



@zwnne

VRIJDAG 9 SEPTEMBER 16:00-17:30 | KAMERLINGH ONNES GEBOUW TE LEIDEN

ontwikkelingen in privacywetgeving (AVG & UAVG)

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



Universiteit
Leiden



1



In deze fase van het onderzoek wilden we ook een oriënterend gesprek voeren met de voorzitter van het college van de Autoriteit Persoonsgegevens (mr. Aleid Wolfsen). *Wegens bezwaren van de Autoriteit Persoonsgegevens met betrekking tot de totstandkoming van de opdracht, en de aard, opzet en scope van het onderzoek en de betrokkenen daarbij, besloot de AP na meerdere gesprekken tussen vertegenwoordigers van het departement en het WODC en medewerkers van de AP aanvankelijk in het geheel niet mee te willen werken aan het onderzoek.* Later werd het alsnog mogelijk een concepteindtekst met vragen voor te leggen. In reactie daarop leverde de AP uitvoerig commentaar en werden antwoorden op gestelde vragen gegeven. De onderzoekers hebben in ruime mate hun voordeel kunnen doen met de schriftelijke reactie van de AP, die op verschillende plaatsen tot aanvulling op de tekst heeft geleid.

2



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

rode draad

toepassing van de AVG

rol van het toezicht



7



interessant debat over de toepassing van de AVG en de rol van de toezichthouders

1. vragen over inzage

Prins in NJB

3. nog steeds het gerechtvaardigd belang

5. cookies en cookiemuren

4. AVG en immateriële schadevergoeding

Bobek in Conclusie bij X vs AP

2. Enschede. Of wat is een «persoonsgegeven» wel of niet?

(de rode draad)



8



rol van de toezichthouder

[1] VRAGEN OVER INZAGE

wat de European Data Protection Board ervan vindt en hoe dat zich (niet) verhoudt met nationale rechtspraak

10



wáár gaat het over?

art. 15
AVG

verzoek moet gepreciseerd zijn,
maar hoeft niet te worden
gemotiveerd

de natuurlijke persoon op wie de
gegevens betrekking hebben

- een **recht** van de **betrokkene**
- om **op verzoek** uitsluitel te krijgen
- over het al dan niet verwerken van
hem betreffende **persoonsgegevens**
- en als dat het geval is om **inzage**
daarin te verkrijgen
- alsmede aanvullende relevante
informatie

gegevens waarover de
verwerkingsverantwoordelijke
beschikt

in beginsel een volledig
overzicht, soms een kopie van
het document

herkomst,
ontvangers etc.

11

wat is de bedoeling van het inzagerecht?

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 inzagerecht gebruiken om te controleren of de hem betreffende gegevens kloppen en op een rechtmatige wijze worden verwerkt

12



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

4.20. Het inzagerecht was voorheen in artikel 12 van de Richtlijn persoonsgegevens vastgelegd. Dat inzagerecht 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 inzagerecht ten opzichte van de Richtlijn persoonsgegevens is gewijzigd. De rechtbank neemt dan ook tot

uitgangspunt dat de uitspraken van het Hof van Justitie van de Europese Unie (HvJEU) en de Hoge Raad die zijn gewezen over het inzagerecht 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

13

wat vinden de toezichthouders?



14



Wat zeggen **DSAR**-guidelines..?

Data Subject
Access Request



- 1 35. If the data subject, who has been asked to specify the scope of its request, confirms to seek **all personal data concerning him or her**, the controller of course has to provide it in full.
- 2 73. [...] It should be emphasised 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
- 3 165. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the **purposes behind the request** should be regarded as **irrelevant**.

15

- 1 35. If the data subject, who has been asked to specify the scope of its request, confirms to seek **all personal data concerning him or her**, the controller of course has to provide it in full.

**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.

**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 alleen **welhaast praktisch ondoenlijk** zijn maar ook een veel te omvangrijke en daarmee kostbare zoektocht van [verweerder] meebrengen.

**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.

16



1

35. If the data subject, who has been asked to specify the scope of its request, confirms to seek **all personal data concerning him or her**, the controller of course has to provide it in full. ...?

rechtbank Noord-Holland van 18 juni 2021, ECLI:NL:RBNHO:2021:6040 7.

In zijn algemeenheid geldt dat een verwerkingsverantwoordelijke mag vragen om precisering als hij een grote hoeveelheid gegevens verwerkt. Dat betekent echter nog niet dat een verwerkingsverantwoordelijke in alle gevallen precisering kan eisen alvorens een zoekslag te verrichten. Naarmate een verzoek meer concreet is, mag van de verwerkingsverantwoordelijke meer inspanning worden verwacht, maar ook bij een algemeen geformuleerd verzoek mag naar het oordeel van de rechtbank worden verwacht dat de verwerkingsverantwoordelijke een zoekslag verricht naar de meest gangbare persoonsgegevens (bijvoorbeeld aan de hand van de NAW-gegevens en het BSN-nummer) in de meest gangbare gegevensbestanden en/of computersystemen/applicaties.

17

2

73. [...] It should be emphasised 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

Art. 12, zesde lid, AVG

[D]e verwerkingsverantwoordelijke [kan], wanneer hij redenen heeft om te twijfelen 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.

