

@zwnne

# Ask Me Anything (about data protection law)

Gerrit-Jan Zwenne Webinar 12 oktober 2021

eLaw Leiden

Stichting  
Contactgroep  
Automatisering

1

eerder

vandaag

A. wanneer is sprake van persoonsgegevens? en wanneer niet?

B. wanneer kunnen gegevens worden gebruikt voor onderzoeksdoeleinden?

C. Internationale gegevensdoorgifte, kan dat nog?

D. het verschil tussen profileren en verzekeren

E. is er een verbod op cookiemuren?

F. controverses over corona

G. vragen over het gerechtvaardigd belang (VoetbalTV)

H. telemarketing

2



3

over de verspreiding van het virus.

Wolfsen eist dat het om maatregelen gaat die de bescherming van persoonsgegevens zo goed mogelijk waarborgen. „Over die spoedwet hebben wij net advies uitgebracht aan het kabinet. Wij sluiten niet uit dat de analyse van die locatie data op een privacy-vriendelijke manier kan, maar dan moet aan strenge normen worden voldaan. Onze adviezen worden meestal opgevolgd, omdat wij een wet buiten werking kunnen stellen als de AVG wordt geschonden”, zegt Wolfsen.

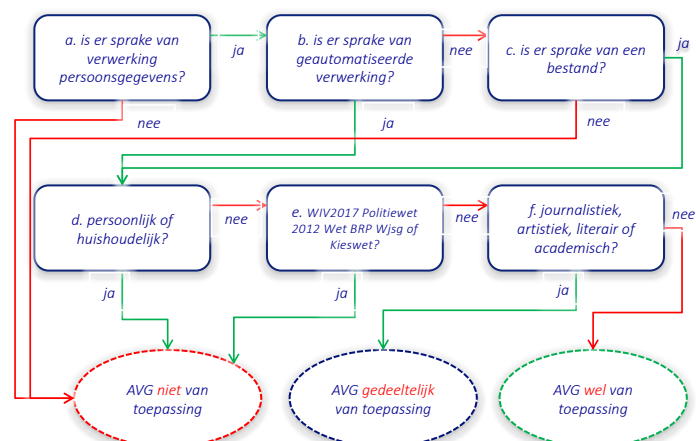
Zorgen over de gevolgen van de coronacrisis leven breder. „Het grootschalig volgen van

4

A.  
*wanneer is sprake van  
 persoonsgegevens?  
 en wanneer niet?*

5

stroomschema...



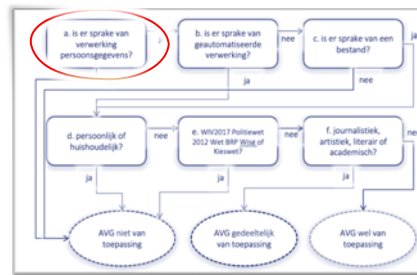
6

## wat is «een verwerking»...?

een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomiseerde procedés

o.a. verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, **gebruiken**, verstrekken door middel van doorzending, verspreiding of enige andere vorm van ter beschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het **afschermen**, **uitwissen** of **vernietigen** van gegevens (enz.)

discussie over het aflezen van de lichaamstemperatuur op een infrarood-thermometer



7

## «verwerking»



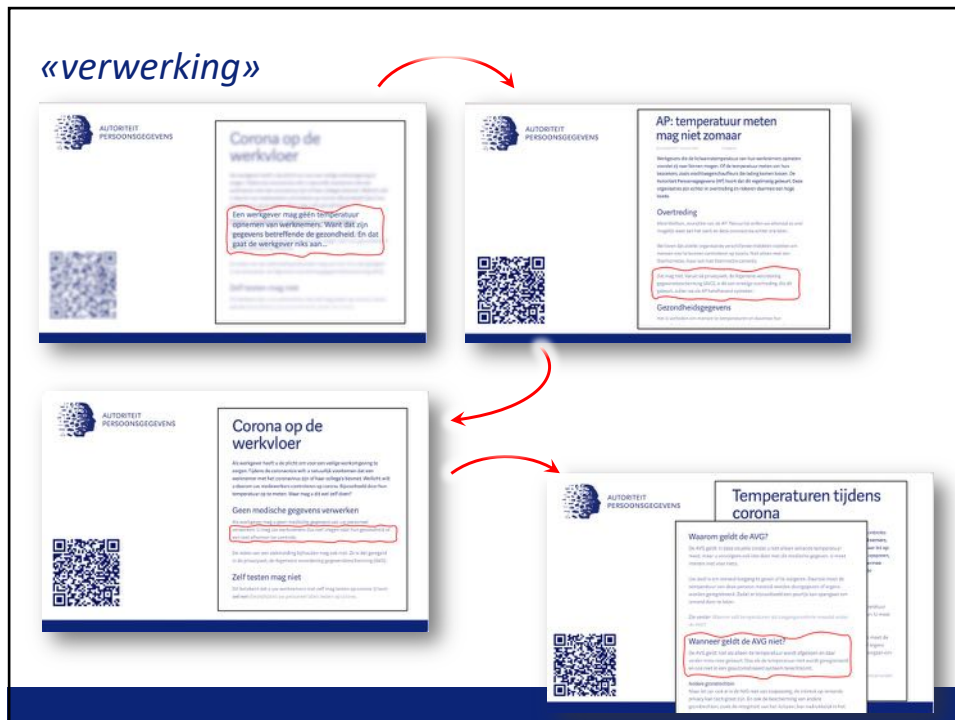
**Mag een bedrijf of werkgever algemene en systematische controles van de lichaamstemperatuur van werknemers en/of bezoekers uitoefenen?**

