

@zwnne

VPR-A SPECIALISATIEOPLEIDING | 2024

e-Privacy: de regels voor spam, telemarketing, geheime nummers, verkeersgegevens. En voor cookies

Prof. mr. G-J. (Gerrit-Jan) ZWENNE | 5 september 2024



Universiteit
Leiden



1

The screenshot shows a news article from NRC. The title is 'UWV negeerde twee jaar lang waarschuwingen over privacyschendingen'. The sub-headline is 'Cookies Een interne toezichthouder zou volgens de NOS en Nieuwsuur al sinds 2020 hebben gewaarschuwd voor de onwettige manier waarop uitkeringsinstantie UWV omsprong met de cookiewet.' The author is Thomas Borst, dated 3 augustus 2023, with a reading time of 1 minute. The article text is as follows:

Uitkeringsinstantie UWV zou al sinds 2020 weet hebben van de wijze waarop de privacy van uitkeringsgerechtigden is geschonden. Dat melden de NOS en Nieuwsuur donderdag op basis van niet-openbare stukken waaruit zou blijken dat een interne toezichthouder verschillende keren heeft gewaarschuwd voor het beleid. Daarbij werden zonder toestemming cookies geplaatst, die vervolgens zijn gebruikt om fraudeurs op te sporen.

Vakbond FNV noemde de beschuldigingen „zeer verontrustend”. „Het UWV moet alle dataverzameling voor opsporing en handhaving direct stoppen. We overwegen een kort geding om dat voor elkaar te krijgen”, aldus FNV-vicevoorzitter Kitty Jong.

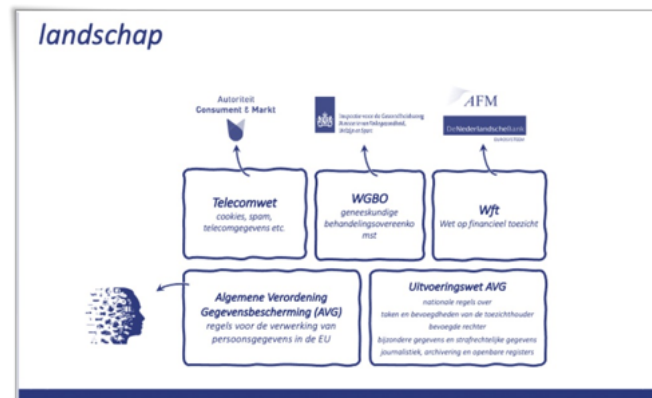
„De ontwikkeling van een cookie consent manager heeft niet voldoende prioriteit gekregen”, reageert het UWV donderdagmiddag. De uitkeringsinstantie erkent in 2020 signalen te hebben gekregen dat de manier waarop cookies werden geplaatst niet aan de Telecommunicatiewet voldeed, maar zegt wel dat vervolgens is besloten een nieuw systeem te bouwen.

De aanpassing bleek alleen „zeer complex” en kostte veel tijd om zorgvuldig te doen, aldus de woordvoerder. „Dat samen heeft de doorlooptijd van de uiteindelijke oplossing verlengd. Met de kennis van nu hadden wij hier meer aandacht en prioriteit voor moeten hebben.”

2

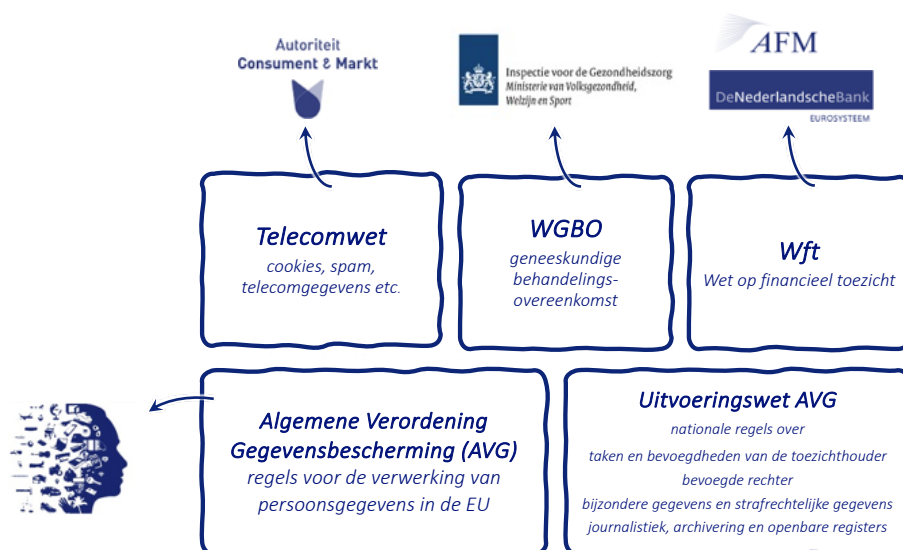
roadmap

- *vertrouwelijkheid en beveiliging*
- *anoniem bellen en gebeld worden, geheim nummer*
- *verkeers- en locatiegegevens*
- *spam en telemarketing, en cookies*



