Cookie Compliance

Een Praktische Gids

Inhoudsopgave

1. Introductie

In het kort

Op 5 juni 2012 is de nieuwe Telecommunicatiewetgeving in werking getreden, waarmee artikel 11.7a (hierna te noemen "Cookiebepaling") wordt geïmplementeerd. Wat betekent deze Cookiebepaling concreet? Met de implementatie van de Cookiebepaling gaan er strengere regels voor het gebruik van cookies gelden. Dit betekent kortgezegd dat er in bepaalde gevallen aan een informatie- en toestemmingsplicht moet worden voldaan.

Scope

De nieuwe Cookiebepaling is van toepassing in geval van het plaatsen van of toegang krijgen tot gegevens op randapparatuur van de gebruiker. Daarbij wordt geen onderscheid gemaakt naar de aard van de gegevens. In dit document zullen wij voor de leesbaarheid spreken over cookies, maar dit beslaat eigenlijk alle technologie die wordt gebruikt om gegevens op te slaan in de randapparatuur van een gebruiker. Behalve om verschillende soorten cookies gaat dit dus ook om geïnstalleerde apps en / of plugins, informatie opgeslagen in de Web Storage, screen size, OS, browser type, device fingerprinting, etc.

Verantwoordelijkheid

De verplichtingen op basis van de Cookiebepaling rusten op degene die verantwoordelijk is voor het plaatsen van cookies en voor het verkrijgen van toegang tot de opgeslagen gegevens. Kortgezegd, als u een online dienst levert en hierbij cookies plaatst zult u in principe aan de verplichtingen opgenomen in de Cookiebepaling moeten voldoen.

Overigens rusten de verplichtingen niet altijd op degene die verantwoordelijk is voor de door gebruiker bezochte site of gevraagde dienst. Het kan voorkomen dat een derde partij cookies plaatst via uw website, omdat er bijvoorbeeld via een site een andere site wordt vertoond, als gevolg waarvan de derde partij ook aan de verplichtingen moet voldoen. Gezien de gedeelde verantwoordelijkheid om de verplichtingen na te komen is het aan te raden om hierbij tot een samenwerking te komen.

'De nieuwe wet is van toepassing in het geval van het plaatsen van of toegang krijgen tot gegevens op randapparatuur van de gebruiker. Daarbij wordt geen onderscheid gemaakt naar de aard van de gegevens. In dit document zullen wij voor de leesbaarheid spreken over cookies.

Wat is het doel van deze gids?

Deze Cookie Compliance Gids geeft u een handvat ten aanzien van de nieuwe Cookiebepaling. Het doel van deze Gids is om het proces in kaart te brengen dat u moet doorlopen om aan de verplichtingen uit de Cookiebepaling te voldoen. Deze Gids geeft echter geen specifiek advies over hoe u de verschillende stappen moet implementeren (dit zal per bedrijf anders zijn.) Aangezien op het moment van schrijven van deze Gids nog veel onduidelijkheden bestaan over de precieze interpretatie van de Cookiebepaling, heeft dit document de status van een levend document. Op het moment dat meer duidelijk is over de interpretatie van de Cookiebepaling zal dit document worden aangepast.

Voor wie is deze gids bedoeld?

Deze Gids is bedoeld voor iedereen die een website heeft en compliant wil worden met de nieuwe wetgeving. Het is niet bedoeld als technische handleiding voor webdevelopers.

Over de auteurs

Dit document is in opdracht van het IAB opgesteld door:

AUKE VAN DEN HOUT

Auke van den Hout is binnen het bestuur van IAB verantwoordelijk voor de portefeuille privacy. Hij is mede oprichter van Adatus, de Europese marktplaats voor 'audience targeting' en heeft meer dan 15 jaar ervaring in data driven advertising in Europa.