De Belgische Gegevensbeschermingsautoriteit beschouwt de **loutere opname** van de lichaamstemperatuur niet als een verwerking van persoonsgegevens. Voor zover dergelijke temperatuuropname dus niet gepaard gaat met een bijkomende registratie of verwerking van persoonsgegevens, is de AVG niet van toepassing.

In het algemeen geldt hier dat een werkgever geen maatregelen kan nemen die het bestaande arbeidsrechtelijk regelgevend kader of instructies van bevoegde overheden te buiten gaan.



8



9

*wat zijn «persoonsgegevens»...?*

↓

*alle gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon*

↓

*als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd*

*kost het een onevenredige inspanning om de desbetreffende natuurlijke persoon te identificeren..?*

*discussies over IP-adressen, MAC-adressen, WiFi-tracking, Utrecht CS, Gemeente Enschede, etc.*

*[Er] 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.*

*Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen.*

10

## Haags fietsendepot

Rb 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.** Daartoe 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 persoonsgegevens.**



12

## AP ziet het anders...(?)

AP brief 25 juni 2018 inzake  
Normenkader digitale  
billboards

De AP heeft in haar Beleidsregels cameratoezicht uitgelegd dat ook sprake kan zijn van persoonsgegevens als personen niet of niet herkenbaar in beeld worden gebracht, zolang de beelden betrekking hebben op een natuurlijke persoon en die persoon identificeerbaar is. [...]

Alleen in uitzonderlijke gevallen zal dus géén sprake zijn van de verwerking van persoonsgegevens, als de camera's technisch zodanig zijn ingericht dat het **absoluut niet mogelijk** is om mensen herkenbaar in beeld te brengen.



AUTORITEIT  
PERSOONSGEGEVENS



Het is niet vereist dat iedere mogelijkheid de gegevens met betrekking tot personen te gebruiken, is uitgesloten. Is deze mogelijkheid weliswaar theoretisch aanwezig maar is ondenkbaar dat dit ook daadwerkelijk gebeurt, dan kan ervan worden uitgegaan dat de gegevens niet als persoonsgegevens worden aangemerkt. Kst II 1997/98, 25892, nr. 3, p. 48

14

en dus volgens AP...

*lees: andere EU-lidstaten met dezelfde wetgeving als Nederland (!)*



## Gebruik telecomdata tegen corona kan alléén met wet

Nieuwsbericht / 1 april 2020

Categorie:

Privacy & corona, Internet en telecom

Locatiegegevens gebruiken om de overheid te helpen in de strijd tegen het coronavirus is niet volledig onmogelijk, maar kan alleen als daar een wettelijke regeling voor bestaat. Dat zegt de Autoriteit Persoonsgegevens (AP) in reactie op ideeën om locatiegegevens van burgers in te zetten om verspreiding van het virus te remmen.

'We zien in andere landen systemen waarbij de overheid locatiegegevens van telecombedrijven gebruikt tegen verspreiding van het coronavirus', zegt AP-voorzitter Aleid Wolfsen.

'Ook in Nederland worden dit soort ideeën geopperd. Maar dit kan niet zomaar. Wij hebben gekeken hoe dit eventueel kan, mocht de Nederlandse overheid dit willen.'

15

en dus, volgens AP...



