





@zwnne

KEUZEVAK INTERNETRECHT

privacy en gegevensbescherming
(en een beetje ePrivacy)

Gerrit-Jan Zwenne 7 oktober 2012

 Universiteit
Leiden



1

actualiteiten...

 InfoCuria
Rechtspraak

Nederlands (nl)

Welkom > Zoekformulier > Lijst van de resultaten > Documenten

Taal van het document: Engels ECLI:EU:C:2021:822 Afdrukken

Provisional text
OPINION OF ADVOCATE GENERAL
BOBEK
delivered on 6 October 2021⁽¹⁾
Case C-345/20
X,
Z,
v
Autoriteit Persoonsgegevens
(Request for a preliminary ruling from the Rechtbank Midden-Nederland (District Court, Central Netherlands, Netherlands))

(Reference for a preliminary ruling - Protection of natural persons with regard to the processing of personal data - Regulation (EU) 2016/679 - Competence of the supervisory authority - Processing operations carried out by courts in the exercise of their judicial capacity - Disclosure of procedural documents to a journalist)

I. Introduction

1. 'Publicity is the very soul of justice. It is the keenest spur to exertion, and the surest of all guards against impropriety. ... It is through publicity alone that justice becomes the mother of security. By publicity, the temple of justice is converted into a school of the first order, where the most important branches of morality are enforced.' ⁽¹⁾



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

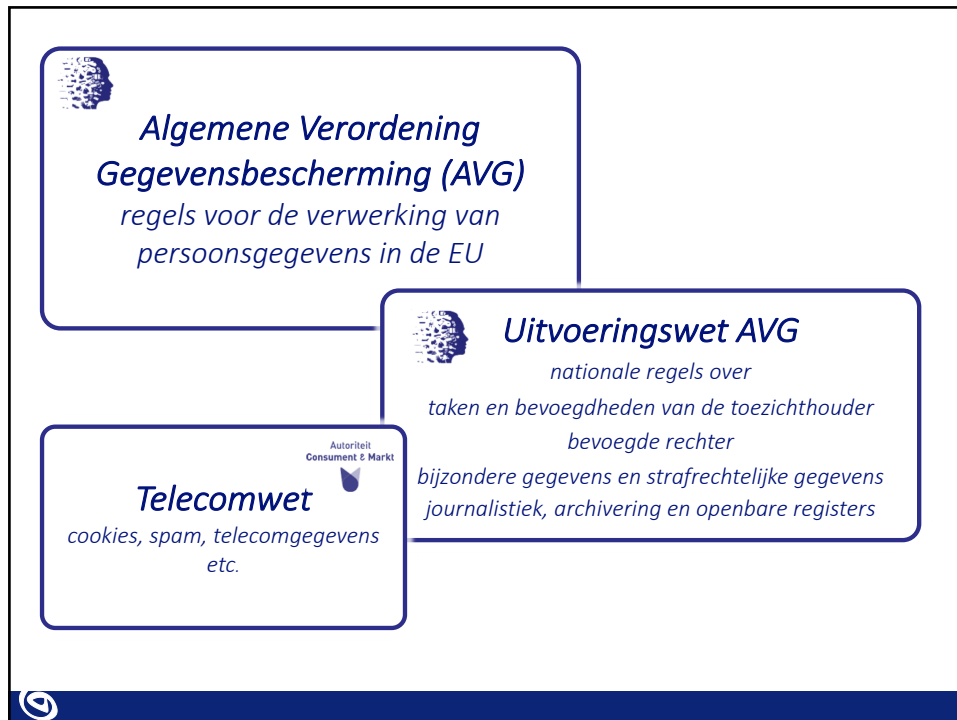
- verwerkingsgrondslagen
- doelbinding en bewaren
- bijzondere gegevens en bsn
- informatieplichten en
- rechten van betrokkenen
- enz.

