GROEP GEGEVENSBESCHERMING ARTIKEL 29

00879/12/NL
WP 194

Advies 04/2012 over ontheffing van de toestemmingsverplichting voor cookies

Goedgekeurd op 7 juni 2012

GROEP GEGEVENSBESCHERMING OVER DE BESCHERMING VAN PARTICULIEREN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS

Ingesteld bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995,

Gezien artikel 29 en artikel 30, lid 1, onder a), en lid 3, van die richtlijn,

Gezien het reglement van orde van de Groep,

HEEFT HET VOLGENDE ADVIES VASTGESTELD:

1 Inleiding

Artikel 5, lid 3, van Richtlijn 2002/58/EG, zoals gewijzigd bij Richtlijn 2009/136/EG, zorgt voor een betere bescherming van de gebruikers van elektronische communicatienetwerken en diensten, door te bepalen dat informatie slechts op de eindapparatuur van een gebruiker (of een abonnee) mag worden opgeslagen of toegang daartoe mag worden verkregen als de gebruiker daartoe toestemming heeft verleend na te zijn voorzien van duidelijke en volledige informatie. Dit vereiste geldt voor alle soorten informatie die op de eindapparatuur van de gebruiker wordt opgeslagen, of waartoe toegang wordt verkregen, maar de aandacht gaat vooral uit naar het gebruik van cookies in de zin van RFC 6265[1]. In dit advies wordt daarom ingegaan op de gevolgen van het herziene artikel 5, lid 3, voor het gebruik van cookies, met dien verstande dat deze term ook soortgelijke technologieën omvat.

Overeenkomstig artikel 5, lid 3, hoeft voor het plaatsen of uitlezen van cookies niet de op informatie berustende toestemming van de gebruiker te worden gevraagd, als die cookies aan een van de volgende criteria voldoen:

Criterium A: het cookie wordt gebruikt *"met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk"*;

Criterium B: het cookie is *"strikt noodzakelijk[…] om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert"*.

De Groep heeft de vereisten met betrekking tot op informatie berustende toestemming in twee adviezen[2] al uitgebreid besproken; in dit document worden de uitzonderingen op het beginsel behandeld in verband met cookies en aanverwante technologieën.

Bij de bespreking worden het recht van de betrokkene om te worden geïnformeerd en het recht dat de betrokkene mogelijk heeft om zich tegen verwerking te verzetten, zoals vastgesteld bij Richtlijn 95/46/EG, buiten beschouwing gelaten, omdat die rechten van toepassing zijn op elke verwerking van persoonsgegevens, ook wanneer er geen cookies worden gebruikt.

---

1 http://tools.ietf.org/html/rfc6265

2 Advies 2/2010 over online reclame op basis van surfgedrag ('behavioural advertising') en advies 16/2011 over de Best Practice Recommendation on Online Behavioural Advertising van EASA/IAB.

2 Analyse

2.1 Criterium A

Het gebruik bij criterium A van de woorden “als uitsluitend doel” geeft een specifieke afbakening aan van het soort verwerking dat met behulp van cookies kan worden verricht en laat weinig ruimte voor interpretatie open. Het is niet voldoende dat het cookie alleen wordt gebruikt als hulpmiddel voor de verzending van een communicatie over een elektronisch communicatienetwerk of om de verzending te bespoedigen of te reguleren. Het criterium wordt alleen vervuld als de communicatie zonder gebruik van het cookie onmogelijk is. Overigens kwam in de oorspronkelijke versie van Richtlijn 2002/58/EG in artikel 5, lid 3 al een ontheffing voor betreffende cookies die worden gebruikt *“met als uitsluitend doel de uitvoering of vergemakkelijking van de verzending van een communicatie over een elektronischecommunicatienetwerk”*. Diezelfde formulering komt ook in de herziene richtlijn voor, maar “*of vergemakkelijking*” is daar geschrapt. Dit kan worden gezien als nog een indicatie dat de Europese wetgever de reikwijdte van de ontheffing die artikel 5, lid 3, biedt als vermeld onder criterium A heeft willen beperken.

Er zijn ten minste drie elementen die kunnen worden aangemerkt als strikt noodzakelijk voor de totstandkoming van communicatie over een netwerk tussen twee partijen:

1) de mogelijkheid om informatie over het netwerk te routeren, en wel door het begin- en eindpunt van de communicatie te identificeren;

2) de mogelijkheid om gegevens in de gewenste volgorde uit te wisselen, namelijk door de datapakketten te nummeren;

3) de mogelijkheid om verzendingsfouten of gegevensverlies te detecteren.

