



Inhoudsopgave

1. Vragen over de wet
 2. Vragen over het toepassingsbereik
 3. Vragen over de uitzonderingen
 4. Vragen van gebruikers
 5. Vragen over de implementatie door marktpartijen
 6. Vragen over ACM
- Bijlage 1: wettekst bij artikel 11.7a Telecommunicatiewet

Voorwoord

Volgens de cookiebepaling, die is opgenomen in artikel 11.7a van de Telecommunicatiewet (hierna kortweg Tw), moeten websites bezoekers informeren en toestemming verkrijgen alvorens zij een cookie of andere gegevens op de computer, laptop of mobiele telefoon plaatsen of lezen. Dit geldt niet voor cookies die noodzakelijk zijn voor de technische werking van de site of bijvoorbeeld analytische cookies die slechts een geringe inbreuk maken op de privacy van gebruikers. ACM ontvangt regelmatig vragen van bedrijven en (overheids)instellingen over de cookiebepaling. Daarnaast zijn er andere technieken die gegevens opslaan en/of toegang verkrijgen tot gegevens op een computer, zoals Javascripts of Web beacons. Waar in het vervolg wordt gesproken over cookies, worden ook deze technieken bedoeld.

In dit document staan de antwoorden op veelgestelde vragen om duidelijkheid te bieden aan partijen. Deze publicatie is een update van de laatste versie van dit document uit maart 2015 en betreft diverse wijzigingen aan de indeling en een uitbreiding ten aanzien van de informatie over het verbod op cookiewalls bij overheidswebsites.

ACM geeft geen juridisch advies. Bedrijven en websitebeheerders zijn zelf verantwoordelijk voor de wijze waarop zij praktische invulling geven aan de cookiebepaling. Consumenten die meer willen weten over cookies, kunnen terecht op ConsuWijzer.¹

¹ <https://www.consuwijzer.nl/>.



1 Vragen over de wet

Wat zijn de regels?

Cookies zijn kleine tekstbestanden die op de computer of alle andere randapparatuur van de gebruiker worden geplaatst bij een bezoek aan een website. Deze cookies kunnen gebruikers volgen over verschillende websites en maken daarmee bijvoorbeeld gerichte advertenties mogelijk. Er zijn cookies die bedoeld zijn om de website zelf beter te laten werken, de zogenaamde functionele en analytische cookies.

De cookiebepaling houdt, behoudens de in de wet opgenomen uitzonderingen, een informatieplicht en een toestemmingsvereiste in. Partijen die cookies plaatsen en/of uitlezen moeten aan de gebruiker vooraf duidelijke en specifieke *informatie* geven over het feit dat zij cookies gebruiken en met welk doel. Daarnaast mogen de cookies alleen geplaatst en/of uitgelezen worden indien daarvoor vooraf rechtsgeldige *toestemming* van de gebruiker is verkregen. De cookiebepaling vereist bovendien dat er sprake moet zijn van het geven van toestemming voor het plaatsen van cookies op de computer of bijvoorbeeld de mobiele telefoon. Overheidswebsites mogen geen 'cookiemuur' gebruiken, waarmee ze bezoekers die geen cookies accepteren de toegang weigeren

Hoe is de cookiebepaling tot stand gekomen?

De cookiebepaling was eerst geregeld in artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen (hierna: BUDE). Op 5 juni 2012 is dit opgenomen in artikel 11.7a Tw. De norm werd vanaf dat moment zwaarder als gevolg van de Europese e-privacy richtlijn 2009/136/EC, die in heel Europa is ingevoerd. Het is vanaf dat moment niet langer voldoende om te *informer* en een weigeringsmogelijkheid te bieden, zoals in artikel 4.1 BUDE was opgenomen. Voortaan diende een gebruiker voor het plaatsen en/of uitlezen van gegevens *toestemming* te hebben gegeven. Toestemming moet worden verkregen via een vrije, specifieke en op informatie berustende wilsuiting.

De cookiebepaling zorgde echter voor veel irritaties bij gebruikers en website eigenaren. Daarom is er per 11 maart 2015 een nieuwe uitzondering op de informatieplicht en het toestemmingsvereiste in artikel 11.7a Tw geïntroduceerd. Deze verruimde uitzondering betreft cookies die informatie geven over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij en die geen of slechts een geringe inbreuk maken op de persoonlijke levenssfeer van de gebruiker. Voor het plaatsen van deze analytische cookies hoeft de eigenaar van de website met de inwerkingtreding van de nieuwe regels de gebruiker niet te informeren en geen toestemming meer te vragen. Voor het plaatsen van cookies die niet onder een uitzondering vallen, moet de website-eigenaar bezoekers vooraf informeren en om toestemming vragen. Zonder te informeren en het verkrijgen van de vereiste toestemming



mogen deze cookies niet worden geplaatst. Daarnaast is een nieuw vijfde lid toegevoegd aan de bepaling die het overheidswebsites verbiedt om een cookiemuur te gebruiken.



2 Vragen over het toepassingsbereik

Zijn de regels alleen van toepassing op computers?

Nee, de regels zijn van toepassing op alle randapparatuur. Hieronder vallen niet alleen computers, maar ook bijvoorbeeld smartphones, spelcomputers en tablets.

Zijn de regels ook van toepassing op met cookies vergelijkbare technieken?

Ja, het toepassingsbereik van de wetsbepaling gaat veel verder dan alleen het plaatsen van cookies. Niet alleen cookies vallen onder deze beschrijving, maar ook Javascripts, Flash cookies, HTML5-local storage, web beacons en alle andere technieken waarbij gegevens worden geplaatst en/of uitgelezen. Slechts indien er in het geheel geen sprake is van het opslaan van gegevens dan wel het uitlezen van gegevens op de randapparatuur van de gebruiker is artikel 11.7a Tw niet van toepassing. De informatie in dit document over cookies heeft daarom ook betrekking op vergelijkbare technieken.

