@zwnne

KEUZEVAK INTERNETRECHT

privacy en gegevensbescherming (en een beetje ePrivacy)

Gerrit-Jan Zwenne 7 oktober2021

Universiteit Leiden

eLaw Leiden

1

actualiteiten…

2

56. If I go to a pub one evening, and I share with four of my friends around the table in a public place (thus unlikely to satisfy the private or household activity exception [..]) a rather unflattering remark about my neighbour that contains his personal data, which I just received by email (thus by automated means and/or is part of my filing system), do I become the controller of those data, and do all the (rather heavy) obligations of the GDPR suddenly become applicable to me? Since my neighbour never provided consent to that processing (disclosure by transmission), and since gossip is unlikely ever to feature amongst the legitimate grounds listed in Article 6 of the GDPR, (30) I am bound to breach a number of provisions of the GDPR by that disclosure, including most rights of the data subject contained in Chapter III

3

vandaag

context

- *kenmerken van de privacywet*
- *en de privacytoezichthouder*

de spelers

- *betrokkene*
- *verwerkingsverantwoordelijke*
- *verwerker*
- *toezichthouder*

het speelveld

- *geheel of gedeeltelijk geautomatiseerde verwerking persoonsgegevens en het bestand*
- *persoonlijk of huishoudelijk en journalistiek, literair of academisch*
- *territoriale werking*

de spelregels

- *verwerkingsgrondslagen*
- *doelbinding en bewaren*
- *bijzondere gegevens en bsn*
- *informatieplichten en*
- *rechten van betrokkenen*
- *enz.*

en een beetje ePrivacy

- *cookies etc.*

4

Algemene Verordening Gegevensbescherming (AVG)

regels voor de verwerking van persoonsgegevens in de EU

Uitvoeringswet AVG

nationale regels over
taken en bevoegdheden van de toezichthouder
bevoegde rechter
bijzondere gegevens en strafrechtelijke gegevens
journalistiek, archivering en openbare registers

Telecomwet

Autoriteit Consument & Markt

cookies, spam, telecomgegevens etc.

5

context

omnibus-wetgeving met grote reikwijdte, in een nogal dynamische context

het juridisch antwoord daarop: open begrippen en vage normen

want dat is toekomst-bestendig en flexibel

maar (vooralsnog) erg weinig rechtspraak

en dus nog veel onopgehelderde begrippen en rechtsonzekerheid

en een (soms wat) grote rol voor (soms wat) activistische toezichthouders

6

spelers

- betrokkenen (‘data subjects’)
  de natuurlijke personen op wie de persoonsgegevens betrekking hebben
- verwerkingsverantwoordelijken
  degenen die doeleinden en middelen van de verwerking bepalen
- verwerkers
  verwerken persoonsgegevens ten behoeve van de verwerkingsverantwoordelijken
- Autoriteit persoonsgegevens (AP)
  toezichthoudende autoriteit, bedoeld in artikel 51, eerste lid, AVG

7

speelveld

8

verwerking van persoonsgegevens

gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon

kost het een onevenredige inspanning om aan de hand van het gegeven de desbetreffende natuurlijke persoon te identificeren..?

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

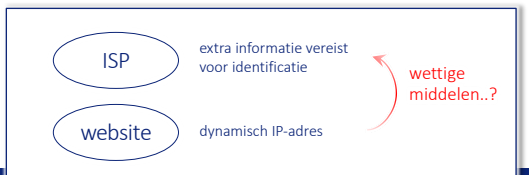
o.a. verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van ter beschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van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

9

Breyer

[E]en dynamisch IP-adres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als een persoon een website bezoekt die door deze aanbieder toegankelijk wordt gemaakt voor het publiek, ten aanzien van die aanbieder [vormt] een persoonsgegeven [..], wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust.