De formulering *“de verzending van een communicatie over een elektronisch communicatienetwerk”* bij criterium A (met name ook het woord “over”) moet worden opgevat als een verwijzing naar elke vorm van gegevensuitwisseling die plaatsvindt met behulp van een elektronisch communicatienetwerk (zoals gedefinieerd in Richtlijn 2002/21/EG), mogelijk met inbegrip van gegevens “op toepassingsniveau” die aan ten minste één van bovengenoemde kenmerken voldoen, zonder dat deze beperkt blijven tot de technische gegevensuitwisselingen die noodzakelijk zijn voor de totstandkoming van het elektronische communicatienetwerk zelf.

Criterium A omvat derhalve cookies die aan ten minste één van de bovengenoemde voor internetcommunicatie gedefinieerde kenmerken voldoen.

2.2 Criterium B

De formulering van criterium B lijkt erop te wijzen dat de Europese wetgever ervoor heeft willen zorgen dat er strenge eisen blijven gelden om voor een ontheffing in aanmerking te komen. Volgens een directe interpretatie van de richtlijn gelden er twee vereisten, wil een cookie aan criterium B voldoen:

1) de dienst van de informatiemaatschappij is door de gebruiker uitdrukkelijk gevraagd: dat wil zeggen, de gebruiker (of abonnee) heeft een positieve actie ondernomen om te verzoeken om een dienst met een duidelijk omlijnd karakter;

2) het cookie is strikt noodzakelijk om de dienst van de informatiemaatschappij mogelijk te maken: dat wil zeggen, als cookies zijn gedeactiveerd, werkt de dienst niet.

In overweging 66 van Richtlijn 2009/136/EG wordt er bovendien op gewezen dat *"[u]itzonderingen op de verplichting om informatie te geven en een recht van weigering aan te bieden moeten worden beperkt tot situaties waarbij de technische opslag of toegang strikt noodzakelijk is voor het wettige doel of om het gebruik mogelijk te maken van een specifieke dienst waarom de abonnee of gebruiker heeft verzocht."* Met andere woorden, er moet een duidelijk verband zijn tussen de strikte noodzakelijkheid van een cookie en de verlening van de dienst van de informatiemaatschappij waarom de gebruiker uitdrukkelijk heeft verzocht, anders geldt de ontheffing niet.

Ook als de richtlijn zo wordt geïnterpreteerd, moet echter nog worden gedefinieerd wat precies wordt verstaan onder *"uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij"*. Een dienst van de informatiemaatschappij kan bestaan uit vele onderdelen, waarvan sommige niet door alle gebruikers worden gebruikt, of slechts voor het gemak worden aangeboden. Een onlinekrant kan bijvoorbeeld voor iedereen gratis toegankelijk zijn, maar voor "ingelogde" gebruikers extra functies bieden, zoals de mogelijkheid om commentaar op artikelen te plaatsen. Voor die extra functies kunnen dan weer andere cookies nodig zijn. In deze specifieke context is de Groep van mening dat "dienst van de informatiemaatschappij" gezien moet worden als de som van een aantal functies en dat de exacte omvang van een dergelijke dienst dus kan afhangen van de functies waarom de gebruiker (of abonnee) heeft verzocht.

Criterium B kan dus worden geformuleerd in termen van de "functies" die een dienst van de informatiemaatschappij levert. Een cookie dat aan criterium B voldoet, moet dan aan de volgende eisen voldoen:

1) Het cookie is noodzakelijk om de gebruiker (of abonnee) een specifieke functie te bieden: als cookies zijn gedeactiveerd, is de functie niet beschikbaar.

2) De functie is door de gebruiker (of abonnee) uitdrukkelijk gevraagd in het kader van een dienst van de informatiemaatschappij.

2.3 Kenmerken van een cookie

Cookies worden vaak ingedeeld aan de hand van de volgende kenmerken:

1) betreft het een "sessiecookie" of een "permanent cookie"?

2) gaat het om "cookies van derden" of niet?

Een sessiecookie is een cookie dat automatisch wordt gewist als de gebruiker de browser afsluit. Een permanent cookie blijft op de eindapparatuur van de gebruiker opgeslagen totdat het tijdstip van verstrijking is bereikt (cookies kunnen verstrijken na bijvoorbeeld enkele minuten, dagen of zelfs jaren).

De term “cookie van derden” kan misleidend zijn:

- in het kader van de gegevensbescherming in de EU wordt in Richtlijn 95/46/EG onder “derde” verstaan: *“de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam, niet zijnde de betrokkene, noch de voor de verwerking verantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de voor de verwerking verantwoordelijke of de verwerker gemachtigd zijn om de gegevens te verwerken”*. Een “cookie van derden” zou dus een cookie zijn dat is geplaatst door een andere voor de verwerking verantwoordelijke dan die welke de door de gebruiker bezochte website exploiteert (zoals blijkt uit de URL die in de adresbalk van de browser te zien is);

- voor de browser wordt het begrip “derde” echter uitsluitend geïdentificeerd aan de hand van de structuur van de URL die in de adresbalk van de browser wordt weergegeven. “Cookies van derden” zijn in dit geval echter cookies die geplaatst zijn door een website die tot een ander domein behoort dan het domein dat in de adresbalk wordt weergegeven, ongeacht of er sprake is van een andere voor de verwerking verantwoordelijke.

