



@zwnne

DINSDAG 7 JUNI 9:00-12:15 | WEBINAR

## ontwikkelingen in privacywetgeving (AVG & UAVG)

Prof. mr. G-J. (Gerrit-Jan) ZWENNE



Universiteit Leiden



1

## interessante debatten over de **toepassing van de AVG** en de **rol van de toezichthouders**

1. vragen over inzage

Prins in NJB

4. nog steeds het gerechtvaardigd belang

3. meldplicht datalekken

5. AVG en collectieve acties en schadevergoeding

Bobek in Conclusie bij X vs AP


2. discussies over begrip «persoonsgegevens»

6. wettelijke plicht of gerechtvaardigd belang?

(de rode draad) 



3

### Als ik op een avond naar een café ga...




toepassing van de AVG

...en tegenover vier vrienden aan tafel in die openbare gelegenheid waarbij ik dus waarschijnlijk niet voldoe aan de uitzondering van de persoonlijke of huishoudelijke activiteit [...] een weinig vleierende opmerking over mijn buurman maak, waarbij ik ook zijn persoonsgegevens vermeld die ik zojuist per e-mail heb ontvangen (dus geautomatiseerd en/of opgenomen in mijn bestand), **word ik dan de verwerkingsverantwoordelijke voor die gegevens en gelden voor mij dan ineens alle (nogal zware) verplichtingen van de AVG? Omdat mijn buurman nooit toestemming heeft gegeven voor die verwerking (verstrekken door middel van doorzending), en omdat roddel waarschijnlijk nooit een van de in artikel 6 AVG opgesomde legitieme gronden zal zijn, zal ik met die verstrekking onvermijdelijk een aantal bepalingen van de AVG schenden, waaronder de meeste rechten van de betrokkene.**





4



### Prins over 'de toezichtreflex' (d.w.z. over AP)



rol van de toezichthouder



Sowieso is het [...] problematisch dat de AP nagenoeg **zonder enige serieuze controle of reflectie** standpunten uitdraagt die zich soms maar moeizaam verhouden met wat rechters of wetgever daarover hebben gezegd. Slechts spaarzaam kunnen deze standpunten door de rechter worden gecorrigeerd.

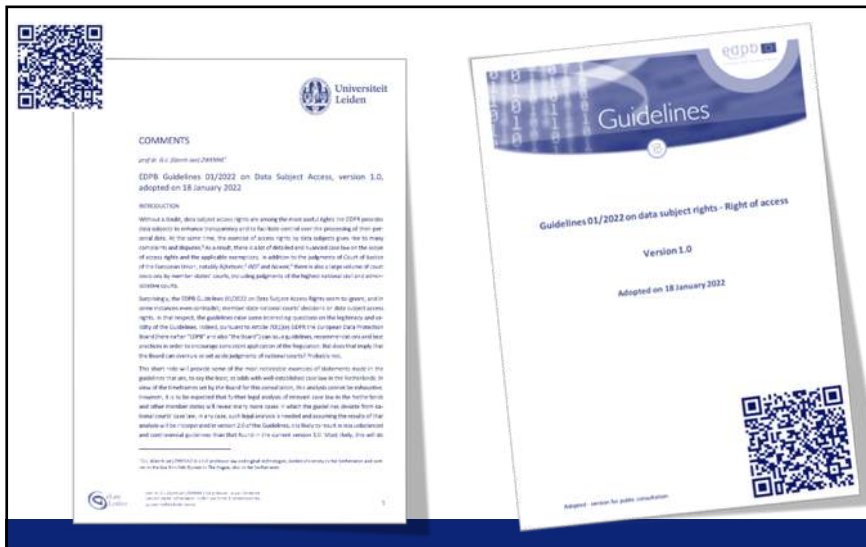
5



6



7



8



9


**EDPB over preciseren**

35 In situations where the controller processes a large amount of data concerning the data subject, the controller may have doubts if a request of access, that is expressed in very general terms, really aims at receiving information on all kind of data being processed or on all branches of activity of the controller in detail. These may arise in situations, where there was no possibility to provide the data subject with tools to specify their request from the beginning or where the data subject did not make use of them. **The controller then faces problems of how to give a full answer while simultaneously avoiding the creation of an overflow of information for the data subject that the data subject is not interested in and cannot effectively handle..**

*EDPB ziet te onbepaalde verzoeken vooral als probleem van de betrokkene, die geen wijs wordt uit de hem te verstrekken gegevens*

*hebben we daarvoor 'tools' nodig en is dat het probleem? waarom niet gewoon de betrokkene vragen zijn verzoek te preciseren?*

*volgens EDPB is het probleem dus vooral 'information overload'*



10


**EDPB over preciseren**

35 There may be ways to solve this problem, depending on the circumstances and the technical possibilities, for example by providing **self-service tools in online contexts** [...]. If such solutions are not applicable, a controller who processes a large quantity of information relating to the data subject may request the data subject to specify the information or processing to which the request relates before the information is delivered (see Recital 63 GDPR). This **exceptional situation** may exist for example in case of a company with several fields of activity or a public authority with different administrative units, if the controller found that numerous data relating to the data subject are processed in those branches as well as in cases where the controller has been collecting data upon frequent activities of the data subject for years.

*myvodafone.nl; mijnneco.nl; mijnoverheid.nl etc.*


*ook voor camerabeelden, bezoekers-registratie, etc..?*

*uitzonderlijke situatie...?*



11

**'fishing expedition'**



Art. 43 Wbp  
De verantwoordelijke kan artikel 35 buiten toepassing laten voor zover dit noodzakelijk is in het belang van: [...]

*(e) de bescherming van de betrokkene of van de rechten en vrijheden van anderen.*


**Hof Den Bosch 11 december 2014, ECLI:NL:GHSHE:2014:5221**  
7.12.8 [H]et hof [is] van oordeel dat het kennisnemingsverzoek van [appellanten] zo weinig concreet is dat gesproken moet worden van een **ontoelaatbare 'fishing expedition'**.

7.12.9. Het voorgaande betekent dat, voor zover daar door de Rabobank nog niet aan was voldaan, de verzoeken van [appellanten] vanwege de onbepaaldheid daarvan moeten worden afgewezen.

*Idem o.a.*  
Hof Den Bosch 1 februari 2018, ECLI:NL:GHSHE:2018:363

12

**'fishing expedition'**



Art. 43 Wbp  
De verantwoordelijke kan artikel 35 buiten toepassing laten voor zover dit noodzakelijk is in het belang van: [...]

*(e) de bescherming van de betrokkene of van de rechten en vrijheden van anderen.*

**AG Wuisman 15 januari 2016, ECLI:NL:PHR:2016:1**  
2.9.1 [...] [V]eeleer valt aan te nemen dat het hof met 'fishing expedition' [...] niet meer heeft aan te geven dan dat het algemene verzoek van [verzoeker] c.s. **een veel te omvangrijke en daarmee kostbare zoektocht binnen bij Rabobank aanwezige documenten, waaronder ook documenten van digitale aard, meebrengt en dat dit in redelijkheid niet van Rabobank valt te vergen.** Dit vindt nog hierin bevestiging dat het hof [...] over het kennisnemingsverzoek van [verzoeker] c.s. opmerkt dat het zo weinig concreet is.

13

## 'fishing expedition'

Art. 43 Wbp

De verantwoordelijke kan artikel 35 buiten toepassing laten voor zover dit noodzakelijk is in het belang van: [...]

(e) de bescherming van de betrokkene of van de rechten en vrijheden van anderen.



**Hof Den Bosch 1 februari 2018, ECLI:NL:GHSHE:2018:363**

3.7.6. In het onderhavige geval is in ieder geval van een concreet en - mede in het licht van de al wel verstrekte informatie - nader onderbouwd verzoek geen sprake. Het voorgaande betekent dat het hof in het onderhavige geval eveneens sprake acht van een 'fishing expedition', nu [appellant] (althans geacht moet worden) slechts een algemeen verzoek heeft (te hebben) gedaan zonder ook maar een begin van verduidelijking te geven waar hij [...] meer duidelijkheid over wenst.

14

## preciseren



Overw. 63 AVG

[...] Wanneer de verwerkingsverantwoordelijke een grote hoeveelheid gegevens betreffende de betrokkene verwerkt, moet hij de betrokkene voorafgaand aan de informatieverstrekking kunnen verzoeken om te **preciseren op welke informatie of welke verwerkingsactiviteiten het verzoek betrekking heeft.**

**Rb A'dam 20 juni 2019, ECLI:NL:RBAMS:2019:4404**

4.11. Integrale honorering van het verzoek van [verzoeker] om alle verwerkte persoonsgegevens zou onder deze omstandigheden niet alle **n welhaast praktisch ondoenlijk zijn** maar ook een veel te omvangrijke en daarmee kostbare zoektocht van [verweerster] meebrengen.

Om aan dit algemene verzoek te voldoen zou [verweerster], alle bij haar aan te treffen documenten – ook die van digitale aard – moeten doorzoeken ten einde daaruit vervolgens die stukken te halen waarin ten minste één persoonsgegeven met betrekking tot [verzoeker] voorkomt en daartoe kosten maken.

Daarbij komt dat in de door [verzoekers] verzochte stukken persoonsgegevens van derden zullen voorkomen, zodat [verweerster] ....

15

## preciseren...



Overw. 63 AVG

[...] Wanneer de verwerkingsverantwoordelijke een grote hoeveelheid gegevens betreffende de betrokkene verwerkt, moet hij de betrokkene voorafgaand aan de informatieverstrekking kunnen verzoeken om te **preciseren op welke informatie of welke verwerkingsactiviteiten het verzoek betrekking heeft.**

**Rechtbank NHLD 23 mei 2019, ECLI:NL:RBNHO:2019:4283**

4.17. Gelet op de grote hoeveelheid gegevens die de rechtbank Amsterdam [verwerkingsverantwoordelijke] verwerkt mag van [verzoekers] worden verwacht dat zij preciseren op welke informatie of welke verwerkingsactiviteit het verzoek betrekking heeft. Dat hebben zij gedaan in het aanvullende verzoekschrift onder I tot en met IX. Voor zover hun verzoek zich ook richt op **andere dan de daarin genoemde gegevens hebben [verzoekers] dat onvoldoende duidelijk gemaakt.**

**Verzoek hoeft niet te worden gemotiveerd. Maar bij veelomvattend verzoek moet verzoeker wél duidelijk maken wat hij/zij wenst in te zien. En waarom(..?)**

16

## algemene zoekslag of diepgravend onderzoek



**Rechtbank NHLD 23 mei 2019, ECLI:NL:RBNHO:2019:4283**

12. [D]e formulering van het verzoek [bepaalt] mede de door het bestuursorgaan te verrichten zoekslag [...]. **In het geval van een algemeen geformuleerd verzoek kan in beginsel van het bestuursorgaan slechts een algemene zoekslag worden gevergd naar de meest gangbare persoonsgegevens (onder meer NAW-gegevens).** Bij een concreter geformuleerd verzoek ligt dit anders. In dat geval kan van een bestuursorgaan een meer diepgravend onderzoek worden gevergd. In eisers geval is sprake van een zeer algemeen geformuleerd verzoek. Voor verweerder was er daarom geen aanleiding om, anders dan eiser meent, ook te zoeken naar andere - minder voor de hand liggende - persoonsgegevens, zoals mogelijk verwerkte IP-adressen van eiser. Dit kon gelet op formulering van het verzoek niet van verweerder worden gevergd. Het IP-adres van eiser is ook geen direct kenbaar persoonsgegeven, dat verweerder bij zijn algemene zoekslag naar eisers persoonsgegevens had moeten betrekken en in het verwerkingsoverzicht had moeten opnemen.