HJEU 19 oktober 2016 C-582/14



10

fietsendepot

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

7. [V]erweerder [heeft] aannemelijk gemaakt dat binnen de gemeente Den Haag géén IP-adressen worden vastgelegd, opgeslagen en gekoppeld aan personen. Er is dan ook geen sprake van directe of indirecte herleidbaarheid naar personen. Daartoe is van belang dat verweerder heeft toegelicht dat IP adressen indirect herleidbaar kunnen zijn tot een persoon, maar dat daarvoor middelen moeten worden ingezet om dit te kunnen vaststellen. Verweerder heeft daarbij aangegeven dat het ondoenlijk qua tijd en mankracht is om van alle burgers met wie gecommuniceerd wordt, de identificatie via een IP-adres te achterhalen. Daarbij is van belang dat de gemeente niet zelf over de gegevens om een koppeling te kunnen maken tussen een IP-adres en een burger beschikt, maar zijn er gegevens nodig van een Internet Service Provider. Nu de verwerking een excessieve inspanning van verweerder vergt, waardoor het gevaar voor identificatie in de praktijk onbeduidend is, kan het IP adres niet beschouwd worden als persoonsgegeven.

11

uitzonderingen

Art. 2.1 AVG

- verwerking t.b.v. persoonlijke of huishoudelijke doeleinden
- Politiewet, Wjsg, WIV2017, Wet BRP, Kieswet

Overw. 18. Tot persoonlijke of huishoudelijke activiteiten kunnen behoren het voeren van correspondentie of het houden van adres-bestanden, het sociaal netwerken en online-activiteiten in de context van dergelijke activiteiten.

Deze verordening geldt wel voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten.

beperkte uitzondering voor verwerkingen met journalistieke, artistieke of literaire en academische doeleinden

12

territoriale werking

EU Nederland

hoofdregel: AVG resp. UAVG is van toepassing op verwerkingen

- i.h.k.v. activiteit van vestiging van verantwoordelijke (of van verwerker) in de EU

geen vestiging in de EU? AVG resp. UAVG toch van toepassing op verwerkingen t.b.v.

- aanbieden van goederen of diensten in de unie
- monitoren van gedrag van betrokkenen in de unie

1. Wie is verantwoordelijke voor (of verwerker m.b.t.) de verwerking?
2. Heeft die verantwoordelijke (of verwerker) een vestiging in de EU resp. Nederland
3. Vindt de verwerking plaats in het kader van activiteiten van die vestiging?

Art. 4 UAVG

Art. 3(1) en (2) AVG

13

spelregels: belangrijkste verplichtingen

verwerkingsgrondslagen

- toestemming (van de betrokkene)
- overeenkomst (met de betrokkene)
- wettelijke plicht
- vitaal belang
- taak van algemeen belang (of uitoefening openbaar gezag)
- gerechtvaardigd belang

welbepaald uitdrukkelijk omschreven verzameldoel

geen verdere verwerking voor onverenigbare doeleinden (doelbinding)

data-minimalisatie

niet langer bewaren dan nodig

privacy-by-design

privacy-by-default

14

spelregels: belangrijkste verplichtingen

Art. 6.1 AVG

verwerkingsgrondslagen

- toestemming (van de betrokkene)
- overeenkomst (met de betrokkene)
- wettelijke plicht
- vitaal belang
- taak van algemeen belang (of uitoefening openbaar gezag)
- gerechtvaardigd belang

welbepaald uitdrukkelijk omschreven verzameldoel

geen verdere verwerking voor onverenigbare doeleinden (doelbinding)

data-minimalisatie

niet langer bewaren dan nodig

privacy-by-design

privacy-by-default

15

spelregels: belangrijkste verplichtingen

verwerkingsgrondslagen

- toestemming (van de betrokkene)
- overeenkomst (met de betrokkene)
- wettelijke plicht
- vitaal belang
- taak van algemeen belang (of uitoefening openbaar gezag)
- gerechtvaardigd belang

Art. 5.1b AVG

welbepaald uitdrukkelijk omschreven verzameldoel

Art. 6.4 AVG

geen verdere verwerking voor onverenigbare doeleinden (doelbinding)

data-minimalisatie 5.1c AVG

niet langer bewaren dan nodig 5.1e AVG

privacy-by-design 25 AVG

privacy-by-default 25 AVG

16

min-of-meer formele verplichtingen…

- informatieverplichtingen
- accountability en documentatieplicht
- data protection impact assessment (“DPIA”)
- functionaris voor gegevensbescherming
- beveiliging en meldplicht datalekken
- derde landen doorgifte