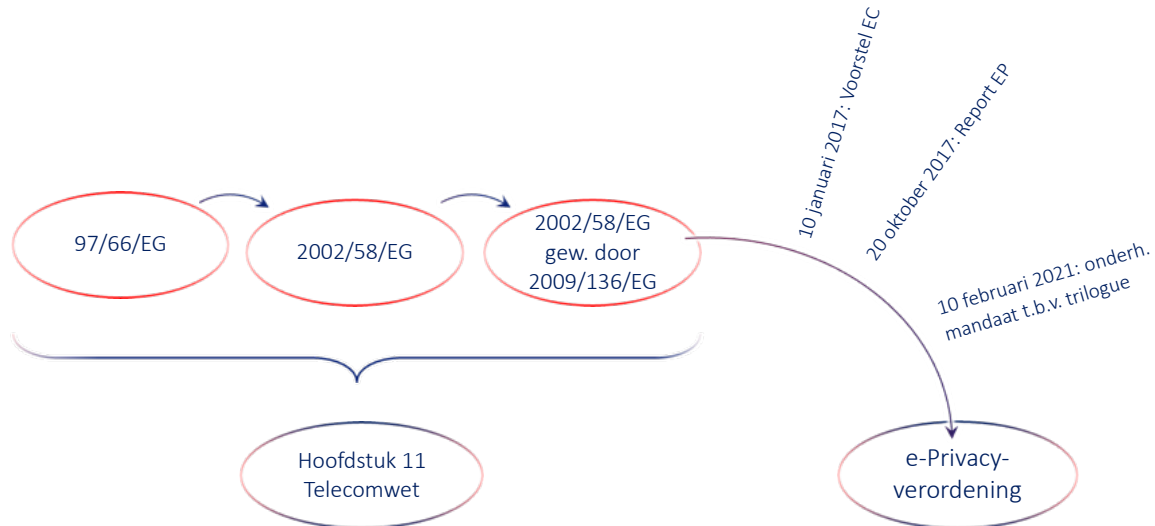
3

landschap



4

van e-Privacyrichtlijn naar -verordening



5

Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code (Telecoms Code)

Art. 2(4)

'electronic communications service' means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services

- (a) 'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
- (b) **interpersonal communications service**
- (c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting

Over The Top ("OTT") Services
e.g. Whatsapp, Signal, Telegram
etc.

Art. 2(5)

a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service

6

vertrouwelijkheid en beveiliging



7

Autoriteit Consument & Markt

Voorlopige bevindingen OPTA over gebruik Deep Packet Inspection

Medio 2011 kwam in het nieuws dat enkele mobiele netwerkaanbieders gebruikmaken van technieken waarmee zij op diepgaand niveau datapakketten analyseren die over hun mobiele netwerk getransporteerd worden. Deze technieken, die doorgaans aangeduid worden met de term Deep Packet Inspection (DPI), zouden inbreuk kunnen maken op de persoonlijke levenssfeer van gebruikers van die netwerken. OPTA heeft daarom besloten een 'quick-scan' te starten onder de vier grootste mobiele netwerkaanbieders: KPN, Vodafone, T-Mobile en Tele2. In deze 'quick-scan' is nagegaan of en hoe deze partijen hun dataverkeer analyseren. Op basis van deze 'quick-scan' concludeert OPTA dat er in dit stadium van het onderzoek op basis van de Telecommunicatiewet geen aanleiding is voor handhavend optreden.

Op basis van de 'quick-scan' concludeert OPTA dat de vier partijen hun dataverkeer analyseren. Hierbij heeft OPTA geen aanwijzingen gevonden dat de onderzochte aanbieders e-mailberichten van hun abonnees lezen, verstuurd foto's bekijken of bijdragen op sociale netwerken lezen. Wel stelt OPTA vast dat de vier aanbieders bij hun analyse kennisnemen van meer informatie dan alleen de informatie die bestemd is voor de afhandeling van verkeer. Zo kan het bijvoorbeeld zijn dat bijgehouden communicatiegeheim in het geding. Ook kan de hoeveelheid en de soort gegevens die de onderzochte aanbieders verwerken en analyseren op gespannen voet staan met de zorgplicht. De zorgplicht verplicht aanbieders om zorg te dragen voor de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van de abonnees.