### Locatiegegevens niet anoniem

Volgens zowel privacywet AVG als de Telecommunicatiewet mogen telecombedrijven niet zomaar gegevens van klanten delen met de overheid. Tenzij al die klanten daarvoor zelf toestemming hebben gegeven of de gegevens anoniem zijn.

Toestemming vragen van alle Nederlanders is in dit geval te omslachtig. En het anoniem maken van dit soort gegevens kan niet, omdat dat nooit onomkeerbaar is.

Wie weet waar iemand woont of werkt en die gegevens combineert met de 'geanonimiseerde' locatiegegevens van heel veel mensen, kan met die combinatie achterhalen wie bij welke locatiegegevens hoort.

'Dat maakt van deze gegevens persoonsgegevens en die mag je niet zomaar delen', zegt Wolfsen.

### Locatiegegevens kunnen helpen

De AP ziet dat het beeld bestaat dat het beperkt en onder strenge voorwaarden gebruiken van locatiegegevens de overheid mogelijk kan helpen om de verspreiding van het virus in te dammen.

16

KST II 2019/20, 35479 Wetsvoorstel Tijdelijke informatieverstrekking RIVM



17

Kst II 2020/21, 35479, nr. 3, p. 6-7

Wetsvoorstel Tijdelijke wet informatieverstrekking RIVM in verband met COVID-19

*Er is misschien een theoretische mogelijkheid om te identificeren. Maar daarmee zijn het nog geen persoonsgegevens...!*

*De informatie [...] is wegens het hoge aggregatieniveau en het minimale getal van 15 per groep per gemeente per uur, naar het oordeel van de regering niet herleidbaar tot identificeerbare natuurlijke personen.*

*Hoewel er studies zijn die de – theoretische – mogelijkheid aantonen om in bepaalde gevallen ook geaggregeerde locatiedata te herleiden tot identificeerbare natuurlijke personen, valt niet redelijkerwijs te verwachten dat de verwerkingsverantwoordelijke of een andere persoon deze middelen gebruikt.*

*De kosten van en de tijd benodigd voor identificatie zonder daarbij gebruik te kunnen maken van de brongegevens (de locatie- en verkeersgegevens die de aanbieders beheren) maken een dergelijke identificatie onwaarschijnlijk.*

*Belangrijk hierbij is dat het de aanbieders op grond van de Telecommunicatiewet verboden is om de brongegevens aan derden ter beschikking te stellen.*



18



controverse...!

Kst II 2020/21, 35479, nr. 3, p. 6-7



Daarbij verwijst de regering naar HvJ EU 19 oktober 2016, C-582/14, **Breyer/Duitsland**, ECLI:EU:C:2016:779. Het Hof overweegt in punt 46 van dit arrest dat herleidbaarheid niet redelijkerwijs kan worden aangenomen indien de identificatie van de betrokkene bij wet verboden is. Ook gelden er voor de aanbieders op grond van de Telecommunicatiewet strenge eisen voor de beveiliging van de brongegevens waardoor ook het risico op onbevoegde toegang tot deze gegevens tot een minimum wordt beperkt.

Tot slot zijn zowel het RIVM als het CBS bij de verwerking van de door de aanbieders verstrekte informatie gebonden aan het doel in artikel 14.7 van de Telecommunicatiewet. Dit betekent dat het voor deze instanties verboden is om de gegevens herleidbaar te maken, als dat technisch al mogelijk zou zijn. **Het gaat hier naar het oordeel van kabinet dan ook om statistische gegevens waarop de AVG niet van toepassing is.**



19



toerisme. Op deze gebieden is een grote behoefte aan snel beschikbare en meer gedetailleerde cijfers over waar mensen zich bevinden.

**Methode**

De methode is tot stand gekomen in een nauwe samenwerking tussen CBS en T-Mobile. Deze samenwerking is december 2019 beëindigd. Om tot de tellingen te komen doorlopen we een aantal stappen waarbij de data al bij de bron (T-Mobile) volledig anoniem gemaakt. De methodebeschrijving van dit onderzoek is onderaan deze pagina te vinden. Transparantie over onze methodes is van belang voor het produceren van officiële statistiek en de samenwerking met andere organisaties.

