook zien dat gegevensbescherming pas tot ontwikkeling komt bij *vermindering* van de regeldruk (minder stoplichtwetgeving, meer rotondewetgeving).

Praktijkvoorbeeld wet- en regelgeving

Artikel 46 UAVG bepaalt dat een nummer dat bij wet is voorgeschreven om een persoon te identificeren, alleen mag worden gebruikt voor de uitvoering van die wet of in andere bij algemene maatregel van bestuur toegestane situaties.

Deze bepaling is met name van belang voor het BSN-stelsel. Dit stelsel bestaat bij de gratie van het argument dat het BSN privacyrisico's inhoudt. Het BSN vergemakkelijk koppeling van gegevens uit verschillende bestanden. Traditioneel zien we dat als een gevaar. In één adem noemen we ook het risico van misbruik van persoonsgegevens en identiteitsfraude.[16]

Maar klopt dat beeld? Het BSN-stelsel is terug te voeren op de invoering van het SoFi-nummer in 1988. Als het BSN echt zo risicovol is, moeten de schadelijke effecten die waren voorspeld in al die jaren en vanwege het grootschalige gebruik van het BSN, zich ook in het echt hebben voorgedaan. In de praktijk gebeuren de dingen immers niet altijd volgens de wet. Maar

[12] Historisch Nieuwsblad 8/2005, 'Het verzet tegen de volkstelling van 1971'

[13] Vgl. prof. J.M.A. Berkvens, *Ontvreemde privacy*, THEMIS 2004-5, p. 267-269

[14] Vgl. 'AVG: beperking of mogelijkheid?', Burgemeesterblad 2019/93, p. 14- 16.

[15] Motie Segers-Oosenbrug, TK 34 000 VII, nr. 21. De minister BZK verwijst in zijn reactie, TK 26 643, nr. 335, overigens naar een toetsmodel dat niet geschikt is voor dit soort wetevaluaties

[16] Webinformatie over het BSN van de Autoriteit Persoonsgegevens, juli 2020

waar zijn de slachtoffers? Hoe groot was hun schade? Wat was precies de casuïstiek? Was het BSN de boosdoener of lag het aan iets anders?

Zo kunnen we ook andere vragen stellen: *is* het BSN eigenlijk wel een identificatienummer? Voor identificatie gebruiken we toch paspoorten, rijbewijzen, identiteitskaarten en, tegenwoordig, DigiD? Is het niet zo dat het BSN is bedoeld om administratieve fouten zoals persoonsverwisselingen tegen te gaan? Is het BSN dan niet eigenlijk een gegevensbeschermings-maatregel in de zin artikel 5.1d AVG (juistheidswaarborg)? En helpt het BSN ook niet om discriminatie tegen te gaan? Uit een nummer als 1043.59.158 kunnen we immers niets afleiden over iemands herkomst – in tegenstelling tot een naam. Waar zijn we precies bang voor als het BSN breder wordt gebruikt én iedereen doet dat met passende waarborgen omkleed? Zou het niet zo kunnen zijn dat mensen juist baat hebben van breder gebruik van het BSN, in plaats van gevaar lopen?

Het zijn dit soort vragen die thuishoren in een DPIA/evaluatie van artikel 46 UAVG. Zonder die DPIA staat de noodzaak van artikel 46 niet vast. Dit zou betekenen dat Nederland te gemakkelijk gebruik heeft gemaakt van de vrije beleidsruimte in de AVG om in zoiets zoals artikel 46 UAVG te voorzien.[17] Modernisering van een dergelijk onderdeel van het Nederlandse gegevens-beschermingsrecht is dan geen optie maar zelfs een *must,* op basis van dwingendrechtelijke EU-harmonisatie.

2 Modernisering en verbetering van de toepassingspraktijk

Het AVG-risicobegrip krijgt vooral uitwerking in hoofdstuk IV AVG. De kern van de zaak is dat besturen van organisaties wordt opgedragen om er voortdurend voor te zorgen dat hun informationele bedrijfsvoering en ketensamenwerking, met passende waarborgen is omkleed.

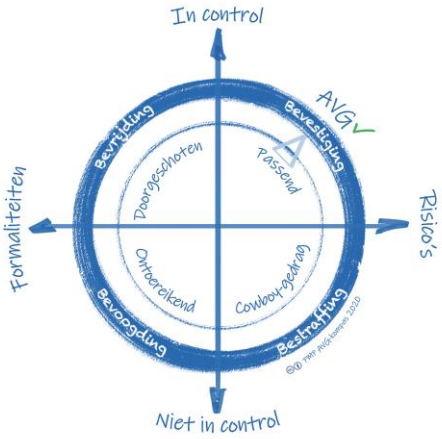
Om uit te vinden wat passend is, zijn opnieuw objectieve risicobeoordelingen nodig. De logische methode hiervoor is de stapsgewijze aanpak die wordt beschreven in artikel 35.7 AVG. De uitkomst ervan levert een lijst op van concrete kwaliteitswaarborgen (KPI's) die in de praktijk moeten worden gebracht.