AUTORITEIT PERSOONSGEGEVENS

Telecomaanbieders passen data-analyse aan na onderzoek CBP

Persbericht / 4 juli 2013 Categorie: Internet en telecom

Het College bescherming persoonsgegevens (CBP) publiceert vandaag zijn rapporten naar aanleiding van het onderzoek naar analyse van het dataverkeer (packet inspection) over het mobiele netwerk door de telecomaanbieders KPN, Tele2, T-Mobile en Vodafone. Deze vier telecomaanbieders zijn de grootste mobiele netwerkaanbieders in Nederland. Tijdens het onderzoek constateerde het CBP bij alle bedrijven overtredingen van de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet (Tw).

De bedrijven bleken onder meer in strijd met de wet op detailniveau gegevens te bewaren over de bezochte websites en gebruikte apps. Deze gegevens worden verzameld en opgeslagen op servers van de telecomaanbieders. Het is niet noodzakelijk om deze gegevens op klantniveau te bewaren.

8

anoniem bellen en gebeld worden

- nummerherkenning
- ongespecificeerde telefoonrekening

anonieme tipgever
klokkenluiders, etc.

Art. 11.9
Tw

- *slachtoffer van stalking, telefoonterreur*

*meldpunt, anonieme
tiplijn, journalist i.v.m
bronbescherming*

- recht op anoniem bellen
- recht om niet anoniem te worden gebeld
- recht om wel anoniem te worden gebeld

maar beperkingen m.b.t. alarmnummers

► niet meer in ePrivacyverordening

recht op gespecificeerde rekening (KPN),
en recht op ongespecificeerde rekening

Art. 11.4
Tw

vaste telefoon in
studentenhuis

Art. 7-8 Rl.
2002/58

Art. 12-14
ePR

'geheim nummer'

- toestemming vereist voor opname gegevens in telefoongids of abonnee informatiedienst
- voor standaardgids of -informatiedienst moet Telco toestemming vragen

Art. 11.6
Tw

→ 18xy: 1850, 1888

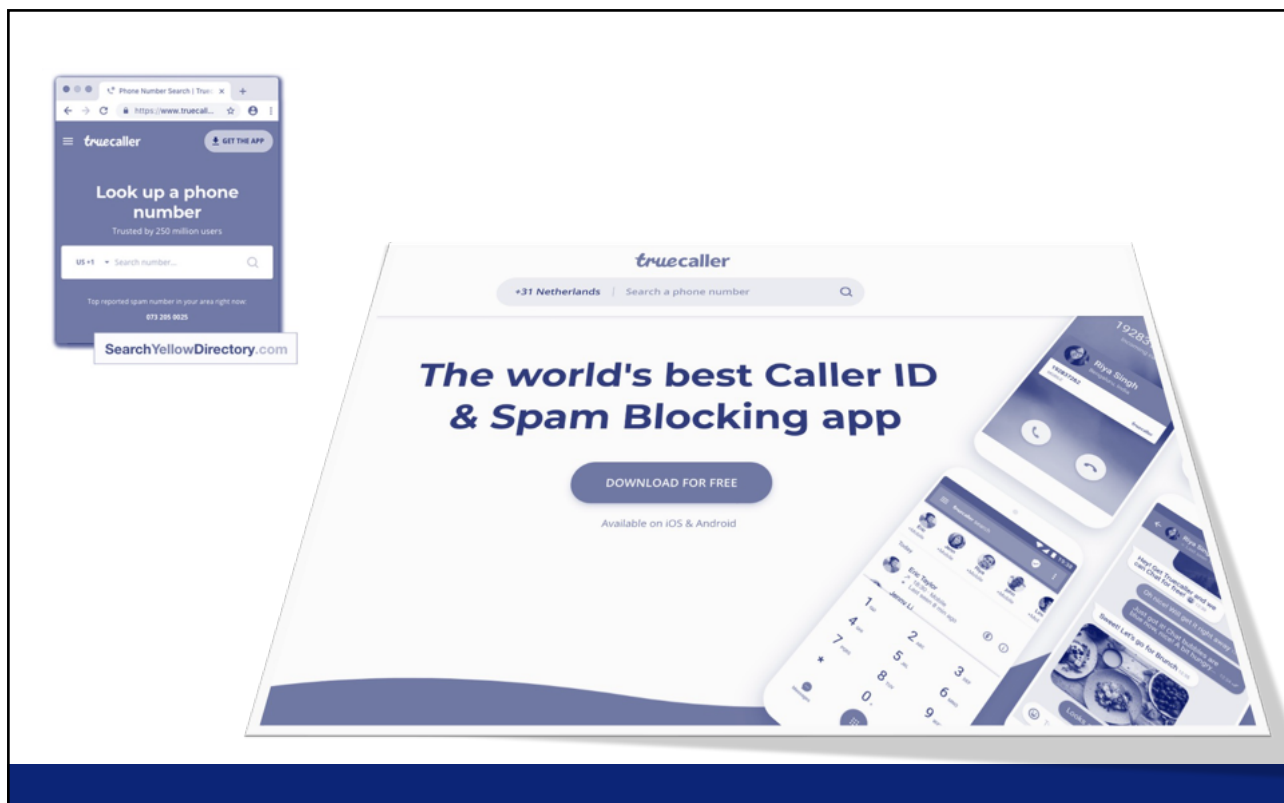
zoeken op naam in
combinatie met adres en
woonplaatsgegevens