Zijn de regels van toepassing op alle cookies?

Nee, er zijn *uitzonderingen* in de wet opgenomen waarbij de informatieplicht en het toestemmingsvereiste niet van toepassing zijn. De gebruiker hoeft dan niet geïnformeerd te worden en ook geen toestemming te geven. De uitzonderingen betreffen het plaatsen en/of lezen van gegevens (op de randapparatuur van gebruikers) die:

- nodig zijn om de communicatie uit te voeren. Hierbij kan gedacht worden aan loadbalancing cookies. Deze cookies zorgen ervoor dat het dataverkeer verdeeld wordt over meerdere servers;
- strikt noodzakelijk zijn voor een door de gebruiker gevraagde dienst. Daarbij valt te denken aan een cookie die nodig is om af te rekenen bij een webshop of ten behoeve van het inloggen bij internetbankieren.
- tot doel hebben om informatie te verkrijgen over de kwaliteit en/of effectiviteit van een geleverde dienst (bijvoorbeeld een website). Bijkomende voorwaarde voor het plaatsen van deze cookies is wel dat er geen of slechts een geringe inbreuk wordt gemaakt op de privacy van de gebruiker. Hierbij kan gedacht worden aan analytische cookies. Deze uitzondering geldt met ingang van 11 maart 2015.

NB. Deze regels gelden zowel voor first- als voor third party-cookies.

Zijn de regels ook van toepassing op een intranet?

Nee, de regels gelden niet bij intranet. Zij zien op het plaatsen en uitlezen van gegevens op de randapparatuur van *gebruikers*. Gebruikers zijn volgens artikel 1.1, sub n, Tw natuurlijke personen of rechtspersonen die gebruik maken van een openbare elektronische



communicatiedienst. Gezien de beslotenheid van een intranet valt deze niet onder het begrip openbare elektronische communicatiedienst.

Zijn de regels ook van toepassing op serverloganalyse?

Nee, de regels gelden niet voor serverloganalyse. Zij zien op het plaatsen en uitlezen van gegevens op de randapparatuur van *gebruikers*. Bij serverloganalyse is er geen sprake van het actief plaatsen of uitlezen van gegevens, maar van het analyseren van de gegevens die door de gebruiker zelf naar de server worden gestuurd. Het gaat hier om analyse van de door de gebruiker bij een initieel *get/http*-request gestuurde informatie. Dit initiële request bevat gegevens over het opgevraagde adres, het opvragende IP-adres, user agents en soortgelijke beperkte gegevens. Alle gegevens die *na* het initiële request worden geplaatst of uitgelezen vallen *wel* onder het bereik van artikel 11.7a Tw. De met de browser meegestuurde gegevens kunnen persoonsgegevens bevatten, waarop de Wet bescherming persoonsgegevens (hierna: Wbp) van toepassing is.

Gelden de regels alleen voor Nederlandse websites?

Nee, de regels gelden niet alleen voor Nederlandse websites. Uit de bepaling volgt dat de norm geldt voor 'een ieder'. Dit betekent dat een ieder die gegevens plaatst op of uitleest die zijn opgeslagen in de randapparatuur van een gebruiker dient te voldoen aan de regelgeving, ongeacht waar deze partij gevestigd is. Bepalend is dat deze norm tot doel heeft gebruikers in Nederland te beschermen. De informatieplicht en het toestemmingsvereiste gelden derhalve voor zowel Nederlandse websites als voor buitenlandse websites die zich (mede) op Nederlandse gebruikers richten. Dat kan bijvoorbeeld worden afgeleid uit de aard van de aangeboden informatie, de mogelijkheid om producten in Nederland te laten bezorgen of uit de omstandigheid dat een website in de Nederlandse taal wordt aangeboden. Hierbij is het domein van de website (.nl/.eu/.com/.net/etc.) niet doorslaggevend.



3 Vragen over de uitzonderingen

Valt de no-follow cookie onder de uitzondering van artikel 11.7a, derde lid, Tw?

De zogenaamde “no-follow cookie” die gebruikt wordt om te registreren dat iemand geen cookies wil, kan gezien worden als een door een gebruiker gevraagde dienst waarbij het plaatsen van gegevens strikt noodzakelijk is. Dit lijkt tegenstrijdig nu de gebruiker immers kenbaar heeft gemaakt *geen* gegevens te willen laten plaatsen. ACM oordeelt dat in dit specifieke geval een no-follow cookie als strikt noodzakelijk gezien mag worden. ACM verlangt hierbij wel de volgende waarborgen:

- de gebruiker moet een keuze gehad hebben tussen het toestaan en weigeren van cookies én gekozen hebben om cookies te weigeren. Indien de gebruiker geen handeling heeft verricht zal de website logischerwijs moeten blijven informeren dat de website voornemens is cookies te plaatsen;
- de website dient de gebruiker te informeren dat een no-follow cookie geplaatst zal worden met als enig doel de registratie van de keuze;
- de website mag een no-follow cookie slechts plaatsen met dat specifieke doel. De no-follow cookie mag slechts een daarvoor strikt noodzakelijke inhoud (bijvoorbeeld no follow=1) kennen en geen unieke identifier(s) bevatten. Het is logischerwijs niet toegestaan om de gebruiker met een no-follow cookie door middel van die cookie (al dan niet in combinatie met andere technieken) alsnog op enige andere wijze (tijdelijk) te volgen en/of dit op enig moment te koppelen aan andere over deze gebruiker beschikbare gegevens.

Vallen cookies voor load-balancing onder de uitzondering van artikel 11.7a, derde lid, Tw?