Hoewel deze twee noties elkaar vaak overlappen, zijn zij niet altijd gelijkwaardig. In dit advies volgen we de eerste aanpak: we gebruiken “cookie van derden” voor cookies die geplaatst worden door een andere voor de verwerking verantwoordelijke dan de voor de verwerking verantwoordelijke die de bezochte website exploiteert. De term “cookie van de eerste partij” wordt gebruikt voor een cookie dat is geplaatst door de voor de verwerking verantwoordelijke (of een daaraan gelieerde verwerker) die de door de gebruiker bezochte website exploiteert (zoals blijkt uit de URL die in de adresbalk van de browser te zien is).

Om te beoordelen of een cookie *“strikt noodzakelijk”* is voor een uitdrukkelijk door de gebruiker gevraagde dienst (criterium A) of beperkt is tot het *“uitsluitend doel”* (van criterium B) worden bepaalde kenmerken in aanmerking genomen.

De levensduur van een cookie dat van de toestemmingsverplichting is vrijgesteld, moet in overeenstemming zijn met het doel waarvoor het cookie dient; het moet verstrijken zodra het niet meer nodig is, rekening houdend met de gerechtvaardigde verwachtingen van de gemiddelde gebruiker of abonnee. Cookies die aan criterium A of B voldoen zijn dus waarschijnlijk cookies die verstrijken als de browsersessie wordt afgesloten of zelfs eerder. Dit is echter niet altijd het geval. Een voorbeeld: in het scenario met een winkelmandje dat in het volgende hoofdstuk aan de orde komt, kan de handelaar het cookie zo instellen dat het ook na het einde van de browsersessie behouden blijft, of dat het pas over enkele uren verstrijkt; als de gebruiker per ongeluk de browser afsluit, heeft hij namelijk wellicht de redelijke verwachting dat de inhoud van het winkelmandje intact is gebleven als hij even later op de website van de handelaar terugkomt. In andere gevallen kan een gebruiker uitdrukkelijk vragen om bepaalde gegevens te behouden voor een volgende sessie, een verzoek waaraan slechts met een permanent cookie kan worden voldaan.

Volgens de eerder gegeven definities zijn “cookies van derden” bovendien doorgaans niet *“strikt noodzakelijk”* voor het bezoek aan de website, aangezien dergelijke cookies doorgaans verband houden met een andere dienst dan die waarom de gebruiker *“uitdrukkelijk heeft gevraagd”*.

Sessiecookies van de “eerste partij” zullen dus waarschijnlijk eerder voor vrijstelling van de toestemmingsverplichting in aanmerking komen dan permanente cookies van “derden”[3]. De genoemde kenmerken kunnen weliswaar als eerste indicator dienen voor de prioritering van maatregelen tot naleving van de voorschriften, maar zijn op zich niet voldoende om vast te stellen of een cookie aan criterium A of B voldoet. Het is voorstelbaar dat een cookie wordt gebruikt voor de authenticatie van gebruikers die op een website willen inloggen. Dit cookie wordt gebruikt om te zorgen dat de gebruiker alleen toegang krijgt tot informatie waartoe hij gerechtigd is. Een soortgelijk cookie kan worden gebruikt voor het identificeren en traceren van gebruikers op verschillende domeinen en voor het verstrekken van gerichte inhoud en advertenties op basis van een profiel dat door de exploitant van de website wordt bijgehouden. Beide cookies kunnen soortgelijk van aard zijn (d.w.z. sessiecookies of permanente cookies), min of meer hetzelfde verstrijkingstijdstip hebben, of ook onder controle staan van derden. Het risico vanuit het gezichtspunt van gegevensbescherming ontstaat veeleer door het doel of de doeleinden van de verwerking dan door de informatie die het cookie bevat.

Uiteindelijk moet dus aan de hand van het doel, de specifieke implementatie, of de specifieke verwerking worden bepaald of een cookie al dan niet kan worden vrijgesteld van de toestemmingsverplichting op basis van criterium A of B.

2.4 Cookies voor meerdere doeleinden

Het is mogelijk dat een cookie voor meerdere doeleinden wordt gebruikt, maar zo’n cookie kan alleen worden ontheven van de toestemmingsverplichting als alle onderscheiden doeleinden waarvoor het wordt gebruikt niet toestemmingsplichtig zijn.