hoe zit het met 'omgekeerd zoek-
diensten (reversed search)..?

Art. 12 Rl.
2002/58

Art. 15
ePR





11

reversed search

SearchYellowDirectory.com
White Pages
Yellow Books
Reverse Phone
List of Countries

Netherlands Phone Numbers

Enter Dutch country code 31 + area code and local number. Search for people in Netherlands, area codes list, major cities.

International Directories
All Area Codes USA, Canada

Netherlands Reverse Lookup

+31

START NOW

3 Easy Steps
1. Click 'Start Now'
2. Free Access - No Sign up!
3. Get Free Printable Forms

onlineformfinder.com

Home / Reverse Phone / 31 Netherlands Phone Numbers

Phone number in Netherlands: +31 - Area Code - Local Number

Country: Netherlands
Country code: 31
Capital of Netherlands: Amsterdam
Area code 20: Amsterdam
Local Time: 06/20/2019 07:56:03 PM
Time Zone: Central European Time (CET)

12

Besluit

Besluit handhavingsverzoek van Telefoongids over omgekeerd zoeken

17-10-2007

De Telefoongids heeft zowel het college van OPTA als het College bescherming persoonsgegevens (CBP) verzocht om handhavende maatregelen tegen een aantal aanbieders van zogenaamde 'omgekeerd zoeken' diensten op internet. Gebruikers van deze (op internet) aangeboden zoekdiensten kunnen met een opgegeven telefoonnummer bijbehorende naam- en adresgegevens vinden, zonder dat de betreffende abonnee voor deze zoekmogelijkheid afzonderlijk toestemming heeft gegeven.

OPTA en het CBP hebben gezamenlijk onderzoek gedaan naar deze 'omgekeerd zoeken' diensten, wat enkele betrokkenen al aangezet heeft om hun activiteiten te wijzigen. Het college van OPTA wijst het verzoek van De Telefoongids af.

Documenten

 Besluit handhavingsverzoek van Telefoongids over omgekeerd zoeken (PDF - 36.38 KB)

13

regels voor verkeersgegevens

- anonimiseren, zodra niet meer nodig voor overbrengen verkeer en facturering
- met toestemming ook voor
 - value added services
 - marketing van elektronische communicatiediensten

GPS gegevens worden niet gebruikt voor overdracht van communicatie, zijn dus wél locatiegegevens maar géén verkeersgegevens (art. 11.5a Tw)

Art. 11.5
Tw

definitie

gegevens die worden verwerkt voor overbrengen van communicatie of facturering ervan

Bijv. tijdstip en duur, oproep, oproepnummer, Cell-ID, omvang e-mailbericht, etc.