■ Zo is het mogelijk dat een ontwikkelde methode bijvoorbeeld uitgroeit tot een internationale standaard. Bij het verwerken van deze gegevens tot statistiek wordt de privacy gegarandeerd. Er wordt immers uitsluitend gewerkt met geanonimiseerde, geaggregeerde data. Dit betekent dat de data niet te herleiden is tot individueel niveau, het blijven geanonimiseerde datasets. Om herleiding naar personen uit te sluiten, zijn er verschillende maatregelen genomen. Zo blijven alle data bij de datacenters van T-Mobile en wordt er gekeken naar reeksen van gebeurtenissen (de activiteit) op het netwerk.

**Resultaten**

De bezoekerspatronen per gemeente zijn **verwerkt**. Door een locatie aan te klikken wordt voor iedere gemeente een patroon zichtbaar van personen, die de gemeente



20

**AUTORITEIT PERSOONSgegevens**

## Boete gemeente Enschede om wifitracking

Boete van 600.000 euro, omdat de gemeente wifitracking gebruikte in de binnenstad op een manier die niet mag. Daardoor was het mogelijk werkloos publiek en mensen die in de binnenstad wonen of werken te volgen.

### Wifitracking in Enschede

De gemeente Enschede betaalde in 2017 een nu bekende op draadloze in de binnenstad te gaan meten. De gemeente huurde daarvoor een bedrijf in dat is gespecialiseerd in het bellen van personen.

Meerkeuzes in de actualiteiten volgen de wifitracking op van de mobiele telefoons van passende mensen. Iedere telefoon wordt apart geregistreerd met een unieke code.

Door te bellen hoewel telefoons er op een bepaald moment rond een mobiliteit zijn, weet je hoe dicht het is. Hoofd je niet een langere periode bij welke telefoon langere tijd mobiliteit heeft, dat weet je al bellen is het volgen van mensen.

21

**B.**

*wanneer kunnen gegevens worden gebruikt voor onderzoekdoeleinden?*

22

## doelbinding (en wetenschappelijk onderzoek)

*persoonsgegevens moeten*

- worden **verzameld** voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en
- mogen vervolgens **niet verder worden verwerkt op een met die doeleinden onverenigbare wijze** ("doelbinding")

*De verdere verwerking met het oog op archivering in het algemeen belang, **wetenschappelijk of historisch onderzoek of statistische doeleinden** wordt [...] niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd*

vermoeden van  
verenigbaarheid!

23

## proportionaliteit en subsidiariteit

*de gevolgen van de gegevensverwerking mogen niet verder gaan dan nodig oftewel*

*is er een evenwichtige verhouding tussen*

- *het onderzoeksbelang waarvoor er wordt verwerkt, en*
- *het privacybelang van het individu op wie de gegevens betrekking hebben..?*

*voor de verwerking zijn geen alternatieven die de privacybelangen minder aantasten*

belangen-  
afweging!

24

verwerkingsverbod voor bijzondere gegevens

uitzondering

verwerking mag wél als

a) verwerking *noodzakelijk* is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden

b) onderzoek dient een *algemeen belang*

c) het vragen van uitdrukkelijke toestemming is *onmogelijk* of kost een *onevenredige inspanning* ;  
én

d) er is voorzien in zodanige *waarborgen* dat het privacybelang niet onevenredig wordt geschaad

gezondheid, geloof, politieke voorkeur, biometrische gegevens etc.

art. 24 UAVG

zie weer: de discussies over telecom-locatiegegevens, WiFi-adressen, etc.

zo(veel) mogelijk anonimiseren!

25

C.

internationale gegevens-  
doorgifte, kan dat nog?

26



27

HJEU 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (Schrems I)

HJEU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559 (Schrems II)

~~EU-US Safe Harbour~~

~~EU-US Privacy Shield~~

~~Model Contracten (Standard Contractual Clauses: or "SCC")~~

maar er moeten wel waarborgen zijn dat er een 'essentially equivalent level of protection' is...