en een beetje ePrivacy

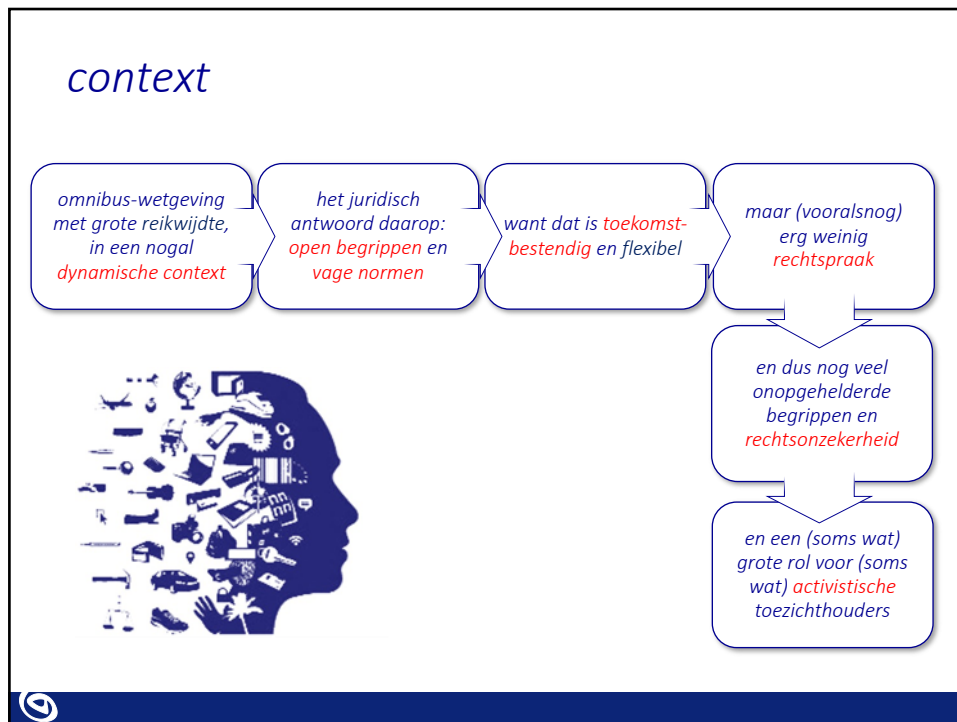
- cookies etc.



4



5



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
behoefte van de
verwerkingsverantwoordelijken
- Autoriteit persoonsgegevens (AP)
toezichthoudende autoriteit, bedoeld in
artikel 51, eerste lid, AVG