Het probleem is dat de meeste organisaties in Nederland nog niet op deze manier werken. Ze hebben bij de invoering van de AVG maatregelen genomen die weliswaar in de AVG worden genoemd, maar waarvan de functie niet wordt begrepen. Vaak is gekozen voor de goedkoopste en meest gemakkelijke weg. Of maakten organisaties het zichzelf juist onnodig moeilijk.

Het resultaat is een verspilling van tijd, energie en geld in verkeerde toepassing van de AVG, en daarmee ook niet-passende oplossingen: verkeerd omgaan met de basisprincipes (bijvoorbeeld gegevensminimalisatie), verkeerd omgaan met grondslagen (vooral verkeerd gebruik van toestemming), verkeerde DPIA's, verkeerde verwerkersafspraken, verkeerde verwerkingsregisters, verkeerde FG's, verkeerde rapportages, verkeerde sturing, verkeerde ketenregie.

[17] Artikel 87 AVG

Het hiernaast weergegeven AVG-kompas helpt om beter te begrijpen wat er landelijk aan de hand is. Nu we het derde jaar zijn ingegaan dat de AVG kracht van wet heeft, zou het zo moeten zijn dat alle organisaties een rechtsboven-koers aanhouden, want dat is waar het in de AVG allemaal om draait: passende maatregelen. De meeste organisaties bevinden zich echter in de andere kwadranten van het kompas. De blauwe buitenrand verwoordt de vier bijbehorende stijlen van fair van toezicht.



Zonder de bakens naar rechtsboven te verzetten, is het onmogelijk om het kwaliteitsniveau van de AVG te bereiken. Ondertussen loopt iedereen onnodig risico – door te weinig te doen of teveel.

Praktijkvoorbeeld toepassingspraktijk

Bij de invoering van de AVG werd vrijwel als eerste het verwerkingsregister van artikel 30 AVG gezien. Veel organisaties hebben plichtmatig zoiets aangelegd. De één maakte zich er snel vanaf. De ander bracht uitvoerig alle data in kaart. Nog afgezien een paar enkele andere verplichtingen, wordt nu vaak gedacht: 'We zijn klaar, want we hebben voldaan aan de AVG'.

Maar een verwerkingsregister biedt geen gegevensbescherming – tenminste, niet als zodanig. Het register wordt niet voor niets pas genoemd in artikel 30. Hieraan vooraf gaat het nemen van passende maatregelen volgens artikel 24 en 25. In de rechtsboven-wereld ontstaan verwerkingsregisters op natuurlijke wijze zonder dat dit extra inspanning hoeft te kosten. Ze bieden nuttig inzicht in de AVG-beleidsvoering, en helpen om met vertrouwen verantwoording af te leggen.

Zolang het die functie nog niet heeft, is het 'hebben om het hebben' onzinnig. De AVG was bedoeld om administratieve lasten terug te dringen.[18] Artikel 30 AVG heeft in ieder geval niet tot doel om een verwerkingsregister te introduceren, enkel en alleen om aan de AP te kunnen overleggen – mocht deze er ooit om vragen.[19]

3 Modernisering en verbetering van toezicht

Het is irreëel om ervan uit te gaan dat één toezichthouder eerlijk toezicht kan houden op alle organisaties in Nederland die persoonsgegevens verwerken. Zo telt Nederland momenteel zo'n 1,9 miljoen bedrijven, waarvan het leeuwendeel wordt gevormd door het MKB, waaronder ontzettend veel ZZP'ers.[20] Tel hierbij op alle stichtingen en verenigingen en alle organisaties in de (semi-)overheidssector.

[18] Vgl. Overweging 89 AVG

[19] Artikel 30.4 AVG

[20] Cijfers CBS, aantal bedrijven in Nederland 2e kwartaal 2020.

De AVG gaat dan ook niet uit van één toezichthouder. In de AVG is toezicht op meerdere niveaus geregeld.