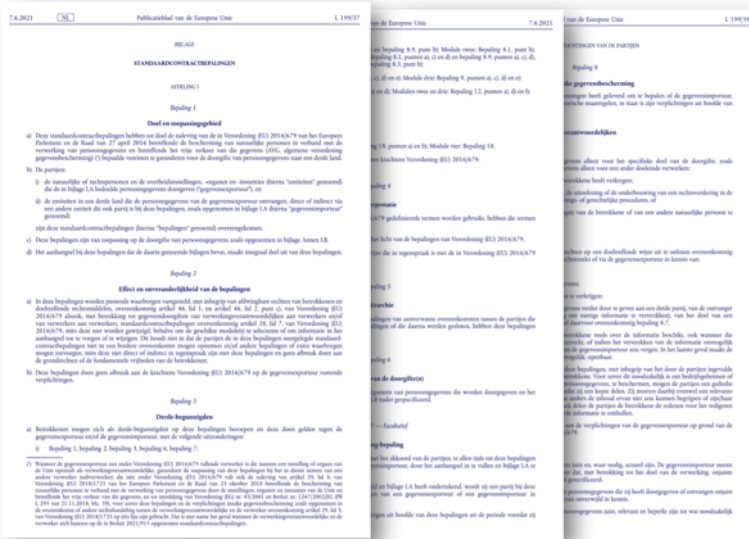
**Schrems II: déjà vu all over again**

prof. mr. G.J. Zwenne en mr. B.D.P. van der Eijk

28

# nieuwe modelcontracten ("SCCs")

ACTUALITEITEN



29

## D. het verschil tussen profileren en verzekeren

30

## profilering (~ prō'fīl'ehr'ing)

Art. 4(4)  
AVG

geautomatiseerde verwerking waarbij aan de hand van persoonsgegevens

- bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd
- met de bedoeling met name het volgende te analyseren of te voorspellen:
  - beroepsprestaties
  - economische situatie
  - gezondheid
  - persoonlijke voorkeuren en interesses
  - betrouwbaarheid en gedrag
  - locatie of verplaatsingen

31

## geautomatiseerde besluitvorming

geautomatiseerde verwerking waarbij aan de hand van persoonsgegevens besluiten worden genomen

géén definitie

wél voorbeelden

- opleggen van snelheidsboeten op grond van bewijs van flitscamera's
- uitnodigen voor een sollicitatiegesprek
- beoordelen van belastingaangiften
- etc.

32

*de regels*

Art. 22  
AVG

*een recht om*

- niet te worden onderworpen aan een besluit dat uitsluitend is gebaseerd op geautomatiseerde verwerking, waaronder profilering
- waaraan voor hem of haar rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.


*uitzonderingen*

- noodzakelijk voor uitvoering van overeenkomst tussen de betrokkene en een verantwoordelijke
- toegestaan bij Uniewetgeving of nationale wetgeving
- uitdrukkelijke toestemming van de betrokkene.



33

E.  
*is er sprake van een verbod  
op cookiemuren..?*



34



## cookieregels

Voordat een cookie wordt geplaatst op een device moet de gebruiker

- goed daarover worden geïnformeerd, én
- moet zijn/haar **toestemming** worden verkrijgen

Artikel 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.

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)

35



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 géén geldige toestemming krijgen van hun bezoekers of gebruikers.



36

## cookiemurenverbod (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*



37

*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 vakantiekookiemuurtoestemming» aankomt.*

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

38

## Voorstel ePrivacyverordening (10 januari 2017)

cookietoestemming kan ook worden gegeven via  
zgn. browserinstellingen

maar gebruikers moeten er iedere zes  
maanden op worden gewezen dat  
toestemming kan worden ingetrokken...



39

### 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 on 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.

40

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 technologies, users are increasingly frustrated to provide consent to use 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 pre-ticked boxes, should be prohibited.

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.

41

*cookies in het zgn. laatste concept d.d. 10 februari jl.*

→ *het onderhandelingsmandaat*

The collage shows several overlapping pages of a legal document. Visible text includes:

- Article 13(3): "Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 10(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged, or a payment may be pursued in accordance with..."
- Article 14(1)(b): "the end-user has given consent, or"
- Article 14(1)(c): "it is strictly necessary for providing a service specifically requested by the end-user"
- Article 14(1)(d): "it is necessary to locate terminal equipment when an end-user makes an emergency communication other than to the single European emergency number '112' or a national emergency number, in accordance with Article 13(3)."
- Article 14(1)(e): "where the processing for purposes other than that for which the information has been collected under this paragraph is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 the person using processing and storage capabilities or collecting information processed by or stored in the end-user's terminal equipment shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia:"
- Article 14(1)(e)(i): "any link between the purposes for which the processing and storage capabilities have been used or the information have been collected and the purposes of the intended further processing;"
- Article 14(1)(e)(ii): "the context in which the processing and storage capabilities have been used or the information have been collected, in particular regarding the relationship between end-users concerned and the provider;"
- Article 2: "The collection of information emitted by terminal equipment of the end-user to enable the use of network services shall be limited to what is strictly necessary for the provision of those services."
- Article 3: "The information to be provided pursuant to paragraph 2a may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner."
- Article 4: "The Commission shall be empowered to adopt delegated acts in accordance with Article 28 concerning the information to be processed by the standardized icons and the procedures for providing standardized icons."