18



2

73. [...] It should be emphasised 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



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. [...].**

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

19



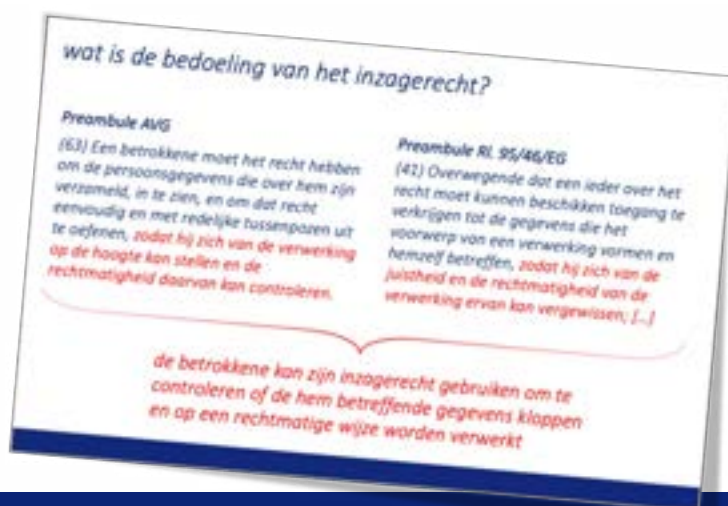
Het is **onevenredig** om een kopie van een identiteitsbewijs te vereisen als de identiteit van de betrokkene op een andere manier kan worden geverifieerd. Bovendien vormt de verwerking van kopieën van identiteitsbewijzen **een groot risico** voor de veiligheid van persoonsgegevens. Daarnaast kan de verwerkingsverantwoordelijke er **niet zeker van zijn dat de kopie authentiek** is en de eigenaar van de identiteitskaart daadwerkelijk de verzoeker is, door bijvoorbeeld (ongeeoorloofde) toegang tot identiteitsbewijzen door huisgenoten en vervalste kopieën van identiteitsbewijzen.

20



3

165. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the **purposes behind the request** should be regarded as **irrelevant**.



21

3

165. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the **purposes behind the request** should be regarded as **irrelevant**.



Rb R'dam 21 januari 2020, ECLI:NL:RBROT:2020:515
4.8 [...] Het inzage-recht 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 procesdossiers** waarin hij als procespartij betrokken was. [...] Het doel van [verzoeker] bij zijn inzage-recht ziet niet op de bescherming van persoonsgegevens zodat sprake is van **misbruik van 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.

22



3

165. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the **purposes behind the request** should be regarded as **irrelevant**.



hof A' dam 3 maart 2020, ECLI:NL:GHAMS:2020:648

3.10 [...] Uit de stukken en de ter gelegenheid van de mondelinge behandeling in hoger beroep door [appellanten] gegeven toelichting blijkt dat zij, kort gezegd, inzage in de gevraagde gegevens wensen teneinde vast te kunnen stellen wat de aanleiding was voor bepaalde door ABN AMRO verrichte handelingen ten aanzien van zijn vermogen en persoonsgegevens. Zo willen zij weten waarom de contact- en adresgegevens van [appellant sub 1] zijn gewijzigd en waarom kredietovereenkomsten zijn aangegaan zonder dat hij daarvoor heeft getekend. [...] *Uit deze stellingen van [appellanten] is niet aannemelijk geworden dat [appellanten] inzage wensen in de door ABN AMRO verwerkte persoonsgegevens ter controle van de juistheid en rechtmatigheid van de verwerking daarvan. [...]* Het hof concludeert dat [appellanten] met de onderhavige verzoeken betreffende [appellant sub 1] de bevoegdheid tot het indienen van inzageverzoeken gebruiken voor een ander doel dan het door de Wpb (oud) en AVG beoogde doel.

23

3

165. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the **purposes behind the request** should be regarded as **irrelevant**.



hof Den Haag 31 oktober 2017, ECLI:NL:GHDHA:2017:3011

7. Dat [appellant] [...] mogelijk *tevens een ander belang heeft (gehad)*, te weten het verkrijgen van gegevens om deze te gebruiken in een gerechtelijke procedure – het hof merkt op dat de tussen partijen bij het gerechtshof Amsterdam aanhangige procedure inmiddels in staat van wijzen is – is ontoereikend om aan te nemen dat hij van dit recht misbruik maakt. *Onder deze omstandigheden kan immers niet worden geoordeeld dat [appellant] zijn recht uitoefent voor een ander doel dan waarvoor het is verleend.*

24



3

165. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the **purposes behind the request** should be regarded as **irrelevant**.



hof Den Haag 14 december 2021, ECLI:NL:GHDHA:2021:2793

*6.2 [appellant] heeft tijdens de mondelinge behandeling in hoger beroep bevestigd dat hij de te verkrijgen gegevens mogelijk zal betrekken in procedures inzake bedoelde verwijten. Naar het oordeel van het hof is echter **onvoldoende aannemelijk geworden dat dit het enige doel is** waarvoor [appellant] zijn informatie- en inzagerechten uitoefent. Ter zitting van het hof heeft [appellant] ook opgemerkt dat zijn doel is na te gaan welke persoonsgegevens van hem op welke wijze door Nauta [verwerkingsverantwoordelijke] zijn verwerkt en of dit rechtmatig is gebeurd, en dat als blijkt dat Nauta daarbij onrechtmatig heeft gehandeld, hij zal bekijken welke Avg-rechten hij kan uitoefenen om die onrechtmatigheid te adresseren. **Dat [appellant] zijn bevoegdheid misbruikt door haar uit te oefenen voor een ander doel dan waarvoor zij is verleend (als bedoeld in art. 3:13 lid 2 BW), kan dus niet worden geoordeeld.***

25

taken van European Data Protection Board

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 zijn richtsnoeren voorgegaan op rechterlijke uitspraken...?