ASOPUS
DE VLIET



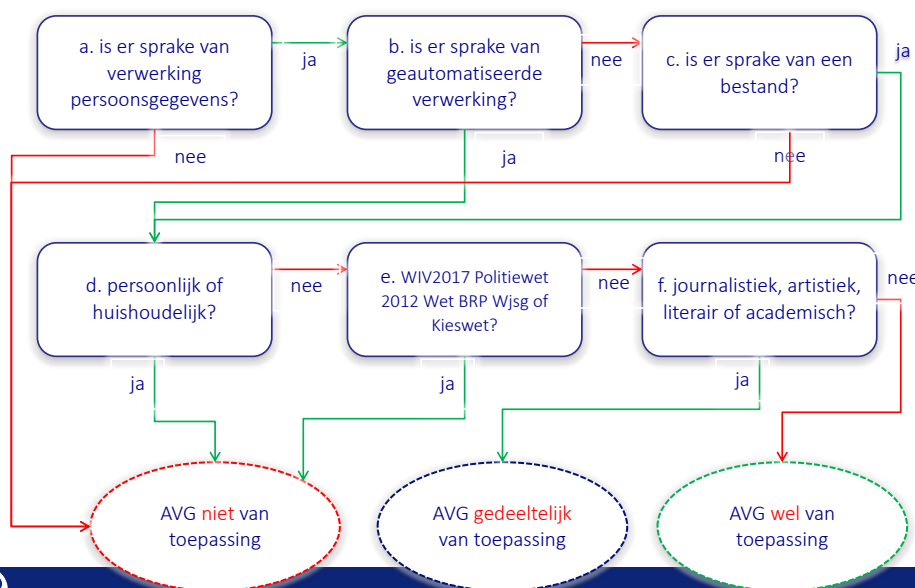
DAVILEX
LEDENADMINISTRATIE SOFTWARE



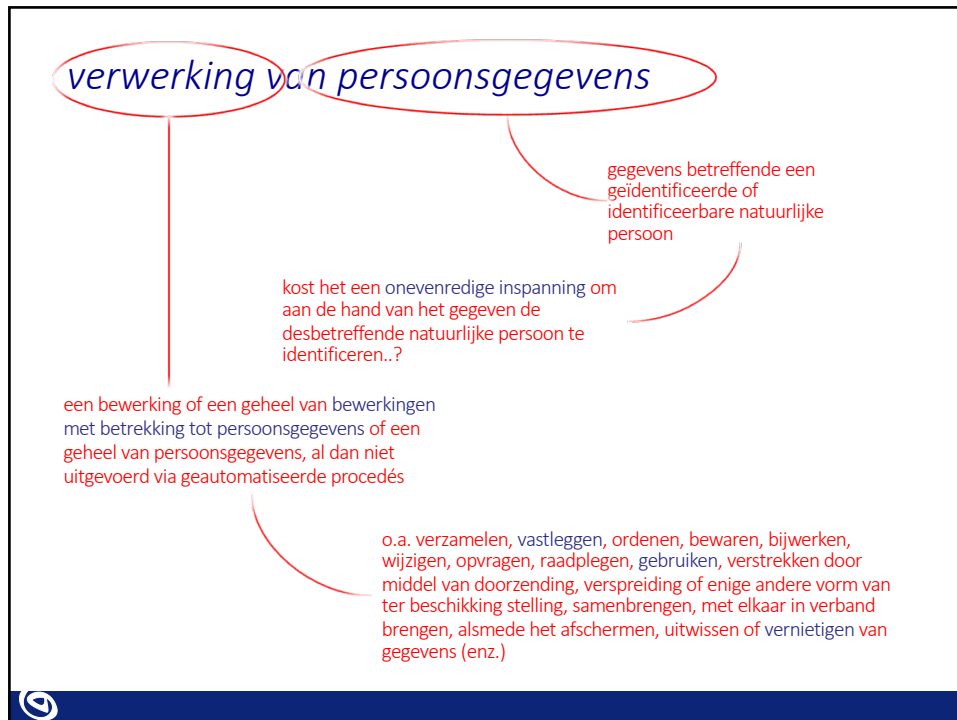
AUTORITEIT
PERSOONSGEGEVENS

7

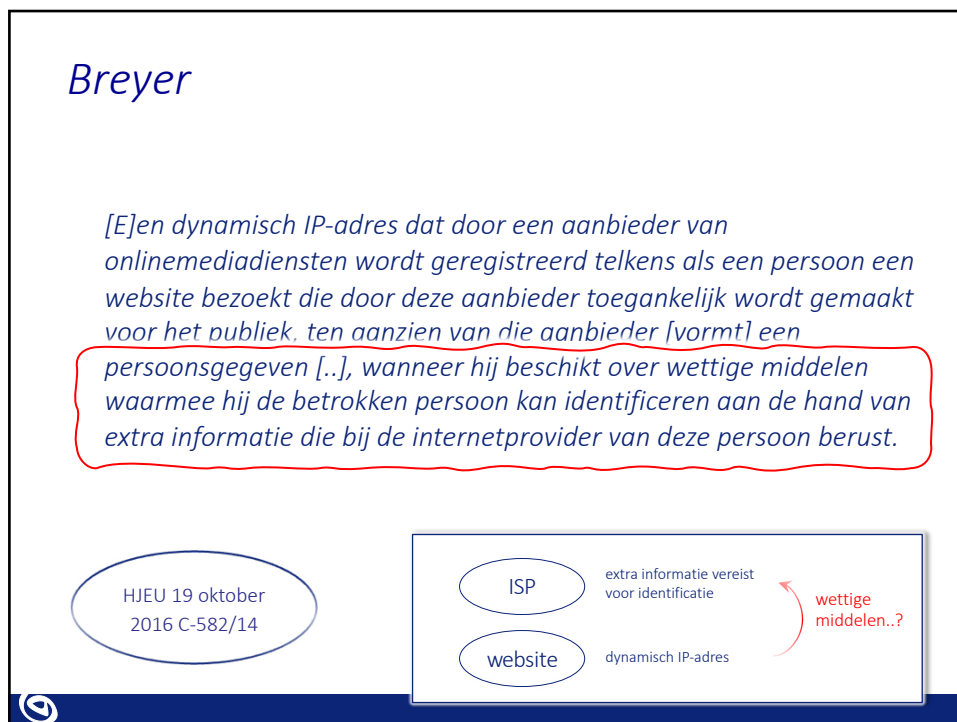
speelveld



8



9



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 ~~reikwijdte 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 persoonsgegevens.

11

uitzonderingen

