



@zwnne

VPR-A SEMINAR | 21 JUNI 2022

Ontwikkelingen en actualiteiten
in het gegevensbeschermingsrecht

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



Universiteit
Leiden
Juridisch Post Academisch Onderwijs

VPR-A

1



Universiteit
Leiden
Juridisch Post Academisch Onderwijs

leidenlaw

CursusaanbodWebinarsSpecialisatieopleiding

docent: Herke Kranenburg

- Wat loopt er nu in Brussel?
- Welke zaken kunnen we binnenkort verwachten u

Actualiteiten (15.00-16.15)
docenten: Gerrit-Jan Zwenne & Hester de Vries

- evaluatie van de UAVG;
- Verzamelwet Gegevensbescherming;
- Richtsnoeren van de EPDB.



advies RvS wel openbaar

nog niet naar Tweede Kamer

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 vleiende 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.



3

overmatig ruime toepassing...



63. [H]et Hof [heeft] [...] **een nogal expansionistische koers** gevaren bij de uitlegging van de werkingssfeer van richtlijn 95/46 en die van de AVG. [...]

65. Naar mijn mening zal ofwel het Hof ofwel de Uniewetgever de werkingssfeer van de AVG echter ooit opnieuw onder de loep moeten nemen. Bij de huidige benadering verwordt de AVG geleidelijk aan tot een van de feitelijk meest veronachtzaamde wetgevingskaders binnen het Unierecht. Dat is niet noodzakelijkerwijs een doelbewuste ontwikkeling. Het is eerder het natuurlijke neveneffect van **de overmatig ruime toepassing van de AVG**, die er op haar beurt toe leidt dat een aantal personen eenvoudigweg **in zalige onwetendheid** verkeert over het feit dat de AVG ook voor hun activiteiten geldt.



4

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



rol van de toezichthouder

Rutte IV: toezichtreflex en Autoriteit Persoonsgegevens

4 Deze week is - met 28 januari als de Dag van de Privacy - een mooi moment om iets over de 'privacyambten' van Rutte IV te zeggen. Ik begin met het toezicht.

Laat ik beginnen met het plan van de Autoriteit Persoonsgegevens (AP) en algoritme-auditor aan te wijzen. Althans de keuze op het eerste gezicht een logische lijkt, zijn er redenen om deze te heroverwegen. Allereerst vanuit het belang van transparantie en verantwoordelijkheid en performance controle. Algoritmen zijn nu al op deze plaats, voorloper van een nog meer uitgebreid gebruik van de hand van de Staat, gegeven op de maatschappelijke implicaties van het gebruik van de sterke gegevens uit een (toekomstige) toezichtreflex. Algoritmen zijn nu al op deze plaats, voorloper van een nog meer uitgebreid gebruik van de hand van de Staat, gegeven op de maatschappelijke implicaties van het gebruik van de sterke gegevens uit een (toekomstige) toezichtreflex.

De AP nagenoeg zonder enige vorm van 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.

De AP nagenoeg zonder enige vorm van 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.

De AP nagenoeg zonder enige vorm van 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.

De AP nagenoeg zonder enige vorm van 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.

De AP nagenoeg zonder enige vorm van 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.

Het Vooraf staat ook op nja.nl/blogs

VOORAF 233

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

rode draad

toepassing van de AVG

rol van het toezicht



6

twee praktijkvoorbeelden

en denk ook aan:

- VoetbalTV & KNLTB
- cookiemuurverbod
- CoronaMelder
- enz.

*De boete die AP aan
Enschede oplegde*

*De DSAR-guidelines
van de EDPB*

7

Enschede: passantentelling of wifitracking?



AUTORITEIT
PERSOONSGEGEVENS

Boete gemeente Enschede om wifitracking

Persbericht / 29 april 2021

Categorie:

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. Ieders telefoon werd apart geregistreerd, met een unieke code.

8

wat is een «persoonsgegeven» ..?

alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon

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

(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.

9

wat is «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

(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.

10

HvJEU: Bodil Lindqvist

Ehvi 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 **naam of anderszins, bijvoorbeeld met hun telefoonnummer** informatie over hun werksituatie en hun liefhebberijen, als een gedeeltelijk geautomatiseerde verwerking van persoonsgegevens aan te merken.

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..

Rb. MNL: Brein/Ziggo

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

Een IP-adres is dus een persoonsgegeven 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.

Dat brein in niet kader van de waarschuwingscampagne (nog gegevens bij Ziggo op te vragen (en, wanneer dat zonder succes vordert) en dat het niet zeker is dat – als zij dat wel doet – doet er niet aan af dat zij wel over dat wettelijke middel beschikt. Het is niet duidelijk of de kosten en mankracht niet excessief zijn in de adressen die Brein verzamelt dus ook ten aanzien van haar g

HvJEU: Breyer

Zie ook: HvJEU 17 juni 2021, C-484/20, ECLI:EU:C:2021:492, nr. 102

[E]en dynamisch IP-adres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als een website bezocht die door deze aanbieder toegankelijk is gemaakt voor het publiek, ten aanzien van die aanbieder (vormt) een persoonsgegeven [...], wanneer hij beschikt over **wettelijke 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

wettelijke middelen?

Rb DHG: fietsendepot

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

7. [Verweerder 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 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 beschikt. Het is niet aan verweerder te maken of 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.