Het is bijvoorbeeld mogelijk een cookie te plaatsen met een unieke naam of waarde, die beide zowel kunnen worden gebruikt om de voorkeuren van de gebruiker vast te leggen als om de gebruiker te traceren. Het vastleggen van de voorkeuren van de gebruiker kan in bepaalde omstandigheden onder een vrijstelling vallen (zoals omschreven in punt 3.6), maar het is zeer onwaarschijnlijk dat het traceren van de gebruiker onder criterium A of B valt. De website dient voor het traceren dus de gebruiker om toestemming te vragen. In de praktijk zal dit ertoe leiden dat de eigenaars van websites voor elk onderscheiden doel een afzonderlijk cookie gebruiken.

Als een website gebruikmaakt van meer dan een cookie of van cookies die voor verschillende doeleinden zijn ingezet, hoeft echter niet voor elk cookie of voor elk doel een aparte banner te worden geplaatst of toestemming te worden gevraagd, zoals de Groep al heeft opgemerkt in advies 16/2011. Eén punt voor informatie en een verzoek om toestemming is doorgaans voldoende, mits een en ander duidelijk en volledig wordt gepresenteerd.

---

[3] Met bepaalde technologieën, vaak aangeduid als “Evercookies” of “zombiecookies” kan een cookie permanent op de eindapparatuur van de gebruiker worden geplaatst, ook als deze een redelijke inspanning verricht om het te verwijderen. Het is zeer onwaarschijnlijk dat een dergelijk cookie, volgens welk scenario dan ook, van de toestemmingsverplichting is vrijgesteld.

3 Scenario's voor de toepassing van cookies

In dit hoofdstuk wordt behandeld hoe de criteria voor ontheffing van de toestemmingsverplichting kunnen worden toegepast in een aantal veel voorkomende scenario's.

3.1 Cookies voor gebruikersinput

In het algemeen zijn cookies voor gebruikersinput sessiecookies waarmee de input van de gebruiker vast wordt gelegd door uitwisseling van een reeks berichten met een dienstverlener. Het gaat hier om cookies van de eerste partij, die typisch gebruikmaken van een sessie-id (een tijdelijk uniek toevalsgetal) en uiterlijk aan het einde van de sessie verstrijken.

Dit type sessiecookies wordt gewoonlijk gebruikt om de input van de gebruiker vast te leggen wanneer deze een uit verschillende pagina's bestaand onlineformulier invult, of als winkelmandje om vast te leggen welke artikelen de gebruiker heeft gekozen door op een knop te klikken (bijvoorbeeld met een tekst als "in winkelmandje").

Deze cookies zijn duidelijk noodzakelijk voor het leveren van een uitdrukkelijk door de gebruiker gevraagde dienst van de informatiemaatschappij. Bovendien zijn deze cookies gekoppeld aan een actie van de gebruiker (zoals het klikken op een knop of het invullen van een formulier). Voor deze cookies geldt daarom een ontheffing op grond van criterium B.

3.2 Authenticatiecookies

Authenticatiecookies worden gebruikt ter identificatie van de gebruiker, zodra deze is ingelogd (bijvoorbeeld op de website van een bank). Deze cookies zijn noodzakelijk voor de authenticatie van de gebruiker bij opeenvolgende bezoeken aan de website en om toegang te krijgen tot toegelaten inhoud, zoals het rekeningsaldo of transacties en dergelijke. Authenticatiecookies zijn doorgaans sessiecookies. Het gebruik van permanente cookies is ook mogelijk, maar mag niet als identiek worden gezien (zie hieronder).

Wanneer een gebruiker inlogt, vraagt hij uitdrukkelijk om toegang tot de inhoud of de functie die voor hem is toegelaten. Als geen gebruik wordt gemaakt van een in een cookie opgeslagen authenticatietoken, zou de gebruiker bij elke nieuwe pagina opnieuw zijn gebruikersnaam en wachtwoord moeten invoeren. De authenticatiefunctie is dus een wezenlijk onderdeel van de dienst van de informatiemaatschappij waarom de gebruiker uitdrukkelijk heeft gevraagd. Voor deze cookies geldt daarom een ontheffing op grond van criterium B.

Het is wel van belang op te merken dat de gebruiker slechts heeft gevraagd om toegang tot de site en tot een specifieke functie met het oog op de uitvoering van de benodigde taak. De authenticatie mag niet worden gebruikt als een gelegenheid om het cookie in te zetten voor een secundair doel, zoals monitoring van het gedrag of het zonder toestemming plaatsen van advertenties.

Voor permanente logincookies waarin een authenticatietoken wordt vastgelegd voor meerdere browsersessies, geldt geen ontheffing op grond van criterium B. Dat is een belangrijk onderscheid, aangezien de gebruiker wellicht niet ogenblikkelijk beseft dat door het sluiten van de browser de authenticatiegegevens niet worden gewist. De gebruiker keert wellicht terug naar de website in de veronderstelling anoniem te zijn, terwijl hij in feite nog steeds is

ingelogd. De gebruikelijke methode, bestaande uit een aankruisvakje en een simpele tekst als "onthoud mij (maakt gebruik van cookies)" bij de verzendknop, is geschikt om toestemming te verkrijgen, zodat in dit geval een ontheffing niet nodig is.