- *Toezicht op het niveau van artikel 24-28 AVG* – Organisatiebesturen zijn verantwoordelijk hun risicobeoordelingen, het nemen van passende maatregelen en bewaking van beleid en maatregelen. Incidentenmanagement zoals het reageren op datalekken en inspelen op verzoeken zoals inzage- en correctierechten helpen hierbij. [21]
- *Toezicht op het niveau van artikel 37-39 AVG* – Organisatiebesturen wijzen waar passend een onafhankelijke toezichthouder aan, FG's. De opvatting dat FG's de interne toezichthouder zijn, heeft geen basis in de AVG. Ze kunnen ook extern worden ingehuurd.[22] FG's zijn als het ware de gegevensbeschermingsaccountant van de organisatie.
- *Toezicht op het niveau van artikel 55-59 AVG* – De lidstaten wijzen één of meer toezichthouders aan op landelijk niveau, die samenwerken binnen het EU Comité voor gegevensbescherming (EDPB).

ZZP'ers en andere micro-informatieverwerkers buiten beschouwing gelaten, beschikt Nederland op die manier over zo'n 1 miljoen partijen die de naleving van de AVG in de gaten moeten houden, waaronder duizenden FG's en één AP.

Het probleem in Nederland is dat het gelaagde AVG-toezicht niet van de grond komt. Daarvoor bevinden nog teveel organisaties en hun FG's zich links in het kompas. Tegelijkertijd erkent de Autoriteit Persoonsgegevens het gelaagde toezicht van de AVG niet, wat hierna wordt geïllustreerd aan de hand van het praktijkvoorbeeld. Bovendien komt het gelaagde AVG-toezicht niet van de grond vanwege een strijdigheid van de UAVG met de AVG:

- Artikel 39 AVG geeft aan dat FG's tot taak hebben om toezicht te houden op de naleving van de AVG, gerelateerde wetgeving en het door de organisatie gevoerde gegevensbeschermingsbeleid.[23]
- Artikel 57 AVG bepaalt dat het landelijke toezicht is belast met monitoring en handhaving van de toepassing van – enkel – de AVG .[24]
- In de UAVG is de bewoording van artikel 39 en 57 AVG door elkaar gehaald in artikelen 6.3 en 15.1, waardoor Nederland aan de AP taken heeft opgedragen die in de AVG zijn voorbehouden aan de FG.

De lidstaten kregen niet de ruimte om op dit punt van AVG af te wijken. Europees-rechtelijk prevaleert de AVG.[25] We zitten nu echter wel met de vraag welke activiteiten van de AP zijn gebaseerd zijn op onjuiste toepassing van de AVG (legaliteitsbeginsel). Aangezien de AP zowel de juiste toepassing van de AVG moet monitoren als wetgevingsadvies moet geven, zou het probleem moeten zijn aangekaart.

Meest cruciaal in Nederland is echter dat de FG-functie beter in de verf moet worden gezet. In de praktijk hebben FG's een kwetsbare positie, ondanks hun bescherming

[21] Zie over inzageverzoeken ook HR 16 maart 2018, ECLI:NL:HR:2018:365

[22] Artikel 37.6 AVG. Een extern ingehuurde FG verdient wellicht zelfs voorkeur om boetes te voorkomen zoals de 50.000 euro boete in België.

[23] Artikel 39.1b AVG

[24] Artikel 57.1a-b AVG

[25] In dezelfde lijn: rechterlijke overweging 6.28 van de in voetnoot 4 aangehaalde uitspraak.

volgens artikel 38 AVG. Zo worden FG's gemakkelijk gemarginaliseerd of gepasseerd, of krijgen ze op andere manieren niet de ruimte voor professionele uitoefening van taken, met name in financieel opzicht. Ook druk uitoefenen op de FG komt voor.

Over de FG schrijft het EU Comité voor gegevensbescherming het volgende:

> *Vóór de invoering van de algemene verordening gegevensbescherming [argumenteerden wij al] dat de functionaris voor gegevensbescherming de hoeksteen is van [gegevensbescherming] en dat het aanstellen van een functionaris voor gegevensbescherming [AVG-naleving] kan vereenvoudigen.*
> *(...)*
> *In de algemene verordening gegevensbescherming wordt erkend dat de functionaris voor gegevensbescherming een sleutelfiguur is in het nieuwe systeem voor gegevensbeheer en worden regels voor zijn/haar aanwijzing, positie en taken vastgelegd. (...).*[26]

Goede FG's zitten dicht bij het vuur en zijn degenen die in de praktijk de naleving van de AVG helpen bewerkstelligen - in die zin zijn FG's evenzeer AVG-handhavers. De monitorende taak van AP is toezicht op afstand, door de algemene gang van zaken te bewaken ('systeemtoezicht'). Wanneer FG's er niet uitkomen, kan de AP te hulp schieten. In die taakverdeling ligt ook rechtsbescherming voor organisaties besloten: wie in samenwerking met een gekwalificeerde FG een rechtsboven-koers aanhoudt, verdient het om door de AP met rust te worden gelaten.[27] De AVG is er niet alleen voor de bescherming van personen maar ook voor de rechtszekerheid van organisaties.