17

### EDPB over het doel van het inzage recht

13. Given the broad aim of the right of access, the aim of the right of access is not suitable to be analyzed as a precondition for the exercise of the right of access by the controller as part of its assessment of access requests. Thus, controllers should not assess “why” the data subject is requesting access, but only “what” the data subject is requesting [...] and whether they hold personal data relating to that individual [...]. Therefore, for example, **the controller should not deny access on the grounds or the suspicion that the requested data could be used by the data subject to defend themselves in court in the event of a dismissal or a commercial dispute with the controller.**

→ *het doel waarvoor de verzoeker het inzage recht gebruikt is niet relevant...*

*betrokkene mag inzage recht gebruiken t.b.v. een ontslagprocedure...*



18

### de uniewetgever over de bedoeling van het inzage recht


**Preambule AVG**  
 (63) Een betrokkene moet het recht hebben om de persoonsgegevens die over hem zijn verzameld, in te zien, en om dat recht eenvoudig en met redelijke tussenpozen uit te oefenen, **zodat hij zich van de verwerking op de hoogte kan stellen en de rechtmatigheid daarvan kan controleren.**

**Preambule RI. 95/46/EG**  
 (41) Overwegende dat een ieder over het recht moet kunnen beschikken toegang te verkrijgen tot de gegevens die het voorwerp van een verwerking vormen en hemzelf betreffen, **zodat hij zich van de juistheid en de rechtmatigheid van de verwerking ervan kan vergewissen; [...]**

*de betrokkene kan zijn inzage recht gebruiken om te controleren of de hem betreffende gegevens kloppen en op een rechtmatige wijze worden verwerkt*

19

### doelstelling van het recht nu en vroeger



**Rb A'dam 9 april 2020, ECLI:NL:RBAMS:2020:2250**


4.20. Het inzage recht was voorheen in artikel 12 van de Richtlijn persoonsgegevens vastgelegd. Dat inzage recht had tot doel de betrokkene in staat te stellen kennis te nemen van de persoonsgegevens die over hem zijn verzameld en te controleren of die gegevens juist zijn en rechtmatig zijn verwerkt.

*Er zijn geen aanwijzingen dat onder de AVG de doelstelling en omvang van dit inzage recht ten opzichte van de Richtlijn persoonsgegevens is gewijzigd. De rechtbank neemt dan ook tot uitgangspunt dat de afspraken van het Hof van Justitie van de Europese Unie (HvJEU) en de Hoge Raad die zijn gewezen over het inzage recht ten tijde van de Richtlijn persoonsgegevens ook gelding hebben nu de AVG van kracht is.*

→ *rechtspraak over art. 35 Wbp of art. 12a RI 95/46/EG heeft onverminderd betekenis voor art. 15 AVG*

20

### rechtspraak over misbruik van het inzage recht



**HR 16 maart 2018, ECLI:NL:HR:2018:365**

3.3.3. [...] Richtlijn 95/46/EG [...] die door de Wbp is geïmplementeerd, [stelt] de betrokkene in staat te controleren of zijn persoonsgegevens juist zijn en rechtmatig zijn verwerkt, ter bescherming van het recht van betrokkene op eerbiediging van zijn persoonlijke levenssfeer. Die controle kan dan leiden tot rectificatie, uitwissing of afscherming van de gegevens. De *onderhavige vordering van [eiseres] is gericht op verkrijging van informatie ten behoeve van de onderhavige procedure en niet op het doel waartoe Richtlijn 95/46/EG strekt. [...] Het gaat hier dus niet om persoonsgegevens in de zin van die richtlijn.*

**Idem:**  
 Rb. NHLD 23 april 2019, ECLI:NL:RBMNE:2019:3762

21



## rechtspraak over misbruik van het inzagerecht

ABRvS 6 november 2019, ECLI:NL:RVS:2019:3754

8. De informatie die [appellant] door middel van de **96 Wob-verzoeken en de 35 Wbp-verzoeken** heeft opgevraagd **houdt verband met dit ontslag uit 2009**. [...] Zoals de rechtbank terecht heeft geoordeeld, is de Wob niet bedoeld om die procedure weer over te doen. Dit geldt eveneens voor de Wbp. [...]

10. De Afdeling [is] van oordeel dat de zwaarwichtige gronden, [die aanwezig zijn als rechten worden gebruikt zonder redelijk doel of voor een ander doel dan waarvoor zij zijn gegeven] zich voordoen. [appellant] heeft **misbruik** gemaakt van de bevoegdheid om Wob- en Wbp-verzoeken in te dienen en daarmee heeft de rechtbank terecht het beroep niet-ontvankelijk verklaard.



Raad  
vanState

22

## rechtspraak over misbruik van het inzagerecht

Rb R'dam 21 januari 2020, ECLI:NL:RBROT:2020:515

4.8 [...] Het inzagerecht heeft tot doel de betrokkene in staat te stellen kennis te nemen van de persoonsgegevens die over hem zijn verzameld en te controleren of die gegevens juist zijn en rechtmatig zijn verwerkt. Ter gelegenheid van de mondelinge behandeling heeft [verzoeker] verklaard dat hij deze verzoeken uitsluitend heeft ingediend om zijn onschuld te bewijzen met stukken die betrekking hebben op

**procesaassiers waarin hij als procespartij betrokken was. Voor zover moet worden geconstateerd dat het doel dat [verzoeker] nastreeft geen betrekking heeft op het controleren of zijn persoonsgegevens juist zijn en rechtmatig zijn verwerkt, maar het te doen is om informatie te verkrijgen die hij wil gebruiken om in een eventueel tegen de Staat te starten procedure (nader) bewijs van zijn onschuld te kunnen leveren.**

Met het van [verzoeker] bij zijn inzageverzoek uitgaan op de bescherming van persoonsgegevens zodat sprake is van **misbruik van recht**.



23

## identificeren verzoeker

### rechtsvragen

- mag een **kopietje paspoort** worden gevraagd om de identiteit van verzoeker vast te stellen?
- en mag worden verlangd dat verzoeker zich **in persoon** identificeert door met ID-bewijs langs te komen?

Art. 12 AVG

6. [D]e verwerkingsverantwoordelijke [kan], wanneer hij redenen heeft om te twifelen aan de identiteit van de natuurlijke persoon die het [inzage]verzoek indient, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.

Wilt u op grond van de Algemene verordening gegevensbescherming (AVG) inzage in uw persoonsgegevens? Dan is de organisatie waarbij u inzage vraagt wettelijk verplicht uw identiteit vast te stellen. Maar de wet geeft niet aan hoe een organisatie dat moet doen.

identiteit vaststellen:  
De organisatie moet uw identiteit vaststellen om te voorkomen dat iemand door uw naam te gebruiken inzage in uw gegevens kan krijgen. Hoe gemakkelijker de gegevens, hoe meer waarborgen er nodig zijn.

identiteitsbewijs niet altijd nodig:  
De organisatie mag niet zomaar vragen om uw identiteitsbewijs, zoals uw paspoort of identiteitskaart. Kan de organisatie uw identiteit ook op een andere, minder vervaagde manier vaststellen? Dan moet de organisatie voor die manier kiezen.



24

Raad  
vanState

ABRvS 9 december 2020, ECLI:NL:RVS:2020:2833

5.1. [I]n beginsel [heeft het college] ten aanzien van de wijze waarop zij de identiteit van de verzoeker wil vaststellen beleidsruimte [...]. Die ruimte wordt mede bepaald door enerzijds het uitgangspunt dat de **identiteitsvaststelling deugdelijk moet zijn**. Anderzijds door het gegeven dat de identiteitsvaststelling **niet zo belemmerend** mag werken dat daarmee aan het recht van de betrokkene zich vrijelijk tot het college te wenden met een inzageverzoek afbreuk wordt gedaan.

5.2. Het uitgangspunt dat een **kopie van een identiteitsbewijs** wordt gevraagd bij een inzageverzoek, wordt **niet onredelijk geacht**. Dit waarborgt een deugdelijke identiteitsvaststelling zonder dat afbreuk wordt gedaan aan het recht van betrokkenen om zich vrijelijk tot het college te wenden. Het college heeft in dit geval opgemerkt dat de **handtekening op het verzoek en op het paspoort niet overeen kwamen met de handtekening op eerder ingediende Wob-verzoeken** van een persoon met dezelfde naam die woont op hetzelfde adres. Het kon zich daarom in redelijkheid op het standpunt stellen dat daardoor twijfel is ontstaan over de identiteit van de verzoeker en alleen een kopie van het paspoort in dit geval niet voldoende was





25

**ABRvS 9 december 2020, ECLI:NL:RVS:2020:2915**

5.1. Het college vraagt standaard [...] om langs te komen op het gemeentehuis om zich te identificeren. Voor [appellant], die aan de andere kant van het land woont, betekent dit dat hij heel ver zou moeten reizen. Er waren in dit geval ook andere mogelijkheden om de identiteit vast te stellen, die een lagere drempel opwerpen. Het overleggen van een kopie van een paspoort wordt bijvoorbeeld in beginsel als een redelijke maatregel aangemerkt om de identiteit te controleren. [...].

[appellant] had een kopie van een gewaarmerkte kopie van zijn paspoort overgelegd. Het college kon aan de hand hiervan zijn identiteit controleren. Zoals het college ter zitting heeft toegelicht, twijfelde het niet aan de identiteit van [appellant]. Er bestond daarom geen reden om aanvullende informatie te vragen of aanvullende eisen te stellen. Dat het mogelijk is om een kopie te vervalsen en dat de gewaarmerkte kopie niet op de juiste wijze gewaarmerkt is, zoals het college heeft aangevoerd, maakt dat niet anders, omdat het college zelf te kennen heeft gegeven dat het niet vermoedde dat de kopie vervalst was of dat er mogelijk een ander persoon achter het verzoek zou zitten. De eis van het college was in dit geval daarom geen redelijke maatregel. De rechtbank heeft ten onrechte geoordeeld dat het college in redelijkheid van [appellant] heeft mogen eisen om langs te komen op het gemeentehuis.





26

**EDPB over het identificeren van de verzoeker**

73. It should be emphasized that using a copy of an identity document as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and as such it should be considered inappropriate, unless it is strictly necessary, suitable, and in line with national law. In such cases the controllers should have systems in place that ensure a level of security appropriate to mitigate the higher risks for the rights and freedoms of the data subject to receive such data. It is also important to note that identification by means of an identity card does not necessarily help in the online context (e.g. with the use of pseudonyms) if the person concerned cannot contribute any other evidence, e.g. further characteristics matching to the user account.

kopietje paspoort of ID-kaart is niet passend  
 maar wat mag dan wel...?



27

**vragen over de taken van de EDPB ('het Comité)**

**Art. 70 AVG**

1. Het Comité zorgt ervoor dat deze verordening consequent wordt toegepast. Daartoe doet het Comité op eigen initiatief of, waar passend, op verzoek van de Commissie met name het volgende: [...]

(e) onderzoeken, op eigen initiatief of op verzoek van een van zijn leden dan wel op verzoek van de Commissie, van kwesties die betrekking hebben op de toepassing van deze verordening, en uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken om te bevorderen dat deze verordening consequent wordt toegepast

betekent dit dat de EDPB kan voorbijgaan aan de nationale rechter...?  
 of dat EDPB-richtsnoeren voorgaan op rechterlijke uitspraken...?



28

**toetsvraag 1**

De Afdeling vindt het uitgangspunt dat een kopie van een ID-bewijs wordt gevraagd bij een inzageverzoek, niet onredelijk

A. Dit is juist  
 B. Dit is onjuist

29

rol van de toezichouder

[2]  
persoonsgegevens, of niet?

over passententellingen en  
wifitracking in Enschede

30

**Boete gemeente Enschede om wifitracking**

18 april 2022

De Autoriteit Persoonsgegevens (AP) geeft de gemeente Enschede een boete van 600.000 euro, omdat de gemeente wifitracking gebruikte in de binnenstad op een manier die niet mag. Daardoor was het mogelijk winkelend publiek en mensen die in de binnenstad wonen of werken te volgen.