42

ACTUALITEITEN

*cookiewall in laatste concept d.d. 10 februari jl.*

[...] [W]here access is provided without direct monetary payment and is made dependent on the consent of the end-user to the storage and reading of cookies for additional purposes, requiring such consent would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of **clear, precise and user-friendly information** about the purposes of cookies and similar techniques, between **an offer that includes consenting** to the use of cookies for additional purposes on the one hand, and **an equivalent offer by the same provider that does not involve consenting** to data use for additional purposes, on the other hand.

Conversely, in some cases, making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a **clear imbalance** between the end-user and the service provider as depriving the end-user of a genuine choice. This would normally be the case for websites providing certain services, such as those provided by **public authorities**. Similarly, such imbalance could exist where the end-user has only few or **no alternatives** to the service, and thus has no real choice as to the usage of cookies for instance in case of service providers in a **dominant position**.

cookiewall is allowed, if

- clear precise and user-friendly information is provided
- user can chose between (a) free services with consent for additional purposes and (b) payed services without consenting for additional purposes

but not if there is no real choice, i.e.

in case of a clear imbalance between end-user and provider, e.g. public authorities or provider with dominant

recital  
20aaaa

43

The screenshot shows the RTL Nieuws website interface. The main headline is "RTL Nieuws start betaalde variant zonder reclame" (RTL News starts paid version without ads), dated 28 maart 2021. The page features a navigation bar with links for "HOME", "NIEUWS", "AGENDA", "KOPSCYFERS", "LUISTERCIJFERS", "PODCAST YDF 50", "OVER ONS", and "CONTACT". A search bar is visible in the top right. The article content includes a large image of the RTL logo and a "NIEUWSBRIEF" (newsletter) sign-up form with fields for "Voornaam", "Achternaam", and "E-mailadres". A "REACTIES" (reactions) section is also visible on the right side of the page.

44

**CNIL.**  
To protect personal data, support innovation, preserve individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL | Q | TW

» Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines

### Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines

29 June 2020

In its decision of 19 June 2020, the Council of State (Conseil d'État) essentially validated the guidelines on cookies and tracking devices adopted by the CNIL on 4 July 2019. The purpose of these guidelines was to clarify the enhanced legal

**GDPR. However, the 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. The CNIL takes note of this decision and will adjust its guidelines and future recommendation to**

On July 4<sup>th</sup>, 2019, as part of its action plan on targeted advertising and following consultation with professionals and civil society, the CNIL adopted guidelines on cookies and other tracking devices in order to clarify the applicable rules and best practices in this area since the entry into force of the General Data Protection Regulation (GDPR).

The purpose of these guidelines is to clarify the conditions under which the GDPR reinforces the rights of Internet users, in order to enable them to maintain control over their personal data against cookies and tracking devices that are frequently used, in particular when browsing websites.

These guidelines were challenged by several professional associations and unions in the online advertising, e-commerce and media sectors.

*[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.*

*consequently, at the moment cookiewalls are not prohibited!*

45

## F. corona-controverses

46

## controverse over meten van lichaamstemperatuur

«verwerking»

Mag een bedrijf of werkgever algemene en systematische controles van de lichaamstemperatuur van werknemers en/of bezoekers uitvoeren?

De Belgische gegevensbeschermingsautoriteit beschouwt de loutere opname van de lichaamstemperatuur niet als een verwerking van persoonsgegevens. Voor zover dergelijke temperatuuropmetingen niet gepaard gaan met een bijkomende registratie of verwerking van persoonsgegevens, is de AVG niet van toepassing.

In het algemeen geldt hier dat een werkgever geen maatregelen kan nemen die het bestaande arbeidsrechtelijk regelgevend kader of instructies van bevoegde overheden te buiten gaan.

«verwerking»

Corona op de werfplaats

AP-temperatuur meten mag niet zomaar

Corona op de werfplaats

Temperaturen tijdens corona

GBA  
gegevensbeschermingsautoriteit

47

## controverse over geanonimiseerde locatiegegevens

en dus volgens AP...

Gebruik telecomdata tegen corona kan alléén met wet

November 17, 2020

Categorie: Privacy & corona, Internet en telecom

Locatiegegevens gebruiken om de overheid te helpen in de strijd tegen het coronavirus is niet volledig onmogelijk, maar kan alleen als daar een wettelijke basis voor bestaat. Dat zegt de Autoriteit Persoonsgegevens (AP) in reactie op vragen om locatiegegevens van burgers in te zetten om verspreiding van het virus te nemen.