3.3 Op de gebruiker gerichte beveiligingscookies

De ontheffing die op grond van criterium B voor authenticatiecookies geldt (zoals hierboven beschreven) kan worden uitgebreid tot andere cookies die specifiek worden ingezet om de beveiliging van de door de gebruiker uitdrukkelijk gevraagde dienst van de informatiemaatschappij te verbeteren. Dit geldt bijvoorbeeld voor cookies waarmee herhaalde foutieve inlogpogingen op een website worden gedetecteerd, of voor soortgelijke mechanismen die het inlogsysteem moeten beschermen tegen misbruik (hoewel deze methode in de praktijk slechts een geringe bescherming biedt). De ontheffing geldt echter niet voor het gebruik van cookies die verband houden met de beveiliging van websites of diensten van derden waarom de gebruiker niet uitdrukkelijk heeft gevraagd.

Terwijl logincookies doorgaans aan het eind van de sessie verstrijken, moeten beveiligingscookies een langere levensduur hebben om hun doel te bereiken.

3.4 Sessiecookies voor multimediaspelers

Sessiecookies voor multimediaspelers worden gebruikt voor het opslaan van technische gegevens die nodig zijn voor het afspelen van video- of audiomateriaal (zoals beeldkwaliteit, snelheid van de netwerkverbinding of bufferinggegevens). Dergelijke multimedia-sessiecookies worden gewoonlijk "flashcookies" genoemd, naar een van de meest gebruikte technologieën voor internetvideo, Adobe Flash. Aangezien dergelijke informatie niet lang hoeft te worden bewaard, moeten deze cookies aan het einde van de sessie worden verwijderd.

Als de gebruiker een website bezoekt met tekst en video, behoren die allebei tot de uitdrukkelijk door de gebruiker gevraagde dienst. De functie voor videoweergave voldoet dus aan criterium B.

Zoals in punt 3.2 al is aangegeven, komen exploitanten van websites slechts voor de ontheffing in aanmerking als zij in flashcookies of andere cookies geen extra informatie opnemen die voor de weergave van het multimediamateriaal niet strikt noodzakelijk is.

3.5 Sessiecookies voor load balancing

Load balancing houdt in dat de verwerking van requests aan een webserver wordt verdeeld over een aantal computers. Dit kan gebeuren met behulp van een "load balancer": de webrequests van de gebruikers gaan naar een gateway voor load balancing, die de requests doorgeleid naar een van de beschikbare interne servers. In sommige gevallen moet deze doorgeleiding tijdens een sessie van kracht blijven: alle requests van een specifieke gebruikers gaan dan naar dezelfde server met het oog op consistente verwerking. Om een server aan te duiden in de pool, zodat de load balancer de requests naar behoren kan doorsturen, kunnen onder meer cookies worden gebruikt. Deze cookies zijn sessiecookies.

De informatie die in het cookie is opgenomen, heeft als uitsluitend doel het aanduiden van het eindpunt van de communicatie (namelijk een van de servers in de pool) en is derhalve

noodzakelijk voor de communicatie via het netwerk. Voor deze cookies geldt daarom een ontheffing op grond van criterium A.

3.6 Cookies voor aanpassing van de gebruikersinterface

Met cookies voor aanpassing van de gebruikersinterface worden de voorkeuren van de gebruiker voor een groep webpagina's opgeslagen, waarbij geen koppeling plaatsvindt met andere permanente identificatoren zoals een gebruikersnaam. Deze cookies worden alleen geplaatst als de gebruiker de dienst uitdrukkelijk vraagt een informatie-item vast te houden, bijvoorbeeld door op een knop te klikken of een vakje aan te kruisen. Hiervoor kunnen zowel sessiecookies als cookies met een levensduur van enkele weken of maanden (afhankelijk van het doel) worden gebruikt.

Een aantal typische voorbeelden:

- taalkeuzecookies worden gebruikt om de taal vast te leggen die de gebruiker op een meertalige website heeft gekozen (bijvoorbeeld door op een vlag te klikken);

- cookies voor de weergave van zoekresultaten worden gebruikt om vast te leggen hoe de gebruiker wenst dat het resultaat van een zoekopdracht wordt weergegeven (bijvoorbeeld door een bepaald aantal resultaten per pagina aan te geven).

Deze aanpassingsfuncties worden door de gebruiker van een dienst van de informatiemaatschappij uitdrukkelijk ingeschakeld (bijvoorbeeld door op een knop te klikken of een vakje aan te kruisen), hoewel zonder extra informatie niet zomaar kan worden aangenomen dat de gebruiker die keuze wil vastleggen voor meer dan één browsersessie (of meer dan een aantal uren). Alleen voor sessiecookies of cookies met korte levensduur geldt daarom een ontheffing op grond van criterium B. Door toevoeging van extra informatie op een prominente plaats (bijvoorbeeld de tekst "maakt gebruik van cookies" naast de vlag) is er voldoende informatie voor een geldige toestemming om de voorkeur van de gebruiker voor langere duur vast te leggen, zodat in dat geval een ontheffing niet nodig is.