Art. 2.1
AVG

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

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

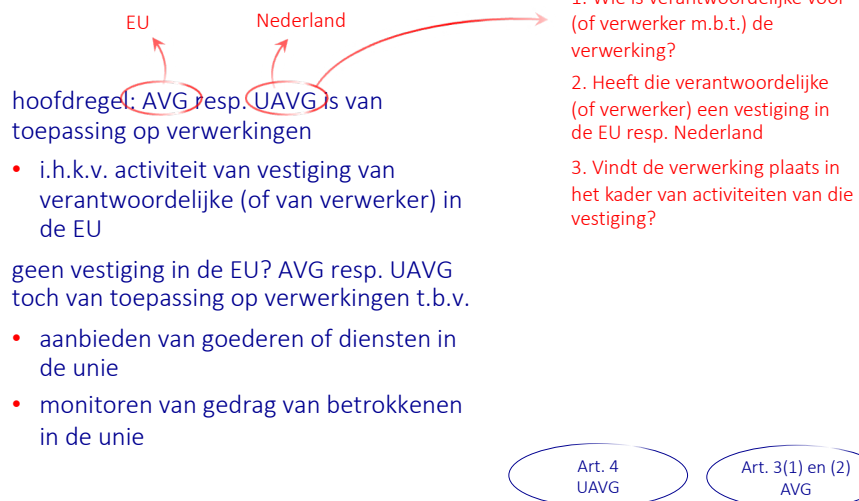
Overw. 18. Tot **persoonlijke of huishoudelijke activiteiten** kunnen behoren het voeren van correspondentie of het houden van adresbestanden, het sociaal netwerken en online-activiteiten in de context van dergelijke activiteiten.