17

min-of-meer formele verplichtingen…

- informatieverplichtingen

Privacy Statement

Dit is het privacy statement van ..... [naam bedrijf], gevestigd te ..... [postcode, plaats] aan de ..... [adres] (hierna: ..... [naam bedrijf]), www..... [internetadres]

Toepasselijkheid

Dit privacy statement is van toepassing op alle privacygevoelige informatie of persoonsgegevens die u aan ons verstrekt, bijvoorbeeld via het contactformulier of bestellingen die u plaatst op onze website. Wij hechten groot belang aan de privacy van onze klanten en betrachten daarom de grootst mogelijke zorgvuldigheid in het behandelen en beschermen van persoonsgegevens. Wij verwerken data overeenkomstig de voorwaarden die daarover worden gesteld in de Algemene Verordening Gegevensbescherming (AVG). ..... [naam bedrijf] is de verantwoordelijke in de zin van de AVG ten aanzien van de verwerking van uw persoonsgegevens. Dit houdt in dat alleen wij bepalen welke persoonsgegevens worden verwerkt, met welk doel en op welke manier. Wij zijn er verantwoordelijk voor dat uw persoonsgegevens op een behoorlijke en zorgvuldige wijze worden verwerkt in overeenstemming met de AVG. In dit privacy statement leggen wij uit welke gegevens wij verwerken en voor welke doeleinden ze worden gebruikt.

Overzicht persoonsgegevens

Hieronder vindt u een overzicht van de persoonsgegeven die wij verwerken:

- Voor- en achternaam
- Geslacht
- Geboortedatum
- Geboorteplaats
- Adresgegevens
- Telefoonnummer
- E-mailadres
- ..... [indien nog u andere persoonsgegevens verwerkt, dan dient u die hier verder in te vullen, bv. bankrekeningnummer, BSN-nummer, IP-adres, etc.]

Doel en grondslagen verwerking persoonsgegevens

[Optie: indien de bezoeker van de website akkoord is gegaan met dit privacy statement door een hokje aan te vinken:] Door akkoord te gaan met dit privacy statement geeft u expliciet toestemming in de zin van artikel 6 lid 1 sub a van de AVG voor het verwerken van uw persoonsgegevens voor de

Art. 12-14 AVG

18

min-of-meer formele verplichtingen…

data protection impact assessment (“DPIA”)

19

min-of-meer formele verplichtingen…

accountability en documentatieplicht

20

tingen…


Uitgelicht

De waarborging van de kwaliteit van de functionaris voor de gegevensbescherming

Prof. mr. dr. G-J. Zwenne*

196

functionaris voor gegevensbescherming

21

rechten voor betrokkenen

inzage, verbetering, afscherming etc.

verzetsrechten

vergeetrechten

gegevensoverdraagbaarheid

geautomatiseerde besluitvorming en profilering

22

bijzondere en strafrechtelijke gegevens

- levensovertuiging of godsdienst
- politieke gezindheid
- lidmaatschap vakbond
- ras, etniciteit
- seksuele leven
- gezondheid
- biometrische ID-gegevens
- genetische gegevens


Het Parool

Al het voetbal op internet, en de privacy...?

De KNVB en mediabedrijf Talpa beginnen deze maand via het platform VoetbalTV met het uitzenden van tienduizend wedstrijden in het amateurvoetbal. De vraag is: staat privacywetgeving dat niet in de weg?

Marcel Wiegman 7 september 2018, 16:14

- strafrechtelijke gegevens

Art. 22-33 UAVG

Art. 9-10 AVG

verwerking bijzondere gegevens verboden, tenzij…

- specifieke uitzonderingen: door bepaalde verwerkers en voor bepaalde doeleinden
- algemene uitzonderingen: met uitdrukkelijke toestemming (enz.), …

23

(42) Indien de verwerking plaatsvindt op grond van toestemming van de betrokkene, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking. [..]. 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.