EMAIL: INFO@IAB.NL / TEL: +31 854010802

ROEL VAN RIJSEWIJK

Roel van Rijsewijk is director bij Deloitte met meer dan 10 jaar ervaring in advisering aan media en technologie bedrijven op het gebied van risico management en compliance. Roel is mede oprichter van Deloitte Online Business Innovation en leidt het innovatieprogramma op het gebied van vertrouwen in de digitale wereld.

EMAIL: RVANRIJSEWIJK@DELOITTE.NL / TEL: +31 652615087

Deze Cookie Compliance Gids geeft u een handvat ten aanzien van de nieuwe Cookiebepaling. Het doel van deze Gids is om het proces in kaart te brengen dat u moet doorlopen om aan de verplichtingen uit de Cookiebepaling te voldoen. Deze Gids geeft echter geen specifiek advies over hoe u de verschillende stappen moet implementeren (dit zal per bedrijf anders zijn).

2. Cookie Compliance Gids

A. Cookie inventarisatie

1. IDENTIFICEER COOKIES

Inleiding

Om aan de verplichtingen opgenomen in de Cookiebepaling te kunnen voldoen is het van belang om te starten met een inventarisatie welke type cookies – en vergelijkbare technieken – uw website plaatst, en/of welke type cookies mogelijk door derde partijen worden geplaatst. Deze fase bestaat dan ook uit het identificeren van de type cookies.

Waarom?

- Het verduidelijkt aan welke verplichtingen uit de Cookiebepaling u zult moeten voldoen.
- Het maakt zichtbaar op welke wijze uw bedrijfsvoering geraakt wordt door de nieuwe Cookiebepaling.
- Het zorgt ervoor dat u gemakkelijker kunt voldoen aan de informatie- en toestemmingsverplichtingen.
- U maakt de toezichthouders kenbaar dat u bewust bent van de problemen rondom de Cookiebepaling en hieraan wil werken.

Ten behoeve van een grondige inventarisatie adviseren wij u de volgende vragen te beantwoorden.

1. Welk type cookies worden er op uw website gebruikt en wie plaatst deze?
2. Waarom worden de cookies gebruikt?
3. Is het een persistent of een session- cookie?
4. Wordt de cookie over meerdere aaneengesloten websites gebruikt of wordt de website uitsluitend op één domein gebruikt?
5. Naar welke data verwijst de cookie/ welke data bevat de cookie?
6. Hoe lang blijven de gegevens waarnaar de cookie verwijst bewaard?

De vragen worden hieronder stapsgewijs doorgenomen:

Stap 1. Welke cookies worden er door wie geplaatst?

- Identificeer welke cookies er op uw website gebruikt worden.
- Let hierbij op de cookies die u zelf op uw website heeft geplaatst (First Party Cookies).
- Identificeer welke cookies door third parties op uw website zijn geplaatst. Let hierbij op de cookies die geplaatst zijn door bijvoorbeeld sociale netwerken en advertising networks (Third Party Cookies).
- Vergeet niet om de gebruikte flash cookies te identificeren!

Tips

- Er zijn tools beschikbaar die behulpzaam kunnen zijn bij het analyseren van cookiegebruik op uw website – meestal in de vorm van plug-ins voor uw browser.

- Bekijk alle onderdelen van uw website die potentieel cookies kunnen plaatsen, zowel door uzelf als door andere partijen. Let hier met name op bij integratie van externe scripts, zoals Like-buttons van Facebook, +1 van Google, etc.

Stap 2. Doel

In deze stap is het van belang per cookie aan te geven met welk doel de cookie wordt geplaatst.

Om u daarbij op weg te helpen kunt u onder andere de volgende vragen stellen:

- Is de cookie geplaatst om ervoor te zorgen dat de producten in het winkelmandje worden onthouden?
- Zorgen de cookies ervoor dat de inhoud van de pagina sneller wordt geladen?
- Worden de cookies gebruikt vanwege bepaalde beveiligingseisen?
- Worden de gegevens gebruikt/uitgelezen door derden en waarom?
- Worden de cookies gebruikt om een gebruiker te herkennen om bij terugkeer naar een website te worden begroet?
- Worden er met behulp van de cookie gegevens verzameld over het gebruik van de website, zoals het aantal unieke bezoekers?