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

12



territoriale werking

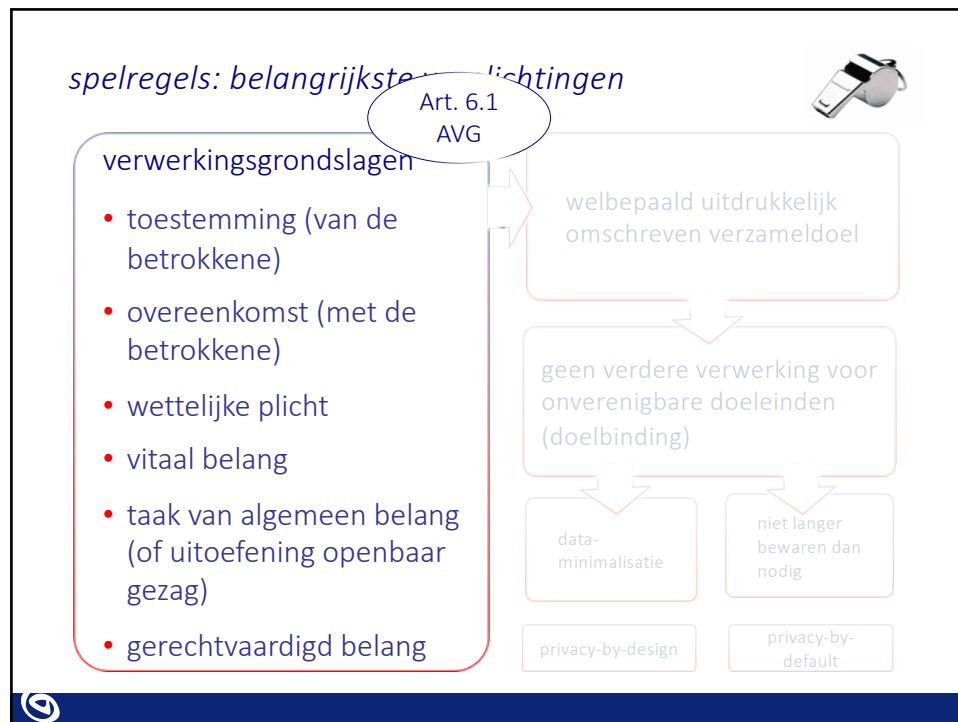


13

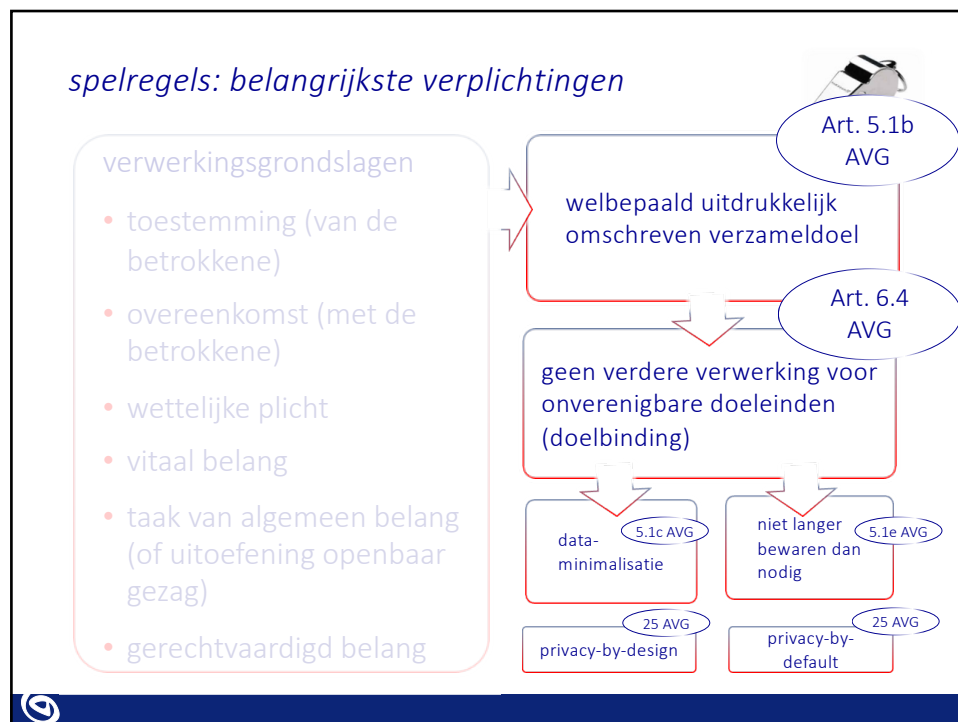
spelregels: belangrijkste verplichtingen



14



15



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

Art. 12-14
AVG



18



min-of-meer formele verplichtingen...

data protection impact
assessment ("DPIA")



