@zwnne

KEUZEVAK TELECOMMUNICATIERECHT | 6 MEI 2022

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

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

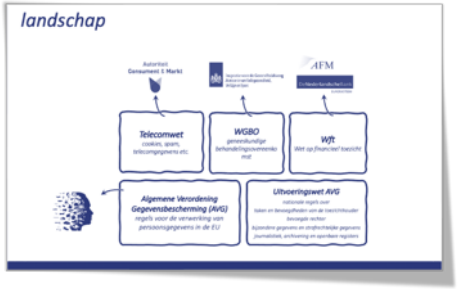
Universiteit Leiden

eLaw Leiden

1

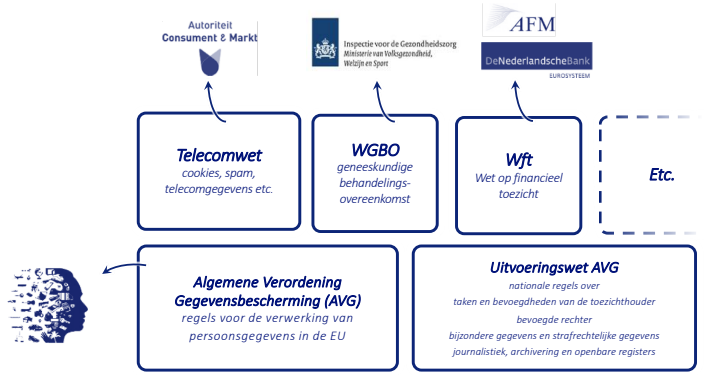
roadmap

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



2

landschap



3

let op!

- *natuurlijke personen die gebruik maken van elektronische communicatie: gebruikers*
- *abonnees*
- *abonnees die rechtspersoon zijn of natuurlijke persoon die handelend in uitoefening van beroep of bedrijf*
- *abonnees die natuurlijke persoon zijn*
- *gebruikers van randapparaten (devices)*
- *consumenten*

- *wie ontlenen aanspraken aan de bepalingen van hoofdstuk 11 Tw?*
- *en op wie rusten de verplichtingen?*
  - *aanbieders van elektronische communicatie (incl. over-the-top)*
  - *aanbieders van telefoongidsen en abonnee-informatiediensten*
  - *verzenders van ongevraagde commerciële communicatie*
  - *websites e.a. die cookies plaatsen en/of uitlezen*

4

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

5

net neutrality & deep packet inspection


AUTORITEIT PERSOONSGEGEVENS

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

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

6

meldloket


Nieuw meldformulier datalekken is live

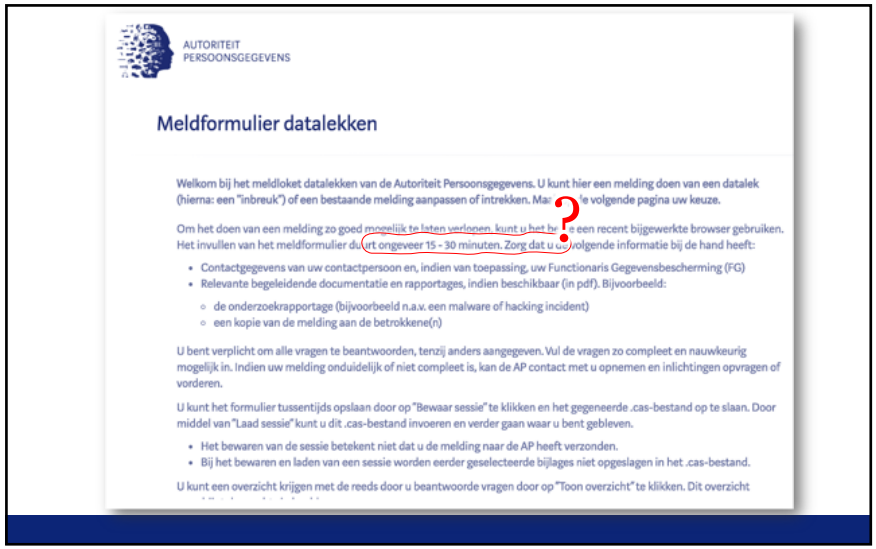
De Autoriteit Persoonsgegevens (AP) heeft een nieuw meldformulier datalekken. Het nieuwe formulier maakt het voor de gebruiker makkelijker om een datalek bij de AP te melden.