3.7 Cookies voor het delen van inhoud via sociale plug-ins

Veel sociale netwerken bieden "sociale plug-inmodules" aan die exploitanten van websites in hun platform kunnen integreren, met name om de gebruikers van sociale netwerken de mogelijkheid te bieden om informatie aan te bevelen aan hun "vrienden" (en om andere, aanverwante functies te bieden, zoals het geven van commentaar). Die plug-ins worden gebruikt voor het opslaan en uitlezen van cookies op de eindapparatuur van de gebruiker; sociale netwerken kunnen zo hun leden identificeren wanneer deze met de plug-ins communiceren.

Bij dit gebruiksgeval is het van belang een onderscheid te maken tussen enerzijds gebruikers die via hun browser zijn "ingelogd" op een account bij een bepaald sociaal netwerk, en anderzijds gebruikers die "niet zijn ingelogd", bijvoorbeeld omdat zij geen lid zijn van het specifieke sociale netwerk of omdat zij niet zijn verbonden met hun account bij het sociale netwerk.

Omdat sociale plug-ins per definitie bestemd zijn voor leden van een bepaald sociaal netwerk, hebben zij voor niet-leden geen nut, en voldoen zij voor die gebruikers dus niet aan criterium

B. Dit geldt ook voor personen die wel lid zijn van het sociale netwerk, maar uitdrukkelijk zijn "uitgelogd", en derhalve ervan uitgaan dat zij niet langer met het sociale netwerk "verbonden" zijn. Niet-leden en uitgelogde leden moet derhalve om toestemming worden gevraagd voordat de sociale plug-in een cookie mag plaatsen.

Veel ingelogde leden verwachten daarentegen dat zij op websites van derden gebruik kunnen maken van en toegang kunnen krijgen tot sociale plug-ins. In dat geval is het cookie strikt noodzakelijk voor een functie waar de gebruiker uitdrukkelijk om heeft gevraagd en geldt dus criterium B. Dergelijke cookies zijn sessiecookies[4]: om hun doel te vervullen, moet hun levensduur eindigen wanneer de gebruiker uit het sociale netwerk uitlogt of de browser wordt afgesloten. Sociale netwerken die cookies wensen te gebruiken voor andere doeleinden (of met een langere levensduur), waarvoor criterium B niet geldt, hebben via hun eigen platform ruim voldoende mogelijkheden om hun leden te informeren en hun toestemming te verkrijgen.

4 Cookies waarvoor geen vrijstelling geldt

In dit hoofdstuk wordt verduidelijkt welke scenario's voor cookiegebruik niet onder de ontheffing op grond van criterium A of B vallen.

4.1 Tracking cookies en sociale plug-ins

Zoals we eerder hebben beschreven, bieden veel sociale netwerken "sociale plug-inmodules" aan, die exploitanten van websites in hun platform kunnen integreren om diensten aan te bieden die kunnen worden aangemerkt als "uitdrukkelijk gevraagd" door de leden. Deze modules kunnen echter ook worden ingezet voor het traceren van personen (zowel leden als niet-leden) met behulp van cookies van derden, voor doeleinden zoals reclame op basis van het surfgedrag, analyse of marktonderzoek.

Als cookies voor dergelijke doeleinden worden gebruikt, zijn zij niet "*strikt noodzakelijk*" voor een functie waar de gebruiker uitdrukkelijk om heeft gevraagd. Voor zulke tracking cookies geldt daarom geen ontheffing op grond van criterium B. Als niet om toestemming wordt gevraagd, is het onwaarschijnlijk dat er een rechtsgrondslag bestaat voor het verzamelen van gegevens via sociale plug-ins over niet-leden van het desbetreffende netwerk. Sociale plug-ins dienen dus standaard geen cookies van derden te plaatsen op pagina's die aan niet-leden worden getoond. Zoals eerder aangegeven, hebben sociale netwerken echter, als zij dergelijke trackingactiviteiten willen ondernemen, ruim voldoende mogelijkheden om hun leden om toestemming te vragen via het eigen platform, nadat zij de gebruikers duidelijke en volledige informatie over deze activiteit hebben verstrekt.

