

@zwnne

KEUZEVAK TELECOMMUNICATIERECHT | 30 APRIL 2021

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

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

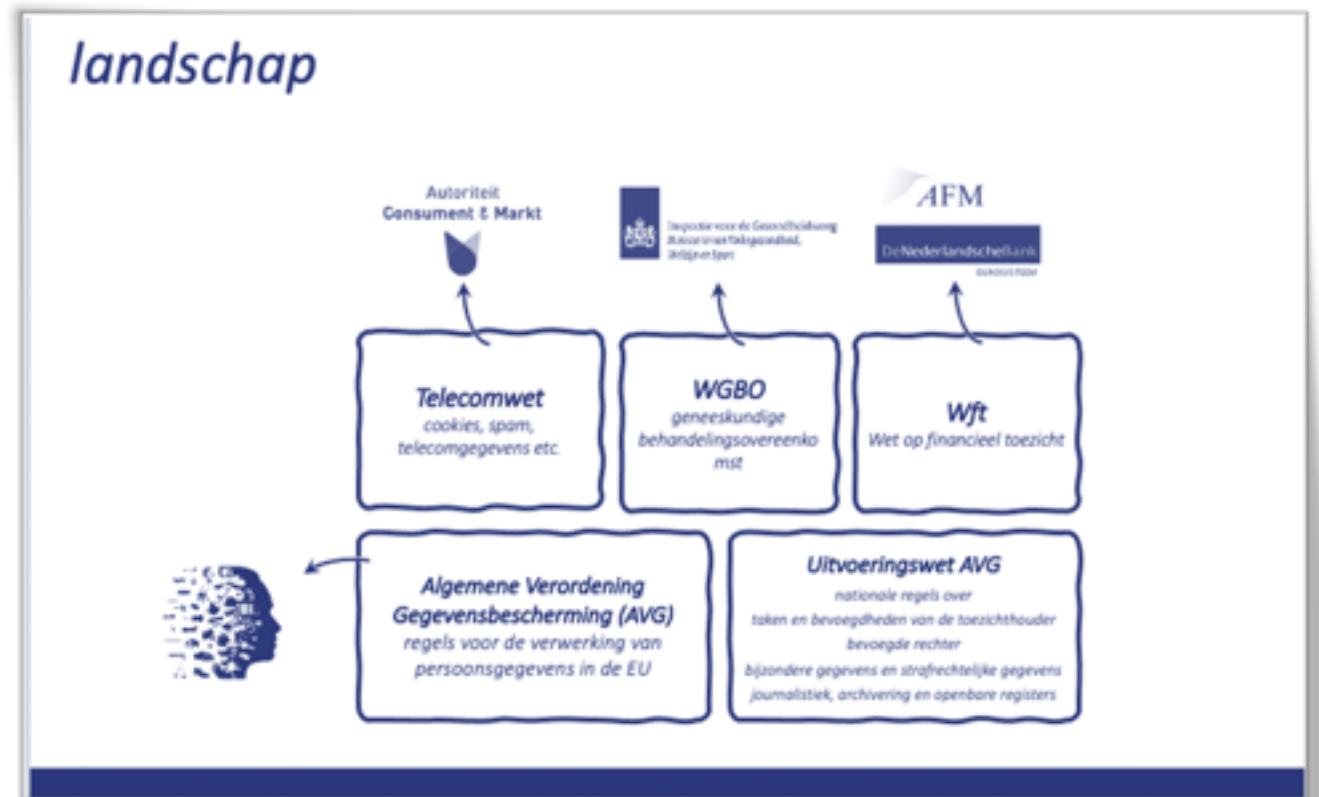


Universiteit
Leiden

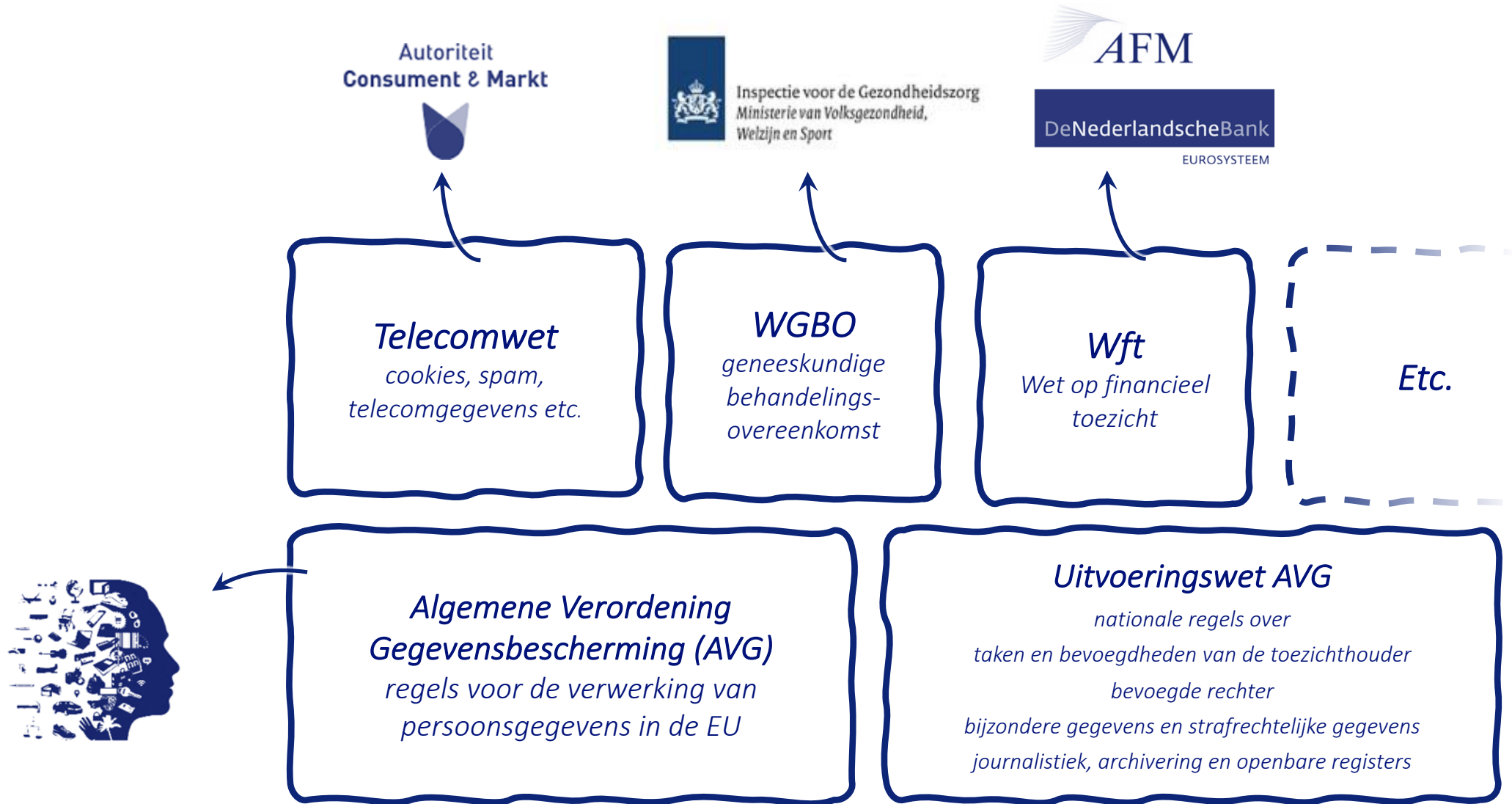


roadmap

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



landschap



vertrouwelijkheid en beveiliging

Art. 11.2
Tw

zorgdragen voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van telecomnetwerk, onderscheidenlijk telecomdienst

- *bescherming persoonsgegevens en privacy van abonnees en gebruikers*
- *vertrouwelijkheid van communicatie*
- *beveiliging én meldplicht beveiligingsinbreuk*

melden bij AP en in voorkomend geval ook bij abonnees en gebruikers!

Art. 11.3
Tw

Art.
11.3a Tw

niet aftappen, afluisteren enz., tenzij

- *met uitdrukkelijke toestemming*
- *integriteit netwerk*
- *overbrengen communicatie*
- *wettelijk voorschrift of bevel*

Deep Packet Inspection (DPI)

Art.
11.2a Tw

Art. 4 Rl.
2002/58

Art. 5
ePR

net neutrality & deep packet inspection

Dutch mobile operators modify data-analysis after investigation Dutch DPA - Results investigation Dutch DPA into packet inspection by the telecom operators

News message / 4 July 2013

The Dutch Data Protection Authority (CBP) today publishes its reports resulting from the investigation into the analysis of data traffic (packet inspection) on the mobile network by the mobile operators KPN, Tele2, T-Mobile and Vodafone. These four operators are the largest mobile network providers in the Netherlands. In the course of the investigation the Dutch DPA has found violations of the Dutch Data Protection Act and the Telecommunications Act at all four operators. The companies are found to have stored data, in breach of the law, on a detailed level about visited