Nieuwe functionaliteiten

Het nieuwe meldformulier heeft nieuwe functionaliteiten:

- Het formulier bepaalt op basis van de antwoorden die u invult welke vragen worden getoond. Zo hoeft u alleen de voor u relevante vragen te beantwoorden.
- U kunt het formulier tussentijds opslaan en op een ander moment verdergaan met uw melding.
- U kunt een sjabloon maken voor veelvoorkomende datalekken of een datalek dat zich in een korte tijd vaak voordoet. Zo hoeft u bepaalde delen van het formulier niet bij elke melding opnieuw in te vullen.
- Het aanvullen van een eerdere melding is eenvoudiger geworden. U hoeft hiervoor niet meer het hele meldformulier opnieuw in te vullen.

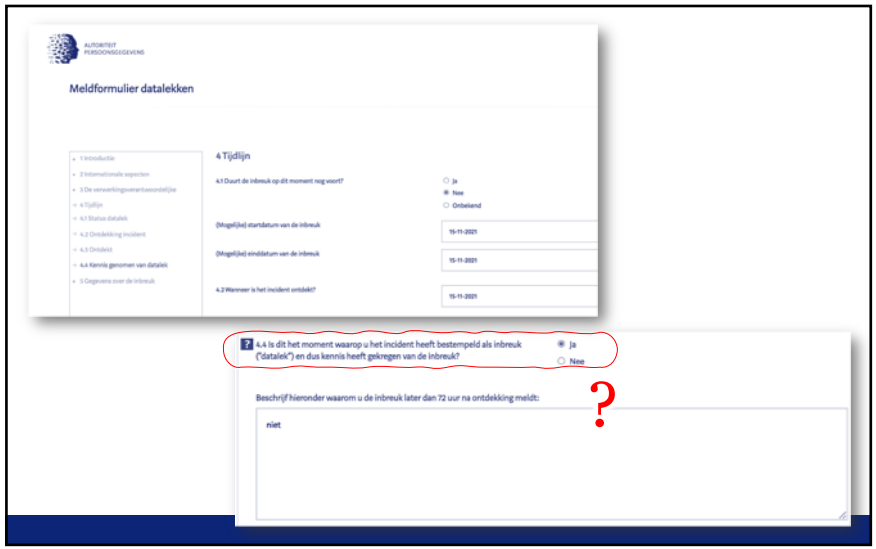
8



9

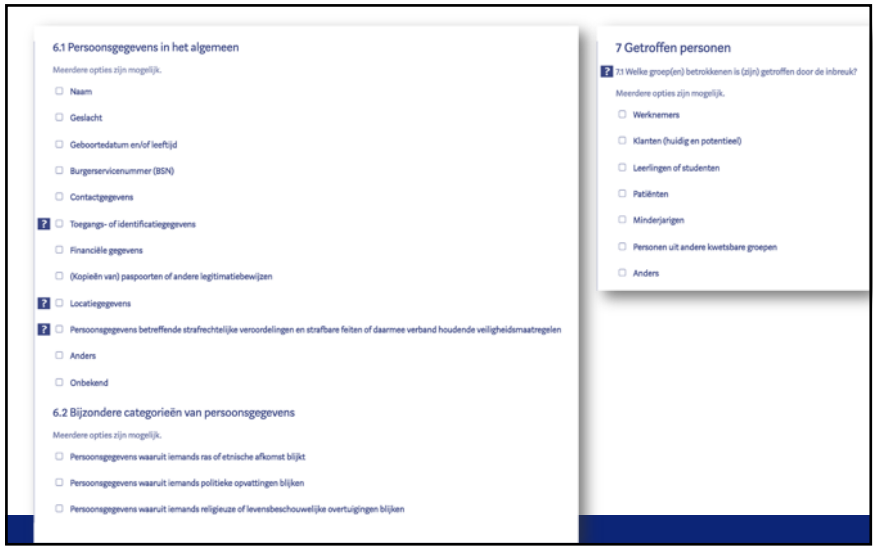
bulkmeldingen…

10

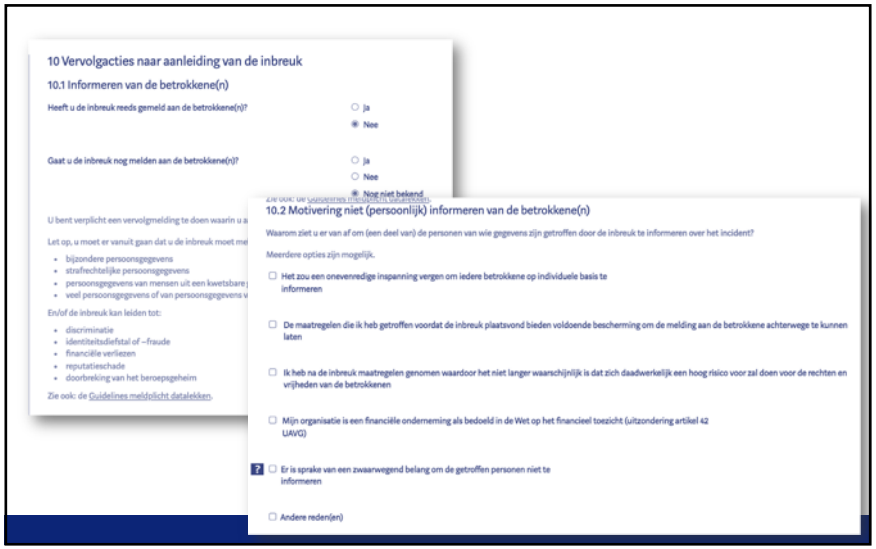


11

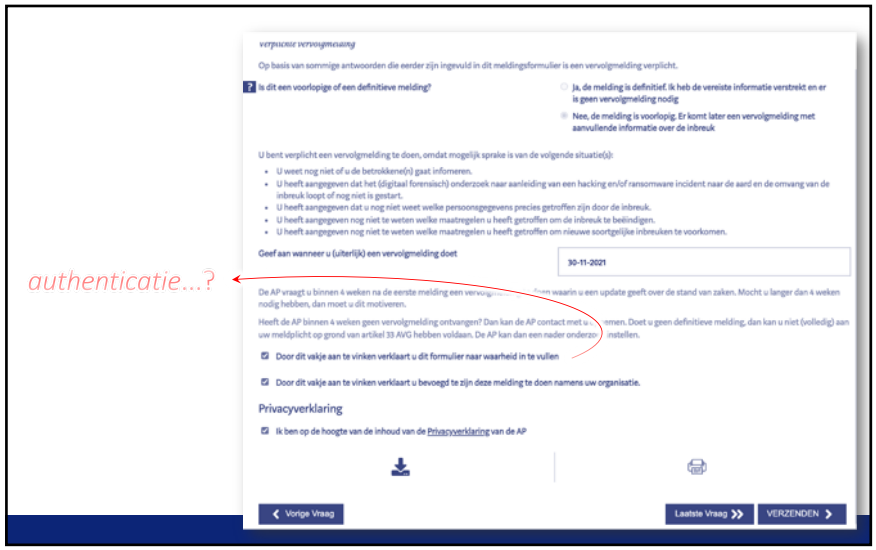
12



13



14



authenticatie...?

15

16

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 communicatie-diensten

gegevens die worden verwerkt voor overbrengen van communicatie of facturering ervan

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

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

Art. 6 en 9 Rl. 2002/58

Art. 6-7 ePR

17

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(?)

18

wat is «anoniem»…?

«niet-identificeerbaar»

(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 Preambule AVG

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

20