Load balancing is een techniek bij computernetwerken die het mogelijk maakt om het werk te verdelen over meerdere computers. Load balancing kan onder meer worden bereikt door gebruik te maken van een ‘load balancer’. Hierbij wordt een verzoek van een gebruiker om een webpagina te bekijken gestuurd naar een load balancing gateway die het verzoek doorstuurt naar een van de beschikbare servers. In sommige gevallen is het nodig dat opeenvolgende verzoeken van een gebruiker naar dezelfde server worden gestuurd. In dit geval kan een cookie worden gebruikt om te onthouden van welke server er gebruik is gemaakt opdat een volgend verzoek daar ook naartoe kan worden gestuurd. De informatie in deze cookie heeft enkel het doel om de gebruikte server te identificeren en de cookie wordt niet langer opgeslagen dan gedurende de internetssessie. *In dit geval* heeft de load balancing cookie het uitsluitende doel om de communicatie over een elektronisch communicatienetwerk uit te voeren en valt het dus onder de uitzondering van artikel 11.7a, derde lid, sub a, Tw. Voor dergelijke cookies hoeft dus niet geïnformeerd te worden en geen toestemming gevraagd te worden.



Vallen social media plug-in cookies onder de uitzondering van artikel 11.7a, derde lid, Tw?

Social media plug-in cookies zijn cookies die het mogelijk maken dat een gebruiker van social media (gedeeltes van) webpagina's kan delen met dat social media-netwerk. Plug-ins op de website van bijvoorbeeld een webwinkel kunnen door middel van het plaatsen en uitlezen van cookies op de randapparatuur van een gebruiker het delen van pagina's via een social media-netwerk mogelijk maken. Deze cookies vallen in beginsel *niet* onder de uitzonderingen van artikel 11.7a, derde lid, Tw. Een gebruiker die geen lid is van een social media-netwerk of een gebruiker die niet is ingelogd op dat social media-netwerk, gaat er namelijk niet vanuit dat hij door middel van cookies verbonden is met een social media-netwerk. Het plaatsen van de cookies is bij die gebruikers niet nodig voor het leveren van een gevraagde dienst. In dat geval moeten gebruikers logischerwijs geïnformeerd worden en moet er toestemming worden verkregen alvorens social media plug-in cookies mogen worden geplaatst.

Wanneer echter een gebruiker is ingelogd op een social media-netwerk, gaat ACM er vanuit dat deze gebruiker wel gebruik wenst te maken van de functionaliteiten van social media plug-in cookies. In dat geval vallen deze cookies onder de uitzondering van artikel 11.7a, derde lid, Tw. Voor een website-eigenaar is het lastig op voorhand te beoordelen of zijn gebruikers wel of niet zijn ingelogd op een social media-netwerk. Hiervoor is een veelgebruikte publieks- en privacyvriendelijke oplossing beschikbaar. Website-eigenaren kunnen werken met niet-actieve, "grijze" social media buttons. Pas nadat een bezoeker bewust op een dergelijke button heeft geklikt zal deze functionaliteit van de website worden geladen en kan het social media-netwerk een cookie plaatsen.

Welke cookies vallen onder de nieuwe uitzondering die per 11 maart 2015 is ingevoerd?

De nieuwe uitzondering per 11 maart 2015 is neergelegd in sub b, tweede volzin van artikel 11.7a, derde lid, Tw. De cookies die hier onder vallen geven informatie over de kwaliteit en/of effectiviteit van een geleverde dienst. In de Memorie van Toelichting geeft de minister hier enkele voorbeelden van:

- Analytische cookies: deze cookies dienen ertoe het gebruik van een bepaalde website te analyseren en in kaart te brengen, zodat de kwaliteit en/of de effectiviteit van de website kan worden verbeterd.
- Affiliate cookies: deze cookies worden gebruikt om bij te houden welke advertentie leidt tot aankoop van een bepaald product, zodat degene die deze advertentie heeft getoond (de affiliate) daarvoor een beloning kan ontvangen van de adverteerder.

Let op: deze cookies zijn alleen uitgezonderd van de informatie- en toestemmingsverplichting wanneer zij geen of slechts geringe gevolgen voor de persoonlijke levenssfeer van de gebruiker hebben. Dit betekent dat de met deze cookies verzamelde gegevens slechts voor bovenstaande doelen gebruikt mag worden en op zodanige wijze dat er geen of slechts geringe gevolgen zijn voor de privacy van de gebruiker. Indien de data door een derde partij



geanalyseerd wordt dan dient met deze derde afgesproken te worden dat deze derde de data alleen ten behoeve van de betreffende website zal gebruiken. Dit kan door het afsluiten van een bewerkersovereenkomst met de derde partij.



4 Vragen van gebruikers

Wat merkt de gebruiker van de cookiebepaling?

De gebruiker merkt van de cookiebepaling dat hij geïnformeerd wordt en toestemming moet geven alvorens een website cookies mag plaatsen op zijn randapparatuur. De gebruiker wordt hiermee in staat gesteld te beslissen of een website gegevens mag opslaan op of toegang mag krijgen tot zijn randapparatuur. Zo kan de gebruiker beter zijn privacy op het internet controleren. Gebruikers kunnen meer informatie krijgen via www.consuwijzer.nl en daar ook melden als de cookiebepaling wordt overtreden.

Recent is de wet gewijzigd, wat betekenen die wijzigingen voor mij als gebruiker?

Artikel 11.7a Tw is op 11 maart 2015 gewijzigd. De wijziging gaat onder meer over cookies die tot doel hebben de kwaliteit en/of effectiviteit van een geleverde dienst van de informatiemaatschappij (zoals een website) te meten en daarbij geen of slechts geringe gevolgen voor de gebruiker opleveren. Voor de gebruiker betekent dit dat voor het plaatsen van deze analytische cookies op de randapparatuur de eigenaar van de website hem niet langer hoeft te informeren en geen toestemming meer hoeft te vragen. Voor een gebruiker betekenen de wijzigingen ook dat hij naar verwachting minder vaak toestemming zal hoeven te geven.