College Bescherming Persoonsgegevens

Postadres Postbus 93378, 2509 AJ Den Haag
Telefoon 070 - 88 500 500 (ma-vr) - 08 88 501 501
Website www.cbpg.nl www.mijnprivacy.nl

College bescherming persoonsgegevens

Onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door KPN B.V.

Z2011-00462

Rapport definitieve bevindingen
Mei 2013 met corrigendum van 12 juni 2013

OPENBARE VERSIE

Question for written answer E-005159/2011
to the Commission
Rule 117

Marjetje Schaake (ALDE) and Sophia in 't Veld (ALDE)

Subject: Regulating net neutrality and use of deep packet inspection

The Dutch telecommunication operator KPN has recently announced that it will charge users to use services such as Skype and Whatsapp¹. The reason given is that KPN's business model of charging for voice calls and SMS text messages cannot compete with the free alternatives. KPN's blocking of competitive online services to their consumers is part of a trend of European telecommunication operators such as Telefonica, T-Mobile Orange and Vodafone, which already block the use of services such as Skype via their networks. Furthermore, KPN uses deep packet inspection (DPI) technology from the French company Alcatel-Lucent to monitor the use of applications over its network². The choice of KPN to charge for the use of certain internet applications is in stark contrast with the principles of net neutrality, which were recently outlined by the Commission in COM(2011)0222 of 19 April 2011. National or European regulators may not always have significant market power in the mobile data market. Furthermore, not all consumers are likely to switch to another operator because of this limitation to their internet experience, even if the operators are transparent about their blocking practices.