24

biometrische gegevens

Rb. A'dam 12 augustus 2019, ECLI:NL:RBAMS:2019:6005

- vingerafdruk gebruikt door werknemers om in te loggen op kassasysteem
- mag dat?
- art. 9.1 UAVG jo. 29 UAVG

→ verbod op verwerking biometrische ID-gegevens

→ uitzondering voor zover noodzakelijk voor authenticatie- en beveiligingsdoeleinden

wél voor kerncentrale, niet voor garagebedrijf

Kamerstukken II 2017/2018, 34 851, nr. 3, p. 109

→ en dus (?) niet voor een schoenenwinkel

MANFIELD
Style & Quality

25

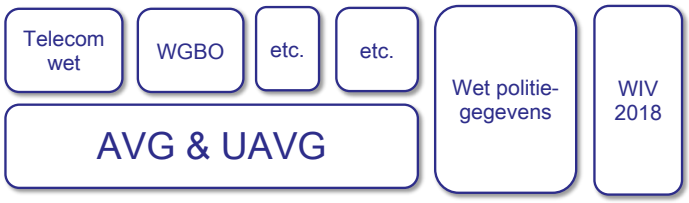
universitair sportcentrum

→ uitdrukkelijke toestemming

alternatief bieden…?

→ administratieve kosten in rekening brengen..?

26



EPRIVACY: HOOFDSTUK 11 TELECOMWET

27

ePrivacyrichtlijn – straks een verordening

- de vertrouwelijkheid van elektronische communicatie, incl. zgn. metadata
- commerciële, ideële of charitatieve elektronische berichten
- cookies en vergelijkbare technieken
- telefoongidsen, nummerherkenning, alarmnummers etc.

d.w.z. inhoud maar ook deep packet inspection, verkeers- en locatie-gegevens

spam, telemarketing, bel-me-niet

cookiemuren enz.

Rl. 2002/58/EG en 2009/36/EG

Hoofdstuk 11 Telecomwet

28

toestemmingsvereiste voor cookies

d.w.z. plaatsen en uitlezen van gegevens op een device

overw. 32, 42-34 AVG

art. 12-14 AVG

- duidelijke en volledige informatie
- toestemming van de gebruiker

art. 7 AVG

uitzonderingen

- uitvoeren communicatie
- levering dienst vd informatiemaatschappij
- privacyneutrale cookies t.b.v. verkrijgen informatie over effectiviteit of kwaliteit → A/B-testing, analytics

art. 11.7a Tw

29

cookiebepaling

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

art. 11.7a, eerste lid, Telecomwet

- duidelijke en volledige informatie overeenkomstig de AVG, en in ieder geval over de doeleinden van de cookies
- toestemming van de gebruiker

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)

30

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

taalinstellingen, voorkeuren, opslaan wachtwoord, betalingen via ideal, enz.

Kst II 2010/11, 32 549, p. 78

analytics, A/B-testing, affiliate cookies, e.d.

31

bewijsvermoeden voor tracking

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

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

32

cookiemurenverbod voor overheid...

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

UWV werken aan perspectief

Belastingdienst

npo

33

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).