11

Enschede: geen onevenredige inspanning, zegt AP

AUTORITEIT PERSOONSGEGEVENEN

Boete gemeente Enschede om wifitracking

Perdbericht 129 april 2021 Categorie

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 winkeland 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 de wifisignalen op van de mobiele telefoons van passerende mensen. Ieders telefoon werd apart geregistreerd, met een unieke code.



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

Bij [VERWERKER] 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 [VERWERKER] 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

toepassing van de AVG

rol van de toezichthouder

12

EDPB DSAR Guidelines



COMMENTS

prof. dr. G.-J. (Gerth-Jan) ZWENNE*

EDPB Guidelines 01/2022 on Data Subject Access, version 1.0, adopted on 18 January 2022

INTRODUCTION

Without a doubt, data subject access rights are among the most useful rights the GDPR provides data subjects to enhance transparency and to facilitate control over the processing of their personal data. At the same time, the exercise of access rights by data subjects gives rise to many complaints and disputes.¹ As a result, there is a lot of detailed and nuanced case law on the scope of access rights and the applicable exemptions. In addition to the judgments of Court of Justice of the European Union, notably *Rijkeboer*,² *IND*³ and *Nowak*,⁴ there is also a large volume of court decisions by member states' courts, including judgments of the highest national civil and administrative courts.

Surprisingly, the EDPB Guidelines 01/2022 on Data Subject Access Rights seem to ignore, and in some instances even contradict, member state national courts' decisions on data subject access rights. In that respect, the guidelines raise some interesting questions on the legitimacy and validity of the Guidelines. Indeed, pursuant to Article 70(1)(a) GDPR the European Data Protection Board (hereinafter "EDPB" and also "the Board") can issue guidelines, recommendations and best practices in order to encourage consistent application of the Regulation. But does that imply that the Board can overrule or set aside judgments of national courts? Probably not.

This short note will provide some of the most noticeable examples of statements made in the guidelines that are, to say the least, at odds with well-established case law in the Netherlands. In view of the timeframes set by the Board for this consultation, this analysis cannot be exhaustive. However, it is to be expected that further legal analysis of relevant case law in the Netherlands and other member states will reveal many more cases in which the guidelines deviate from national courts' case law. In any case, such legal analysis is needed and assuming the results of that analysis will be incorporated in version 2.0 of the Guidelines, it is likely to result in less unbalanced and controversial guidelines than that found in the current version 1.0. Most likely, this will do

*G.-J. (Gerth-Jan) ZWENNE is a full professor law and digital technologies, Leiden University in the Netherlands and part of the law firm Hys Rijkman in The Hague, also in the Netherlands.



prof. dr. G.-J. (Gerth-Jan) ZWENNE | full professor | senior lecturer for Law and Digital Technologies | Leiden Law School | Leiden University | g.j.zwenne@law.leidenuniv.nl

1



13



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**.

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**

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**.

14



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 [verweerster] 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.

15



AP: Boete DPG Media voor onnodig opvragen identiteitsbewijs

De Autoriteit Persoonsgegevens (AP) legt DPG Media een boete op van 325.000 euro. Het media bedrijf krijgt de boete omdat mensen die hun gegevens wilden inzien of laten verwijderen, daarvoor eerst een identiteitsbewijs moesten opwaarderen. Dat is in deze situatie niet nodig. Hierdoor wordt het media bedrijf AP voor persoonsgegevens 10.

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:2020:2833

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.

16

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 procesdossiers** waarin hij als procespartij betrokken was. [...] Het doel van [verzoeker] bij zijn inzagerecht 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, uitwijssing 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.**

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.**



17

slotsom

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

al was het maar omdat er nog veel meer aankomt:

- Digital Market Act
- Digital Services Act
- AI-verordening
- ePrivacyverordening
- enz.

Bobek

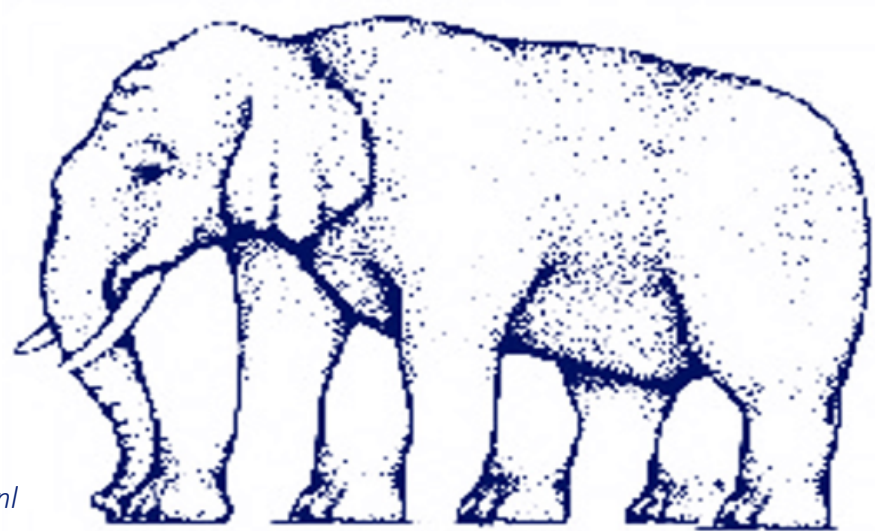
Prins

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

we doen er goed aan...



18



g.j.zwenne@law.leidenuniv.nl