1. Does the Commission agree that KPN is violating the principle of net neutrality by charging for access to certain internet services? If not, why not?
2. Does the Commission agree that insufficient provisions are in place to uphold the principles of net neutrality for all internet users? If not, why not?
3. What will the Commission do to stop the trend of telecommunication operators blocking competitive services for their customers?
4. Is the Commission considering regulating net neutrality ex ante, as suggested in the conclusion of the Commission's opinion?
5. Does the Commission agree that using DPI technology is a violation of several fundamental human rights, applicable European data protection and privacy rules, notably Directive 95/46/EC and possibly Article 3 of the internationally recognised Convention on Cybercrime?

¹ <http://www.nu.nl/internet/2498071/kpn-gaat-mobiele-diensten-blikken.html>
² <http://www.engadget.com/2011/05/12/dutch-telco-kpn-using-deep-packet-inspection-to-monitor-mobile-c>



Meldloket datalekken Autoriteit Persoonsgegevens

Welkom bij het meldloket datalekken van de Autoriteit Persoonsgegevens. U kunt hier een melding van een datalek doen of een bestaande melding aanpassen of intrekken. Kies hieronder wat u wilt doen.

Om uw melding van een datalek via het meldloket datalekken zo goed mogelijk te laten verlopen, kunt u het beste een moderne browsersversie gebruiken.

Is het versturen van de melding goed verlopen, dan krijgt u op uw scherm meteen een ontvangstbevestiging te zien. In de ontvangstbevestiging staan de gegevens die u heeft ingevoerd met daarbij een meldingsnummer. Dit meldingsnummer heeft u nodig om de melding aan te passen of in te trekken. U kunt de melding niet online raadplegen. Maak daarom meteen een print voor uw eigen administratie voordat u het browservenster afsluit.

Lees ook onze informatie over meldplicht datalekken en de Richtsnoeren voor de melding van datalekken.

Wilt u een datalek melden maar bent u geen vertegenwoordiger van de organisatie? Dan kunt u gebruik maken van ons tipformulier.

Telefonische informatie over de meldplicht datalekken

Op deze website vindt u informatie en antwoorden op vragen over de meldplicht datalekken. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de Autoriteit Persoonsgegevens. Het telefoonnummer is 088 - 1805 255 (voor dit nummer betaalt u uw gebruikelijke telefoonkosten).

Heeft uw organisatie een datalek geconstateerd? Kies voor een nieuwe melding indienen.

→ NIEUWE MELDING

Wilt u een melding die u eerder heeft gedaan aanpassen of aanvullen? Kies voor een bestaande melding aanpassen. Let op: houd het meldingsnummer dat u kreeg toen u de eerdere melding deed bij de hand.

→ BESTAANDE MELDING WIJZIGEN

Wilt u een melding die u eerder heeft gedaan ongedaan maken? Kies voor een bestaande melding intrekken. Let op: houd het meldingsnummer dat u kreeg toen u de eerdere melding deed bij de hand.

→ MELDING INTREKKEN

Een nieuwe melding doen

- Voor het melden van een datalek vult u onderstaand formulier in.
- Lees ook onze informatie over meldplicht datalekken en raadpleeg de Richtsnoeren voor de melding van datalekken van de Europese privacytoezichhouders.
- Nadat u een melding heeft gedaan, krijgt u een meldingsnummer te zien ter bevestiging. Registreer dit nummer voor verdere communicatie met de Autoriteit Persoonsgegevens.

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?

Nieuwe melding

Op grond van welke wettelijke bepaling doet u deze melding?

Telecommunicatiewet (Tw)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel

Naam van het bedrijf of de organisatie

Adres

Postcode

Plaats

In welke sector is de organisatie of het bedrijf actief?

Kies er een

Overige sector, te weten:

Wie meldt het datalek?

Naam

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Kies er een
Geslacht, geboortedatum en/of leeftijd	Kies er een
Burgerservicenummer (BSN)	Kies er een
Contactgegevens	Kies er een
Toegangs- of identificatiegegevens	Kies er een
Financiële gegevens	Kies er een
(Kopieën van) paspoorten of andere legitimatiebewijzen	Kies er een
Locatiegegevens	Kies er een
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Kies er een
Onbekend / anders, namelijk:	

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Kies er een
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Kies er een
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Kies er een
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Kies er een
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Kies er een

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Kies er een
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Kies er een
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Kies er een
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Kies er een
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Kies er een
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Kies er een
Anders, namelijk	

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Kies er een
Identiteitsdiefstal of -fraude	Kies er een
Financiële verliezen	Kies er een
Reputatieschade	Kies er een
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Kies er een
Ongeoorloofde ongedaanmaking van pseudonimisering	Kies er een

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? Kies er een

Wanneer heeft u het datalek gemeld aan de betrokkenen?

Wanneer gaat u het datalek melden aan de betrokkenen?

Wat is de inhoud van de melding aan de betrokkenen?

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?

Waarom ziet u af van het melden van het datalek aan de betrokkenen? Kies er een

Als het informeren van alle betrokkenen een onevenredige inspanning zou vergen, licht dan toe hoe u door een openbare mededeling of een soortgelijke maatregel de betrokkenen gaat informeren.

Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?

Welke andere redenen heeft u om de betrokkenen niet te informeren?