**Wifitracking in Enschede**


De gemeente Enschede besloot in 2017 om via sensoren de drukte in de binnenstad te gaan meten. De gemeente huurde daarvoor een bedrijf in dat is gespecialiseerd in het tellen van passanten.

Meetkastjes in de winkelstraten vingden wifi signalen op van de mobiele telefoons van passerende mensen. Ieders telefoon werd apart geregistreerd, met een unieke code.

Door te tellen hoeveel telefoons er op een bepaald moment rond een meetkastje zijn, weet je hoe druk het is. Houd je over een langere periode bij welke telefoon langs welk meetkastje komt, dan verandert dit 'tellen' in het volgen van mensen.

Uit onderzoek van de AP bij de gemeente Enschede blijkt dat dit aan de hand was. De privacy van burgers was dus niet goed gewaarborgd, omdat zij konden worden gevolgd zonder dat dit noodzakelijk was.

Het was niet de intentie van de gemeente om individuen te volgen. En de AP heeft ook geen aanwijzingen gevonden dat dit is gebeurd. Maar het inzetten van wifitracking die dit mogelijk maakt, is op zichzelf al een ernstige overtreding van privacywet AVG.



31

*Is er sprake van «persoonsgegevens»...?*

alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon

→ "de betrokkene" of "data subject"

*kost het al dan niet een onevenredige inspanning om de betrokkene te identificeren?*

*is alleen een uniek nummer (IP-adres, Mac-adres) voldoende om te spreken van identificatie..?*

*maar, wat is identificeren eigenlijk..?*

*is «single-out» of «onderscheiden van anderen» voldoende om te spreken van identificeren?*

32

**«identificeerbaar»**

Art. 4(1) AVG  
als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identicator  
bijvoorbeeld een naam, identificatienummer, locatiegever, online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

(26) [...] Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.

(30) Natuurlijke personen kunnen worden gekoppeld aan online-identificatoren via hun apparatuur, applicaties, instrumenten en protocollen, zoals internetprotocol (IP)-adressen, identificatiecookies of andere identificatoren zoals radiofrequentie-identificatietags. Dit kan sporen achterlaten die, met name wanneer zij met unieke identificatoren en andere door de servers ontvangen informatie worden gecombineerd, kunnen worden gebruikt om profielen op te stellen van natuurlijke personen en natuurlijke personen te herkennen.

*IP-adres, MAC-adres*

33



«*identificeren*» wat is dat eigenlijk..?

~ **vaststellen wie iemand is:** ze hebben de dode geïdentificeerd

~ **aantonen wie je bent:** kunt u zich identificeren?

**zich** ~ voorstellen dat hij een ander is: hij identificeert zich met het slachtoffer

**Art. 27a WvSv**  
De verdachte wordt ten behoeve van het vaststellen van zijn identiteit gevraagd naar zijn naam, voornamen, geboorteplaats en geboortedatum, het adres waarop hij in de basisregistratie personen is ingeschreven en het adres van zijn feitelijke verblijfplaats. Het vaststellen van zijn identiteit omvat tevens een onderzoek van een identiteitsbewijs


34

NN.PL133C.V.071030.100

HR 4 september 2012  
ECLI:NL:HR:2012:BX4153

verdachte weigert bekend te maken wie zij is en daarom wordt zij in de stukken aangeduid met een nummer

zo een verdachte wordt aangemerkt als een **anonieme, d.w.z. niet geïdentificeerde** verdachte



35

*deugdelijke vaststelling van identiteit*

Artikel 12 AVG  
6. [...] [D]e verwerkingsverantwoordelijke [kan], wanneer hij redenen heeft om te twifelen aan de identiteit van de natuurlijke persoon die het verzoek indient als bedoeld in de artikelen 15 tot en met 21, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.

Alle antwoorden op mijn vragen

**Vragen over het recht op inzage**

Hoe weet een organisatie of ik het ben als ik een inzageverzoek doe?

Voordat de organisatie uw inzageverzoek in behandeling neemt, zal de organisatie meestal controleren wie u bent. Zij kan dat op verschillende manieren doen.

Minst privacygevoelig  
Wil een organisatie uw identiteit controleren? Dan moet zij daarvoor die manier kiezen die het minst privacygevoelig is.

Het is bijvoorbeeld lang niet altijd noodzakelijk om een kopie van uw identiteitsbewijs te vragen. Vraagt u bijvoorbeeld om inzage bij een webshop? Dan is uw klantnummer **of in combinatie met** uw naam en adres meestal genoeg om uw identiteit te verifiëren.

36

«*single-out*»...?

[data subject is] a natural person person who can be **identified or singled out**, directly or indirectly, alone or in combination with associated data, by means reasonably likely to be used by the controller ...

Draft LIBE-report of Albrecht January 2013

Art. 4(1) AVG


[data subject is] an identifiable natural person is one who can be identified, **or singled out**, directly or indirectly, in particular by reference to an identifier

...


37

### kamerbrief

Wat artikel 4 (begripsbepalingen) betreft, is er geen enkele steun voor het verder verfijnen van het begrip «persoonsgegevens» met categorieën als «singling out». De voorgestelde definitie lijkt Nederland en veel lidstaten al gecompliceerd genoeg.



Kamerstukken II 2012/13, 32761, nr. 51




38

### HvJEU: Bodil Lindqvist

EHvJ 6 november 2003, C-101/01, ECLI:EU:C:2003:596

24. Het in [...] begrip persoonsgegevens omvat volgens de definitie in artikel 2, sub a, daarvan iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Hieronder valt vanzelfsprekend iemands naam tezamen met zijn telefoonnummer of gegevens over zijn werksituatie en zijn liefhebberijen. [...]

27. Derhalve moet op de eerste vraag worden geantwoord, dat het vermelden van verschillende personen op een internetpagina met hun naam of anderszins, bijvoorbeeld met hun telefoonnummer of informatie over hun werksituatie en hun liefhebberijen, als een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens [...] is aan te merken.




39

### HvJEU: Scarlet SABAM

51 Het staat namelijk vast dat het rechterlijk bevel tot invoering van het litigieuze filtersysteem een systematische analyse van alle inhoud veronderstelt en de verzameling en identificatie van de IP-adressen van de gebruikers die illegale inhoud via het netwerk versturen. Aangezien die IP-adressen de precieze identificatie van die gebruikers mogelijk maken, vormen zij beschermde persoonsgegevens..

HvJEU 24 november 2011, C-70/10



40

### HvJEU: Breyer

Zie ook: HvJEU 17 juni 2021, C-597/19, ECLI:EU:C:2021:492, nr. 102

HvJEU 19 oktober 2016 C-582/14 ECLI:EU:C:2016:779

[E]en dynamisch IP-adres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als een persoon een website bezoekt die door deze aanbieder toegankelijk wordt gemaakt voor het publiek, ten aanzien van die aanbieder [vormt] een persoonsgegeven [...], wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust.



ISP extra informatie vereist voor identificatie

website dynamisch IP-adres


wettige middelen..?

41

### Rb DHG: fietsendepot

Rechtbank Den Haag 20 oktober 2020, ECLI:NL:RBDHA:2020:9590

7. [V]erweerder [heeft] aannemelijk gemaakt dat binnen de gemeente Den Haag géén IP-adressen worden vastgelegd, opgeslagen en gekoppeld aan personen. Er is dan ook geen sprake van directe of indirecte herleidbaarheid naar personen. Daartoe is van belang dat verweerder heeft toegelicht dat IP-adressen indirecte herleidbaarheid kunnen zijn tot een persoon, maar dat daarvoor middelen moeten worden ingezet om dit te kunnen vaststellen. Verweerder heeft daarbij aangegeven dat het ondoenlijk qua tijd en mankracht is om van alle burgers met wie gecommuniceerd wordt, de identificatie via een IP-adres te achterhalen. Daarbij is van belang dat de gemeente niet zelf over de gegevens die een koppeling kunnen maken tussen een IP-adres en een burger beschikt, maar zijn er gegevens nodig van een Internet Service Provider. Nu de verwerking een excessieve inspanning van verweerder vergt, waardoor het gevaar voor identificatie in de praktijk onbeduidend is, kan het IP adres niet beschouwd worden als persoonsgegevens.




42

### Rb. MNL: Brein/Ziggo

Rechtbank Midden NLD 2 februari 2022 ECLI:NL:RBMNE:2022:297


Een IP-adres is dus een persoonsgeven voor degene die wettelijke mogelijkheden heeft om dat IP-adres met behulp van informatie van een isp aan een persoon te koppelen. Uit het [Breyer]-arrest lijkt te volgen dat het begrip “wettelijke mogelijkheden” door het Europese Hof ruim wordt opgevat. In het Breyer-arrest is immers overwogen dat van die wettelijke mogelijkheden geen sprake is indien de identificatie van de betrokkene bij de wet verboden wordt of in de praktijk ondoenlijk is, bijvoorbeeld omdat zij – gelet op de vereiste tijd, in werkelijkheid onbeduidend lijkt. De voorzieningenrechter concludeert daarom dat de mogelijkheid om (al dan niet via de rechter) NAW-gegevens van de gebruiker van een IP-adres bij de isp op te vragen, wel onder de in het Breyer-arrest bedoelde wettelijke middelen valt.

gegevens bij Ziggo op te vragen (en, wanneer dat zonder succes blijft, deze van Ziggo te vorderen) en dat het niet zeker is dat – als zij dat wel doet – zij die gegevens ook verkrijgt, doet er niet aan af dat zij wel over dat wettelijke middel beschikt, dat de daarmee gemoeide tijd, kosten en mankracht niet excessief zijn in de genoemde zin en dat de IP adressen die Brein verzamelt dus ook ten aanzien van haar gelden als persoonsgegevens.



43

### terug naar Enschede: geen onevenredige inspanning, zegt AP



Bij [LEVERANCIER] is [...] de exacte locatie van de sensoren bekend en heeft men toegang tot het werkgeheugen en de software die draait op elke sensor. Tegelijk met een nieuwe detectie van een mobiel apparaat door een sensor is het bijvoorbeeld voor iemand van [LEVERANCIER] mogelijk om ter plaatse of via een camera waar te nemen welke persoon binnen het bereik van de sensor komt lopen. Vooral op stille momenten in de binnenstad leidt dit direct tot identificatie van de natuurlijke persoon. Ter controle kan de persoon worden gevraagd naar zijn/haar MAC-adres. Deze locatie van identificeren is mogelijk in geval van gepseudonimiseerde MAC-adressen en de bijbehorende locatiegegevens, omdat ook dan op het moment van detectie ter plaatse of via een camera de persoon in kwestie waargenomen kan worden

alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt...?

44

### toetsvraag 2

De rechtbank Den Haag vond dat de Gemeente Den Haag geen inzage hoefde te geven in de IP-adressen die waren geregistreerd.