4.2 Advertenties van derden

Voor cookies van derden met het oog op reclame op basis van het surfgedrag geldt geen ontheffing van de toestemmingsverplichting, zoals de Groep in de adviezen 2/2010 en 16/2011 uitvoerig heeft uitgelegd. Deze verplichting om toestemming te vragen strekt zich natuurlijk ook uit tot alle aanverwante operationele cookies van derden die bij het adverteren worden gebruikt voor doelen als frequency capping (het beperken van het aantal keren dat een

[4] In punt 3.2 is aangegeven waarom voor permanente authenticatiecookies geen vrijstelling geldt.

gebruiker een advertentie te zien krijgt), financiële logging, advertentienetwerken, opsporing van klikfraude, onderzoek en marktanalyse, productverbetering en debuggen, aangezien geen van deze doelen kan worden geacht samen te hangen met een dienst of een functie van een dienst van de informatiemaatschappij waarom de gebruiker uitdrukkelijk heeft gevraagd, zoals criterium B vereist.

De Groep neemt op dit gebied sinds december 2011 actief deel aan de werkzaamheden van het World Wide Web Consortium (W3C) om de technologie en de betekenis van Do Not Track te standaardiseren. Cookies bevatten vaak unieke identificatoren aan de hand waarvan het gedrag van gebruikers in de tijd op verschillende websites kan worden gevolgd, en deze identificatoren kunnen worden gecombineerd met andere identificerende of identificeerbare gegevens. De Groep is dan ook bezorgd over de mogelijkheid dat bepaalde cookies die noodzakelijk worden genoemd voor operationele doeleinden, zouden worden uitgesloten van de toepassing van Do Not Track. De doeleinden zijn: frequency capping, financiële logging, audits door derden, beveiliging, contextuele inhoud, onderzoek en marktanalyse, productverbetering en debuggen[5]. De Do Not Track-norm kan alleen zorgen voor naleving van de voorschriften door bedrijven die bij Europese burgers cookies plaatsen, als Do Not Track ook inderdaad betekent dat geen gegevens worden verzameld, zonder uitzonderingen. Dat betekent dat wanneer een gebruiker heeft aangegeven dat hij niet wil worden getrackt (DNT=1), er geen identificator met het oog op tracking mag worden geplaatst of anderszins verwerkt. Er zijn reeds technische oplossingen beschikbaar, en aan andere wordt momenteel gewerkt, die binnen webbrowsers of aan serverzijde functioneren om de genoemde operationele doeleinden te bereiken en zo het privacy by design-beginsel in de praktijk te brengen.

4.3 Analyse door de eerste partij

Deze analyse betreft statistische instrumenten om de omvang van het publiek van een website te meten, waarbij vaak gebruikt wordt gemaakt van cookies. Website-eigenaars gebruiken vaak zulke instrumenten om het aantal unieke bezoekers te schatten, de belangrijkste zoektermen te vinden waarmee de website via een zoekmachine kan worden gevonden, of problemen in verband met het navigeren op de website op te sporen. Analyse-instrumenten maken tegenwoordig gebruik van allerlei verschillende modellen voor het verzamelen en analyseren van gegevens, die uiteenlopende risico's voor de bescherming van gegevens opleveren. Analyse door de "eerste partij" met gebruikmaking van cookies van de "eerste partij" leidt duidelijk tot andere risico's dan analyse door een "derde" met gebruikmaking van cookies van een "derde". Er zijn ook instrumenten die gebruikmaken van cookies van de eerste partij, terwijl de analyse door een derde wordt verricht. Die derde wordt als een voor de verwerking medeverantwoordelijke aangemerkt indien de derde de gegevens voor zijn eigen doeleinden gebruikt, of als een verwerker, indien de derde dit als gevolg van een technische of contractuele regeling niet kan of mag doen.

Hoewel deze instrumenten vaak als voor exploitanten van websites "strikt noodzakelijk" worden beschouwd, zijn zij niet strikt noodzakelijk om een door de gebruiker of abonnee uitdrukkelijk gevraagde functie aan te bieden. De gebruiker kan namelijk toegang krijgen tot alle functies die de website biedt, ook als dergelijke cookies uitgeschakeld zijn. Deze cookies vallen dus niet onder een ontheffing op grond van criterium A of B.

---

5 http://www.w3.org/TR/tracking-compliance/

Volgens de Groep is het echter niet waarschijnlijk dat analysecookies van de eerste partij een privacyrisico opleveren, indien zij strikt worden beperkt tot geaggregeerde statistieken ten behoeve van de website-exploitant en worden ingezet door websites die in hun privacybeleid al duidelijke informatie geven over deze cookies en passende privacywaarborgen bieden. In ieder geval mag de gebruiker verwachten dat hij op gebruikersvriendelijke wijze toestemming kan weigeren voor het verzamelen van zijn gegevens en dat de website-exploitant mechanismen toepast om andere reeds verzamelde identificerende informatie, zoals het IP-adres, volledig te anonimiseren.