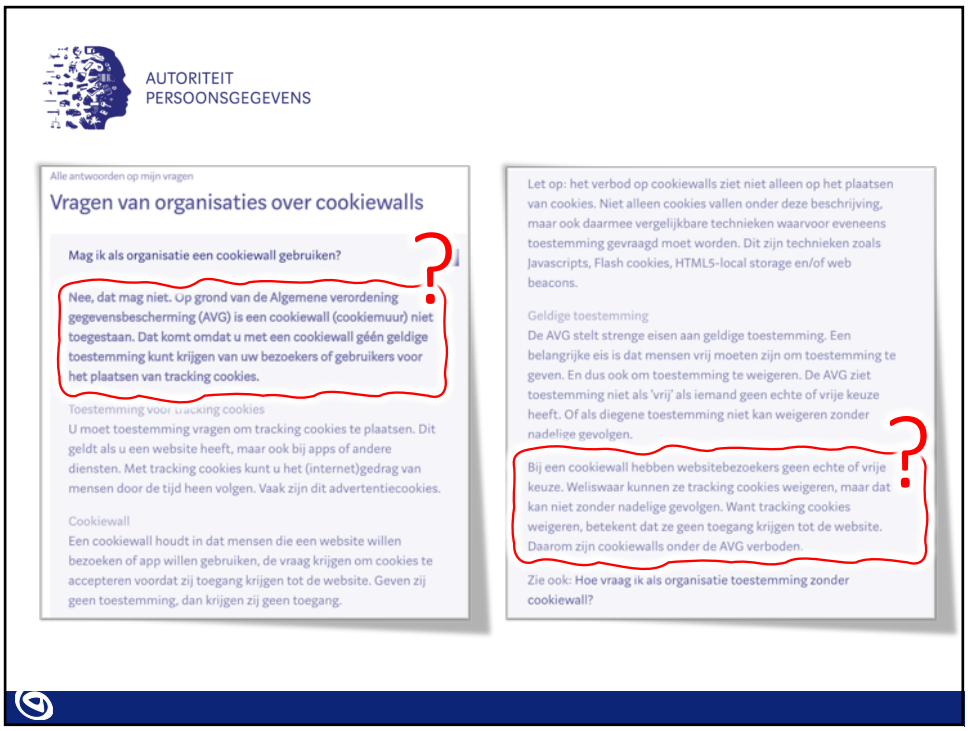
Cookiewalls

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.

?