A. Dit is juist  
B. Dit is onjuist

45



rol van de toezichouder

## [3] meldplicht datalekken

een vernieuwd en verbeterd  
meldloket

46

## meldplicht datalekken

**melding bij toezichouder**

tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen

**melding bij betrokkene**

waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen

Art. 33  
AVG

Art. 34  
AVG



**Wie?**  
verwerkingsverantwoordelijke

**Wat?**  
inbreuk op beveiliging van persoonsgegevens

**Wanneer?**  
onverwijld d.w.z. in beginsel binnen 72 uur na bekend worden van het datalek

**Hoe?**  
Meldloket Datalekken (AP)  
zo-mogelijk individueel (betrokkenen)

47



**AP legt Uber boete op voor te laat melden datalek**

**Haga beboet voor onvoldoende interne beveiliging patiëntendossiers**

**Boete voor ziekenhuis vanwege overtreden AVG**

**Rb DHG 31 maart 2021, ECLI:NL:RBDHA:2021:3090**  
[Haga heeft] ten tijde van belang **wel maatregelen [...] genomen** om te voorkomen dat persoonsgegevens in het digitale patiëntendossier worden ingezien door onbevoegde medewerkers, zoals onder meer de invoering van een **extra waarschuwing** die in beeld komt als een medewerker een dossier opent, de verplichtstelling van een **e-learningcursus** voor alle medewerkers die toegang hebben tot het elektronische patiëntendossier, de aanscheping van de **arbeidsovereenkomsten** en het waar mogelijk aanscherpen van **autorisaties**.

€110.000

48

**UWW krijgt boete voor slechte beveiliging bij verzending groepsberichten**

**AP: Boete orthodontiepraktijk vanwege onbeveiligde patiëntenwebsite**

**Boete PWW Overijssel vanwege niet melden datalek**

**Boete Booking.com voor te laat melden datalek**

**Ziekenhuis OLVG beboet om onvoldoende beveiliging medische dossiers**

**AP beboet Transavia om slechte beveiliging persoonsgegevens**

49

### toetsvraag 3

Uber kreeg van AP een boete van 6.000.000 euro voor het te laat melden van een datalek

A. Dit is juist  
B. Dit is onjuist

50

**Meldplicht datalekken: facts & figures**  
Overzicht feiten en cijfers 2020

Aantal meldingen: 23.976

Meerjarentrend: ↑ 30%

Stijging meldingen hacking & malware

Rapportage Datalekken 2020

Dit wetsvoorstel leidt voor het Cbp tot enkele nieuwe bestuurlijke lasten. De meldplicht bij doorbrekingen van beveiligingsverplichtingen leidt, naar thans wordt geschat tot 66.000 meldingen per jaar.

KST II 2012/13, 33662, nr. 3 p. 17

Onderstaande grafiek laat het verloop van het aantal datalekmeldingen sinds 2016 zien:

Deze grafiek toont het aantal ontvangen datalekmeldingen per maand in 2020:

51

**Jaarverslag AP 2021, p. 20**

**Wat de AP niet kon doen**

De AP heeft een zeer groot en divers taakdomein. Daarnaast heeft de AP een omvangrijk pakket aan wettelijke taken. Om effectief te zijn als toezichhouder, is het van belang dat de AP voldoende middelen en capaciteit heeft om deze taken uit te voeren.

Door tekorten in capaciteit en middelen heeft de AP, net zoals in 2020, in 2021 scherpere keuzes moeten maken. De AP heeft gekozen voor de activiteiten waarbij de impact voor burgers het grootst is. Hierdoor heeft de AP andere activiteiten niet of minder kunnen doen. Ook nemen de achterstanden bij activiteiten nog steeds toe.

**Klachten**  
Veel burgers dienen een klacht in over organisaties die de AVG niet naleven. De AP moet deze klachten behandelen, maar is onvoldoende in staat om organisaties waarover wordt geklaagd aan te spreken op hun gedrag. Of om er door middel van onderzoek en handhaving voor te zorgen dat zij de AVG alsnog gaan naleven.

**Datalekmeldingen**  
Er kwamen in 2021 ongeveer 25.000 meldingen binnen van datalekken. Slechts bij enkele honderden meldingen kan de AP actie ondernemen, bijvoorbeeld door organisaties aan te spreken op hun werkwijze en hen te helpen deze te verbeteren. Of door een onderzoek te starten naar de mate waarin een bedrijf voldoende beveiligingsmaatregelen had getroffen.

**Verkennde onderzoeken**  
De AP doet ook onderzoeken die niet direct gericht zijn op handhaving, maar die zijn bedoeld om te zien of bepaalde sectoren voldoen aan verplichtingen uit de AVG. De toezichten uit een verkennend onderzoek vormen onder andere input voor risicoanalyses ten behoeve van de risicotaxatie van de AP. Door de geringe capaciteit in 2021 heeft de AP slechts twee onderzoeken kunnen afsluiten en geen nieuwe verkennde onderzoeken op kunnen starten.

**Innovatie**  
Door de beperkte capaciteit en middelen heeft de AP in 2021 niet kunnen investeren in de innovatie van haar toezicht door de inzet van technologie. Investerings middelen het toezicht van de AP effectiever kunnen maken. Bijvoorbeeld door vaak voorkomende toezichtactiviteiten te automatiseren. Of door een diepgaande analyse van de aan de AP ter beschikking staande bronnen zoals de klachten en datalekmeldingen.

*d.w.z. 1 a 2 procent...*

*'slechts bij enkele honderden meldingen kan AP actie ondernemen'*

*'niet kunnen investeren in innovatie van toezicht'*

*API's kunnen helpen*

52

**AG CONNECT**  
the amazing world of IT

**Stijgende werklust door datalekken zorgt voor frustraties bij gemeenten**  
"Meldingen moeten efficiënter kunnen."

**2,5 tot 4 uur werk**  
Uit het onderzoek wordt duidelijk dat de afhandeling van datalekken een werklust meebrengt van zo'n 2,5 tot 4 uur, afhankelijk van de ernst. In bijzondere gevallen kan de werklust veel verder lopen. Daarbij neemt het aantal meldingen van datalekken bij de overheid jaarlijks fors toe, blijkt uit jaarlijkse cijfers van de AP. En vooral daar gaan veel uren in zitten.

Hoogleraar recht en de informatiemachtig Gerrit Jan Zwenne (Universiteit Leiden) sluit zich aan bij Iena: "De AP stelt nu dat een melding in vijftien tot dertig minuten kan worden gemaakt, maar binnen die tijd zal het vrijwel onmogelijk zijn om een melding af te ronden. Het zou heel plezierig zijn wanneer er API wordt ontwikkeld waarmee een organisatie datalekken in het eigen systeem kan verwerken en snel kan doorzenden naar het meldpunt."

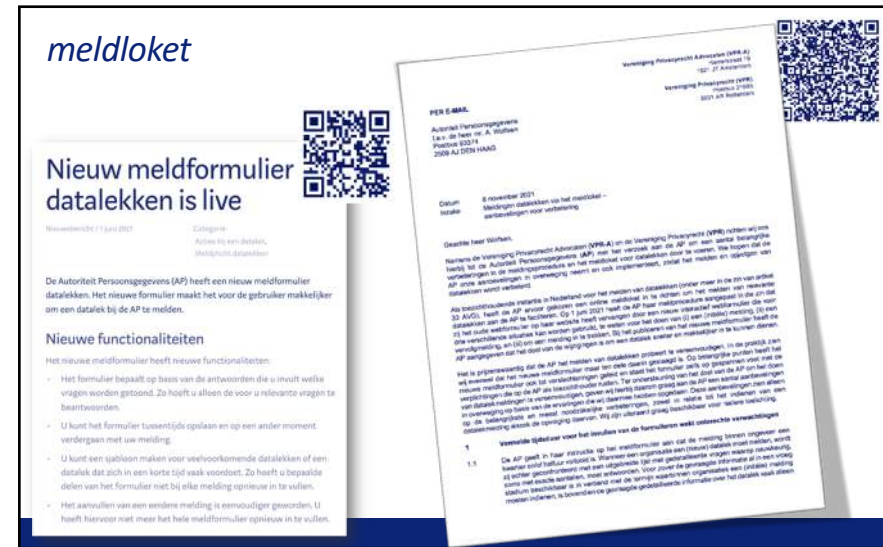
**AP handmatig melden blijft nodig**  
De Autoriteit Persoonsgegevens stelt in een reactie dat er concluderend wordt aan het verbeteren van het meldproces van een datalek. Het belang van een goede en volledige melding maken staat voorop. "We willen melders sneller en makkelijker maken, maar handmatig aanvullen blijft noodzakelijk, daar staan we niet om te vragen. Ook de hoeveelheid werklust van een datalek heeft de AP geen gegevens beschikbaar. Een voorbeeld geeft aan dat de tijd die iemand werklust aan niet-gemiddelde datalekken momenteel 'hoveens minder dan 0% bedraagt'."

53

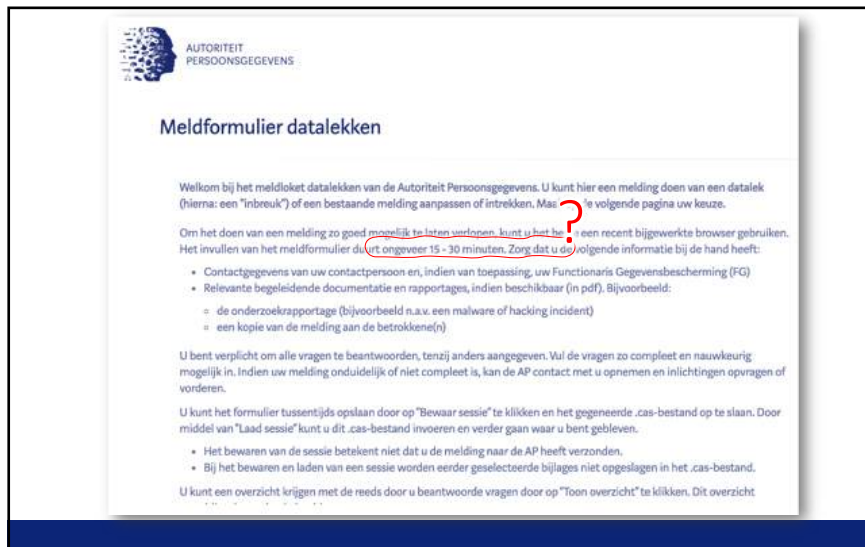




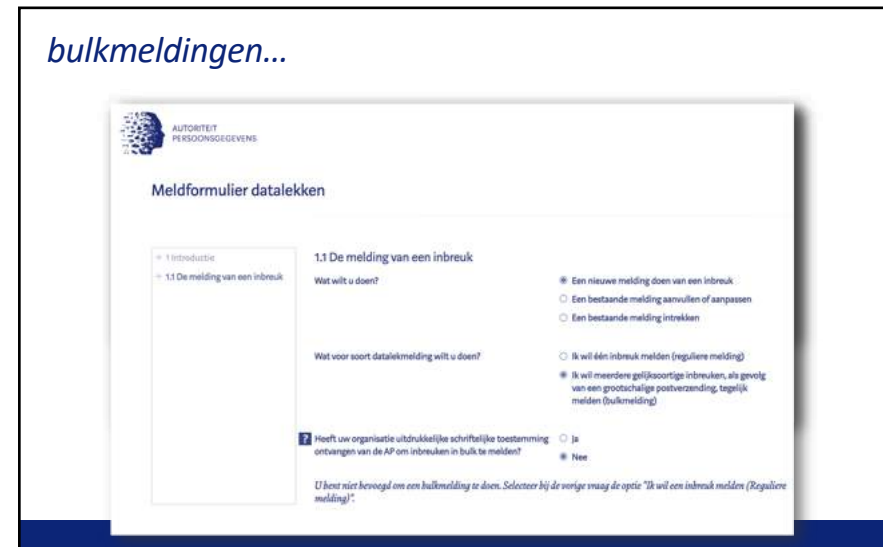
56



57



58



59

60

61

62

63

**verplichte meldingsplicht**  
Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

**Is dit een voorlopige of een definitieve melding?**

Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig.

Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk.

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(n):

- U weet nog niet of u de betrokkene(n) gaat informeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet:

De AP vraagt u binnen 4 weken na de eerste melding een verificatie... waarin u een update geeft over de stand van zaken. Mocht u langer dan 4 weken nodig hebben, dan moet u dit motiveren.

