@zwnne

KEUZEVAK INTERNETRECHT

privacy en gegevensbescherming (en een beetje ePrivacy)

Gerrit-Jan Zwenne 27 februari 2020

Universiteit Leiden

eLaw Leiden

vandaag

context
- kenmerken van de privacywet
- en de privacytoezichthouder

de spelers
- de betrokkene
- de verwerkingsverantwoordelijke
- de verwerker

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

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

ePrivacy
- cookies, spam etc.

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

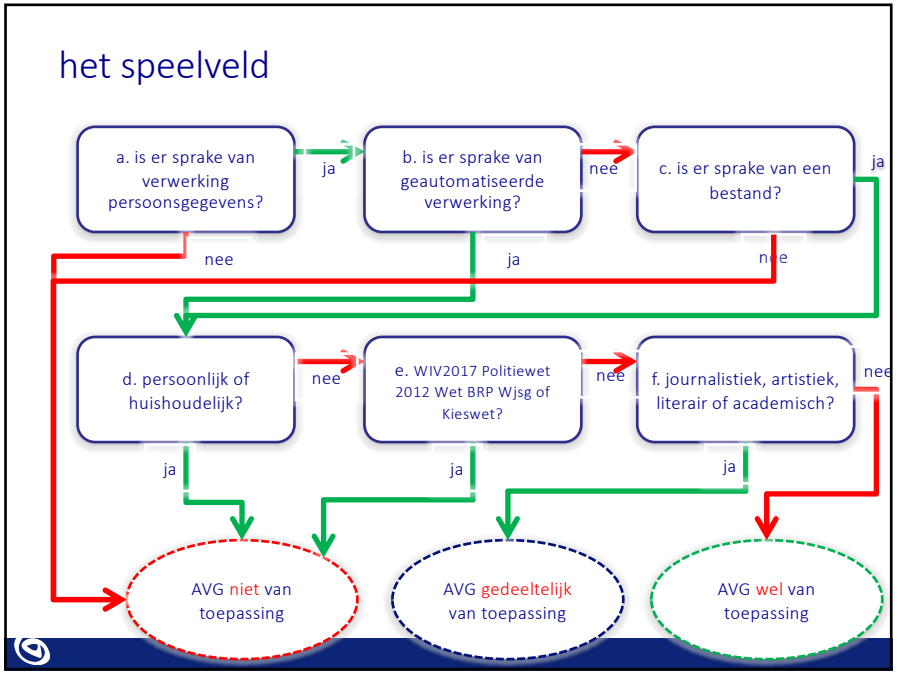
en dus nog veel onopgehelderde begrippen en rechtsonzekerheid

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

de 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

het speelveld



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..?

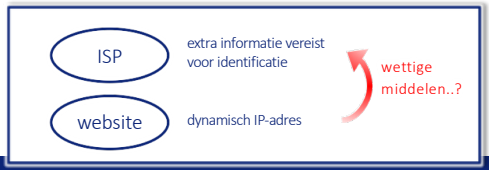
een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés

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.)

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



uitzonderingen

Art. 2(1) en (2)c 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

territoriale werking

hoofdregel: AVG is van toepasssing op verwerkingen

- i.h.k.v. activiteit van vestiging van verantwoordelijke (of van verwerker) in de EU
- geen vestiging in de EU? AVG 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
3. Vindt de verwerking plaats in het kader van activiteiten van die vestiging?

Art. 4 UAVG

Art. 3(1) en (2) AVG

de 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

min-of-meer formele verplichtingen…

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

rechten voor betrokkenen

- inzage, verbetering, afscherming etc.
- verzetsrechten
- vergeetrechten
- gegevensoverdraagbaarheid
- geautomatiseerde besluitvorming en profilering

bijzondere en strafrechtelijke gegevens

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


Het Parool

Nederland | Wereld | Kunst & Media | Sport | Columns & Opinie

Plus

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

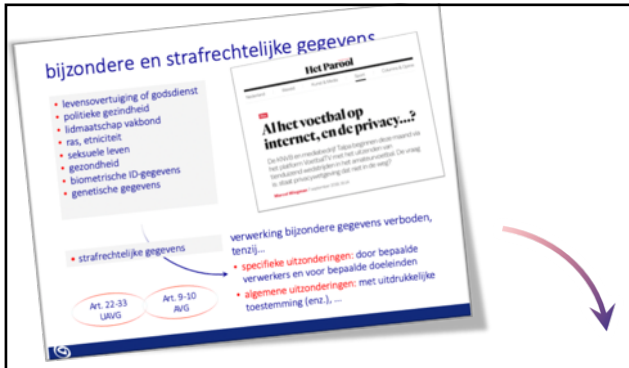
- strafrechtelijke gegevens

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.), …



(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.