Art. 6 en 9
RI. 2002/58

Art. 6, 6a,
6b, 6c-7 ePR

14

gebruik geanonimiseerde en geaggregeerde telecomgegevens t.b.v bestrijding van COVID-19

Wél

- om te zien in hoeverre maatregelen effectief zijn
- om in te schatten hoe de pandemie zich ontwikkelt

Bijv. als in Nederland de terrassen opengaan en in België nog niet

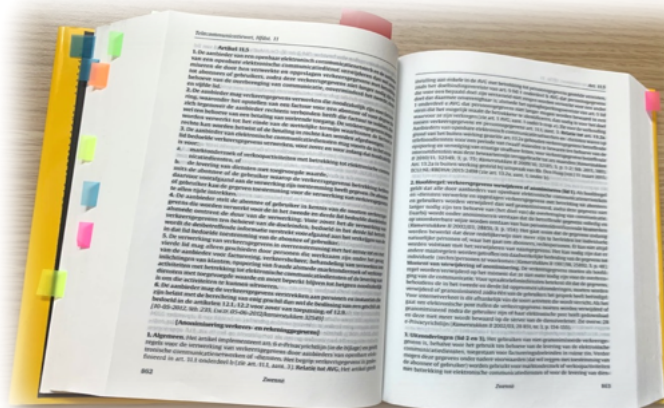
Maar *niet*

- om individuen te volgen en hen aan te spreken op hun gedrag

Singapore, China(?)



15



anonimiseren!



16

wat is «anoniem»...?

(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.

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

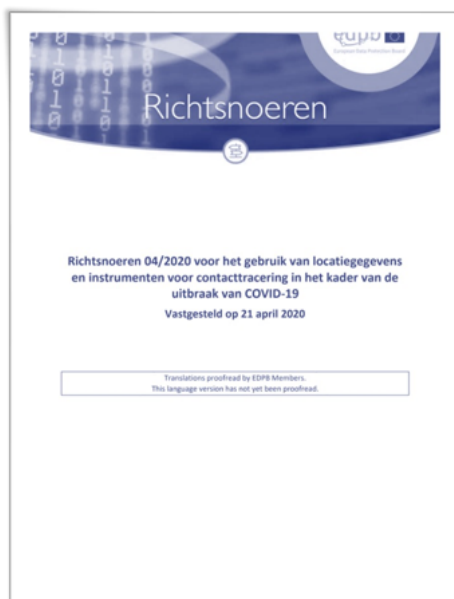
overw. 26
Preamble AVG

«niet-identificeerbaar»

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.

Kamerstukken II 1997/98, 25892, nr. 3, p. 48

gebruik geanonimiseerde en geaggregeerde telecomgegevens t.b.v bestrijding van COVID-19 – wat de EDPB erover zei...



Met anonimisering wordt bedoeld op het gebruik van een reeks technieken die het onmogelijk maken om gegevens met een “redelijke” inspanning te koppelen aan een geïdentificeerde of identificeerbare natuurlijke persoon. Bij deze “**redelijkheidstoets**” moet rekening worden gehouden met zowel objectieve aspecten (vereiste tijd en technische middelen) als contextuele elementen die per geval kunnen verschillen (zoals zeldzaamheid van een verschijnsel, populatiedichtheid, aard en volume van de gegevens). Als de gegevens niet door deze toets komen, zijn ze niet geanonimiseerd en blijft de AVG er dus op van toepassing.

gebruik geanonimiseerde en geaggregeerde telecomgegevens t.b.v bestrijding van COVID-19 – wat AP ervan vond...

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'.

d.w.z EU-lidstaten met dezelfde wetgeving als Nederland (!)

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 helpen om de verspreiding van het virus in te dammen.



19

POLITICO



As European governments rushed to embrace technology to fight the coronavirus, a plainspoken Dutchman emerged as a thorn in their side. Aleid Wolfsen's message: Don't pretend your solutions are privacy-friendly.

In a group that normally keeps disagreements quiet, Wolfsen stands out. A former politician and mayor of Utrecht who had no formal training in data protection when he took on his role in 2016, he has repeatedly been at odds with other watchdogs, most of whom do not have a political background.



The official in charge of Europe's grouping of privacy regulators was also keen to play down any disagreements. There is "no difference in the positions" of different privacy regulators and the "Dutch case was a specific case," Andrea Jelinek said, while a spokesperson for the group, the European Data Protection Board, added: "The legal concept of anonymization is not an absolute concept."

Europe's Data Protection Supervisor, who had OK'd the Commission's use of telecoms data to track the coronavirus, said: "There is a difference between the technical impossibility of doing something to the very end, and something which we would call an effective anonymization."