Heeft de AP binnen 4 weken geen vervolgmelding ontvangen? Dan kan de AP contact met u opnemen. Doet u geen definitieve melding, dan kan u niet (volledig) aan uw meldplicht op grond van artikel 33 AVG hebben voldaan. De AP kan dan een nader onderzoek instellen.

Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen.

Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

**Privacyverklaring**

Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP.

[← Vorige Vraag](#) [Laatste Vraag >>](#) [VERZENDEN >](#)

64

**AUTORITEIT PERSOONSGEGEVENS**

## Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.

U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst: 01-09-2018 16:02:00

Uniek nummer: 00000000-0000-0000-0000-000000000000

### 0. Over deze melding

Gaat het om een nieuwe of bestaande:  Een nieuwe melding indienen

65

*pro forma melding (tekstsuggestie)*

*“Er is naar oordeel van verwerkingsverantwoordelijke géén sprake van een inbreuk op de beveiliging van de persoonsgegevens. Voor het geval dat daarover verschil van inzicht kan bestaan, wordt zekerheidshalve, en zonder aanvaarding van enige gehoudenheid daartoe, deze melding gedaan.”*

66

toetsvraag 4

De Vereniging Privacyrecht Advocaten of VPR-A is een door de NOvA erkende specialisatievereniging

A. Dit is juist  
B. Dit is onjuist

67





rol van de toezichouder

[4]  
nog steeds het  
gerechtvaardigd belang

deze maand VoetbalTV bij de Raad  
van State

68





HARMONISATIE  
De normutleg van onze eigen toezichouder leidt er daarmee toe dat de regels in Nederland anders worden toegepast dan in andere lidstaten. Dat is in strijd met de doelstelling van de Europese Unie om te loomen tot een eenvormig, geharmoniseerd kader van privacyregels.

De normutleg zet daarmee Nederlandse ondernemingen op achterstand en opzichte van ondernemingen in andere lidstaten van de Europese Unie.

Ten slotte, last but not least, zijn er neer principiële bedenkingen. De normutleg van de Autoriteit Persoonsgegevens past in een trend waarbij nadrukkelijk en radicaal afstand wordt genomen aan marktwerking. Uiteraard valt daarover van alles te zeggen. De vraag is echter of het aan een objectieve en onafhankelijke privacytoezichouder is stelling en nemen in dat in zeven politieke debat. Vij denken van niet.

69

verwerkingsgrondslagen

art. 6.1 AVG

- a) ondubbelzinnige toestemming (van de betrokkene)
- b) noodzakelijk voor de uitvoering van overeenkomst (met de betrokkene)
- c) noodzakelijk om te voldoen aan een wettelijke plicht (die op de verwerkingsverantwoordelijke rust)
- d) noodzakelijk om vitale belangen te beschermen
- e) noodzakelijk voor de vervulling van een taak van algemeen belang
- f) noodzakelijk voor behartiging van gerechtvaardigd belang, tenzij privacybelang van betrokkene prevaleert

70

Art. 6.1 AVG

De verwerking is rechtmatig indien en voor zover [..]

(f) de verwerking is **noodzakelijk** voor de behartiging van de **gerechtvaardigde belangen** van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, **zwaarder** wegen dan die belangen, met name wanneer de betrokkene een kind is.

**driestappentoets**

1. Is er een gerechtvaardigd belang?
2. Is de verwerking noodzakelijk voor dat gerechtvaardigd belang?
3. Worden de privacybelangen van betrokkenen niet teveel aangetast daardoor?

71

## driestappentoets

1. Is er een gerechtvaardigd belang?
2. Is de verwerking noodzakelijk voor dat gerechtvaardigd belang?
3. Worden de privacybelangen van betrokkenen niet teveel aangetast daardoor?

72

AP, Normuitleg 'gerechtvaardigd belang' 1 november 2019

driestappentoets

1. Is er een gerechtvaardigd belang?
2. Is de verwerking noodzakelijk voor dat gerechtvaardigd belang?
3. Worden de privacybelangen van betrokkenen niet teveel aangetast daardoor?

73

AUTORITEIT  
PERSOONSgegevens

Wat ook niet als een gerechtvaardigd belang kwalificeert, is bijvoorbeeld: het enkel dienen van **zuiver commerciële belangen, winstmaximalisatie**, het zonder gerechtvaardigd belang volgen van het gedrag van werknemers of het (koop)gedrag van (potentiële) klanten, etc.

AP, Normuitleg 'gerechtvaardigd belang' 1 november 2019

driestappentoets

1. Is er een gerechtvaardigd belang?
2. Is de verwerking noodzakelijk voor dat gerechtvaardigd belang?
3. Worden de privacybelangen van betrokkenen niet teveel aangetast daardoor?

74

AUTORITEIT  
PERSOONSgegevens

## Boete voor tennisbond vanwege verkoop van persoonsgegevens

Nieuwsbericht / 3 maart 2020      Categorie: Direct marketing

De Autoriteit Persoonsgegevens (AP) legt tennisbond KNLTB een boete op van 525.000 euro voor het verkopen van persoonsgegevens. De KNLTB heeft in 2018 onrechtmatig tegen betaling persoonsgegevens van een paar honderdduizend van zijn leden verstrekt aan twee sponsors.

De Koninklijke Nederlandse Lawn Tennisbond (KNLTB) verstrekte de sponsors persoonsgegevens zoals naam, geslacht en adres, zodat zij een selectie van KNLTB-leden konden benaderen met tennisgerelateerde en andere aanbiedingen. De ene sponsor ontving persoonsgegevens van 50.000, de andere van meer dan 300.000 leden. Die sponsors benaderden een deel van die KNLTB-leden per post of telefoon.

75



## VoetbalTV

Rb MNL 23 november 2020,  
ECLI:NL:RBMNE:2020:5111

18. Met de strikte toepassing die verweerder hier hanteert, is hij niet toegekomen aan zo'n beoordeling als het HvJ hier omschrijft. Daarmee heeft verweerder het gerechtvaardigd belang dus niet op een open en flexibele manier uitgelegd, zoals wel zou moeten. Hij miskent daarmee dat het begrip 'gerechtvaardigd' belang vooral als buitengrens dient voor de beoordeling en niet als een drempel. Er zijn de rechtbank verder ook geen uitspraken bekend waarin het HvJ, zonder nadere beoordeling van de belangen van zowel de verwerker als de betrokkene(n), constateert dat de verwerker in het geheel geen gerechtvaardigd belang heeft bij de verwerking en alleen al daarom onrechtmatig handelt. Verweerders uitleg dat het eiseres in de kern alleen maar gaat om het te gelde maken van persoonsgegevens en dat dit belang nooit een gerechtvaardigd belang kan zijn, gaat eraan voorbij dat het HvJ het op voorhand uitsluiten van bepaalde legitieme belangen nu juist verbiedt. Evenmin volgt de rechtbank de conclusie van verweerder dat de noodzakelijkheidstoets en de belangenafweging zinledig zijn, als wordt aangenomen dat het belang dat eiseres nastreeft een gerechtvaardigd belang is.



76

## toetsvraag 5

AP vindt dat het enkel dienen van zuiver commerciële belangen en/of winstmaximalisatie niet kwalificeert als gerechtvaardigd belang (i.d.z.v. art.6.1(f) AVG)

- A. Dit is juist
- B. Dit is onjuist

77

toepassing van de AVV

[5]  
collectieve acties en  
schadevergoeding

hoe de schade te verhalen die is  
veroorzaakt door een overtreding  
van de AVG?

78



79

### lopende zaken...

<b>Data Privacy Stichting vs. Facebook</b> <ul style="list-style-type: none"> <li>• grondslag- en transparantievereisten, verwerkingsverbod bijzondere gegevens, cookieregels</li> <li>• verklaring voor recht</li> <li>• Rb A'dam 30 juni 2021, ECLI:NL:RBAMS:2021:3307</li> </ul>	<b>St. Onderzoek Marktinformatie, St. Take Back Your Privacy, st. Massaschade &amp; Consument vs. TikTok</b> <ul style="list-style-type: none"> <li>• grondslag- en transparantievereisten, derde landendoorgifte (etc.)</li> <li>• verklaring voor recht (etc.), schadevergoeding</li> </ul>	<b>Privacy First vs Staat (Min. J&amp;V)</b> <ul style="list-style-type: none"> <li>• rechtmatigheid van kentekenregistratie o.b.v. art. 126j Sv</li> <li>• verklaring voor recht, verbod kentekenregistratie</li> <li>• RbDHG 1 december 2021, ECLI:NL:RBDHA:2021:13165</li> </ul>
<b>St. The Privacy Collective vs. Oracle en Salesforce</b> <ul style="list-style-type: none"> <li>• cookieregels, profilering, grondslag- en transparantie-vereisten, doelbinding etc.</li> <li>• verklaring voor recht, schadevergoeding</li> </ul>	<b>Privacy First vs Staat (Min. Financiën)</b> <ul style="list-style-type: none"> <li>• rechtmatigheid van UBO-register, AMLD4, AMLD5, art. 15a Handelregisterwet</li> <li>• verklaring voor recht, buitenwerkingstelling art. 15a Handelsregisterwet, prejudiciële vragen</li> <li>• Rb DHG 18 maart 2021, ECLI:NL:RBDHA:2021:2457</li> </ul>	<b>Amnesty International c.s. vs Staat (Min. Defensie en Minf. J&amp;V)</b> <ul style="list-style-type: none"> <li>• controles i.h.k.v. Mobiel Toezicht Veiligheid (MTV) door de Koninklijke Marechaussee</li> <li>• verwerkingsverbod bijzondere gegevens, profilering</li> <li>• verklaring voor recht, resp. verbod</li> <li>• Rb DHG 22 sept. 2021, ECLI:NL:RBDHA:2021:10280</li> </ul>
<b>St. Stop Online Shaming en St. Expertisebureau Online Kindermisbruik vs [X] handelend onder de naam [Y]</b> <ul style="list-style-type: none"> <li>• rechtmatigheid website vagina.nl</li> <li>• verwerkingsverbod bijzondere gegevens</li> <li>• verklaring voor recht</li> </ul>	<b>St. Stop Online Shaming vs St. Slachtoffers latrogene Nalatigheid-Nederland</b> <ul style="list-style-type: none"> <li>• rechtmatigheid website</li> <li>• grondslag- en transparantievereisten</li> <li>• verbod website</li> </ul>	

80

### lopende zaken: principieel

<b>Privacy First vs Staat (Min. J&amp;V)</b> <ul style="list-style-type: none"> <li>• rechtmatigheid van kentekenregistratie o.b.v. art. 126j Sv</li> <li>• verklaring voor recht, verbod kentekenregistratie</li> <li>• RbDHG 1 december 2021, ECLI:NL:RBDHA:2021:13165</li> </ul>
<b>Privacy First vs Staat (Min. Financiën)</b> <ul style="list-style-type: none"> <li>• rechtmatigheid van UBO-register, AMLD4, AMLD5, art. 15a Handelregisterwet</li> <li>• verklaring voor recht, buitenwerkingstelling art. 15a Handelsregisterwet, prejudiciële vragen</li> <li>• Hof DHG 16 november 2021, ECLI:NL:GHDHA:2021:2176</li> </ul>

81

### lopende zaken: ontvankelijkheid en bevoegdheid (pre-WAMCA)

geen openbaarmaking dagvaarding en geen vermelding rechtspraak.nl

'procedure tegen verwerkingsverantwoordelijke [...] wordt ingesteld bij de gerechten van de lidstaat waar de verwerkingsverantwoordelijke [...] een vestiging heeft.