43



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

44



rol van de toezichthouder

[2]
persoonsgegevens, of niet?

over passententellingen en
wifitracking in Enschede

45





Boete gemeente Enschede om wifitracking

Mededeling 17-04-2022

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 ving de wifisignalen op van de mobiele telefoons van passerende mensen. Iedere 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 volgen.

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.

46

Is er sprake van «persoonsgegevens» ...?

alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon

"de betrokkene" of het "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 identificatie...?

47



wat is «identificeren»

~ 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

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





deugdelijke vaststelling van identiteit

Art. 12.6 AVG

[D]e verwerkingsverantwoordelijke [kan], wanneer hij redenen heeft om te twijfelen 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.



50

«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 identifier

bijvoorbeeld een naam, identificatienummer, locatiegegevens, online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

IP-address, MAC-address

(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.

51



«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 ...

52

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



53



Hof van Justitie: 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.



54

Hof van Justitie: 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..

*HJEU 24 november
2011, C-70/10*



55

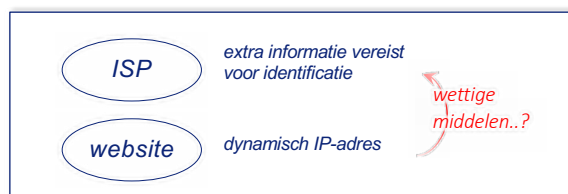


Hof van Justitie: Breyer

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

HJEU 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.**



rechtbank Den Haag: 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 indirect herleidbaar 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 om een koppeling te 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 persoonsgegeven.





Afdeling: fietsendepot

ABRvS 13 juli 2022 ECLI:NL:RVS:2022:1993

5.3 [...] [D]e Afdeling [is] met de rechtbank van oordeel dat het college aannemelijk heeft gemaakt dat binnen de gemeente die IP-adressen niet worden opgeslagen, vastgelegd en gekoppeld aan personen en dat de gemeente zelf niet beschikt over de benodigde gegevens om een koppeling te kunnen maken tussen die IP-adressen en een burger. Een daadwerkelijk gevaar voor identificatie is onbeduidend.

rechtbank Midden-Nederland: Brein/Ziggo

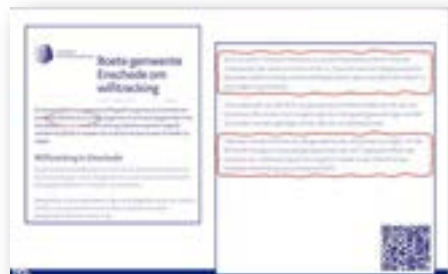
Rechtbank Midden-Nederland 2 februari 2022 ECLI:NL:RBMNE:2022:297

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, kosten en inspanning – een excessieve inspanning vergt, zodat het gevaar voor identificatie 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.





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. Dezelfde manier 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...?