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

Met anonimisering wordt gedoeld 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.

21

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.

22

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

men 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 Benaissa van Bits of Freedom. „Niets is zo permanent als een tijdelijke maatregel", reageert ook

23

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 ier watchdogs, most of whom do not s 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."

24

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

Wetsvoorstel Tijdelijke wet informatieverstrekking RIVM in verband met COVID-19

Er is misschien een theoretische mogelijkheid om te identificeren.

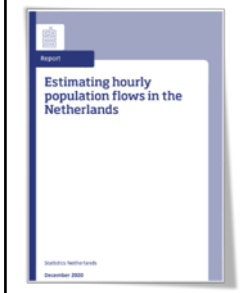
Maar daarmee zijn het nog geen persoonsgegevens…!

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

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

De kosten van en de tijd benodigd voor identificatie zonder daarbij gebruik te kunnen maken van de brongegevens (de locatie- en verkeersgegevens die de aanbieders beheren) maken een dergelijke identificatie onwaarschijnlijk. Belangrijk hierbij is dat het de aanbieders op grond van de Telecommunicatiewet verboden is om de brongegevens aan derden ter beschikking te stellen.

25



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

27

géén bewaarplicht

Wat?

- *verkeers- en lokatie-gegevens*
- *naw-gegevens*

Hoe lang?