«We zien andere landen systemen waarbij de overheid locatiegegevens van telecombedrijven gebruikt tegen verspreiding van het coronavirus», zegt AP-voorzitter Aald Wulfen.

Ook in Nederland worden dit soort ideeën geopperd. Maar die kan niet zomaar. Wij hebben gekeken hoe dit eventueel kan, mocht de Nederlandse overheid dit willen.

lees: andere EU-lidstaten met dezelfde wetgeving als Nederland (...)

48

## controverse over vaccinatiegegevens

verwerkingsverbod voor  
gezondheidsgegevens



zorgdragen voor een veilige  
werkomgeving (Arbowet)

goed werkgeverschap

49

### de Volkskrant

INTERVIEW ALEID WOLFSEN

#### Aleid Wolfsen, voorzitter van de privacywaakhond, over de corona-app: 'De belofte van Google en Apple is te mager'

De veelbesproken app CoronaMelder werd op de eerste dag al ruim 430.000 keer gedownload. Maar wat de Autoriteit Persoonsgegevens betreft is er nog veel mis met de privacy. Voorzitter Aleid Wolfsen maakt zich zorgen.

Laurens Verhagen 18 augustus 2020, 18:09



De door de minister geraadpleegde landsadvocaat is **nogal kritisch op uw advies. Zo zou u weinig aandacht hebben voor de buitengewone omstandigheden die de app noodzakelijk maken. Wat vindt u van die kritiek?**

'Die zit op de grens van het ongepaste. Over de ernst van corona bestaat bij ons geen enkele twijfel, maar juist in tijden van crises moet je kritisch blijven en helder nadenken. De Nederlandse burger moet zeker weten dat niemand bij zijn persoonlijke gegevens kan komen, ook al is de app vrijwillig.'

**Uw critici zeggen dat de app door deze harde opstelling vertraging kan oplopen**

'Dat is echt onzin. Die appathon met de eerste ideeën voor de app was er al in april. Wij hebben toen dag en nacht doorgewerkt om

50



## G. gerechtvaardigd belang (VoetbalTV)

51

### gerechtvaardigd belang...

Artikel 6.1 AVG

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

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



52



53



AUTORITEIT  
PERSOONSGEGEVENS

*nieuw: een positieve toets(!)*

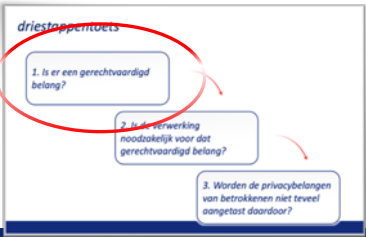
*[V]oorwaarde is dat de belangen van de verwerkingsverantwoordelijke of een derde kwalificeren als gerechtvaardigd. Dat houdt in dat die belangen in (algemene) wetgeving of elders in het recht zijn benoemd als een rechtsbelang. Een belang dat ook in rechte beschermd wordt, dat beschermingswaardig wordt geacht en dat in beginsel gerespecteerd moet worden en 'afgedwongen' kan worden.*

*De verwerkingsverantwoordelijke of derde moet zich dus op een (geschreven of ongeschreven) rechtsregel of rechtsbeginsel kunnen beroepen.*

AP, Normuitleg 'gerechtvaardigd belang' 1 november 2019

*zgn. positieve toets: uit de wet of rechtsbeginsel moet blijken dat het belang gerechtvaardigd is*

*en dus geen negatieve toets, waarbij het belang gerechtvaardigd is, tenzij het bij wet of rechtsbeginsel is verboden*



54

 **AUTORITEIT  
PERSOONSgegevens**

*wat géén gerechtvaardigd belang kan  
zijn, volgens de toezichthouder...*

‘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

55

*wat vinden anderen..?*

AG Bobek 19 december 2018, Zaak C-40/17 (Fashion ID)

Richtlijn 95/46 bevat wat het begrip „gerechtvaardigd belang” betreft geen definitie of opsomming. Dit begrip is tamelijk flexibel en open van aard. Mits op zichzelf wettig, bestaat er geen type van belang dat per se uitgesloten is.