Stap 3. Levensduur

- Geef per cookie aan of het een session-cookie is of een persistent cookie.
- Identificeer hoe lang de cookie bewaard wordt.

Stap 4. Aantal websites

- Geef per cookie aan of het gebruikt wordt om op meerdere websites informatie te verzamelen, en zo ja, welke dat zijn.
- Stel vast of cookies die op meerdere websites gebruikt worden, overal dezelfde functie hebben, of dat de functie(s) verschillen.

Stap 5. Naar welke data verwijst de cookie?

In deze stap onderzoekt u welk type data de cookie bevat en / of naar welke data de cookie verwijst.

- Bevat de cookie zelf persoonsgegevens?
- Welke andere data worden er in de cookie zelf opgeslagen?
- Stel vast naar welke data de cookie verwijst in uw eigen omgeving en databases.
- Leg vast welke data er allemaal van de gebruikers verzameld wordt in de databases.
- Stel vast welk andere data uit andere databases hieraan kan worden gekoppeld.

Stap 6. Bewaartermijn

Behalve de levensduur van de cookie zelf, moet u vaststellen hoe lang de data waar de cookie naar verwijst, bewaard blijft.

- Stel vast welke procedures gelden voor het vernietigen van gebruikersdata binnen de verschillende databases.
- Ga na of in de praktijk aan deze procedures voldaan wordt.

Tips voor het identificeren van cookies

- Let erop dat u het gebruik van cookies op alle pagina's analyseert, in elke fase waarin uw gebruiker zich op uw website bevindt.

- Verzeker uzelf ervan dat u een volledig overzicht hebt van alle websites en webpagina's waar u verantwoordelijk voor bent.

2. Cookie Impact Beoordeling

Wij adviseren u - nadat u alle verschillende typen cookies hebt geïnventariseerd die op uw website worden gebruikt - voor de volledigheid ook een cookie impact beoordeling uit te voeren.

Het doel van de Cookiebepaling is namelijk om de internetgebruiker meer controle te geven over zijn privacy. Daarvoor is het van belang dat u inzicht krijgt in de impact op de privacy van websitebezoekers door het gebruik van cookies.

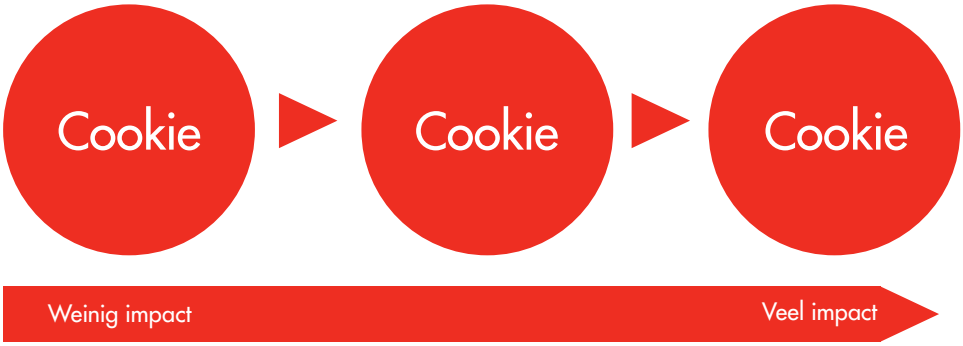
Middels deze beoordeling evalueert u de impact van ieder type cookie op de privacy van uw websitegebruiker. Vervolgens kunt u zich bewust worden van de gevolgen die een bezoek aan uw website heeft op een gebruiker en kunt u kritisch kijken naar de cookies die u plaatst.

Beoordeel deze impact door onderstaande stappen te volgen.

Stap 1. First party cookies

Gebruik de vragen en antwoorden uit de cookie inventarisatie fase om deze cookie impact beoordeling uit te voeren.