60

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

61



toetsvraag 3

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

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

83

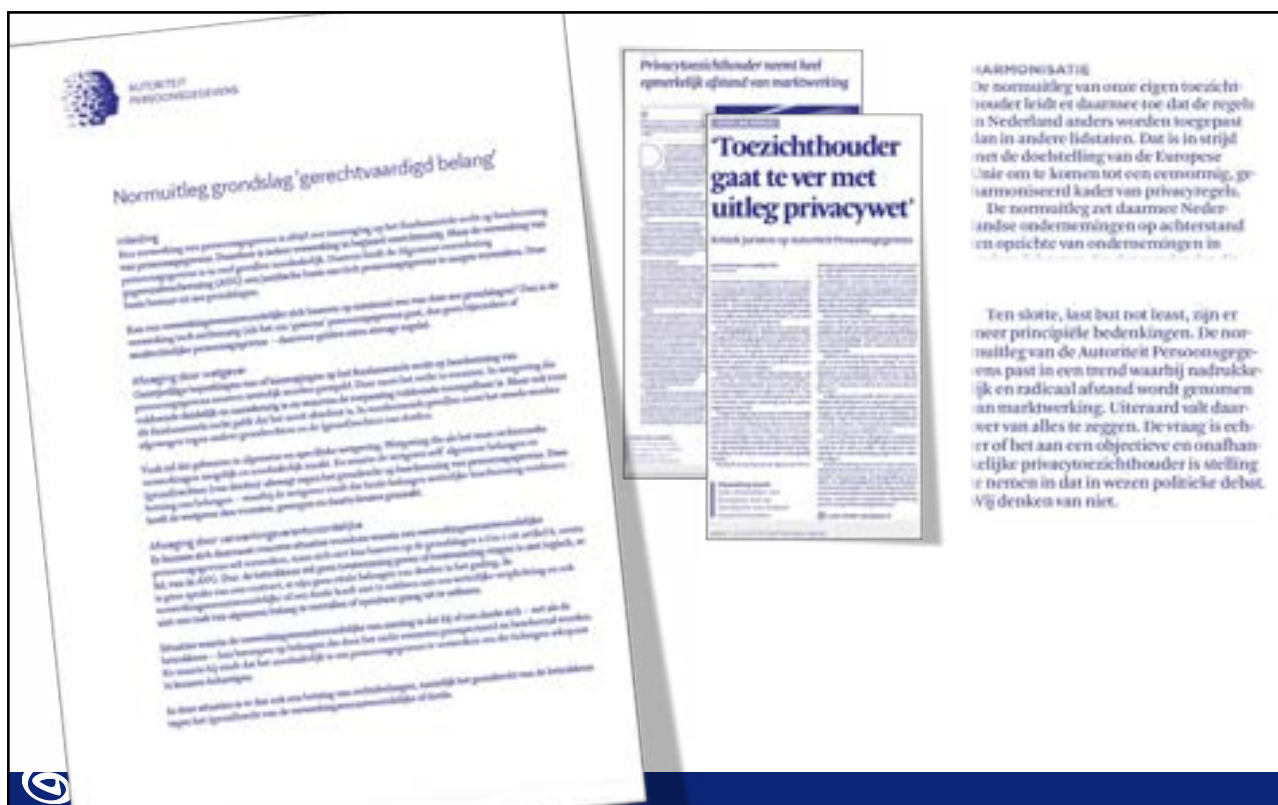


rol van de toezichthouder

[3]
nog steeds het
gerechtvaardigd belang

VoetbalTV en KNLTB

84



85

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*

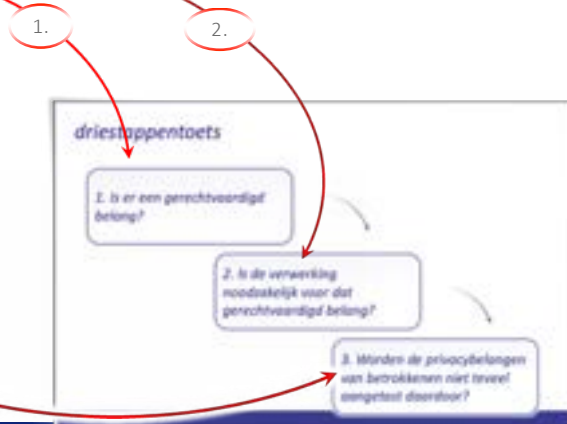
86



de zgn. f-grond

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.



87

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?

88



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



89



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.



90



rechtbank Midden-Nederland / VoetbalTV

rechtbank Midden-Nederland 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.



Afdeling / VoetbalTV

ABRvS 27 juli 2022, ECLI:NL:RVS:2022:2173

[...] Het is aan de AP om te beoordelen wat de verwerkingsverantwoordelijke werkelijk doet, te bezien of gestelde belangen daarmee overeenkomen en ook werkelijk worden behartigd door de verwerking en of deze gerechtvaardigd zijn. Naar het oordeel van de Afdeling dient deze toets plaats te vinden in stap 1 en heeft de rechtbank dit dus terecht zo overwogen. Met de rechtbank wordt geoordeeld dat in dit geval, gelet op de door VoetbalTV genoemde andere belangen, die niet van commerciële aard zijn, geen sprake is van een louter commercieel belang. De vraag of een uitsluitend commercieel belang op zichzelf een gerechtvaardigd belang in de zin van artikel 6, eerste lid, aanhef en onder f, van de AVG kan zijn, hoeft daarom niet te worden beantwoord. De AP heeft ten onrechte bij de beoordeling van de eerste voorwaarde de door VoetbalTV gestelde belangen [...] niet meegewogen. Gelet op de aard van de activiteiten van VoetbalTV - het maken van beelden van voetbalwedstrijden en deze ter beschikking stellen aan derden, waaronder degenen die in beeld gebracht willen worden - is de verwerking van persoonsgegevens noodzakelijk voor meer dan alleen de commerciële belangen van VoetbalTV. De AP heeft dan ook op onjuiste gronden vastgesteld dat VoetbalTV in strijd met artikel 6, eerste lid, aanhef en onder f, van de AVG heeft gehandeld.





Bescherm de Autoriteit Persoonsgegevens privacy, of verstoort ze de vrije markt?

Persoonsgegevens De Nederlandse Autoriteit Persoonsgegevens neemt in de EU een aparte positie in als het gaat om wat bedrijven mogen met persoonsgegevens. Volgens jurisprudentie verstoort AP het vrije ondernemerschap. Is dat zo?

Winst geen rechtvaardiging

In document schiet de AP dat „het enkel dienen van zuiver commerciële belangen” niet kan worden gekwalificeerd als een gerechtvaardigd belang. Op basis van dit standpunt komt de toezichthouder later in de maand tot de boete voor VoetbalTV. Het winsttoegmerk van de streamingdienst vormt volgens de AP geen rechtvaardiging voor het afdrukken van beelden van spelers en fans zonder dat zij daar individueel toestemming voor geven.