34

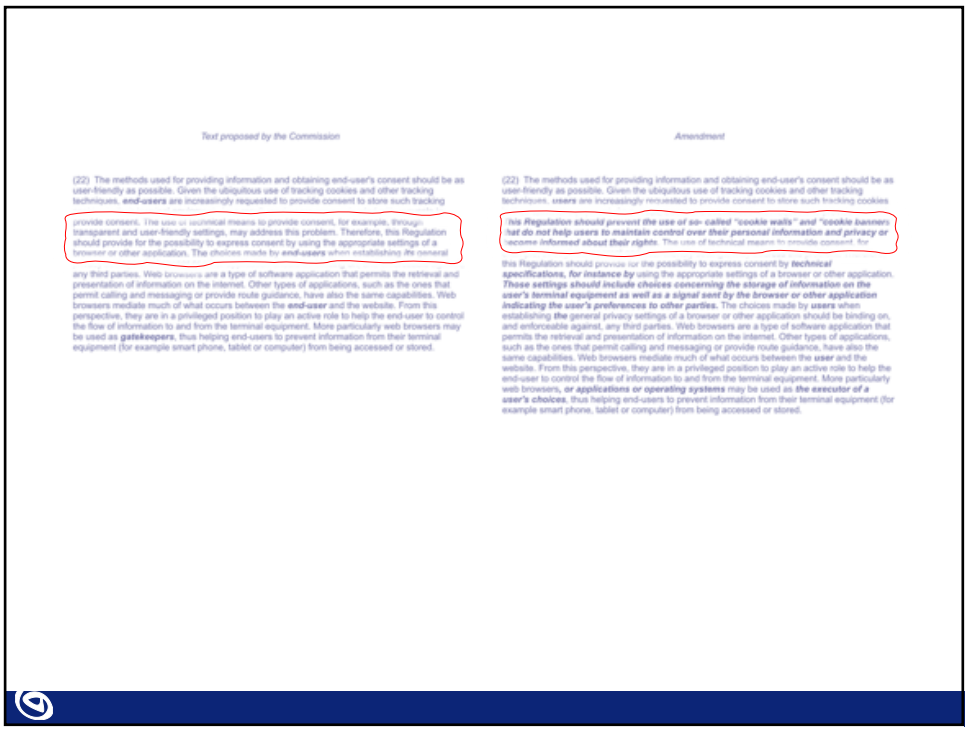


35

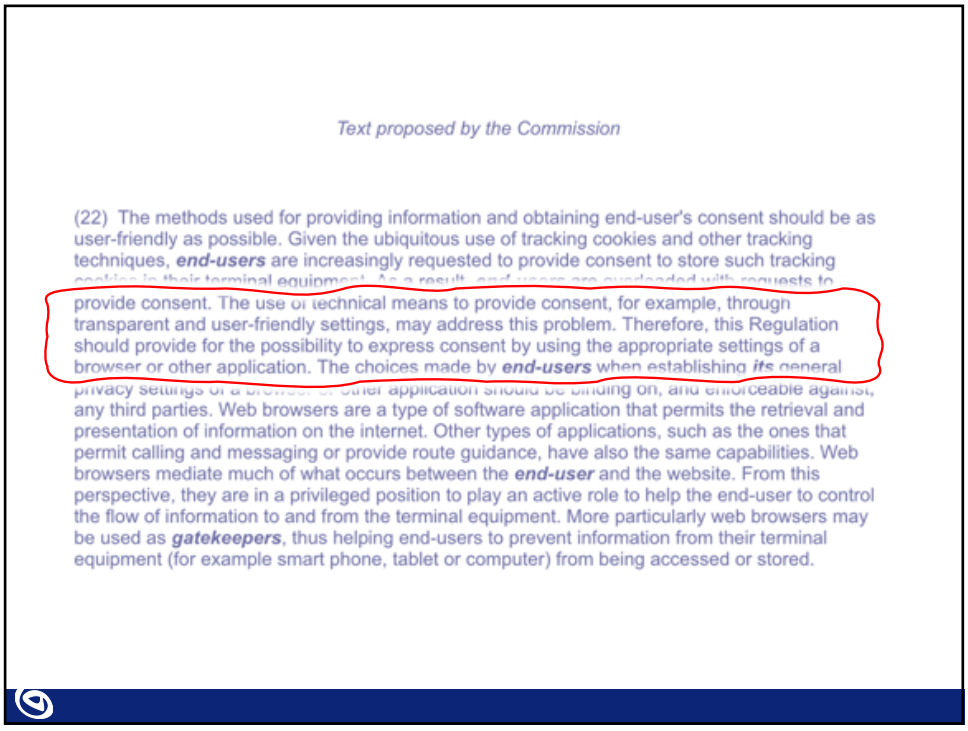
Een cookiemuur is over het algemeen dan ook een rechtmatige manier om aan het toestemmingsvereiste in de cookiebepaling te voldoen. Ook al is dit niet de meest gebruiksvriendelijke manier en is het technisch ook nooit noodzakelijk, het staat de websitehouder in beginsel wel vrij om te bepalen of hij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

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

36


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

37

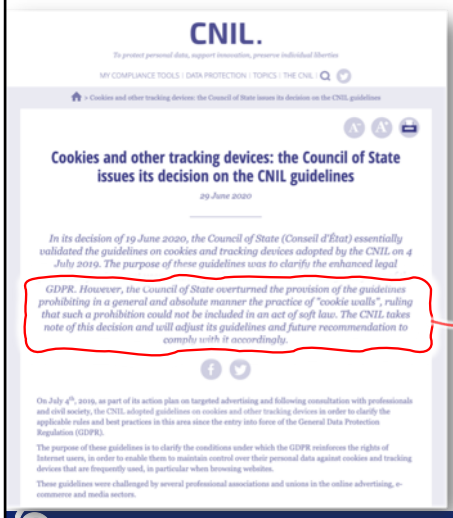

Text proposed by the Commission
(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking
provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general
any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

38

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 by way of transparent and user friendly settings, may address this problem. 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.

39


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 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.

40

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*


Council of the European Union

Brussels, 10 February 2021
(OR. en)

6087/21

Interinstitutional File:
2017/0003(COD)

TELECOM 52
COMPET 90
MI 93
DATAPROTECT 34
CONSOM 38
JAI 131
DIGIT 25
FREMP 26
CYBER 33
CODEC 178

OUTCOME OF PROCEEDINGS
From: General Secretariat of the Council
To: Delegations
No. prev. doc.: 5840/21
No. Cion doc.: 5358/17
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)
- Mandate for negotiations with EP

Delegations will find in the Annex the Mandate on the above mentioned Proposal for a Regulation adopted by the Permanent Representatives Committee on 10 February 2021.

6087/21 TREE.2.B PR/rk 1 EN

41

g.j.zwenne@law.leidenuniv.nl

VRAGEN....!?

42