20



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 locatiedata op een privacy-vriendelijke

men 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 mensen die daar geen toestemming voor hebben gegeven, is door de AVG echt *not done* geworden. Dat lijkt met die locatiedata nu weer aan de kant te worden geschoven”, zegt Benaisa van Bits of Freedom. „Niets is zo perma-



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 persoons-
gegevens...!*



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.

spam en telemarketing

ongevraagde elektronische communicatie
voor commerciële ideële of charitatieve
doeleinden met of zonder menselijke
tussenkoms

telemarketing

hogere kosten,
dus tot 1 juli
2021 opt-out

oproepautomaat, fax, spam,
e-mail, sms, etc

A guaranteed delivery of 50
million e-mails for under a
thousand bucks. And you need
only one sucker in a million to
recover your start-up costs

Art. 11.7
Tw

lagere kosten, dus opt-in

Wijz. Telecomwet i.v.m. invoeren van een opt-in-
systeem voor het overbrengen van ongevraagde
communicatie voor commerciële, ideële of
charitatieve doeleinden aan natuurlijke personen
KST 35421; Stb 2021, 10

Art. 13 Rl.
2002/58

Art. 16
ePR

vanaf 1 juli 2021 opt-in

24

commercieel (ideëel of charitatief):

elke vorm van communicatie bestemd voor het
aanprijzen van de goederen, diensten of het imago
van een onderneming, instelling of persoon die een
commerciële, industriële of ambachtelijke activiteit
of een gereguleerd beroep uitoefent

'commercieel' moet worden begrepen als
'direct marketing', aldus Cbb 5 juni 2014,
ECLI:NL:CBB:2014:206, Mediaforum
2014/10, p. 264-268, m.nt. Zwenne & Van
Hooijdonk.

25

spamverbod

art. 11.7
lid 1-3 Tw

hoofdregel

toestemming nodig voor ongevraagde commerciële (charitatieve, ideële) elektronische communicatie

art. 7, overw. 32, 42-43 AVG: vrije, specifieke en op informatie berustende wilsuiting -- dus niet via algemene voorwaarden of kleine letters...

'zonder menselijke tussenkomst' zoals; belautomaten, email, sms, fax, whatsapp enz.

uitzonderingen

1. zgn. bestaande klanten
2. daarvoor bekend gemaakte elektronische contactgegevens
3. ontvanger buiten EER

'warme contacten'

26

bestaande klanten ('warme contacten')

art. 11.7
lid 3 Tw

géén toestemming nodig

- als voor de communicatie wordt gebruik gemaakt van elektronische contactgegevens verkregen in het kader van de verkoop van een eigen dienst of product, en
- alleen voor eigen gelijksoortige diensten en producten
- en opt-out..!
 - bij vastleggen contactgegevens, en
 - in iedere communicatie (bericht)

e-mailadressen, mobiele telefoonnummers, sociale netwerkaccounts

Rb. Rotterdam 2 oktober 2014 ECLI:NL:RBROT:2014:8039.
CBB 17 maart 2016, ECLI:NL:CBB:2016:60

sluit niet uit dat er nog geen verkoop heeft plaatsgevonden! Of toch wel?

wat verwacht de (potentiële) klant?

d.w.z. van dezelfde juridische entiteit

afmeldmogelijkheid (if you wish to unsubscribe...)

27

telemarketing

*ongevraagde elektronische communicatie
mèt menselijke tussenkomst*

niet alleen consumenten maar ook
 ► zzp-ers, eenmanszaken, maten in
 een maatschap, vof's enz.

hoofdregel

ongevraagd bellen van natuurlijke personen voor commerciële (ideële, charitatieve) doeleinden is toegestaan