Onder juristen leidt dit standpunt al direct tot kritiek. Promovendus Bob van Eijk en hoogleraar recht en informatiewetenschap Gerrit Jan Zwenne van de Universiteit Leiden schrijven een opiniestuk. Het Financieel Dagblad vraagt de toezichthouder hieraan ingaat tegen jurisprudentie van de hoven en Europese rechters. Ook zij stellen een winsttoegmerk niet uit als een gerechtvaardigd belang. Bovendien zou de AP politiek bedrijven.

„De normatieve van de Autoriteit Persoonsgegevens past in een trend waarbij nadrukkelijk en radicaal afstand wordt genomen van marktwerking. (...) De vraag is of het aan een objectieve en onafhankelijke privacytoezichthouder is om oordelen te nemen in dat in wezen politieke debat. Wij denken van niet”, schrijven van Eijk en Zwenne.

Een paar maanden later roept de Europese Commissie zich groepen zich ook met de zaak te bemoeien. De Commissie wil de functionarissen van de interne markt in de EU zou in het geding zijn. In een brief aan voorzitter Alred Wollben van de AP - die ABC recent in handen kreeg - waarschuwt Brussel dat de Nederlandse toezichthouder met zijn strikte interpretatie van privacywet AVG het vrije ondernemerschap bedreigt.

AP normitieg gerechtvaardigd belang

Therefore, it is difficult to reconcile the strict interpretation of the Dutch DPA of what can constitute a legitimate interest with the intended effect that the EU legislators wanted to attribute to Article 6(1)(f) GDPR. It should also be borne in mind that the fact that a pure commercial interest is 'legitimate' does not entail that the data controller can immediately rely on Article 6(1)(f) GDPR. In fact, this will depend on the outcome of the second and third leg of the three-part test.

b. The second and the third leg of the test: The Google Spain and Fashion ID cases

Concerning the second and the third leg of the test, we would like to draw attention to the jurisprudence of the CJEU. The CJEU has on a number of occasions established that the legitimate interest ground foresees a concrete balancing of the legitimate interests of the controller, on the one hand, and the fundamental rights and freedoms of the data subject, on the other. The fact that the Dutch DPA generally and categorically considers commercial interests to be legitimate interests, accounts to the strict interpretation of the legitimate interest ground.

93

Mag u persoonsgegevens verwerken?

Elke keer als u persoonsgegevens verwerkt, is dat een inbreuk op de privacy van de mensen waar u mee gaat. Daarom mag u alleen persoonsgegevens verwerken als het echt niet anders kan. Dus: als u zonder deze gegevens uw doel niet kunt bereiken.

Grondslagen uit de AVG

De AVG kent zes verschillende manieren om persoonsgegevens te verwerken. In de privacywet, de Algemene Verordening Gegevensbescherming (AVG), staan de volgende grondslagen:

Grondslag zelf bepalen

U kunt zelf bepalen welke grondslag voor u van toepassing is. Dit is een belangrijke keuze. De Autoriteit Persoonsgegevens heeft een checklist om u te helpen kiezen. U kunt de grondslag kiezen die het meest past bij uw situatie.

De 6 grondslagen

In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

- U heeft toestemming van de betroffene voor het verwerken.
- U hebt noodzakelijk om gegevens te verwerken voor een overeenkomst die u met de betroffene heeft gesloten.
- U hebt noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent.
- U hebt noodzakelijk om gegevens te verwerken om de belangen van de betroffene te beschermen.
- U hebt noodzakelijk om gegevens te verwerken om een publiek belang te dienen.
- U hebt noodzakelijk om gegevens te verwerken om een gerechtvaardigd belang te dienen.

Vragen over de grondslag gerechtvaardigd belang

Wie toetst u of u zich mag baseren op de grondslag 'gerechtvaardigd belang'?

Ook uw verwerking kan worden toegestaan op basis van de grondslag 'gerechtvaardigd belang'. Het is belangrijk om te weten dat u niet zomaar kunt zeggen dat u zich baseert op de grondslag 'gerechtvaardigd belang'. Het is belangrijk om te weten dat u niet zomaar kunt zeggen dat u zich baseert op de grondslag 'gerechtvaardigd belang'.

De 6 voorwaarden voor de grondslag 'gerechtvaardigd belang' zijn:

- U heeft noodzakelijk om gegevens te verwerken voor een overeenkomst die u met de betroffene heeft gesloten.
- U hebt noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent.
- U hebt noodzakelijk om gegevens te verwerken om de belangen van de betroffene te beschermen.
- U hebt noodzakelijk om gegevens te verwerken om een publiek belang te dienen.
- U hebt noodzakelijk om gegevens te verwerken om een gerechtvaardigd belang te dienen.
- U hebt noodzakelijk om gegevens te verwerken om een gerechtvaardigd belang te dienen.

U kunt ook zelf bepalen welke grondslag voor u van toepassing is. Dit is een belangrijke keuze. De Autoriteit Persoonsgegevens heeft een checklist om u te helpen kiezen. U kunt de grondslag kiezen die het meest past bij uw situatie.