8.2 Maatregelen om de inbreuk aan te pakken

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder? Kies er een

Als er sprake is van een grensoverschrijdende gegevensverwerking, om welke EU-landen gaat het dan?

Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen? Kies er een

Ja, namelijk

Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen? Kies er een

Ja, namelijk

9. Overig

Is naar uw mening deze melding compleet? Kies er een

Herhaal de letters en cijfers uit dit plaatje. Dit is nodig om misbruik te voorkomen.



☐ Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen en dat de in de melding verstrekte informatie juist is.

Annuleren

→ VERSTUREN



Ontvangstbevestiging

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

U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het

onderstaande meldingsnummer is de melding bekend bij de Autoriteit

Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst

15-08-2018 15:00:00

Uniek nummer

15-08-2018-15:00:00-15:00:00-15:00:00

0. Over deze melding

Gaat het om een nieuwe of bestaande

Een nieuwe melding indienen

verkeersgegevens

Art. 11.5
Tw

- *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 locatiegegevens maar géén verkeersgegevens (art. 11.5a Tw)

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
Rl. 2002/58

Art. 6-7 ePR

gebruik geanonimiseerde 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

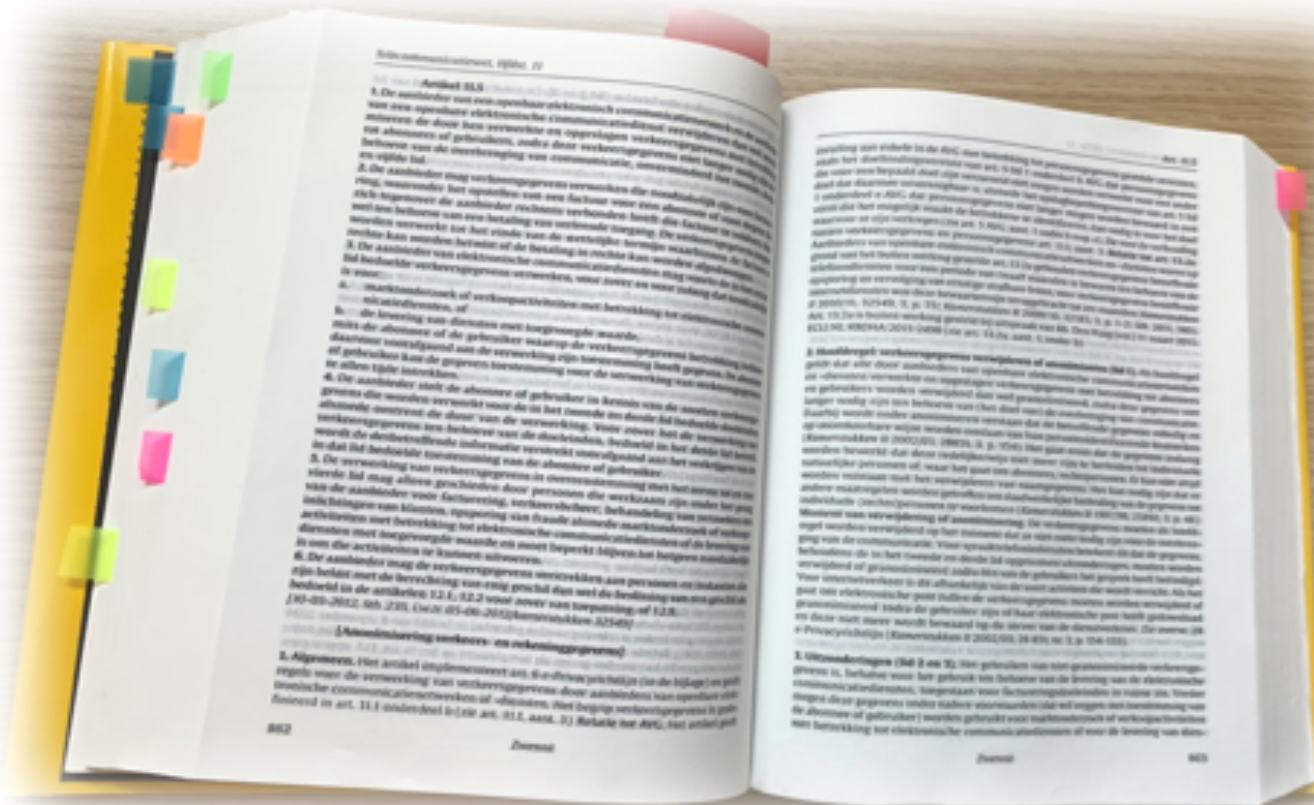
Bijv. als in Nederland de terrassen opengaan en in België nog niet

En níet

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

Singapore, China(?)





anonymiseren!

Privaat- en gegevens- beschermingsrecht

AVG, AVG en andere privacywetgeving

Zevende druk

REDACTIE:

G.J. Zwenne

H.R. Kranenburg

TEKST &
COMMENTAAR

Wolters Kluwer

Wolters Kluwer

RAA

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

«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.

overw. 26
Preambule AVG

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

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



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.

echter, 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'.

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.



PHILADELPHIA, PA. (AP) —

De Algemene verordening gegevensbescherming werkt. Twee jaar na de invoering zijn weinig boetes uitgedeeld. Mensen en organisaties zijn zich veel bewuster geworden van de privacyregels. „Dataproductie emancipeert tot allesomvattend monstrecht“, zegt de toezichhouder.