Het is van belang dat u deze impact als een glijdende schaal ziet (zie figuur hieronder).



Stap 2. Third party cookies

Als er via uw website cookies van derde partijen worden geplaatst, dan is het ook van belang om te beoordelen welke mate van inbreuk op de privacy van uw websitegebruikers deze cookies kunnen hebben en hoe deze partij omgaat met de informatie- en toestemmingsvereisten.

HIERVOOR KUNT U:

1. Contact opnemen met de betreffende partij om te informeren, hetgeen wij adviseren; en/of:
2. Het privacybeleid van deze partij beoordelen.

Plaats ook deze cookies op de hierboven aangegeven glijdende schaal van cookie impact.

3. Cookie categorisatiegids

Met de resultaten uit de inventarisatie fase kunt u de cookies onderverdelen in een tweetal categorieën: Deze twee categorieën zijn afkomstig uit de Cookiebepaling.

Categorie 1

Op basis van de inventarisatie fase kunt u beoordelen of het type cookies dat u plaatst, valt onder een van de volgende uitzonderingen:

- De technische opslag of toegang tot gegevens heeft uitsluitend als doel om de communicatie over een elektronisch communicatienetwerk uit te voeren. De communicatie op de website kan in sommige gevallen uitsluitend plaatsvinden door een cookie te gebruiken. Dit is bijvoorbeeld het geval als een taalinstelling wordt onthouden.
- Opslag of toegang tot de gegevens is strikt noodzakelijk. De wetgever heeft bepaald dat strikt noodzakelijk cookiegebruik uitgezonderd is van de cookie-verplichtingen (mits u geen persoonsgegevens verwerkt). Een voorbeeld hiervan is een webwinkelwagentje cookie. Het is van belang dat u redeneert vanuit het perspectief van de websitegebruiker of een bepaald cookiegebruik strikt noodzakelijk is. Indien dit het geval is, dan betreft dit cookies die in lijn met de Cookiebepaling strikt noodzakelijk worden geacht.

In deze gevallen hoeft u niet te voldoen aan het toestemmingsvereiste zoals opgenomen in de Cookiebepaling, mits u hiermee geen persoonsgegevens verwerkt.

Ten behoeve van de transparantie kunt u overwegen om de gebruiker te informeren over het plaatsen van dergelijke cookies. Dit hoeft niet in een pop-up of iets dergelijks maar kan in de privacy policy.

Categorie 2

Mochten de cookies niet onder de eerste categorie vallen dan betreft het in principe cookies die niet strikt noodzakelijk zijn.

Voor deze cookies is voorafgaande toestemming vereist. Daarnaast dient de gebruiker geïnformeerd te worden over onder meer het plaatsen van cookies en de gevolgen hiervan.

Doet u aan klantprofilering of retargeting? Dan zult u zonder twijfel voorafgaande toestemming moeten verkrijgen van uw websitegebruikers.

Twijfelt u over in welke categorie een specifieke cookie geplaatst zou moeten worden? Dit zal best voorkomen want er is nog veel onduidelijk. Voor het bepalen van een juiste aanpak zou een risico-beoordeling moeten worden gedaan, zoals beschreven in het volgende hoofdstuk.

B. Compliance pad

1. Risico Beoordeling

Er zullen cookies zijn waarbij het niet geheel duidelijk is of het gebruik ervan strikt noodzakelijk wordt geacht en of er dus toestemming nodig is. In dit geval raden wij u aan een risico beoordeling uit te voeren om de juiste compliance aanpak te kunnen kiezen. Een compliance aanpak voor deze cookies moet rekening houden met:

- Het belang van het gebruik van een cookie en de daaraan gerelateerde gegevens voor de organisatiedoelstellingen.
- De impact van het gebruik van cookies op de privacy van de gebruiker.