94



toetsvraag 4

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



95



toepassing van de AVV

[4]
collectieve acties en
schadevergoeding

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

96



97

Data Privacy Stichting vs. Facebook • grondslag- en transparantievereisten, verwerkingsverbod bijzondere gegevens, cookieregels • verklaring voor recht Rb A'dam 30 juni 2021, ECLI:NL:RBAMS:2021:3307	St. Onderzoek Marktinformatie, St. Take Back Your Privacy, st. Massaschade & Consument vs. TikTok • grondslag- en transparantievereisten, derde landendoorgifte (etc.) • verklaring voor recht (etc.), schadevergoeding	Privacy First vs Staat (Min, J&V) • rechtmatigheid van kentekenregistratie o.b.v. art. 126jj Sv • verklaring voor recht, verbod kentekenregistratie RbDHG 1 december 2021, ECLI:NL:RBDHA:2021:13165
St. The Privacy Collective vs. Oracle en Salesforce • cookieregels, profilering, grondslag- en transparantievereisten, doelbinding etc. • verklaring voor recht, schadevergoeding Rb A'dam 29 oktober 2021, ECLI:NL:RBAMS:2021:6200 Rb A'dam 29 december 2021, ECLI:NL:RBAMS:2021:7647	Privacy First vs Staat (Min. Financiën) • rechtmatigheid van UBO-register, AMLD4, AMLD5, art. 15a Handelsregisterwet • verklaring voor recht, buitenwerkingstelling art. 15a Handelsregisterwet, prejudiciële vragen Rb DHG 18 maart 2021, ECLI:NL:RBDHA:2021:2457	Amnesty International c.s. vs Staat (Min. Defensie en Minf. J&V) • controles i.h.k.v. Mobiel Toezicht Veiligheid (MTV) door de Koninklijke Marechaussee • verwerkingsverbod bijzondere gegevens, profilering • verklaring voor recht, resp. verbod Rb DHG 22 sept. 2021, ECLI:NL:RBDHA:2021:10280
St. Stop Online Shaming en St. Expertisebureau Online Kindermisbruik vs [X] handelend onder de naam [Y] • rechtmatigheid website vagina.nl • verwerkingsverbod bijzondere gegevens • verklaring voor recht	St. Stop Online Shaming vs St. Slachtoffers latrogene Nalatigheid-Nederland • rechtmatigheid website • grondslag- en transparantievereisten • verbod website	

98



lopende zaken: ontvankelijkheid en bevoegdheid (pre-WAMCA)

Data Privacy Stichting vs. Facebook

- grondslag- en transparantievereisten, verwerkingsverbod bijzondere gegevens, cookieregels
- verklaring voor recht (geen schadevergoeding!)
- Rb A'dam 30 juni 2021, ECLI:NL:RBAMS:2021:3307

'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'

geen openbaarmaking dagvaarding en geen vermelding rechtspraak.nl

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

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

- rechtbank A'dam is bevoegd op grond van 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



100

TPC vs Salesforce & Oracle



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

St. The Privacy Collective vs. Oracle en Salesforce

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

Rb A'dam 29 oktober 2021, ECLI:NL:RBAMS:2021:6200

Rb A'dam 29 december 2021, ECLI:NL:RBAMS:2021:7647



5.11 TPC dient feitelijk te onderbouwen hoeveel gedupeerden deze actie daadwerkelijk ondersteunen en aldus wat de omvang is 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.

101



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*

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



102

102

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* recht 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



103



Deventer: €500

Rb Overijssel 28 mei 2019
ECLI:NL:RBOVE: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*.



104

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 persoonsgegeven 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



105



Gronings Stadsblog: €250

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

4.106. Er 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 enerzijds blijvend. Anderzijds beperkt het verlies van controle zich (vooral nog) tot een 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**.



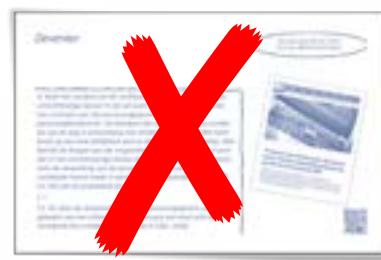
106

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



107



Pieter Baan Centrum hoger beroep

Raad
vanState

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)



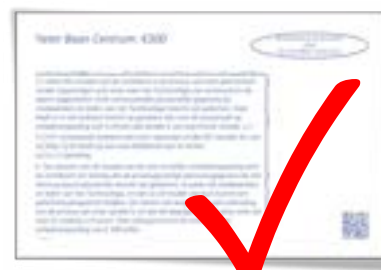
108

Pieter Baan Centrum hoger beroep: €500

Raad
vanState

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

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. [...]



109



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.**



110

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.



111



SVB: nihil

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

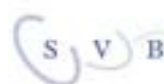
ABRvS 4 maart 2020,
ECLI:RVS:2020:674

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



112

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 beroepsschrift 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.



113



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



114

Heemskerk: nihil

Rb. Noord Holland 16 augustus 2022,
ECLI:NL:RBNHO:2022:7329

9.3 Niet gebleken is dat de gegevens van eiseres bij derden terecht zijn gekomen. Eiseres heeft geen identiteitsfraude ondervonden en geen verdachte brieven, fishing mails of telefoontjes ontvangen die in verband kunnen worden gebracht met het datalek. Naar het oordeel van de rechtbank komt eiseres niet in aanmerking voor schadevergoeding nu zij niet met concrete en objectieve gegevens heeft onderbouwd dat zij ten gevolge van het datalek geestelijk letsel heeft opgelopen en van een aantasting in de persoon 'op andere wijze' als hiervoor bedoeld niet reeds sprake is bij de enkele schending van een fundamenteel recht. Uit de e-mails van de maatschappelijk werker en de huisarts blijkt enkel dat zij praat over haar dossiervermissing respectievelijk de kwestie met de gemeente. De overgelegde e-mails rechtvaardigen niet de conclusie dat sprake is van geestelijk letsel.