Tijdens de parlementaire behandeling van de wijziging is ook gesproken over het toestemmingsvereiste. Toestemming van de gebruiker kan ook worden afgeleid uit een handeling, te weten de zogenaamde impliciete toestemming. Hiervan is bijvoorbeeld sprake wanneer de internetgebruiker doorsurft op de website, *nadat* hij duidelijk en volledig is geïnformeerd over welke cookies er op de website gebruikt worden en dat hij bij doorsurfen toestemming voor het plaatsen en/of lezen daarvan geeft.

Daarnaast is het (semi-)overheidswebsites verboden om een cookiemuur te gebruiken. Dit houdt in dat de toegang van dergelijke websites niet langer volledig afhankelijk mag zijn van toestemming van de gebruiker voor het gebruik van alle cookies.

Help, ik heb geen toestemming gegeven tot het plaatsen van cookies maar zie nog steeds advertenties!

De wet is er niet om het tonen van advertenties te verbieden, maar om de privacy van de gebruiker te beschermen. Ook zonder toestemming tot het plaatsen van cookies mag een website de gebruiker te allen tijde advertenties tonen, mits bij deze advertenties geen toegang wordt verkregen tot dan wel gegevens worden opgeslagen op de randapparatuur van de gebruiker.



Waarom zie ik op het internet zoveel informatiebalkjes over cookies?

De gebruiker ziet op het internet zoveel informatiebalkjes over cookies omdat de wet een ieder die gegevens op de randapparatuur van de gebruiker wil opslaan of uitlezen verplicht de gebruiker hierover te informeren en daarvoor toestemming te verkrijgen. De wetgever heeft de wijze waarop dat wordt gedaan vrijgelaten. Het staat de website-eigenaar dus vrij om zelf te bepalen welke oplossing het beste bij zijn website past, zolang er voldoende informatie wordt verschaft en er via een vrije, specifieke en op informatie berustende wilsuiving toestemming wordt verkregen. De website slaat uw keuze meestal op in een cookie, zodat u als gebruiker in beginsel slechts één keer uw toestemming hoeft te geven. Dit betekent wel dat wanneer alle cookies worden verwijderd, de website niet meer weet welke keuze er is gemaakt. De gebruiker zal dan op een later moment opnieuw geïnformeerd worden en toestemming moeten geven voor het gebruik van cookies.



5 Vragen over de implementatie door marktpartijen

Hoe zit het met het informeren en toestemming verkrijgen?

De informatieplicht en het toestemmingvereiste vormen de kern van artikel 11.7a Tw. Deze onderwerpen zijn onlosmakelijk verbonden met elkaar; zonder goede informatie is het niet mogelijk een rechtsgeldige toestemming te verkrijgen. Net zoals bij de regels omtrent het spamverbod uit artikel 11.7 Tw dient er bij artikel 11.7a Tw sprake te zijn van een toestemming die op grond van de Wbp “vrij, specifiek en op informatie berustend” is. Partijen mogen zelf bepalen op welke wijze informatie wordt verstrekt en toestemming wordt verkregen. Het verkrijgen van toestemming zal echter (net zoals in artikel 11.7 Tw) niet kunnen gebeuren door middel van een (vage) verwijzing naar bijvoorbeeld algemene voorwaarden, privacy en/of permission statements. Voor een gebruiker moet de informatie volstrekt helder zijn. Hij moet weten waarom en waarvoor hij toestemming geeft en tot hoever de door hem gegeven toestemming strekt. Voor het verkrijgen van een adequate toestemming is vereist dat de benodigde informatie gemakkelijk vindbaar is en tevens gemakkelijk te begrijpen moet zijn. Dit kan afhankelijk zijn van de doelgroep die de website tracht te bereiken.

Hoe voldoe ik aan de informatieplicht?

Om te voldoen aan de informatieplicht van artikel 11.7a, eerste lid, onder a, Tw dient de gebruiker geïnformeerd te worden omtrent de doeleinden waarvoor de plaatser gegevens wenst op te slaan en/of toegang tot gegevens wil. Het is belangrijk dat de gebruiker geïnformeerd wordt waarom de website een cookie plaatst en met welk doel dit gebeurt, zodat de gebruiker weet waarvoor hij toestemming geeft. Deze informatie moet altijd op een direct zichtbare plek op de website getoond worden en geschreven zijn in een bij de doelgroep van de website aansluitend taalgebruik. De taalkeuze van de uitleg over cookies kan dus afhankelijk zijn van de doelgroep van de website. Informeren door middel van een globale verwijzing naar algemene voorwaarden, privacy en/of permission statements is onvoldoende. ACM beveelt aan om in de informatie alle cookies en/of andere technieken te benoemen en toe te lichten. Daarbij kunnen zowel de cookies waarvoor toestemming verkregen dient te worden als de cookies die vallen onder de uitzondering van artikel 11.7a, derde lid, Tw benoemd worden. De gebruiker wordt zo optimaal geïnformeerd en zal sneller kunnen beslissen over het geven van toestemming. Binnen de industrie zijn door diverse brancheorganisaties industriebrede oplossingen opgesteld die gebruikt kunnen worden om te informeren over cookies. Let op: u mag dus na het enkel informeren nog geen cookie plaatsen. Daarvoor is ook toestemming van de gebruiker nodig.

Moet ik als website eigenaar ook informeren en toestemming vragen voor het gebruik van cookies door derden op mijn website?