19

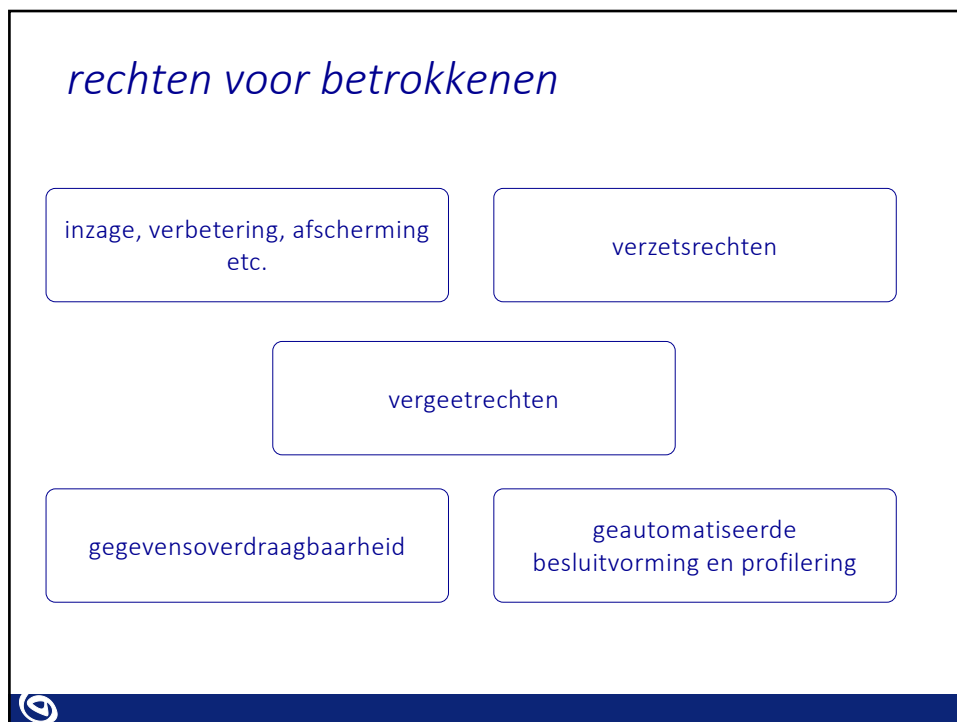
min-of-meer formele verplichtingen...

accountability en
documentatieplicht

20



21



22



bijzondere en strafrechtelijke gegevens

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



- 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 zov(noodzakelijk) oor
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

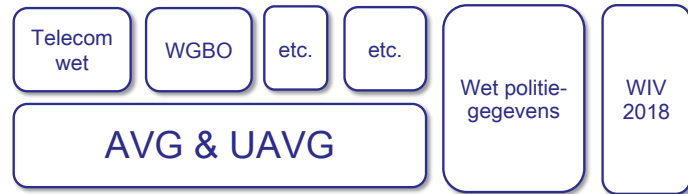


uitdrukkelijke
toestemming

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
- cookie-muren enz.