115



Dus...

In beginsel moet **met concrete gegevens** worden **aangehouden** 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) of toch niet (Heemskerk)...?

116

116

intussen in Duitsland en Oostenrijk

Bundesverfassungsgericht 14 January 2021,
ECLI:DE:BVerfG:2021:rk20210
114.1bvr285319

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...

117

117



rol van de toezichthouder

[5] over cookies en cookiemuren

mag het of mag het niet? en
wie bepaalt dat dan?

133

cookiebepaling

Art. 11.7a Telecomwet

Onverminderd de Algemene verordening gegevensbescherming is het **via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker**, alleen toegestaan op voorwaarde dat de betrokken gebruiker:

- a) is voorzien van **duidelijke en volledige informatie** overeenkomstig de Algemene verordening gegevensbescherming, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en
- b) daarvoor **toestemming** heeft verleend.

plaatsen en uitlezen
van cookies



Art. 13-14 AVG: o.a. eigen identiteit, doeleinden en 'nadere informatie voor zover nodig om zorgvuldige verwerking te waarborgen'

is de toestemming
rechtsgeldig als er sprake is
van een cookiemuur..?

is de toestemming in
vrijheid gegeven...?

toestemming mag niet worden geacht
vrijelijk te zijn verleend indien de
betrokkene geen echte of vrije keuze heeft
of zijn toestemming niet kan weigeren of
intrekken zonder nadelige gevolgen
(overw. 42 Preambule AVG)

135



uitzonderingen

Art. 11.7a
lid 3 TW

geen toestemmingvereiste of informatieplicht als:

- cookies strikt noodzakelijk zijn om de gevraagde dienst van de informatiemaatschappij te leveren
- én privacyongevaarlijke effectiviteits- of kwaliteitscookies...
- cookies die nodig zijn om de communicatie over een elektronisch communicatienetwerk uit te voeren

analytics, A/B-testing,
affiliate cookies, e.d.

taalinstellingen, voorkeuren,
opslaan wachtwoord,
betalingen via ideal, enz.
KST II 2010/11, 32 549, p. 78

136

bewijsvermoeden

Art. 11.7a
lid 4 TW

- cookies gebruikt voor verzamelen, combineren of analyseren van gegevens over het gebruik van verschillende diensten van de informatiemaatschappij
- worden vermoed persoonsgegevens verwerkingen te zijn

- AVG van toepassing
- AP bevoegd

KST II 2011/12, 32 549,
nr. 39

137



cookiemuren-verbod (voor overheid e.d.)

Art 11.7 lid
5 Tw

De toegang van de gebruiker tot een dienst van de informatiemaatschappij die wordt geleverd door of namens een krachtens publiekrecht ingestelde rechtspersoon wordt niet afhankelijk gemaakt van het verlenen van toestemming

a contrario: geen verbod op cookiemuren voor niet krachtens publiekrecht ingestelde rechtspersonen...(?)



Belastingdienst



werken aan perspectief



138

parl. geschiedenis

Een cookiemuur is over het algemeen dan ook een rechtmatige manier om aan het toestemmingsvereiste in de cookiebepaling te voldoen. Ook al is dit niet de meest gebruiksvriendelijke manier en is het technisch ook nooit noodzakelijk, het staat de websitehouder in beginsel wel vrij om te bepalen of hij een bezoeker die geen toestemming geeft voor het gebruik van cookies, al dan niet toegang geeft tot zijn website. Dit kan anders zijn als de bezoeker zo afhankelijk is van de via een bepaalde website aangeboden diensten en informatie, dat er door het gebruik van de cookiemuur geen sprake meer kan zijn van een «vrije» wilsuiting wanneer de bezoeker vervolgens het vukje «ik geef toestemming» aanklikt.

vóórdat de AVG van toepassing was

Kamerstukken II 2013/14, 33902, nr. 3, p. 29

139



AUTORITEIT PERSOONSGEGEVENS



Wettelijke regels voor cookies

Voor het gebruik van cookies gelden wettelijke regels. Dat zijn in de eerste plaats regels uit de Telecommunicatiewet (Tw).

Maar op tracking cookies (in combinatie met overige gegevens die over het websitebezoek worden verzameld) is ook de Algemene verordening gegevensbescherming (AVG) van toepassing.

Uitleg over de wettelijke eisen aan andere soorten cookies is te vinden op de website van de Autoriteit Consument en Markt (ACM).

Cookiewalls

Op grond van de AVG zijn cookiewalls niet toegestaan. Dat komt omdat de AVG bepaalde eisen stelt aan de benodigde toestemming voor het plaatsen van tracking cookies.

Met een cookiewall (cookiemuur) kunnen websites, apps of andere diensten geen geldige toestemming krijgen van hun bezoekers of gebruikers.