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

universitair sportcentrum

→ uitdrukkelijke toestemming

→ alternatief bieden…?

→ administratieve kosten in rekening brengen..?

EPRIVACY: HOOFDSTUK 11 TELECOMWET

ePrivacyrichtlijn – straks (?) een verordening

- de vertrouwelijkheid van elektronische communicatie, incl. metadata → d.w.z. inhoud maar ook deep packet inspection, verkeers- en locatie-gegevens
- commerciële, ideële of charitatieve elektronische berichten → spam, telemarketing, bel-me-niet
- cookies en vergelijkbare technieken
- telefoongidsen, nummerherkenning, alarmnummers etc. → cookiemuren enz.

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

Hoofdstuk 11 Telecomwet

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

art. 11.7a Tw

beta-testing, analytics

cookiemuren-verbod

Art 11.7(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

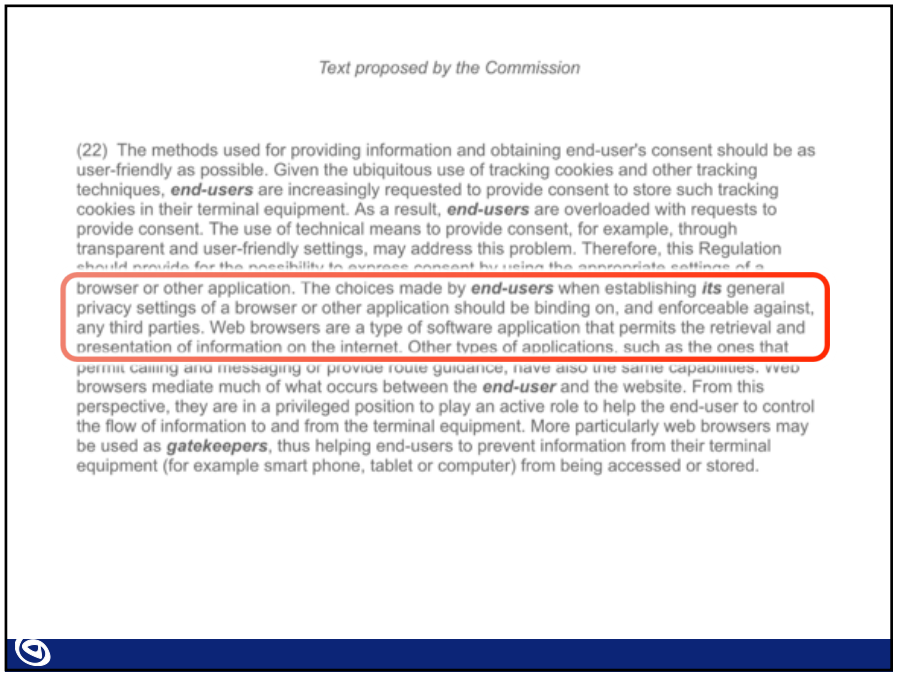
cookiemuren-discussie

Text proposed by the Commission

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

Amendment

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, ***users*** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, ***users*** are overloaded with requests to provide consent, ***This Regulation should prevent the use of so- called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights.*** The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. 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.



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

browser or other application. The choices made by ***end-users*** when establishing ***its*** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that

permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the ***end-user*** and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as ***gatekeepers***, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

Amendment

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, ***users*** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, ***users*** are overloaded with requests to provide consent. ***This Regulation should prevent the use of so- called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights***. The use of technical means to provide consent, for [illegible] 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.

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?

g.j.zwenne@law.leidenuniv.nl

VRAGEN….!?