Een dergelijke procedure kan ook worden ingesteld bij de gerechten van de lidstaat waar de betrokkene gewoonlijk verblijft'

o.b.v. zgn. opt-out mechanisme

collectieve actie kan 'onafhankelijk van de opdracht van betrokkene' worden ingesteld

• rechtbank A'dam is bevoegd (Brussels I bis-vo. en Rv, alsmede art. 79.2 AVG) verw. 147)

• geen aanleiding tot het stellen van prejudiciële vragen

• weldegelijk sprake van gelijksoortige belangen i.d.z.v. art. 305a BW

• voldaan aan de vereisten van art. 80.2 AVG

82

### lopende zaken...

<b>Data Privacy Stichting vs. Facebook</b> <ul style="list-style-type: none"> <li>• grondslag- en transparantievereisten, verwerkingsverbod bijzondere gegevens, cookieregels</li> <li>• verklaring voor recht</li> <li>• Rb A'dam 30 juni 2021, ECLI:NL:RBAMS:2021:3307</li> </ul>	<b>St. Onderzoek Marktinformatie, St. Take Back Your Privacy, st. Massaschade &amp; Consument vs. TikTok</b> <ul style="list-style-type: none"> <li>• grondslag- en transparantievereisten, derde landendoorgifte (etc.)</li> <li>• verklaring voor recht (etc.), schadevergoeding</li> </ul>	<b>Privacy First vs Staat (Min. J&amp;V)</b> <ul style="list-style-type: none"> <li>• rechtmatigheid van kentekenregistratie o.b.v. art. 126j Sv</li> <li>• verklaring voor recht, verbod kentekenregistratie</li> </ul>
<b>St. The Privacy Collective vs. Oracle en Salesforce</b> <ul style="list-style-type: none"> <li>• cookieregels, profilering, grondslag- en transparantie-vereisten, doelbinding etc.</li> <li>• verklaring voor recht, schadevergoeding</li> </ul>	<b>Privacy First vs Staat (Min. Financiën)</b> <ul style="list-style-type: none"> <li>• rechtmatigheid van UBO-register, AMLD4, AMLD5, art. 15a Handelregisterwet</li> <li>• verklaring voor recht, buitenwerkingstelling art. 15a Handelsregisterwet, prejudiciële vragen</li> <li>• Rb DHG 18 maart 2021, ECLI:NL:RBDHA:2021:2457</li> </ul>	<b>Amnesty International c.s. vs Staat (Min. Defensie en Minf. J&amp;V)</b> <ul style="list-style-type: none"> <li>• controles i.h.k.v. Mobiel Toezicht Veiligheid (MTV) door de Koninklijke Marechaussee</li> <li>• verwerkingsverbod bijzondere gegevens, profilering</li> <li>• verklaring voor recht, resp. verbod MTV</li> <li>• Rb DHG 22 sept. 2021, ECLI:NL:RBDHA:2021:10280</li> </ul>
<b>St. Stop Online Shaming en St. Expertisebureau Online Kindermisbruik vs [X] handelend onder de naam [Y]</b> <ul style="list-style-type: none"> <li>• rechtmatigheid website vagina.nl</li> <li>• verwerkingsverbod bijzondere gegevens</li> <li>• verklaring voor recht</li> </ul>	<b>St. Stop Online Shaming vs St. Slachtoffers latrogene Nalatigheid-Nederland</b> <ul style="list-style-type: none"> <li>• rechtmatigheid website</li> <li>• grondslag- en transparantievereisten</li> <li>• verbod website</li> </ul>	

83

### lopende zaken: representativiteit

Wrakingsverzoek tegen rechter-plaatsvervanger, tevens hoogleraar, toegewezen. [...] rechter heeft als wetenschapper onvoldoende distantie betrachting tot de zaak van verzoekers o.a. door een tweet.

5.11 TPC dient feitelijk te onderbouwen hoeveel gedupeerden deze actie daadwerkelijk ondersteunen en aldus wat de omvang van de door haar vertegenwoordigde vordering. **Dat heeft TPC niet gedaan.**

Op de website van TPC konden en kunnen bezoekers de steunknop aanklikken. Ten tijde van de mondelinge behandeling **had TPC ruim 75.000 keer op deze manier een steunbetuiging verkregen.** [...] **Het enkel klikken op de steunknop betekent nog niet dat daarmee een steunbetuiging is verkregen zoals is beoogd met het representativiteitsvereiste.** Informatie over de aard en de inzet van de procedure ontbreekt in het scherm. Hierin staat niet vermeld tegen welke partijen de actie is gericht. Oracle en Salesforce worden niet genoemd. Evenmin volgt hieruit dat een persoon door het aanklikken van de steunknop zich als gedupeerde aanmeldt voor deze collectieve actie of zal worden gerekend tot de achterban voor wie TPC in deze procedure opkomt. Een omschrijving van de gedupeerden voor wie TPC opkomt, ontbreekt. **De conclusie van TPC dat meer dan 75.000 personen uit haar achterban hun steun kenbaar hebben gemaakt door te klikken op de steunknop, kan dan ook niet worden gevolgd.**

St. The Privacy Collective vs. Oracle en Salesforce

- cookieregels, profilering, grondslag- en transparantie-vereisten, doelbinding etc.
- verklaring voor recht, schadevergoeding




84

### lopende zaken: schadevergoeding


St. Onderzoek Marktinformatie, St. Take Back Your Privacy, st. Massaschade & Consument vs. TikTok

- grondslag- en transparantievereisten, derde landendoorgifte (etc.)
- verklaring voor recht (etc.), **schadevergoeding**

St. The Privacy Collective vs. Oracle en Salesforce

- cookieregels, profilering, grondslag- en transparantie-vereisten, doelbinding etc.
- verklaring voor recht, **schadevergoeding**

op welke wijze, en in hoeverre, moet de betrokkene aantonen dat de geleden schade het gevolg is van de overtreding van de verordening..?



85

### Pieter Baan Centrum: €300


Rb Gelderland 19 december 2018  
ECLI:NL:RBGEL:2018:5551

5.1 Naar het oordeel van de rechtbank is de privacy van eiser geschonden omdat rapportages over eiser naar het Tuchtcollege zijn verstuurd en de daarin opgenomen strikt vertrouwelijke persoonlijke gegevens bij medewerkers en leden van het Tuchtcollege terecht zijn gekomen. Eiser heeft er in dit verband terecht op gewezen dat voor de aanspraak op schadevergoeding **niet is vereist dat sprake is van psychische schade.** [...]

5.2 Het voorgaande betekent dat eiser ingevolge artikel 49, tweede lid, van de Wbp **niet** heeft op een naar billijkheid vast te stellen schadevergoeding.

6. Ten aanzien van de hoogte van de vast te stellen schadevergoeding acht de rechtbank van belang dat de privacygevoelige persoonsgegevens bij een **kleine groep professionals** terecht zijn gekomen, te weten bij medewerkers en leden van het Tuchtcollege, en dat zij uit hoofde van hun functie een **geheimhoudingsplicht** hebben. Dit neemt niet weg dat van een schending van de privacy van eiser sprake is, en dat dit begrijpelijkerwijs **door eiser als naar en nadelig is ervaren.** Alles afwegend acht de rechtbank een **schadevergoeding van € 300** billijk.

**kleine groep professionals met geheimhoudingsplicht**



86

### Deventer: €500

Rb Overijssel 28 mei 2019  
ECLI:NL:ROVE:2019:1827

9. Naar het oordeel van de rechtbank is eiser als gevolg van dat onrechtmatige besluit **in zijn persoon aangetast wegens verlies van controle over zijn persoonsgegevens.** Dat is een persoonlijkheidsrecht. Dit betekent dat eiser op grond van artikel 82 van de Avg in samenhang met artikel 6:106 van het BW recht heeft op een naar billijkheid vast te stellen schadevergoeding. Wat betreft de hoogte van die vergoeding neemt de rechtbank in acht dat in het onrechtmatige besluit geen rechtvaardiging is gegeven voor de verwerking van de persoonsgegevens van eiser. De rechtbank neemt mede in aanmerking het gestelde onder 75, 85 en 146 van de preambule bij de Avg.

[...]

11. Nu door de verspreiding van zijn persoonsgegevens sprake is geweest van een schending van de privacy van eiser acht de rechtbank een **schadevergoeding van € 500,-** billijk.




87


**UWV: €250**

Rb A'dam 2 september 2019  
ECLI:NL:RBAMS:2019:6490

18. [...] Als gevolg van die schending heeft [eiseres] reële en niet verwaarloosbare nadelen geleden. De belangen waarin zij is getroffen zijn de belangen die de voorschriften van de AVG juist beoogt te beschermen. Art. 82 AVG bepaalt dat degene die materiële of immateriële schade heeft geleden als gevolg van een inbreuk op deze verordening, het recht heeft om van de verwerkingsverantwoordelijke [...] schadevergoeding te ontvangen voor de geleden schade. Alle schade moet worden vergoed en het begrip schade moet – overeenkomstig de doelstellingen van de AVG – ruim worden uitgelegd (par. 146 Considerans), [...]

18. Nu het verlies van controle over haar persoonsgegevens betreffende de langdurige ziekte blijvend is, dit anderzijds uitsluitend (medewerkers van) [werkgever 2] betreft en dit geen gevolgen heeft gehad voor haar economische of maatschappelijke positie, terwijl de als gevolg van de inbreuk opgetreden angst en stress in tijd beperkt is geweest, wordt een schadevergoeding van € 250,00 passend en billijk geacht. [...]

kleine groep medewerkers, geen economische en maatschappelijke gevolgen, angst en stress beperkt




88

**Gronings Stadsblog: €250**

Rb Nrd NLD 15 januari 2020  
ECLI:NL:RBNNE:2020247

4.106. (...) is sprake [...] van een schending van een fundamenteel recht, die naar zijn aard en gelet op de ernst daarvan meebrengt dat aanspraak bestaat op vergoeding van schade. Dit laatste volgt ook uit de AVG. Art. 82 AVG bepaalt dat degene die materiële of immateriële schade heeft geleden als gevolg van een inbreuk op de verordening, het recht heeft om van de verwerkingsverantwoordelijke of de verwerkingsverantwoordelijke te ontvangen voor de geleden schade. Alle schade moet worden vergoed en het begrip schade moet – overeenkomstig de doelstellingen van de AVG – ruim worden uitgelegd (par. 146 van de preambule bij de AVG), hetgeen betekent dat het enkele feit dat de schade niet exact gepreciseerd kan worden en mogelijk relatief gering van omvang is geen grond kan vormen om elke aanspraak daarop af te wijzen.

4.107. (...) het verlies van controle van [gedaagde 2] over zijn persoonsgegevens is [...] blijvend. Anderzijds beperkt het verlies van controle zich (vooralsnog) tot de medewerker van [eiser 1] ([naam A]) en één derde. [gedaagde 2] stelt weliswaar dat hij negatieve gevolgen heeft gehad van het handelen van [eiser 1], maar niet duidelijk is waar die negatieve gevolgen uit hebben bestaan. Het lag, gelet op zijn daarop gerichte vordering, op de weg van [gedaagde 2] dat inzichtelijk te maken. Nu [gedaagde 2] dat niet heeft gedaan, maar het schadebegrip ruim uitgelegd moet worden en de rechtbank het aannemelijk acht dat [gedaagde 2] als gevolg van het handelen van [eiser 1] negatieve effecten heeft ervaren, bijvoorbeeld angst en stress, wordt een schadevergoeding van € 250,00 passend en billijk geacht.