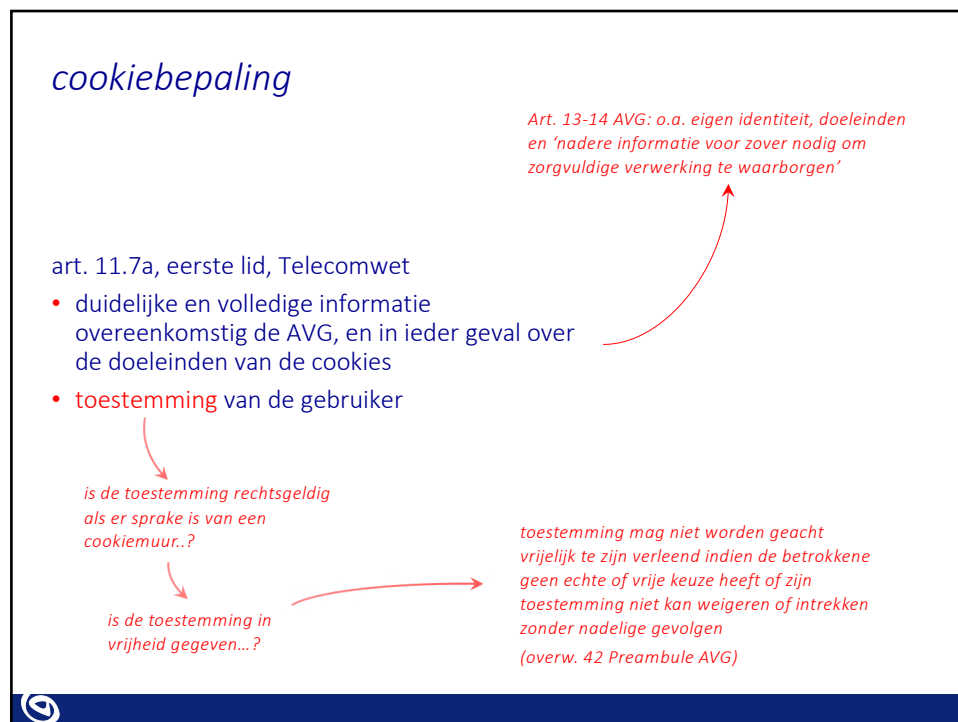
RI. 2002/58/EG
en 2009/36/EG

Hoofdstuk 11
Telecomwet

28



29



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

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

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

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

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



Belastingdienst



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



AUTORITEIT
PERSOONSGEGEVENS

Alle antwoorden op mijn vragen

Vragen van organisaties over cookiewalls

Mag ik als organisatie een cookiewall gebruiken?

Nee, dat mag niet. Op grond van de Algemene verordening gegevensbescherming (AVG) is een cookiewall (cookiemuur) niet toegestaan. Dat komt omdat u met een cookiewall géén geldige toestemming kunt krijgen van uw bezoekers of gebruikers voor het plaatsen van tracking cookies.

Toestemming voor tracking cookies

U moet toestemming vragen om tracking cookies te plaatsen. Dit geldt als u een website heeft, maar ook bij apps of andere diensten. Met tracking cookies kunt u het (internet)gedrag van mensen door de tijd heen volgen. Vaak zijn dit advertentiecookies.

Cookiewall

Een cookiewall houdt in dat mensen die een website willen bezoeken of app willen gebruiken, de vraag krijgen om cookies te accepteren voordat zij toegang krijgen tot de website. Geven zij geen toestemming, dan krijgen zij geen toegang.

Let op: het verbod op cookiewalls ziet niet alleen op het plaatsen van cookies. Niet alleen cookies vallen onder deze beschrijving, maar ook daarmee vergelijkbare technieken waarvoor eveneens toestemming gevraagd moet worden. Dit zijn technieken zoals Javascripts, Flash cookies, HTML5-local storage en/of web beacons.

Geldige toestemming

De AVG stelt strenge eisen aan geldige toestemming. Een belangrijke eis is dat mensen vrij moeten zijn om toestemming te geven. En dus ook om toestemming te weigeren. De AVG ziet toestemming niet als 'vrij' als iemand geen echte of vrije keuze heeft. Of als diegene toestemming niet kan weigeren zonder nadelige gevolgen.

Bij een cookiewall hebben websitebezoekers geen echte of vrije keuze. Weliswaar kunnen ze tracking cookies weigeren, maar dat kan niet zonder nadelige gevolgen. Want tracking cookies weigeren, betekent dat ze geen toegang krijgen tot de website. Daarom zijn cookiewalls onder de AVG verboden.

Zie ook: Hoe vraag ik als organisatie toestemming zonder cookiewall?

35

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

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 <i>its</i> 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 expose 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.

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 cookies in their terminal equipment. As a result, end-users are confronted 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 <i>its</i> 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.

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 technologies, users are increasingly asked to consent to the use of such technologies 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 pre-installing cookies, should be prohibited.

this Regulation should provide for the possibility to express consent by **technical specifications, for instance by** using the appropriate settings of a browser or other application. **Those settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties.** The choices made by **users** when establishing the general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the **user** and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers, **or applications or operating systems** may be used as **the executor of a user's choices**, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

39

[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.

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.

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



41

g.j.zwenne@law.leidenuniv.nl

VRAGEN....!?

42