- *12 mnd voor telefonie*
- *06 mnd 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*

Vzr Rb A'dam 11 maart 2015 ECLI:NL:RBDHA:2015:2498

buitenwerking-stelling..!

28

anoniem bellen en gebeld worden

Art. 11.9 Tw

- *recht op anoniem bellen*
- *recht om niet anoniem te worden gebeld*
- *recht om wél anoniem te worden gebeld*

maar beperkingen m.b.t. alarmnummers

- *nummerherkenning*
- *ongespecificeerde telefoonrekening*

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

Art. 11.4 Tw

Art. 7-8 Rl. 2002/58 *Art. 12-14 ePR*

29

'geheim nummer'

Art. 11.6 Tw

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

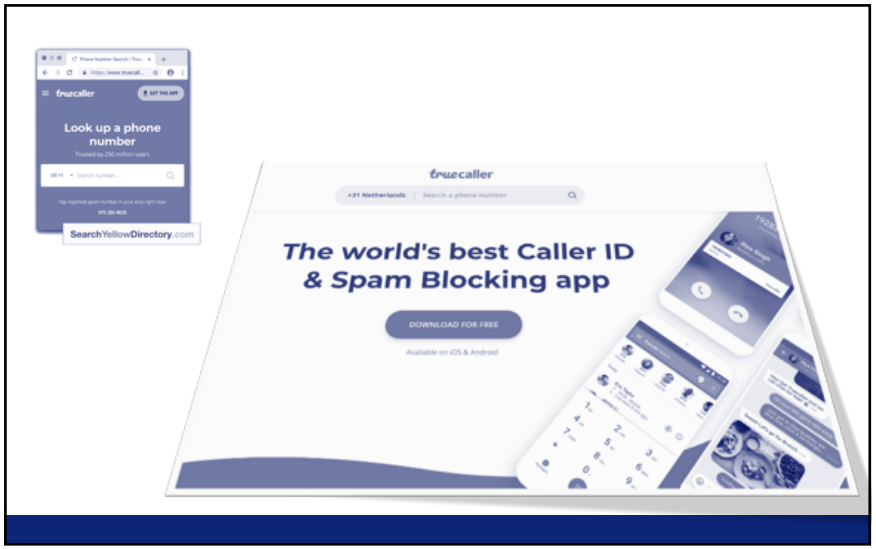
18xy: 1880, 1800, 1801

zoeken op naam in combinatie met adres en woonplaatsgegevens

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

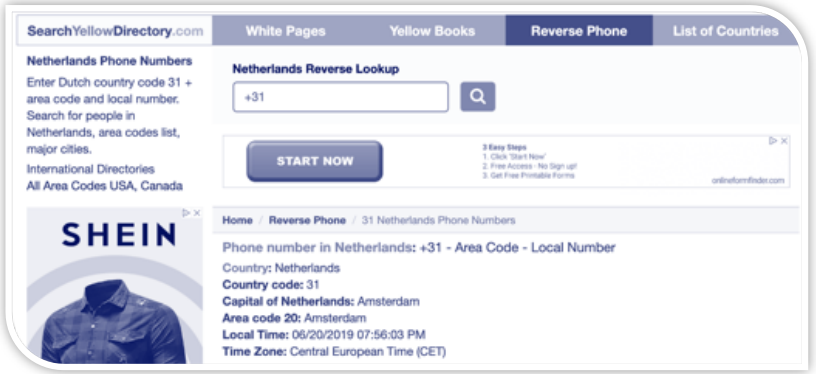
Art. 12 Rl. 2002/58 *Art. 15 ePR*

30



31

reversed search



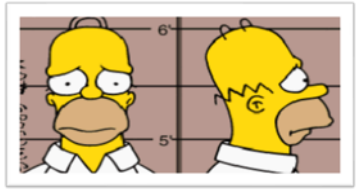
32

33

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!"



34

spam en telemarketing

Art. 11.7 Tw

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

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

35

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.

36

regels voor ongevraagde commerciële elektronische communicatie

met en 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

37

spamverbod

art. 11.7 lid 1-3 Tw

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

hoofdregel: opt-in

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

'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'

38

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
  - 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
- alleen voor eigen gelijksoortige diensten en producten
  - wat verwacht de (potentiële) klant?
  - d.w.z. van dezelfde juridische entiteit
- en opt-out..!
  - bij vastleggen contactgegevens, en
  - in iedere communicatie (bericht)
    - afmeldmogelijkheid (if you wish to unsubscribe...)