De website-eigenaar is het eerste aanspreekpunt van ACM. Meestal vraagt de website-eigenaar namelijk ook toestemming namens de derde partijen. Wanneer iedere derde partij zelf om toestemming zou moeten vragen binnen de beperkte, door de website-eigenaar



aangeboden ruimte, zal de informatie onoverzichtelijk worden en vaak erg lang. Ook kan het dan voorkomen dat iedere advertentie van een derde partij een afzonderlijke toestemmingspop-up zou moeten bevatten voordat de advertentie getoond kan worden. In de praktijk is het dus de website-aanbieder die aan ACM kan aantonen dat ook de cookies van derden volgens de regels van artikel 11.7a Tw worden geplaatst. De website-eigenaar heeft namelijk een zekere verantwoordelijkheid over cookies die via zijn website worden geplaatst.

Kan ik ten aanzien van de informatieplicht over het cookiegebruik in het geval van cookies van derden volstaan met een verwijzing naar de informatie van deze derden?

Het kan zijn dat (met toestemming) via uw website gegevens van derden worden geplaatst op randapparatuur van gebruikers en/of deze gegevens worden uitgelezen. Ook ten aanzien van deze derden dient u te voldoen aan de informatieplicht zoals deze volgt uit artikel 11.7a, eerste lid, onder a, Tw. Om te voorkomen dat u integraal alle informatie van deze derden dient op te nemen in uw eigen informatie kunt u daarbij verwijzen naar de eigen informatie van deze derden. Uiteraard moet ook die informatie van derden voldoen aan de wettelijke eisen.

Wat zijn de wettelijke vereisten voor toestemming?

Om te voldoen aan het vereiste van de toestemming, dient er bij artikel 11.7a Tw sprake te zijn van een toestemming die op grond van de Wbp bestaat uit een “vrije, specifieke en op informatie berustende wilsuiting”. De wilsuiting vereist dat de gebruiker een handeling verricht tot het geven van toestemming. Uit de Memorie van Toelichting bij de wetswijziging van 11 maart 2015 blijkt dat er ook sprake is van een rechtsgeldige toestemming als de internetgebruiker doorsurft op de website, nadat hij duidelijk en volledig is geïnformeerd over de cookies die worden geplaatst. Bovendien moet het voor de gebruiker duidelijk zijn dat zijn toestemming voor het plaatsen van cookies wordt afgeleid uit het feit dat hij gebruik blijft maken van de website. Hierover moet de gebruiker op een direct zichtbare plaats worden geïnformeerd.

Let op: wanneer de gebruiker drukt op een “meer informatie”-knop, of een soortgelijke knop, dan kan hieruit niet worden afgeleid dat hij akkoord gaat met het plaatsen van cookies. Ook kan er geen toestemming worden afgeleid uit het verlaten en opnieuw bezoeken van een website of het vernieuwen van de pagina. Uit een niet-handelen na het intypen van de URL, of het enkele invoeren van de URL, kan ook geen toestemming voor het gebruik van cookies worden afgeleid.

Wie moet de toestemming verkrijgen?

Een ieder die gegevens op de randapparatuur van een gebruiker plaatst of uitleest zal daarvoor toestemming moeten hebben verkregen. Dat kunnen bij een bezoek aan één website verschillende partijen zijn. Deze plaatser kan de website-eigenaar zijn, maar het kan ook een derde zijn die met de website-eigenaar is overeengekomen dat hij via de website cookies mag



plaatsen of uitlezen. Het is aan deze partijen om te bepalen of er meerdere malen toestemming wordt verkregen of dat de website ervoor kiest om namens alle partijen de toestemming te verkrijgen. De eigenaren van de websites zijn het aanspreekpunt voor de informatie die hun website biedt over cookies en de gegevens die er bij een bezoek aan de website worden geplaatst en uitgelezen. De gebruiker bezoekt immers de website van de website-eigenaar en niet de website(s) van de adverteerder(s). De website-eigenaar kan zich daarom niet onttrekken aan zijn verantwoordelijkheid om te voorkomen dat derde partijen via zijn website zonder toestemming gegevens plaatsen en/of uitlezen.

Mag ik als private partij de toegang tot mijn website ontzeggen aan mensen die geen toestemming geven?

Het is voor een website niet verplicht een gebruiker toegang te geven en die toegang kan in beginsel afhankelijk worden gemaakt van het accepteren van een cookie. Als een gebruiker geen toestemming geeft voor het plaatsen van een cookie is het mogelijk dat een website niet goed werkt. Ook andere belangen van de websitehouder kunnen ertoe leiden dat de websitehouder ervoor kiest om de toegang tot de website afhankelijk te maken van het geven van toestemming. Zo kan het voorkomen dat er alleen toegang tot de website wordt verleend indien de gebruiker toestemming geeft voor het plaatsen van tracking-cookies die de voorkeuren van de gebruiker opslaan zodat gerichte advertenties kunnen worden getoond. Op die manier betaalt de gebruiker voor het bezoeken van de website.

Ondanks het feit dat dit niet erg gebruiksvriendelijk is om toestemming af te dwingen, staat het de websitehouder in beginsel vrij om zijn website op deze manier in te richten. ACM wil benadrukken dat – hoewel het gebruik van een cookiemuur in de meeste gevallen is toegestaan - het gebruik van een cookiemuur wel tegen de geest van de wet in gaat. De cookiebepaling beoogt namelijk de gebruiker een keuze te geven ten aanzien van zijn privacy en het gebruik van zijn persoonsgegevens op het internet. Als websites gebruikers alleen toegang geven indien alle cookies worden geaccepteerd, wordt de gebruiker juist beperkt in zijn keuze.

In welke gevallen is het voor private partijen niet toegestaan om de toegang tot de website te ontzeggen aan mensen die geen toestemming geven?