Kst II 2997/98, 25892, nr. 3, p. 86

Een gerechtvaardigd belang van de verantwoordelijke kan aanwezig worden geacht in het geval dat de betreffende verwerking voor laatstgenoemde noodzakelijk is om zijn reguliere bedrijfsactiviteiten te kunnen verrichten. De verantwoordelijke kan zijn beroep of bedrijf niet goed uitoefenen indien hem de mogelijkheid zou worden ontzegd de met het oog daarop noodzakelijke gegevens te verwerken.

AP Onderzoeksrapport Bluetrace 1 september 2016

Het verzamelen van informatie over aantallen winkelbezoekers, drukte op bepaalde tijden en bijvoorbeeld de route die het publiek loopt door een winkel, door middel van wifi-tracking, kan op zichzelf een gerechtvaardigd commercieel belang zijn van de winkeliers en Bluetrace

overweging 47 Preambule AVG

De verwerking van persoonsgegevens ten behoeve van **direct marketing** kan worden beschouwd als uitgevoerd met het oog op een gerechtvaardigd belang.

Irish Data Protection Commissioner

What Kinds of Legitimate Interests Are Covered?  
As set out in Article 6(1)(f) GDPR, the legitimate interests which ground reliance on this legal basis may either be those of the controller itself or the interests of third parties. The types of legitimate interests may include **commercial interests**, individual interests, or broader societal benefits.

56




57

VoetbalTV

Rb Midden-NLD 23 november 2020, ECLI:NL:RBMNE: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.




58

## VoetbalTV

Rb Midden-NLD 23 november 2020, ECLI:NL:RBMNE: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 in de verwerking en alleen al daarom onrechtmatig handelt. Verweerders uitspraak aan de eiseres in de kern alleen maar gaat om het te gelde maken van persoonsgegevens en dat dit belang nooit een gerechtvaardigd belang kan worden. Het gaat eraan voorbij dat het HvJ het op voorhand uitsluiten van bepaalde belangen nu juist verbiedt. Evenmin volgt de rechtbank de conclusie van de verweerder dat de noodzakelijkheidstoets en de belangenafweging zinloos zijn als wordt aangenomen dat het belang dat eiseres nastreeft een gerechtvaardigd belang is.



59

ACTUALITEITEN

*en toch: zomaar een recent informatieverzoek van de toezichthouder...*

VRAGEN MET BETREKKING TOT DE GRONDSLAG

2. Licht toe op basis van welke grondslag, bedoeld in artikel 6, eerste lid, van de AVG, de verwerkingen met betrekking tot de dienst plaatsvinden.

a. beschrijf het desbetreffende belang, en overleg de in uw DPIA's vermelde legitieme interest assessment(s) indien deze is of zijn opgesteld

b. licht toe of het desbetreffende belang een eigen belang is, of dat van een derde (en in het laatste geval: welke derde)

c. licht toe in hoeverre dit belang in rechte wordt beschermd (dat wil zeggen: tot uiting komt in concrete wetgeving en/of algemene rechtsbeginselen)

nog steeds een positieve toets..!?

60

## H. telemarketing

61

1 juli 2021

ACTUALITEIT

Home > Onderwerpen > Bescherming van consumenten >

### Nieuwe regels voor telefonische verkoop (telemarketing)

Vanaf 1 juli 2021 mogen bedrijven **consumenten** niet langer ongevroegd bellen om producten of diensten te verkopen. **Goede doelen** mogen goede doelen niet langer ongevroegd bellen voor een donatie. Dit is het gevolg van een wijziging in de Telecommunicatiewet die consumenten meer bescherming moet bieden.

*incl. zzp-ers* →

#### Telefonische verkoop alleen voor klanten of na toestemming

Volgens de nieuwe regels mogen bedrijven of ideële organisaties (zoals goede doelen) alleen in de volgende gevallen bellen:

- De consument is een **klant van het bedrijf** (of is de afgelopen 3 jaar klant geweest).
- De consument is **aanwezig geweest** bij een bijeenkomst van de organisatie of is bij een bijeenkomst aanwezig geweest.

Verder geldt:

- Een bedrijf of goed doel mag mensen niet onder druk zetten om toestemming te geven.
- Het moet duidelijk zijn voor welke producten of diensten de toestemming geldt (en voor hoelang).
- Anoniem bellen mag niet meer. Het telefoonnummer van de organisatie moet zichtbaar zijn.
- Het gebruik van vooraf aangevinkte vakjes is niet toegestaan.
- De consument moet de toestemming makkelijk kunnen intrekken.

62



*@zwnne*

# vragen?

zwenneblog • g.j.zwenne@law.leidenuniv.nl • @zwnne