39

telemarketing

ongevraagde elektronische communicatie mét menselijke tussenkomst

hoofdregel (tot voor kort)

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

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

uitzondering

- zgn. 'bestaande klanten' met betrekking tot eigen gelijksoortige producten
  - direct of indirect promoten van product, organisatie of onderneming...

40

telemarketing

ongevraagde elektronische communicatie mét menselijke tussenkomst

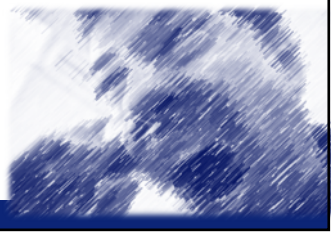
hoofdregel nu!

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

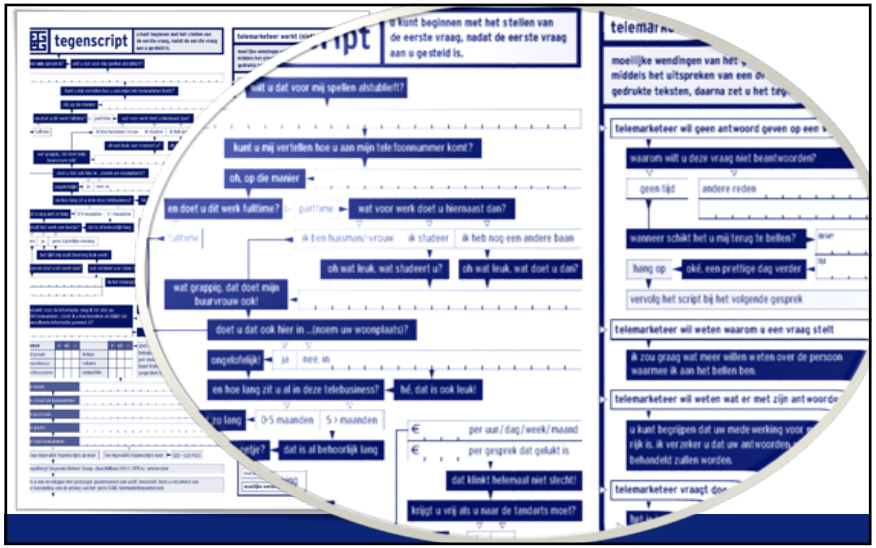
- op basis van opt-in
  - niet alleen consumenten maar ook zzp-ers, eenmanszaken, maten in een maatschap, vof's enz.

uitzondering

- zgn. 'bestaande klanten' met betrekking tot eigen gelijksoortige producten
  - direct of indirect promoten van product, organisatie of onderneming...



41



42

cookies e.d.

43

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.

ICTRecht incasseert €8200 dankzij cookiepopup met incassotoestemming

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 Analytischcookies 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.

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

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

is de toestemming in vrijheid gegeven...?

toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen

(overw. 42 Preambule AVG)

44

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

45

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

46

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

npo

UWV werken aan perspectief

47

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.

??

48

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 niet vrije «ik geef toestemming» aanklikt.

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

49

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. As a result, end-users may be 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. ***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.

50

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.

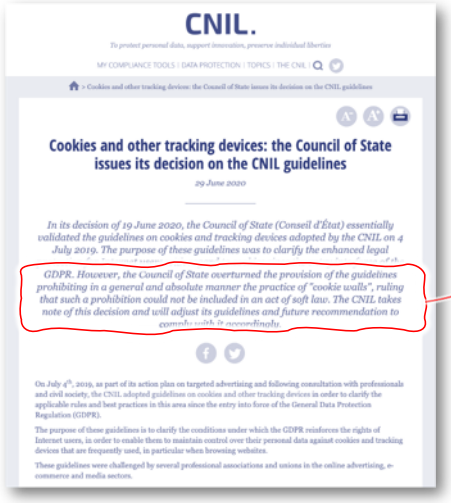
51

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.

52


CNIL.

To protect personal data, support innovation, preserve individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL

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

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

29 June 2020

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

GDPR. However, the Council of State overturned the provision of the guidelines prohibiting in a general and absolute manner the practice of "cookie walls", ruling that such a prohibition could not be included in an act of soft law. The CNIL takes note of this decision and will adjust its guidelines and future recommendation to

On July 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.

53

ePrivacy Regulation

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


Council of the European Union

Brussels, 10 February 2021

Interinstitutional File:

OUTCOME OF PROCEEDINGS

From: General Secretariat of the Council

To: Delegations

Subject: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

EN

54

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

55