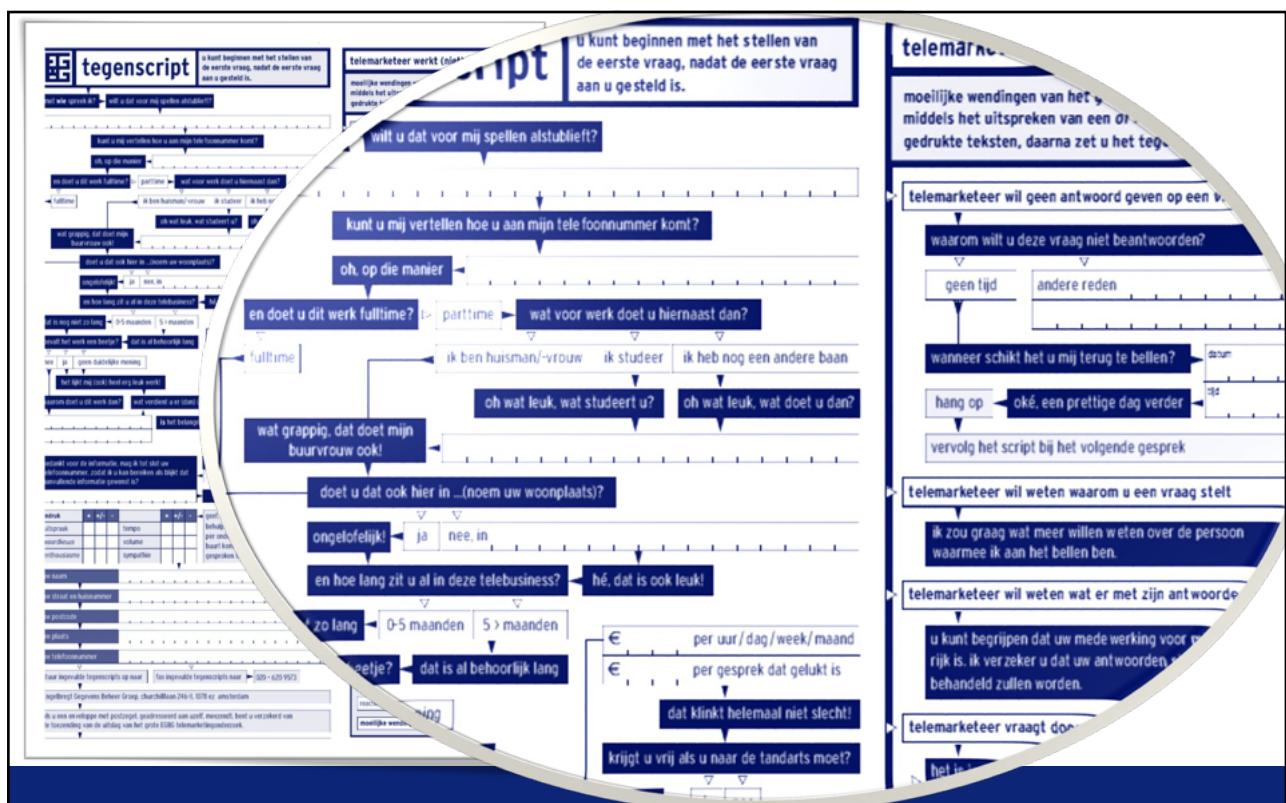
- op basis van opt-out, en
- gebruikmaking van een 'ontdubbeld' belbestand

uitzondering

- zgn. 'bestaande klanten' met betrekking tot eigen gelijksoortige producten

opschonen aan de hand van
bestanden van bel-me-niet

- direct of indirect promoten van product, organisatie of onderneming...



Cie voorstel (10 januari 2017)

- niet alleen regels voor telcos & ISPs maar ook voor OTTs!
- meer aandacht voor vertrouwelijkheid van onlinegedrag
- cookietoestemming kan ook worden gegeven via browserinstellingen
- bij telemarketing moet call center het gebruikte nummer bekend maken
- strengere en gedetailleerdere regels voor 'metadata' en 'content'
- één toezichthouder: AP

Over the Top: Netflix, Whatsapp etc.

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

of een special telemarketing-nummer gaan gebruiken...

30

cookies e.d.

Cookies op NPO Start
NPO plaatst Functionele cookies, om deze website naar behoren te laten functioneren en Analytische cookies waarmee wij het gebruik van de website kunnen meten. Deze cookies gebruiken geen persoonsgegevens. Geef hieronder uw toestemming voor cookies die wel persoonsgegevens verwerken. Meer uitleg over cookies

☒ ☐ Ik wil Sociale Media koppelingen: hiermee staat het plaatsen van cookies door social medianetwerken toe, deze netwerken kunnen u volgen en uw internetgedrag gebruiken voor andere doeleinden

☒ ☐ Ik wil gepersonaliseerde advertenties: hiermee ontvangt u gepersonaliseerde STER-advertenties die worden afgestemd op uw internetgedrag. Via deze cookies kan je internetgedrag gevolgd worden door advertentienetwerken. Op onze jeugdsites worden geen gepersonaliseerde advertenties getoond.

☒ ☐ [Cookies](#)