89

**Deventer hoger beroep: nihil**

ABRvS 1 april 2020  
ECLI:NL:RBNNE:2020:899

33. [...] Het algemene uitgangspunt dat schade moet worden onderbouwd, geldt ook hier. Er is geen grond voor het oordeel dat een inbreuk op de AVG zonder meer aantasting van de integriteit van een persoon impliceert en daarmee tot vergoedbare schade leidt. Anders dan [appellant sub 2] betoogt, kan dit niet worden afgeleid uit overwegingen 85 en 146 van de AVG. Dat een inbreuk op persoonsgegevens kan resulteren in (im)materiële schade en dat een betrokkene volledige en daadwerkelijke vergoeding van de door hem geleden schade moet ontvangen, betekent niet dat een normschending per definitie tot schade leidt en dat schade niet reëel en zeker moet zijn geleden. [...]

34. In dit geval doet zich niet een situatie voor waarbij de nadelige gevolgen van de normschending voor de hand liggen. [...] Het gaat niet om ernstig verwijtbaar gedrag met zo ernstige gevolgen, dat dit als een inbreuk op een fundamenteel recht moet worden gekwalificeerd.



Idem:  
• ABRvS 1 april 2020, ECLI:NL:RBNNE:2020:900  
• ABRvS 1 april 2020, ECLI:NL:RBNNE:2020:901



90


**Pieter Baan Centrum hoger beroep**

ABRvS 1 april 2020  
ECLI:NL:RVS:2020:898

32. [...] Ook als het bestaan van geestelijk letsel in voornoemde zin niet kan worden aangenomen, is niet uitgesloten dat de aard en de ernst van de normschending en van de gevolgen daarvan voor de benadeelde, meebrengen dat van de in artikel 6:106, aanhef en onder b, BW bedoelde aantasting in zijn persoon 'op andere wijze' sprake is. In zo een geval zal degene die zich hierop beroept de aantasting in zijn persoon met concrete gegevens moeten onderbouwen. Dat is slechts anders indien de aard en de ernst van de normschending meebrengen dat de in dit verband relevante nadelige gevolgen daarvan voor de benadeelde zo voor de hand liggen, dat een aantasting in de persoon kan worden aangenomen. Van een aantasting in de persoon 'op andere wijze' als bedoeld in artikel 6:106, aanhef en onder b, BW is niet reeds sprake bij de enkele schending van een fundamenteel recht.

schade hoeft niet te worden onderbouwd als de nadelige gevolgen zo voor de hand liggen dat 'aantasting in de persoon' kan worden aangenomen

Zie:  
HR 15 maart 2019, ECLI:NL:HR:2019:376 (EBI)



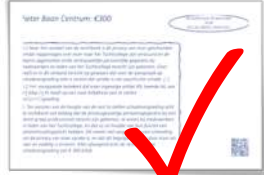
91


**Pieter Baan Centrum hoger beroep: €500**

ABRVs 1 april 2020  
ECLI:NL:RVS:2020:898

Raad van State

36. [appellant] [heeft] recht heeft op toekenning van een vergoeding voor immateriële schade. [...]  
Gelet op de omstandigheden van dit geval, waaronder de aard, duur en ernst van de inbreuk, zal de Afdeling deze schade naar billijkheid vaststellen op € 500. Daartoe neemt de Afdeling in aanmerking de bijzondere gevoeligheid van de aard van de persoonsgegevens die in dit geval zonder toestemming van [appellant] zijn verwerkt. Voor de verwerking van bijzondere (gevoelige) persoonsgegevens als bedoeld in artikel 9 van de AVG, is in de AVG een hoger beschermingsniveau is neergelegd dan voor gewone persoonsgegevens. De nadelige gevolgen van de verstrekking van de gevoelige persoonsgegevens liggen voor de hand. [...]





92

**Oldambt: €500**

Rb Nrd NLD 12 januari 2021,  
ECLI:NL:RBNNE:2021:106

4.27 [eiser] heeft naar het oordeel van de kantonrechter niet, althans onvoldoende, gesteld dat hij als gevolg van het onrechtmatig handelen van de gemeente op objectieve gronden vastgesteld psychisch letsel heeft opgelopen, in de zin van een in de psychiatrie erkend ziektebeeld. [...]  
4.28. De kantonrechter is wél van oordeel dat [eiser] anderszins in zijn persoon is aangetast. De persoonlijke levenssfeer van [eiser] is bij herhaling door de gemeente geschonden vanwege het - in strijd met de AVG - meermalen publiceren van het BSN-nummer, het e-mailadres en het telefoonnummer van [eiser] op de gemeentelijke website, zonder dat [eiser] daarvoor toestemming aan de gemeente had verleend (vgl. r.o. 36 van de uitspraak van de Afdeling). Het gaat hierbij ook om naar hun aard gevoelige gegevens, zeker waar het betreft het BSN-nummer van [eiser]. De nadelige gevolgen van het lekken daarvan, zoals identiteitsfraude, liggen voor de hand. [...]  
Gelet op de omstandigheden van het onderhavige geval, waaronder de aard, duur, frequentie en ernst van de inbreuk, afgezet tegen de omstandigheid dat niet is gebleken dat de datalekken tot concrete negatieve gevolgen hebben geleid, zal de kantonrechter deze schadevergoeding naar billijkheid vaststellen op een bedrag van € 500,00.





93

**zwartelijstartsen.com: €5000(!)**

Hof Arnhem-Lw. 6 april 2021,  
ECLI:NL:GHARL:2021:3206

minus €1000, nl. het bedrag dat al in de strafzaak was toegewezen

5.1 [Het hof zal de] Stichting SIN veroordelen om binnen veertien dagen na het wijzen van dit arrest al de persoonsgegevens van appellant, waaronder ook de verwijzing naar de uitspraken van het CTG van 2 september 2010, van de websites www.sin-nl.org en www.zwartelijstartsen.nl te verwijderen en verwijderd te houden [...]  
Het gevorderde bedrag van € 5.000,- voor immateriële schade [...] zal het hof toewijzen minus het bedrag van € 1.000,- dat al door de strafrechter aan appellant als benadeelde partij is toegekend. [...]  
Nu het hier gaat om langdurige aantasting in eer en naam, waarvan appellant (evenals zijn partner) naar aan te nemen valt aanzienlijke hinder heeft ondervonden in zijn privéleven en in zijn mogelijkheden om een betaalde baan te vinden, is het hof van oordeel, ook gezien andere uitspraken van Nederlandse rechters, dat het gevorderde bedrag gezien de maatstaf van artikel 6:106 lid 1 aanhef, sub b BW een billijk bedrag is.





94

**SVB: nihil**


Rb. Mid-NNLD 4 mei 2021,  
ECLI:NL:RBMNE:2021:1865


ABRVs 4 maart 2020,  
ECLI:RVS:2020:674

onrechtmatige verstrekking van persoonsgegevens door SvB aan Belastingdienst/Toeslagen

36. De aard en de ernst van de privacyinbreuk zijn in dit geval niet zodanig dat de nadelige gevolgen zo voor de hand liggen dat een aantasting in de persoon kan worden aangenomen. Het uitgangspunt is dan dus dat eiser moet bewijzen dat zijn dochter in haar persoon is aangetast en dat hij de geleden schade met concrete gegevens moet onderbouwen. De rechtbank oordeelt dat eiser daarin niet is geslaagd. Op de zitting heeft hij erop gewezen dat de met het startbericht verstrekte persoonsgegevens digitaal heel lang kunnen blijven bestaan en dat dit schadelijk kan zijn voor zijn dochter. Eiser heeft op deze manier slechts in algemene bewoordingen gesteld dat schade is geleden en heeft dat niet kunnen concretiseren. Hij heeft dan ook niet aannemelijk gemaakt dat het verstrekken van de persoonsgegevens van zijn dochter aan de Belastingdienst/Toeslagen heeft geleid tot de aantasting van haar persoon en dat de gevolgen van de inbreuk haar rechtstreeks hebben getroffen.  
37. De rechtbank overweegt hierbij dat de algemene vrees voor identiteitsfraude onvoldoende is voor een veroordeling in immateriële schade. Hoewel deze vrees voorstelbaar is en identiteitsfraude als gevolg van de privacyinbreuk niet uit te sluiten is, is dat onvoldoende concreet om nu uit te kunnen concluderen dat eisers dochter in haar persoon is aangetast.

- schade ligt niet voor de hand
- eiser moet schade aantonen
- met concrete gegevens
- algemene vrees voor ID-fraude is onvoldoende





95



**Almelo: 2 x €125**

Rb. Overijssel 31 mei 2021, ECLI:NL:RBOVE:2021:2264

besluit van gemeente om niet te voldoen aan verwijderingsverzoek o.g.v. art. 17.1 AVG

15. Naar het oordeel van de rechtbank is [naam] als gevolg van het **bestreden besluit**, dat een onrechtmatig karakter heeft, in zijn persoon aangetast door verlies van controle over zijn persoonsgegevens. Het betreft een aantasting van een persoonlijkheidsrecht. Dat betekent dat eiseres op grond van artikel 82 van de AVG in samenhang met artikel 6:106 van het Burgerlijk Wetboek recht heeft op een naar billijkheid vast te stellen schadevergoeding.

16. Het uitgangspunt is dat eiseres de door haar gestelde schade met concrete gegevens moet onderbouwen. Gelet op de omstandigheden van het geval en het langdurig verzet van verweerder tegen een redelijk verzoek tot vernietiging van het Jeugdwet-dossier van [naam], heeft de gemachtigde van eiseres in het aanvullend beroepschrift van 9 september 2020 aangevoerd het billijk te achten dat zowel voor [naam] als voor zijn wettelijk vertegenwoordigster een bedrag van € 1.500,- wordt toegekend wegens immateriële schade.

17. De rechtbank volgt de gemachtigde van eiseres hierin niet vanwege het ontbreken van concrete gegevens. De rechtbank acht een **schadevergoeding van € 125,- voor eiseres en eenzelfde bedrag aan schadevergoeding voor [naam] redelijk** en zal verweerder hiertoe veroordelen.




96

**Rotterdam: €2500**

Rb. Rotterdam 12 juli 2021, ECLI:NL:RBROT:2021:6822

besluit van gemeente om medische gegevens niet uit dossier te verwijderen (art.17.1 AVG?)

4.2. Verzoekster stelt als gevolg van het handelen van verweerder ten minste **€25.000,-** aan schade te hebben geleden.

4.3. Ten aanzien van de hoogte van de vast te stellen schadevergoeding is van belang dat de privacygevoelige persoonsgegevens gedurende een periode van ongeveer tien jaar door verweerder zijn bewaard, ondanks verschillende verzoeken van verzoekster tot vernietiging van de gegevens. **De rechtbank acht voldoende aannemelijk dat in die tien jaar de persoonlijke gegevens van verzoekster zijn verwerkt en meerdere personen en/of instanties van de inhoud kennis hebben kunnen nemen zonder dat zij daartoe gerechtigd waren en dat verzoekster op grond daarvan immateriële schade heeft geleden.** De schade begroot de rechtbank, met inachtneming van de in 4.1. genoemde uitspraak van de Afdeling (waarin een schadevergoeding is toegekend van € 500,- voor een kortdurende onrechtmatige verwerking van medische gegevens) en de lengte van de periode dat de gegevens onrechtmatig zijn bewaard en verwerkt, op **€ 2.500,-**.

4.4. De stelling van verzoekster dat door het onrechtmatig bewaren en bewerken van haar gegevens haar carrière is beschadigd en zij daardoor onder andere inkomensverlies heeft geleden, acht de rechtbank niet aannemelijk gemaakt. Het verzoek om materiële schadevergoeding wordt daarom afgewezen.

- medische gegevens
- ten onrechte bewaard 10 jaar bewaard
- toegankelijk voor meerdere personen en instanties



97

Dus...