140

discussie over invoering van een verbod op cookiewalls

Text proposed by the Commission

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking

provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its consent

any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

Amendment

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, users are increasingly requested to provide consent to store such tracking cookies

this Regulation should prevent the use of so-called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights. The use of technical means to provide consent, for

this Regulation should provide for the possibility to express consent by technical specifications, for instance by using the appropriate settings of a browser or other application. Those settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties. The choices made by users when establishing the general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers, or applications or operating systems may be used as the executor of a user's choices, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

141



Text proposed by the Commission

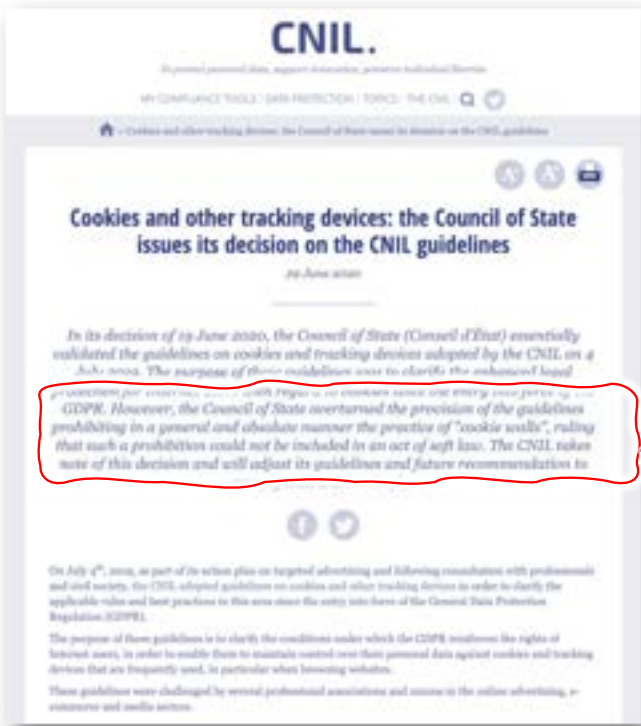
(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, **end-users** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, **end-users** are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by **end-users** when establishing **its** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the **end-user** and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as **gatekeepers**, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

142

Amendment

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, **users** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, **users** are overloaded with requests to provide consent. **This Regulation should prevent the use of so-called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights.** The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by **technical specifications, for instance by** using the appropriate settings of a browser or other application. **Those settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties.** The choices made by **users** when establishing **the** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the **user** and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers, **or applications or operating systems** may be used as **the executor of a user's choices**, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

143

[T]he Council of State overturned the provision of the guidelines prohibiting in a general and absolute manner the practice of "cookie walls", ruling that such a prohibition could not be included in an act of soft law.

het is niet aan de toezichthouder, maar aan de wetgever om de regels te stellen

144

ePrivacy Regulation



- requirement to obtain the **explicit consent** from end-users before using cookies and trackers on your website, or any other technology that stores personal data on users' terminal equipment (hardware and software)
- **cookie walls** are allowed, if the user is offered an equivalent that does not involve giving consent to cookies and trackers
- possibility to **whitelist cookie providers** in their browser settings and encourage providers to make it easy for users to amend whitelists and to withdraw their consent at any time

145



ter afsluiting

we moeten ons bezinnen op
toepassing van de Avg en het
toezicht daarop

waarom?

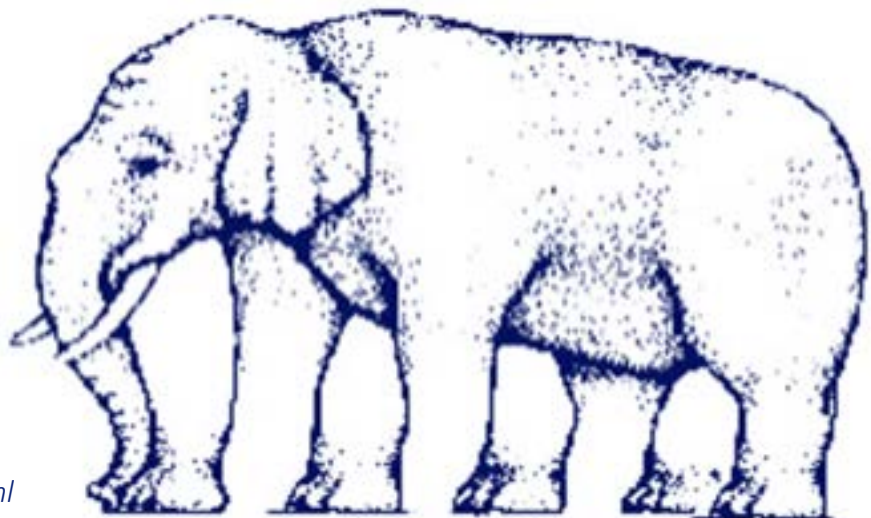
omdat de Avg anders geen
betekenis meer heeft en het
toezicht daarop ongeloofwaardig
wordt

Bobek

Prins

toezichthouder is geen wetgever
of rechter en is dus terughoudend
met het introduceren van hele
nieuwe regels

146



g.j.zwenne@law.leidenuniv.nl

147