NU.nl maakt gebruik van cookies.
NU.nl gebruikt cookies (en andere technieken) en verzamelt daarmee informatie over het gebruik van de website onder andere om deze te analyseren en te verbeteren, voor social media en om er voor te zorgen dat je voor jou relevante informatie en advertenties te zien krijgt. Sanoma deelt de informatie die zij verkrijgt via haar websites middels het gebruik van cookies en vergelijkbare technieken, waaronder ook persoonsgegevens, in een samenwerkingsverband genaamd NLProfil van Buymedia Nederland met De Persgroep en Telegraaf Media Groep, om gezamenlijke groepsprofielen op te stellen. Ook biedt Sanoma enkele adverteerders de mogelijkheid de door Sanoma verzamelde informatie ook buiten haar websites te gebruiken bij het inkopen van advertentie ruimte. Tot slot kunnen enkele adverteerders zelf bij het tonen van hun advertenties cookies plaatsen om zo zelf informatie te verzamelen. Meer weten over deze cookies, klik hiernaast op "Meer informatie". Door gebruik te maken van deze website of door hiernaast op akkoord te drukken, geef je aan akkoord te zijn met het gebruik van cookies en het verzamelen van informatie aan de hand daarvan door ons en door derden op de websites van Sanoma en met de verstrekking van uw (persoons)gegevens aan De Persgroep en Telegraaf Media Groep voor de totstandkoming van de gezamenlijke groepsprofielen. Wil je niet alle soorten cookies toestaan, klik dan op "Cookie instellingen aanpassen".

[Akkoord](#)
[Cookie instellingen aanpassen](#)
[Privacy- en cookiebeleid](#)
[Meer informatie tonen](#)

31

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:

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

plaatsen en uitlezen van cookies



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 Preamble AVG)

32

uitzonderingen

Art. 11.7a
lid 3 TW

geen toestemming 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

33

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 en in dat geval verwerkingsgrondslag vereist, zoals

- toestemming, of
- uitvoering overeenkomst, of
- gerechtvaardigd belang

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

34

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



35

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 veldje «ik geef toestemming» aanklikt.

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

36



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.

37

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* general

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.

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

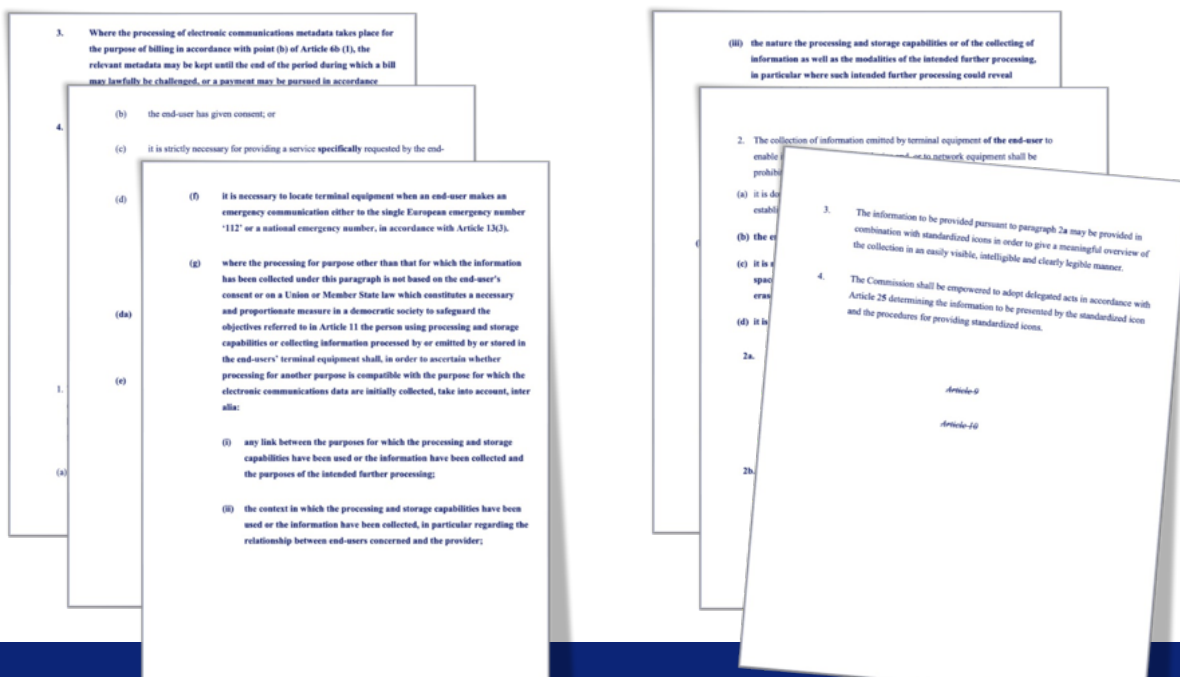
provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application.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

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. Moreover, 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.

40

cookies in het concept d.d. 10 februari jl.



41

cookiewall in het zgn. concept d.d. 10 februari jl.

“onderhandelingsmandaat”

[...] [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

42

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

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL

Home > 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 comply with it accordingly.

On July 4th, 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!

43

vragen?
g.j.zwenne@law.leidenuniv.nl