In beginsel moet **met concrete gegevens** worden **aangetoond** dat er schade is geleden als gevolg van de overtreding

tenzij de schade zo **voor de hand ligt** dat 'aantasting in de persoon' kan worden aangenomen

relevant zijn

- verwijtbaarheid gedrag en ernst van gevolgen (Deventer)
- aard duur en ernst van de overtreding (Pieter Baan)
- gevoeligheid van de gegevens (Pieter Baan)
- bij een datalek ligt ID-fraude voor de hand (Oldambt)

98

**intussen in Duitsland en Oostenrijk**

Bundesverfassungsgericht 14 January 2021, ECLI:DE:BVerfG:2021:rk20210114.1bvr285319


Oberster Gerichtshof 12 May 2021 questions asked to CJEU

The facts to be assessed in the main proceedings raised the question under which conditions Art. 82(1) GDPR grants a claim for monetary damages and which understanding of this provision is to be given in particular with regard to recital 146, third sentence, which requires a **broad interpretation of the concept of damage** in light of the case law of the Court of Justice of the European Union that fully complies with the objectives of the GDPR

- Does the award of compensation under Article 82 GDPR [...] also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?
- Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence?
- Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the **existence of a consequence of the infringement** of at least some weight that goes beyond the upset caused by that infringement?

wordt vervolgd...

99

 toepassing van de AVV

**[6]**  
wettelijke plicht of  
gerechtvaardigd belang?

beantwoording prejudiciële vragen in HR 3  
december 2021, ECLI:NL:HR:2021:1814

100

art. 6.1 AVG

**verwerkingsgrondslagen**

- a) ondubbelzinnige toestemming (van de betrokkene)
- b) noodzakelijk voor de uitvoering van overeenkomst (met de betrokkene)
- c) noodzakelijk om te voldoen aan een wettelijke plicht (die op de verwerkingsverantwoordelijke rust)
- d) noodzakelijk om vitale belangen te beschermen
- e) noodzakelijk voor de vervulling van een taak van algemeen belang
- f) noodzakelijk voor behartiging van gerechtvaardigd belang, tenzij privacybelang van betrokkene prevaleert

} BKR-registratie:  
c- of f-grond..?

101

**het belang van de verwerkingsgrondslag**

om een zgn. bijzonderheidscodering uit het Centraal Krediet Informatiesysteem van BKR te verwijderen maken consumenten gebruik van hun wissingsrecht en/of hun recht van bezwaar

bijv. betalingsachterstand, roodstaan, studieschuld

art. 21.1 AVG

dat kan evenwel alleen als de kredietaanbieder dit niet doet ter naleving van een wettelijke plicht maar ter behartiging van een gerechtvaardigd belang

art. 6.1(f) AVG

art. 17.1 AVG

art. 6.1(c) AVG

102

**de vraag is dus:**

is de registratie van bijzonderheidscodes door de bank in CKI van BKR inherent aan het voldoen aan de wettelijke plicht om deel te nemen aan BKR?

- ja, want een bank kan niet deelnemen aan BKR zonder deze registraties
- neen, want de registratie is vereist door het CKI-reglement, niet door de wet

let op: geen toetsvraag!

103

### verwerkingsgrondslag voor de kredietaanbieder

zeg: een bank, postorderbedrijf, mobiele telecoomaanbieder

waarvan een kredietaanbieder gebruik maakt als hij van iemand persoonsgegevens opneemt in het Centraal Krediet Informatie Systeem (CKI) van BKR

bijv. bijzonderheidscode "A" d.w.z. de aanduiding dat sprake is van een betalingsachterstand

• wettelijke plicht (art. 6.1c AVG) of  
• gerechtvaardigd belang (art. 6.1f AVG)...

104

### verwerkingsgrondslag voor de kredietaanbieder

- d.w.z. art. 4:32 en 4:34 Wet financieel toezicht (Wft) én
- art. 114 Besluit Gedragstoezicht financiële ondernemingen (Bgfo) én
- Reglement CKI

geen wissingsrecht (art. 17.3b AVG) en geen recht van bezwaar (art. 21.1 AVG)

wel Santander-toets (HR 9 september 2011, ECLI:NL:HR:2011:808097)

- wettelijke plicht (art. 6.1c AVG) of
- gerechtvaardigd belang (art. 6.1f AVG)

wel een wissingsrecht (art. 17.1 AVG) en een recht van bezwaar (art. 21.1 AVG)

105

### verwerkingsgrondslag voor bank

- art. 4:32 en 4:34 Wft én
- art. 114 Bgfo
- Reglement CKI

kredietaanbieder moet deelnemen aan kredietregistratiestelsel, zoals BKR

kredietaanbieder moet informatie inwinnen over financiële positie van consument, om overkreditering te voorkomen

voordat hij met een consument een kredietovereenkomst (meer dan €250) aangaat, moet kredietaanbieder het kredietregistratiestelsel raadplegen

deelnemers aan BKR moeten eigen kredietovereenkomsten opnemen in CKI

wettelijke plicht (art. 6.1c AVG) ?

106

### BKR-registratie door kredietaanbieder: c- of f-grond?

hof Den Bosch 6 augustus 2020, ECLI:NL:GHSHE:2020:2536 en hof Arnhem-L. 17 december 2020, ECLI:NL:GHARL:2020:10564

- bank moet voldoen aan wettelijke plicht om deel te nemen aan een stelsel van kredietregistratie o.g.v. art. 4:32 Wft
- bank verwerkt ter uitvoering van haar wettelijke plicht de persoonsgegevens van de verzoeker, dus o.b.v. c-grond
- verzoeker kan geen gebruik maken van art. 17.1 en art. 21.1 AVG, wél geldt de Santander-toets
- de termijn van art. 35.2 AVG is niet van toepassing; verzoeker is niet niet-ontvankelijk

hof Den Haag 8 september 2020, ECLI:NL:GHDHA:2020:2068

- bank moet voldoen aan wettelijke plicht om deel te nemen aan een stelsel van kredietregistratie o.g.v. art. 4:32 Wft
- maar bank is o.g.v. die wettelijke plicht niet gehouden om een concrete registratie te doen in een individueel geval: bank verwerkt niet o.b.v. c-grond maar f-grond
- verzoeker kan wel gebruik maken van art. 21.1 AVG
- maar wel binnen de termijn van art. 35.2 AVG, anders niet-ontvankelijkheid

rechtbank A'dam 21 januari 2021, ECLI:NL:RBAMS:2021:174

prejudiciële vragen aan de Hoge Raad (art. 392, eerste lid, onderdeel b, Rv)

- verwerkt bank om te voldoen aan een wettelijke verplichting (c-grond) of ter behartiging van een gerechtvaardigd belang (f-grond)..?
- komt aan de betrokkene een beroep toe op het recht van gegevenswissing en het recht van bezwaar (art. 17 resp 21 AVG)..?
- als hem geen recht op bezwaar toekomt, leidt dat er dan toe dat art. 35 UAVG geen rol speelt..?

107

### wanneer is sprake van een wettelijke plicht?

geldt ook voor taak van algemeen belang of uitoefening openbaar gezag

art. 6.3

- de rechtsgrond van de plicht is vastgesteld bij unierecht of lidstatelijk recht dat van toepassing is op de verwerkingsverantwoordelijke
- in die rechtsgrond **moet het doel** van de verwerking staan
- die rechtsgrond **kan specifieke bepalingen bevatten** om de toepassing van de regels van **déze** verordening aan te passen
- unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel

bijv. types van gegevens; betrokkenen; entiteiten waaraan en doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; doelbinding; opslagperiodes etc.

overw. 45

- de verwerking moet een grondslag te hebben in unierecht of lidstatelijke recht.
- **geen specifieke wetgeving vereist is voor elke afzonderlijke verwerking**
- voldoende is wetgeving die als basis fungeert voor verscheidene verwerkingen o.g.v. een wettelijke verplichting die op de verwerkingsverantwoordelijke rust
- unierecht of het lidstatelijke recht moet het doel van de verwerking bepalen

108

### wat is een wettelijke plicht?

idem: taak van algemeen belang (art 6.1e AVG)

overw. 41

- niet noodzakelijkerwijs **een door een parlement vastgestelde wetgevingshandeling**
- deze rechtsgrond of wetgevingsmaatregel moet evenwel **duidelijk en nauwkeurig** zijn, en de toepassing daarvan moet **voorspelbaar** zijn voor degenen op wie deze van toepassing is

CKI-reglement...?

WP29 06/2014

De wetgeving kan in bepaalde gevallen slechts een algemene doelstelling vaststellen, terwijl **meer specifieke verplichtingen op een ander niveau worden vastgesteld**, bijvoorbeeld in secundaire wetgeving of in een bindend besluit van een overheidsinstantie in een concreet geval.

109

### wat is een wettelijke plicht?

Kst II 2017/18, 34 851, nr. 3, p. 35

Deze wettelijke verplichting behoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om (bepaalde) persoonsgegevens te verwerken. Het komt namelijk ook voor dat de verwerking van persoonsgegevens een basis vindt in een **ruimer geformuleerde zorgplicht of wettelijke verplichting**. In dat geval heeft de verwerkingsverantwoordelijke een grotere eigen verantwoordelijkheid inzake het beoordelen van de noodzakelijkheid van de verwerking in het licht van het voldoen aan de wettelijke verplichting. **Zonder verwerking van de gegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn.**


110

### Conclusie AG Rank-Berenschot

Conclusie 15 september 2021, ECLI:NL:PHR:2021:831

Mijns inziens moet de verwerking van persoonsgegevens door een kredietinstelling, door middel van een registratie in het CKI van het BKR, worden getoetst aan het bepaalde in **artikel 6 lid 1, aanhef en onder f, AVG**.

Het bepaalde in art. 6 lid 1, aanhef en onder c, AVG leent zich mijns inziens bij de huidige stand van de wet- en regelgeving niet voor toepassing op de verwerking van persoonsgegevens in het CKI van het BKR.



111

### Hoge Raad

HR 3 december 2021  
ECLI:NL:HR:2021:1814

Art. 4:32 lid 1 Wft en art. 4:34 lid 1 Wft, zoals nader uitgewerkt in art. 114 BGfo, verplichten kredietaanbieders weliswaar tot deelname aan en raadpleging van een stelsel van kredietregistratie, maar deze wettelijke bepalingen zijn *niet voldoende duidelijk en nauwkeurig en de toepassing ervan is niet voldoende voorspelbaar* voor degenen op wie deze wettelijke bepalingen van toepassing zijn, zoals art. 6 lid 3 AVG eist [...].

Uit die wettelijke bepalingen blijkt immers niet welke persoonsgegevens in het CKI geregistreerd moeten of mogen worden, wat de voorwaarden voor een dergelijke registratie zijn en onder welke voorwaarden en binnen welke termijnen tot verwijdering van persoonsgegevens moet worden overgegaan. *Een en ander wordt wel geregeld in het CKI-reglement, maar dat reglement berust niet op een wettelijke grondslag; de registratie van persoonsgegevens in het CKI vindt plaats op grond van een overeenkomst tussen het BKR en kredietaanbieders*



112

### de vraag is dus:

is de registratie van bijzonderheidscodes door de bank in CKI van BKR inherent aan het voldoen aan de wettelijke plicht om deel te nemen aan BKR?

- ja, want een bank kan niet deelnemen aan BKR zonder deze registraties
- neen, want de registratie is vereist door het CKI-reglement, niet door de wet

113

### toetsvraag 6

Volgens de Hoge Raad vindt de registratie van persoonsgegevens in het CKI van BKR plaats op grond van een overeenkomst tussen het BKR en kredietaanbieders en niet ter naleving van een wettelijke plicht (i.d.z.v. art. 6.1(c) AVG)

- A. Dit is juist
- B. Dit is onjuist



DANK VOOR UW AANDACHT  
g.j.zwenne@law.leidenuniv.nl

114

128