Order your copy today! **Wilmar Mack**, **Historian**, **Paula Barnett**

[illegible][illegible]

Bescherming van persoonsgegevens is een
Sociaal-omgeving die mensen deze bescherming
de facto dat zij worden bedacht door de Autoriteit
Persoonsgegevens (APG) in Nederland, onder de
AVG worden niet te heren zijn toegestaan.

Verzitter (Vergadering) van de werkgroep
de (niet) te heren zijn toegestaan.

[illegible]

De AVG dwingt tot nadenken vóór doen



1

1

over
W
die
goe
wet
kab

die
na
men
mee

Volfsen
de besch
d moge
hebben
inet. Wi

locatie
het katoen
n worde
est op
hij is

spreiding
 eist dat
 herming
 lijk waa
 a wij net
 j sluiten

data op
n, midd
n vold
gevolgd

g van h
het on
g van pe
rborger
advies
n niet ui

an. Onze
, omdat

et virus
n maatr
ersoons
n. „Over
uitgebr
t dat de

privacy-
et aan s
e advies
t wij een
b. 111

- Regelen van gegeven en die spooracht aan analyse

vriende
 streng
 zen wor
 n wet bu
 G.

gaat
as zo
oed-
n het
van

lijke
not-
rden
iten

123

?

dicht bij elkaar staan. De medische dossiers bij de huisarts van mensen die geen toestemming gaven voor gebruik ervan door anderen, zijn toegankelijk gemaakt voor huisartsenposten en eerste hulpen in het ziekenhuis. Het kabinet werkt aan een spoedwet om locatiegegevens van mobiele bellers te laten onderzoeken door het RIVM, om zo voorspellingen te doen 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 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.

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 Benaïssa van Bits of Freedom. „Niets is zo permanent als een tijdelijke maatregel”, reageert ook





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."



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.

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.***





Report

Estimating hourly population flows in the Netherlands

Statistics Netherlands
December 2020



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

géén bewaarplicht

Wat?

- verkeers- en lokatie-gegevens
- naw-gegevens

Hoe lang?

- 12 maanden voor telefonie
- 06 maanden voor internet

Waarvoor?

- onderzoek, opsporing en-of vervolgen ernstige misdrijven

HvJEU 8 april 2014 C-293/12 en C594/12

- inmenging in fundamentele rechten op bijzonder ernstige wijze
- wél sprake van een algemeen belang, nl. strijd tegen ernstige criminaliteit en uiteindelijk openbare veiligheid
- maar met richtlijn 2006/24/EG zijn niettemin grenzen overschreden die ingevolge het evenredigheidsbeginsel in acht moeten worden genomen



anoniem bellen en gebeld worden

Art. 11.9
Tw

- *nummerherkenning*
 - *ongespecificeerde telefoonrekening*
- *recht op anoniem bellen*
 - *recht om niet anoniem te worden gebeld*
 - *recht om wél anoniem te worden gebeld*
maar beperkingen m.b.t. alarmnummers

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

Art. 11.4
Tw

Art. 7-8 Rl.
2002/58

Art. 12-14
ePR

'geheim nummer'

Art. 11.6
Tw

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

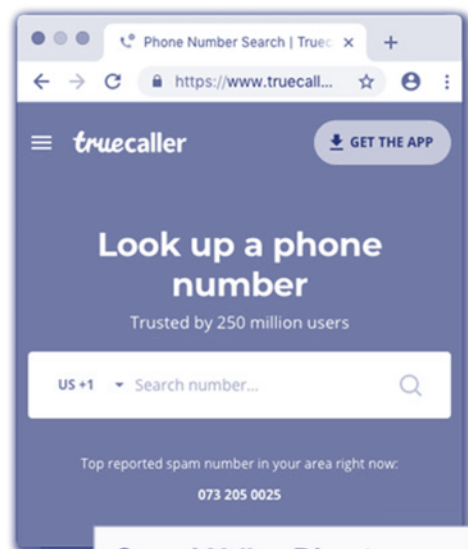
→ 18xy: 1880, 1800, 1801

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



SearchYellowDirectory.com



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



[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)

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

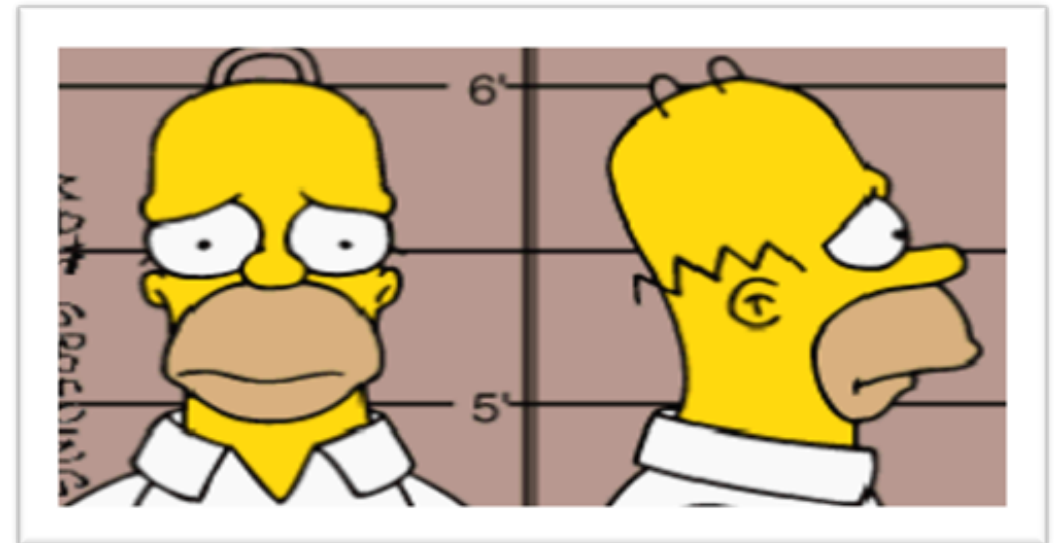
-  [Besluit handhavingsverzoek van Telefoongids over omgekeerd zoeken \(PDF - 36.38 KB\)](#)
-