Er zijn gevallen waarin het gebruik van een cookiemuur door een private website-eigenaar niet is toegestaan. Dit is het geval wanneer de toestemming van de gebruiker niet meer “vrij” zou zijn omdat de gebruiker zo een groot belang heeft bij het bezoeken van de website, waardoor het niet bezoeken van de website significant negatieve gevolgen met zich mee kan brengen. De wetgever benoemt drie situaties waarin er in ieder geval sprake is van significant negatieve gevolgen en er dus geen sprake is van vrije toestemming in het geval van het gebruik van een cookiemuur:

1. De gebruiker kan hierdoor een wettelijke plicht niet goed uitvoeren;
2. De gebruiker kan hierdoor geen gebruik maken van een wettelijk recht; of
3. het tot gevolg heeft dat de gebruiker minder goede gezondheidszorg kan genieten.



Mag ik als overheidswebsite de toegang tot mijn website ontzeggen aan mensen die geen toestemming geven?

Het is voor (semi-)overheidswebsites niet toegestaan om gebruik te maken van een zogenaamde cookiemuur. Op grond van artikel 11.7a, vijfde lid, Tw mogen rechtspersonen die bij of krachtens het publiekrecht zijn ingesteld de toegang tot de website niet ontzeggen aan gebruikers die geen toestemming geven voor het plaatsen of uitlezen van gegevens. Hieronder vallen openbare lichamen en bijzondere rechtspersonen die bij of krachtens de wet zijn ingesteld en die geen rechtspersonen zijn als genoemd in de artikelen 2:2 en 2:3 Burgerlijk Wetboek (BW). Ook rechtspersonen die een dienst verlenen namens een krachtens publiekrecht ingestelde rechtspersoon mogen geen cookiemuur voeren. Beslissend hierbij is de mate waarin er namens een krachtens publiekrecht ingestelde rechtspersoon wordt gehandeld. Er zal sprake moeten zijn van een rechtspersoon die is ingesteld met het doel om uitvoering te geven aan een wettelijke taak. Hieronder vallen geen rechtspersonen die slechts voor een klein deel uitvoering geven aan een publieke taak of rechtspersonen die subsidie krijgen van de overheid maar verder geen publieke taak uitvoeren.

Hoe kan ik het beste toestemming verkrijgen van de gebruikers op mijn website?

De wetgever heeft bewust ruimte gelaten aan de markt om in te vullen op welke wijze een website toestemming kan verkrijgen van haar gebruikers. In de praktijk kiezen veel websites ervoor om hun gebruikers te informeren en toestemming te verkrijgen middels bijvoorbeeld een pop-up, een floating box, een info balk of een overlay. Het staat de eigenaar van een website daarmee vrij om te kiezen voor een methode die aansluit bij het concept van de website en de gebruikers daarvan. Belangrijk is dat er bij de gebruiker die toestemming geeft sprake is van een vrije, specifieke en op informatie berustende wilsuiting, zoals bedoeld in artikel 1, onder i, Wbp. De wilsuiting vereist dat de gebruiker een handeling verricht tot het geven van toestemming. Indien een gebruiker de keuze heeft tot het geven van toestemming, maar geen keuze heeft gemaakt, kan daaruit niet zonder meer worden afgeleid dat de gebruiker toestemming heeft gegeven. Inmiddels zijn er verschillende plugins voor websites beschikbaar die gebruikers attenderen op de regelgeving. Tevens zijn er verschillende plugins beschikbaar waarmee op een correcte wijze toestemming verkregen kan worden van gebruikers. Als eenmaal de toestemming van de gebruiker is verkregen, kan deze toestemming worden opgeslagen in een cookie, zodat het niet nodig is om bij elk bezoek opnieuw toestemming te verkrijgen.

Kan ik toestemming verkrijgen voor meerdere domeinen?

Indien de gebruiker wordt geïnformeerd over de te gebruiken cookies en de verschillende domeinen, kan de toestemming gelden voor meerdere domeinen. Het moet voor de gebruiker volstrekt helder zijn dat er voor meerdere domeinen toestemming wordt verkregen. Tevens moet de gebruiker de mogelijkheid hebben om een complete lijst met de domeinen in te zien zodat er gesproken kan worden van een toestemming die specifiek en op informatie berustend



is.

Bij het verkrijgen van een gebundelde toestemming voor meerdere domeinen moet in ieder geval op gelet worden dat de toestemming specifiek genoeg blijft:

1. De gebruiker moet redelijkerwijs kunnen verwachten dat er voor die domeinen gebundelde toestemming wordt gegeven. Om te kunnen spreken van een toestemming die specifiek is, is vooral relevant dat het moet gaan om websites die dezelfde *soort dienst* aanbieden.
2. De websites moeten daarnaast dezelfde techniek(en) gebruiken. Er kan niet voor een lijst met verschillende technieken die eventueel op de verschillende domeinen gebruikt zouden kunnen worden in één keer toestemming worden verkregen. De informatie die wordt aangeboden zal dan namelijk onvoldoende specifiek zijn.

Let op: de toestemming geldt alleen voor de domeinen en cookies waarover de gebruiker is geïnformeerd. Indien u later een domein of cookie aan de lijst toevoegt zult u daarvoor (opnieuw) toestemming moeten verkrijgen.

Moet een gebruiker bij ieder bezoek toestemming geven?

Nee. Een gebruiker hoeft niet bij elk herhaald bezoek aan een website opnieuw toestemming te geven als hij al een keer toestemming heeft gegeven. De toestemming blijft geldig gedurende de levensduur van de cookie tenzij een gebruiker zijn toestemming intrekt, bijvoorbeeld door het verwijderen van de cookie. Ook zal de toestemming niet meer geldig zijn indien de website-eigenaar de aard van de gegeven toestemming heeft veranderd, bijvoorbeeld door een aanpassing in zijn privacy- en/of cookiebeleid.

Hoe weet ik of een toestemming door een gebruiker is ingetrokken?