Mocht artikel 5, lid 3, van Richtlijn 2002/58/EG worden herzien, dan is het passend dat de Europese wetgever overweegt een derde ontheffingscriterium toe te voegen voor cookies die strikt beperkt zijn tot cookies van de eerste partij ten behoeve van geanonimiseerde en geaggregeerde statistieken.

Analyses door de website-exploitant zelf moeten duidelijk worden onderscheiden van analyse door derden; laatstgenoemde maken gebruik van een gemeenschappelijk cookie voor het verzamelen van gegevens over de wijze waarop de gebruiker van website naar website navigeert, en leveren daardoor een veel groter privacyrisico op.

5 Samenvatting en richtsnoeren

Uit de analyse door de Groep blijkt dat voor de volgende soorten cookies onder bepaalde voorwaarden ontheffing kan worden verleend van de verplichting om de op informatie berustende toestemming van de gebruiker te vragen, mits de cookies niet ook voor andere doeleinden worden gebruikt:

1) cookies voor gebruikersinput (sessie-id): voor de duur van een sessie, of in sommige gevallen permanente cookies met een levensduur van slechts enkele uren;

2) authenticatiecookies die gebruikt worden voor authenticatiediensten: voor de duur van een sessie;

3) op de gebruiker gerichte beveiligingscookies om misbruik bij authenticatie op te sporen: voor de duur van een sessie;

4) sessiecookies voor multimediaspelers, zoals Flash Player-cookies: voor de duur van een sessie;

5) sessiecookies voor load balancing: voor de duur van een sessie;

6) permanente cookies voor de aanpassing van de gebruikersinterface: voor de duur van een sessie;

7) Cookies van derden voor het delen van inhoud via sociale plug-ins: voor ingelogde leden van een sociaal netwerk.

Wat sociale netwerken betreft, merkt de Groep echter op dat toestemming moet worden verkregen voor het gebruik van sociale plug-incookies voor andere doeleinden dan het aanbieden van een functie die door de eigen leden uitdrukkelijk is gevraagd, met name indien die doeleinden ook inhouden dat gebruikers worden gevolgd op verschillende websites.

De Groep wijst erop dat voor cookies van derden voor reclamedoeleinden altijd de toestemming van de gebruiker moet worden gevraagd. Diens toestemming is ook vereist voor operationele doeleinden die met het aanbieden van advertenties van derden samenhangen, zoals frequency capping, financiële logging, advertentienetwerken, opsporen van klikfraude, onderzoek en marktanalyse, productverbetering en debuggen. Hoewel bij sommige operationele doeleinden de ene gebruiker van de andere wordt onderscheiden, is het gebruik van unieke identificatoren voor deze doeleinden in beginsel niet gerechtvaardigd. Dit punt is in het bijzonder relevant in de context van het debat over de implementatie van de Do Not Track-norm in Europa.

Uit de analyse blijkt tevens dat analysecookies van de eerste partij niet zijn ontheven van de verplichting om toestemming te verkrijgen, maar slechts beperkte privacyrisico's met zich meebrengen, mits in redelijke waarborgen is voorzien, waaronder passende informatieverstrekking, de mogelijkheid om gemakkelijk een opt-out te krijgen en mechanismen voor volledige anonimisering.

Aan de hand van de analyse en de scenario's voor het gebruik van cookies, zoals in dit advies gepresenteerd, kunnen enkele basisrichtsnoeren worden geformuleerd:

1) bij de toepassing van criterium B is het van belang te onderzoeken wat strikt noodzakelijk is vanuit de positie van de gebruiker, niet die van de dienstverlener;

2) als een cookie voor verschillende doeleinden wordt gebruikt, komt het slechts in aanmerking voor een ontheffing van de toestemmingsverplichting als voor elk afzonderlijk doel een ontheffing geldt;

3) sessiecookies van de eerste partij komen veel eerder voor vrijstelling van de toestemmingsverplichting in aanmerking dan permanente cookies van derden. Of een ontheffing mogelijk is, moet echter altijd worden beoordeeld aan de hand van het doel van het cookie, veeleer dan aan de hand van een technisch kenmerk van het cookie.

Om te beslissen of voor een cookie niet de verplichting geldt om de op informatie berustende toestemming van de gebruiker te verkrijgen, zal uiteindelijk zeer zorgvuldig moeten worden beoordeeld of het cookie voldoet aan een van de twee ontheffingscriteria van artikel 5, lid 3, van Richtlijn 2002/58/EG, zoals gewijzigd bij Richtlijn 2009/136/EG. Als na zorgvuldig onderzoek substantiële twijfel blijft bestaan over de vraag of een ontheffingscriterium van toepassing is, moet een website-exploitant zich goed afvragen of er geen mogelijkheid is om op een eenvoudige, niet hinderlijke wijze de gebruiker om toestemming te vragen en zo elke rechtsonzekerheid te vermijden.

Gedaan te Brussel, 7 juni 2012

Voor de Groep
De voorzitter
Jacob Kohnstamm