spam: automated calling device (robocalls)



"Greetings, friend. Do you wish to look as happy as me? Well, you've got the power inside you right now. So use it. And send \$1 to Happy Dude, 742 Evergreen Terrace, Springfield. Don't delay; eternal happiness is just \$1 away!"

"Greetings friend, this is Homer Simpson, aka, Happy Dude. The courts have ordered me to call everyone, and apologize for my telemarketing scam. I'm sorry. If you can find it in your heart to forgive me, send \$1 to Sorry Dude, 742 Evergreen Terrace, Springfield. You have the power!"



spam en telemarketing

Art. 11.7
Tw

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

*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*

telemarketing

lagere kosten, dus opt-in

hogere kosten, dus opt-out

*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 II 2019/20, 35421, nrs. 1-6*

Art. 13 Rl.
2002/58

Art. 16
ePR

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 gereglementeerd 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 Hooidonk.

regels voor ongevraagde commerciële elektronische communicatie

zonder menselijke tussenkomst

art.11.7 jo. 11.8 Tw
ongevraagde elektronische communicatie

art. 3:15e BW
dienst van de informatiemaatschappij

art. 21.2 AVG
verwerking persoonsgegevens t.b.v. direct marketing

zelfregulering
DDMA RCC Code
Email

spamverbod

art. 11.7
lid 1-3 Tw

hoofdregel: opt-in

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: opt-out

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

procurement@bedrijfsnaam.nl..?

‘warme contacten’

bestaande klanten ('warme contacten')

art. 11.7
lid 3 Tw

géén toestemming nodig (opt-out)

- 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

wat verwacht de (potentiële) klant?

d.w.z. van dezelfde juridische entiteit

afmeldmogelijkheid (if you wish to unsubscribe...)

telemarketing

} *ongevraagde elektronische communicatie
mèt menselijke tussenkomst*



hoofdregel (nu nog even)

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

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

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

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





tegenscript

u kunt beginnen met het stellen van de eerste vraag, nadat de eerste vraag aan u gesteld is.

met wie spreekt ik? - wilt u dat voor mij spelen alstublieft?

kunt u mij vertellen hoe u aan mijn telefoonnummer komt?

oh, op die manier

en doet u dit werk fulltime? - parttime

ik ben huismans/vrouw ik studeer ik heb nog een andere baan

oh wat leuk, wat studeert u? - oh wat leuk, wat doet u dan?

wat grappig, dat doet mijn buurvrouw ook!

doet u dat ook hier in ... (noem uw woonplaats)?

ongelofelijk! - ja nee, in

en hoe lang zit u al in deze telebusiness? - hé, dat is ook leuk!

zo lang - 0-5 maanden 5 > maanden

hoeveelje? - dat is al behoorlijk lang

€ per uur / dag / week / maand

€ per gesprek dat gelukt is

dat klinkt helemaal niet slecht!

krijgt u vrij als u naar de tandarts moet?

ja nee

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

tegenscript

telemarketeer werkt (niet)

script

u kunt beginnen met het stellen van de eerste vraag, nadat de eerste vraag aan u gesteld is.

wilt u dat voor mij spelen alstublieft?

kunt u mij vertellen hoe u aan mijn telefoonnummer komt?

oh, op die manier

en doet u dit werk fulltime? - parttime

wat voor werk doet u hiernaast dan?

fulltime

ik ben huismans/vrouw

ik studeer

ik heb nog een andere baan

oh wat leuk, wat studeert u?

oh wat leuk, wat doet u dan?

wat grappig, dat doet mijn buurvrouw ook!

doet u dat ook hier in ... (noem uw woonplaats)?

ongelofelijk!

ja

nee, in

en hoe lang zit u al in deze telebusiness?

hé, dat is ook leuk!

zo lang

0-5 maanden

5 > maanden

hoeveelje?

dat is al behoorlijk lang

€ per uur / dag / week / maand

€ per gesprek dat gelukt is

dat klinkt helemaal niet slecht!

krijgt u vrij als u naar de tandarts moet?

telemarketeer

moeilijke wendingen van het gesprek middels het uitspreken van een of meerdere gedrukte teksten, daarna zet u het tegenscript

telemarketeer wil geen antwoord geven op een vraag

waarom wilt u deze vraag niet beantwoorden?