Als een gebruiker een cookie verwijdert of heeft laten verwijderen door bijvoorbeeld de browser of een virusscanner, dient de website die de betreffende cookie geplaatst heeft ervan uit te gaan dat de gebruiker zijn toestemming heeft ingetrokken. Bij een herhaald bezoek van dezelfde gebruiker dient deze vervolgens weer, net zoals iedere nieuwe gebruiker, geïnformeerd te worden en zijn of haar toestemming te worden verkregen. Indien technisch mogelijk kan de website-eigenaar de gebruiker erop wijzen dat deze al eerder toestemming heeft gegeven en vragen of de gebruiker deze eerder gegeven toestemming wil verlengen. Een herhaald bezoek kan logischerwijs ook door dezelfde gebruiker plaatsvinden door middel van een bezoek met een ander apparaat. Tevens kan in het geval van meerdere gebruikers op een apparaat sprake zijn van een herhaald bezoek. In alle gevallen dient de plaatser ervan uit te gaan dat als er geen cookies (meer) op het apparaat staan er geen toestemming door een gebruiker is gegeven.



Geldt de toestemming voor alle gebruikers van het apparaat?

De toestemming geldt voor de gebruiker die deze toestemming heeft gegeven. In het geval meerdere gebruikers gebruik maken van hetzelfde apparaat ligt het aan het gebruik van dit apparaat. Als de website-eigenaar een eerder geplaatste cookie kan uitlezen, kan deze ervan uitgaan dat daarvoor toestemming is gegeven. Het is immers goed mogelijk dat verschillende gebruikers gebruik maken van hetzelfde profiel en/of browser waarvoor deze toestemming is gegeven. Indien de website-eigenaar in zijn registratie ziet dat er toestemming is gegeven, maar geen cookie meer zichtbaar is, dient de website-eigenaar ervan uit te gaan dat er geen sprake is van toestemming en moet deze (opnieuw) de toestemming verkrijgen. Dit kan het geval zijn als op één apparaat gebruik wordt gemaakt van verschillende gescheiden profielen en/of van verschillende browsers, waardoor cookies op verschillende plekken staan opgeslagen.

Hoe zit het met de browserinstellingen? Kan een gebruiker door middel van een instelling in zijn browser tonen waarvoor hij wel of geen toestemming geeft?

ACM juicht een gebruiksvriendelijke oplossing toe waarbij het geven van toestemming via de browserinstellingen kan worden geregeld. Hierover wordt op Europees niveau gesproken. Momenteel kunt u als plaatser/uitlezer van cookies er nog niet van uitgaan dat als de browser cookies accepteert de gebruiker daar dan ook toestemming voor zal hebben gegeven. Veel browsers staan ingesteld op het accepteren van alle cookies. Uit het feit dat de gebruiker dit niet heeft aangepast kunt u geen toestemming voor het gebruik van cookies afleiden. De Do Not Track systemen van de huidige browsers zijn op dit moment nog onvoldoende. Het is niet toegestaan te wachten met de implementatie van de cookiebepaling in afwachting van de ontwikkelingen op dit vlak. ACM houdt de mogelijke ontwikkelingen op dit terrein in de gaten.

Ik lees veel over een ‘omgekeerde bewijslast’ bij tracking cookies, hoe zit dat?

Bij zogenaamde “*tracking cookies*” kan sprake zijn van verwerking van persoonsgegevens. In dat geval moet de plaatser en/of uitlezer van tracking cookies zich houden aan de Wbp. Het College bescherming persoonsgegevens (hierna: CBP) houdt toezicht op dit deel van de bepaling. Het *rechtsvermoeden ten aanzien van tracking cookies*, dat geplaatst is na artikel 11.7a, eerste lid, onder b, Tw maakt ook onderdeel uit van de cookiebepaling. Door dit rechtsvermoeden mag het CBP er van uitgaan dat bij het gebruik van tracking cookies persoonsgegevens worden verwerkt en partijen zich dus moeten houden aan de Wbp, tenzij degene die tracking cookies plaatst en/of leest kan aantonen dat hij géén persoonsgegevens verwerkt.

Hoe kan ik bewijzen dat er toestemming is verkregen?

Het is aan u om aan te tonen dat op een juiste wijze toestemming is verkregen van de gebruiker voor het plaatsen van cookies. De wet schrijft niet voor op welke wijze dit aangetoond dient te worden. Een mogelijke wijze om aan te tonen dat van de gebruiker toestemming is verkregen,



is door het registreren van de wijze waarop de toestemming is verkregen, hoe de gebruiker daarbij geïnformeerd werd én het tijdstip waarop de toestemming is verkregen. Het bewijs van toestemming alleen is niet voldoende. Er moet ook aangetoond kunnen worden dat de gebruiker op de juiste wijze is geïnformeerd.

In veel gevallen is het moeilijk om te bewijzen dat een specifieke gebruiker toestemming heeft gegeven voor het plaatsen van een cookie. Het is daarom ook voldoende als de website eigenaar aantoont dat hij een waterdicht proces had waarmee hij de gebruiker correct heeft geïnformeerd en waarmee hij op correcte wijze de toestemming heeft verkregen. Met waterdicht proces wordt bedoeld dat het proces altijd leidt tot een rechtsgeldige toestemming. Hierbij is van belang dat aangetoond kan worden dat het proces op een bepaald moment in het verleden ook op de beschreven manier heeft gewerkt. Dit betekent dat er een soort versiebeheer zal moeten worden toegepast. Op deze manier kan dus ook worden bewezen dat de website eigenaar toestemming heeft verkregen.

Uit de wet volgt dat ACM bevoegd is om een onderzoek te starten en eventueel handhavend op te treden tot maximaal vijf jaar nadat een mogelijke overtreding heeft plaatsgevonden. Gedurende deze periode dient u dan ook te kunnen aantonen dat u op de juiste wijze toestemming heeft verkregen van de gebruiker dan wel om de voornoemde gegevens te bewaren om desgevraagd aan ACM te kunnen verstrekken.