Een serieus probleem, tot slot, is het grote verschil kwaliteit tussen FG's. De AP meldt dat inmiddels 10.500 FG's zijn aangemeld.[28] FG's werken vaak voor meerdere organisaties. Het gaat om zo'n 6.000 'unieke' FG's. Uit gesprekken met de AP en vakgenoten komt het beeld naar voren dat maar weinig FG's voldoen aan het wettelijk competentieprofiel volgens artikel 37.5 AVG.[29] Waarschijnlijk voldoet zo'n 5% nu aan de eisen. 15% is veelbelovend en zal daar binnen enkele jaren op eigen kracht in slagen. Maar als dat klopt is 80% van de FG's in Nederland nog onder de maat. Dat is niet alleen kwalitatief problematisch maar e.e.a. werkt ook verstorend op het vlak van aanbod en vergoedingen.

1. Breng artikel 6.3 en 15.1 UAVG in lijn met artikel 39 en 57 AVG
2. Verbeter de rechtsbescherming van FG's, o.m. door een werkbare klokkenluidersregeling
3. Investeer in een landelijk netwerk van kwaliteit-FG's via erkende opleidingen en examens
4. Blaas het initiatief Kwaliteitsregister NRFG nieuw leven in[30]
5. Bevorder bij de AP het systeemtoezicht

[26] EDPB, Richtlijnen voor functionarissen voor gegevensbescherming, WP 243 rev.01

[27] Bij de introductie van de FG in de WBP, eind jaren '90, werd dat al afgesproken. Zie voor een overzicht van parlementaire stukken mijn inbreng bij de 1e internetconsultatie, https://bit.ly/321KHOU.

[28] AP jaarverslag 2019, p. 11

[29] In de praktijkhandreiking *Hoe ben je FG?* wordt het wettelijk profiel uitgesplitst in logische competenties. Zie p. 96-100, 130-133

[30] Dit initiatief kwam tot stilstand door het vertrek van een secretaris-generaal bij het ministerie van JenV

Praktijkvoorbeeld verbetering toezicht

December 2019 legde de AP een boete op van ruim een half miljoen euro aan de tennisbond KNLTB.[31] De AP vindt dat de KNLTB een ernstige overtreding heeft begaan van de AVG. Dit naar aanleiding van klachten van enkele KNLTB-leden in 2018 over nieuwe ledenservice van de KNLTB op basis van samenwerking met bedrijven in de sportsector (ledenkortingsregeling).

Dat de AP klachten zou ontvangen, lag voor de hand. De KNLTB telt ruim 550.000 leden. Hiertussen zitten altijd mensen die bezwaren zien. Van de faciliteiten van de KNLTB om bezwaren kenbaar te maken, was door de klagers geen gebruik gemaakt. In plaats daarvan was men direct naar de AP gestapt, wat de AP aanmoedigt.[32]

In de regel zijn het de FG's die klachten onderzoeken.[33] In het geval van de KNLTB besloot de AP echter om zelf onderzoek in te stellen. Dit leidde tot een doublure want de FG KNLTB (ondergetekende) was zelf ook al aan de slag gegaan, los van de klachten.

AP weigerde om samen te werken met de FG, wat leidde tot een nieuwe klacht – deze keer over belemmering van AVG-taakuitoefening. De AP wees de FG-klacht af onder verwijzing naar artikel 6/15 UAVG. Vervolgens betrok de FG de Nationale Ombudsman. [34] Deze heeft aangegeven dat de rechter de knoop dient door te hakken. Ook wijst de NO erop dat het aan de landelijke politiek is om wet- en regelgeving te controleren, evenals de implementatie daarvan.[35]

Wat het boetebesluit betreft: de FG had de AP in 2018 erover geïnformeerd dat de KNLTB serieus werk maakt van AVG-management (rechtsboven-aanpak). Ook bij de vormgeving van het nieuwe ledenservicebeleid was de AVG een leidend principe. Uit de AVG-risicoanalyse bleek daarnaast dat korting-aanbiedingen geen ernstige risico's voor de leden met zich meebrengen. Dat de AP toch spreekt van een ernstige overtreding de AVG, is verbijsterend. De boete is niet alleen onterecht maar is ook een disincentive voor good governance.

[31] Boetebesluit van 20 december 2019

[32] Promotie via de AP-website en via radio en televisie, zoals in het televisieprogramma Radar.

[33] Artikel 38.4 AVG.

[34] Brief aan de voorzitter van de Autoriteit Persoonsgegevens van 22 februari 2019

[35] Brief van de Nationale Ombudsman van 16 juni 2020