geen tijd

andere reden

wanneer schikt het u mij terug te bellen?

daarom

hang op

oké, een prettige dag verder

ja

vervolg het script bij het volgende gesprek

telemarketeer wil weten waarom u een vraag stelt

ik zou graag wat meer willen weten over de persoon waarmee ik aan het bellen ben.

telemarketeer wil weten wat er met zijn antwoord

u kunt begrijpen dat uw medewerking voor ons belangrijk is. ik verzeker u dat uw antwoorden serieus behandeld zullen worden.

telemarketeer vraagt door

het is leuk

35 421

Wijziging van de Telecommunicatiewet in verband met het invoeren van een opt-in-systeem voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan natuurlijke personen

A

GEWIJZIGD VOORSTEL VAN WET

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:
Alzo Wij in overweging genomen hebben, dat het wenselijk is om, ter bescherming van de persoonlijke levenssfeer van eindgebruikers van elektronische communicatiediensten, het verzenden van communicatie voor commerciële, ideële of charitatieve doeleinden aan natuurlijke personen slechts toe te staan indien deze natuurlijke persoon de verzender daarvoor voorafgaand toestemming heeft gegeven;
Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

ARTIKEL I

De Telecommunicatiewet wordt als volgt gewijzigd:

A

(Vervallen)

B

Aan artikel 11.6 wordt een lid toegevoegd, luidende:
5. Dit artikel is van toepassing op abonnees die natuurlijke personen zijn.

C

Artikel 11.7 komt te luiden:

Artikel 11.7

1. Het gebruik van automatische oproep- en communicatiesystemen zonder menselijke tussenkomst, faxen en elektronische berichten voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden is verboden, tenzij de verzender kan aantonen dat

2. Het eerste lid is van overeenkomstige toepassing op het gebruik van andere dan de in het eerste lid bedoelde middelen voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan natuurlijke personen. Bij het gebruik van andere dan de in het eerste lid bedoelde middelen voor het met toestemming overbrengen van deze ongevraagde communicatie aan natuurlijke personen, geeft de verzender de desbetreffende natuurlijke persoon bij iedere boodschap duidelijk en expliciet de gelegenheid om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van zijn contactgegevens.

toestemming vereist voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan een rechtspersoon of een natuurlijke persoon die handelt in de uitoefening van zijn beroep of bedrijf, indien:

- de verzender gebruik maakt van elektronische contactgegevens die door de desbetreffende eindgebruiker voor het ontvangen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden zijn bestemd en bekendgemaakt en deze worden gebruikt in overeenstemming met de door de eindgebruiker aan de contactgegevens verbonden doeleinden, of
- de desbetreffende eindgebruiker is gevestigd buiten de Europese Economische Ruimte en voldaan wordt aan de in het desbetreffende land geldende voorschriften met betrekking tot het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden.

4. In afwijking van het eerste en tweede lid, kan een verzender die kan aantonen dat hij gebruik maakt van elektronische contactgegevens die hij heeft verkregen van zijn klanten in het kader van de verkoop van een product of dienst, die elektronische contactgegevens gebruiken voor het overbrengen van ongevraagde communicatie voor commerciële doeleinden ten behoeve van eigen gelijksoortige producten of diensten, mits de verzender de betreffende eindgebruiker duidelijk en expliciet de gelegenheid heeft geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van die elektronische contactgegevens:

- op het ogenblik dat zij worden verzameld, en
 - ingeval de abonnee of gebruiker zich bij de verzameling niet tegen het gebruik heeft verzet, bij elke verzonden boodschap.
5. Het vierde lid is van overeenkomstige toepassing op:
- contactgegevens die ideële of charitatieve organisaties hebben verkregen in het kader van een schenking aan die ideële of charitatieve organisatie; of
 - voor zover sprake is van gebruikmaking van andere dan de in het eerste lid bedoelde middelen, op contactgegevens die ideële of charitatieve organisaties van de eindgebruiker hebben verkregen in het kader van:

- 1°. vrijwilligerswerk bij die organisatie;
 - 2°. het bijwonen van manifestaties van die organisatie.
6. Op het gebruik van elektronische berichten voor de in het eerste lid bedoelde doeleinden zijn de vereisten van artikel 15a, eerste lid, onderdelen a tot en met c, van boek 3 van het Burgerlijk Wetboek van overeen-

Artikel 11.7

1. Het gebruik van automatische oproep- en communicatiesystemen zonder menselijke tussenkomst, faxen en elektronische berichten voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden is verboden, tenzij de verzender kan aantonen dat de desbetreffende eindgebruiker daarvoor voorafgaand toestemming heeft verleend.

2. Het eerste lid is van overeenkomstige toepassing op het gebruik van andere dan de in het eerste lid bedoelde middelen voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan natuurlijke personen. Bij het gebruik van andere dan de in het eerste lid bedoelde middelen voor het met toestemming overbrengen van deze ongevraagde communicatie aan natuurlijke personen, geeft de verzender de desbetreffende natuurlijke persoon bij iedere boodschap duidelijk en expliciet de gelegenheid om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van zijn contactgegevens.

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 advertentiernetwerken. Op onze jeugdsites worden geen gepersonaliseerde advertenties getoond.

☒ Opslaan



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 advertentieruimte. 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](#)

cookiebepaling

plaatsen en uitlezen
van cookies

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.