6 Vragen over ACM

Wat is ACM?

Op 1 april 2013 is de Instellingswet Autoriteit Consument en Markt in werking getreden. Vanaf die datum is de Autoriteit Consument en Markt (ACM) de rechtsopvolger van de Consumentenautoriteit, de Nederlandse Mededingingsautoriteit en de Onafhankelijke Post- en Telecommunicatie Autoriteit. Sindsdien oefent ACM de bevoegdheden uit van deze drie rechtsvoorgangers. Op de website www.acm.nl staat informatie over onder meer de organisatie, missie, strategie, marktvisie en speerpunten.

Hoe gaat ACM handhaven?

ACM handhaaft zowel de informatieverplichting als het toestemmingsvereiste van artikel 11.7a Tw. ACM handhaaft op basis van eigen onderzoek en op basis van signalen uit de markt. ACM heeft hiervoor de beschikking over digitale rechercheurs. Gebruikers kunnen tips over mogelijke misstanden rondom de cookiebepaling indienen via ConsuWijzer: www.consuwijzer.nl. Als de overtreder niet in Nederland, maar in een andere Europese lidstaat gevestigd is, kan ACM besluiten een zaak voor te leggen aan de toezichthouder in die lidstaat. Naast ACM is voorts ook het CBP, als toezichthouder op de Wbp, bevoegd tot handhaving van (delen van) artikel 11.7a Tw.

Wat is de maximumboete die ACM op kan leggen?

De Tw geeft ACM de bevoegdheid om bij overtreding van regels boetes tot maximaal € 450.000 op te leggen. Dit maximum geldt ook voor overtreding van de cookiebepaling. De hoogte van de boete die daadwerkelijk wordt opgelegd bij een concrete overtreding hangt echter af van verschillende factoren. De factoren die meespelen bij het bepalen van de hoogte van de boete bij een concrete overtreding zijn vastgelegd in de Beleidsregels van de Minister van Economische Zaken voor het opleggen van bestuurlijke boetes door de ACM. Naast het opleggen van boetes kan ACM ervoor kiezen om andere instrumenten in te zetten, zoals het waarschuwen van een partij of het opleggen van een last onder dwangsom om een overtreder te bewegen zijn overtreding te staken.

Kan ACM kijken naar mijn implementatie van de wet op mijn website en deze goedkeuren?

Nee. ACM geeft geen individuele adviezen ten aanzien van correcte implementatie van artikel 11.7a Tw op uw website. ACM verstrekt wel algemene informatie over de regels aan bedrijven via www.acm.nl/nl/onderwerpen/loket. ACM ververst regelmatig dit document met veelgestelde vragen en antwoorden op haar website.

ACM geeft geen definitief akkoord (een 'groen stempel') voor een door een website-eigenaar gekozen oplossingen. Enerzijds omdat een website vaak dynamisch is en van tijd tot tijd



aangepast wordt waardoor de website mogelijk na de wijziging niet meer voldoet. Anderzijds omdat een groen stempel van ACM andere partijen mogelijk tot “kopieergedrag” aanzet omdat die oplossing immers een groen stempel van ACM heeft verkregen. Dit zou innovatie kunnen tegengaan.

Kunnen consumenten een klacht indienen bij ACM als ze ongevraagd cookies op de computer of alle andere randapparatuur hebben gekregen?

Ja. Consumenten kunnen deze signalen melden bij ConsuWijzer: www.consuwijzer.nl.

Disclaimer

ACM heeft bij het samenstellen en beantwoorden van de bovenstaande vragen over de cookiebepaling de grootst mogelijke zorgvuldigheid in acht genomen. Dit document geeft slechts antwoord op algemene vragen en ziet niet op individuele gevallen. Aan de tekst kunnen geen rechten worden ontleend.

Als u aanvullende vragen heeft, dan kunt u een e-mail sturen naar cookies@acm.nl.



Bijlage 1: wettekst van artikel 11.7a Tw

Artikel 11.7a Telecommunicatiewet

“1. Onverminderd de Wet bescherming persoonsgegevens 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 Wet bescherming persoonsgegevens, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en*
- b. daarvoor toestemming heeft verleend.*

2. De in het eerste lid, onder a en b, genoemde vereisten zijn ook van toepassing in het geval op een andere wijze dan door middel van een elektronisch communicatienetwerk wordt bewerkstelligd dat via een elektronisch communicatienetwerk informatie wordt opgeslagen of toegang wordt verleend tot op het randapparaat opgeslagen informatie.

3. Het bepaalde in het eerste lid is niet van toepassing indien het de opslag of toegang betreft:

- a. met als uitsluitend doel de communicatie over een elektronisch communicatienetwerk uit te voeren,*
- b. die strikt noodzakelijk is om de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren of – mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker – om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij.*

4. Een handeling als bedoeld in het eerste lid, die tot doel heeft gegevens over het gebruik van verschillende diensten van de informatiemaatschappij door de gebruiker of de abonnee te verzamelen, combineren of analyseren zodat de betrokken gebruiker of abonnee anders behandeld kan worden, wordt vermoed een verwerking van persoonsgegevens te zijn, als bedoeld in artikel 1, onderdeel b, van de Wet bescherming persoonsgegevens.

5. 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 als bedoeld in het eerste lid.

6. Bij of krachtens algemene maatregel van bestuur kunnen in overeenstemming met Onze Minister van Veiligheid en Justitie nadere regels worden gegeven met betrekking tot de in het eerste lid, onder a en b, genoemde vereisten en de in het derde lid genoemde uitzonderingen. Het College bescherming persoonsgegevens wordt om advies gevraagd over een ontwerp van bedoelde algemene maatregel van bestuur.”