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

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

is de toestemming in
vrijheid gegeven...?

ICTRecht incasseert €8200 dankzij cookiepopup met incassotoestemming

1 april 2013 door [Amoud Engelfriet](#)

Dankzij het gemak waarmee mensen online akkoord gaan met cookiepopups heeft ICTRecht een bedrag van €8200 mogen incasseren via automatische incasso. Dat maakte het juridisch adviesbureau vandaag bekend. Naast de bekende teksten over Analyticscookies en sociale media bevatte de cookiepopup ook de tekst "Tevens geeft u toestemming €100 van uw bankrekening te laten afschrijven". Een dergelijke tekst is rechtsgeldig, nu bezoekers expliciet op "Akkoord" moesten klikken.

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)

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

bewijsvermoeden

Art. 11.7a
lid 4 TW

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

- *AVG van toepassing*
- *AP bevoegd*

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

cookiemuren-verbod (voor overheid e.d.)

Art 11.7 lid
5 Tw

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

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



Belastingdienst



werken aan perspectief





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.



anders...

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

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

anders...

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. ***These 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.

anders...

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.

anders...

Amendment

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



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

requirements for Internet users, which aimed to clarify the conditions of the 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.

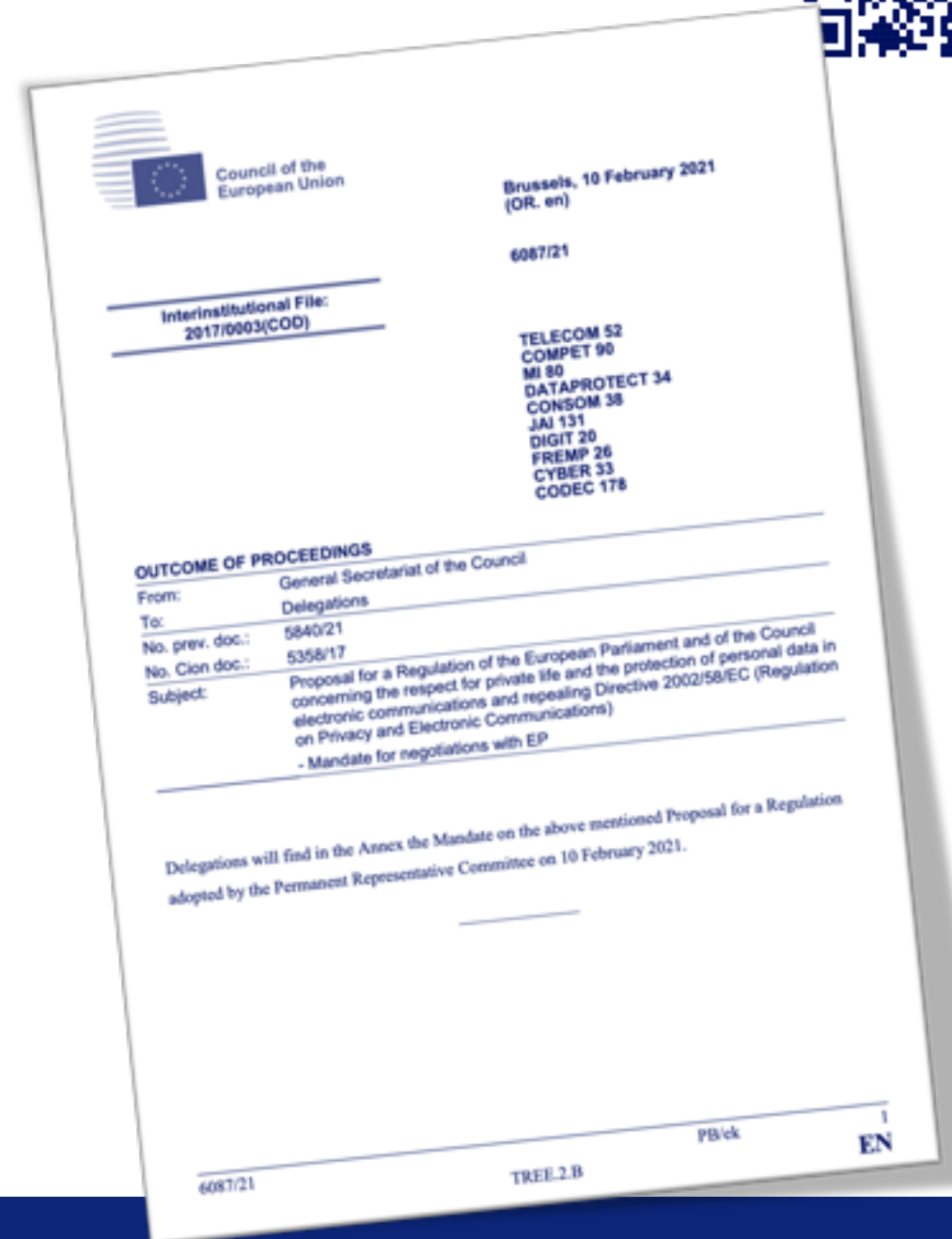
These guidelines were challenged by several professional associations and unions in the online advertising, e-commerce and media sectors.

[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.

ePrivacy Regulation 2021



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



vragen?

g.j.zwenne@law.leidenuniv.nl