Hierbij geven wij de volgende overwegingen mee:

- Indien het belang van het gebruik van de cookie en de daaraan gerelateerde gegevens voor de organisatiedoelstellingen laag is, zou u kunnen overwegen te stoppen met het gebruik van deze cookie, zeker als de impact van het gebruik van cookies op de privacy van de gebruiker hoog is.

- Indien het belang van het gebruik van de cookie voor organisatiedoeleinden hoog is, én de impact op de privacy van de gebruiker hoog is, dan is het expliciet vragen van toestemming de voor de hand liggende keuze. In dit geval moet u in uw informatievoorziening naar de consument toe naast een hele goede uitleg over het belang van de cookie voor uw organisatie en de voor- en nadelen voor de consument als hij de cookie wel/niet accepteert, ook nog heel duidelijk aangeven hoe de gegevens worden gebruikt, bewaard en beschermd.

- Indien de impact op de privacy van de gebruiker verwaarloosbaar is en het belang van het gebruik van de cookie voor de organisatiedoelstellingen hoog, kunnen extra stappen gezet worden voor het verkrijgen van zekerheid van de aanpak, zoals het inwinnen van advies van experts, het toetsen van de aanpak aan standaarden, en de aanpak van anderen die gebruik maken van deze cookies en het opbouwen van een goed onderbouwde case.

Nu u weet welke categorie cookies via uw website worden geplaatst, kunt u gaan bepalen op welke manier u aan de informatieplicht en de toestemmingsvereiste gaat voldoen. Wij verwijzen u hierbij naar de volgende hoofdstukken.

2. Informatieplicht in de praktijk

Dit hoofdstuk geeft u handvatten over op welke wijze u aan de informatieplicht kunt voldoen.

Informatie verstrekken

De cookiebepaling schrijft niet voor op welke wijze de websitegebruiker geïnformeerd moet worden. Wel is helder dat de verstrekte informatie vooraf op ondubbelzinnige wijze duidelijk en volledig moet zijn. Dit betekent dat iedere websitebezoeker vooraf aan het plaatsen van de cookie op de hoogte moet worden gebracht van:

1. Het feit dat er een cookie wordt geplaatst;
2. Door wie er een cookie wordt geplaatst;
3. Wat het doel is van deze cookie;
4. Hoe lang de cookie wordt bewaard;
5. Wie toegang krijgt tot de gegevens;
6. Of de cookie wordt hergebruikt en door wie.

Zichtbaar maken informatie cookiegebruik

Het is in ieder geval onvoldoende om het gebruik van cookies te beschrijven in uw privacy policy. Het is namelijk van belang dat u zich ervan kunt vergewissen dat de gebruikers de informatie hebben opgenomen.

Tips

- Zorg ervoor dat uw gebruikers niet om de informatie heen kunnen
- Beschrijf het privacy en cookiebeleid in eenvoudige, voor iedereen te begrijpen taal

Groeperen cookies

U hoeft uw websitebezoekers niet over ieder afzonderlijk gebruik van een cookie te informeren, maar u mag het cookiegebruik groeperen naar soort en doel van de cookie.

Voordelen van informatieplicht

Door volledig transparant te zijn over het gebruik van cookies op uw website, zal het vertrouwen van uw bezoeker toenemen. Voor een volledige informatievoorziening is het verstandig om het volgende toe te voegen aan de informatie:

- Waarom uw website deze cookies nodig heeft
- Wat het voordeel is voor uw websitegebruiker
- Maak het voor de gebruiker helder dat hij zijn gegeven toestemming te allen tijde kan intrekken en op welke wijze hij dit kan doen.

3. Het verkrijgen van toestemming in de praktijk

Uit de categorisatie fase is duidelijk geworden voor welke cookies u specifiek toestemming dient te verkrijgen. Dit hoofdstuk maakt duidelijk op welke wijze u aan de toestemmingsvereiste kunt voldoen.

Het mag duidelijk zijn dat het verkrijgen van toestemming nauw samenhangt met de informatieplicht. Het moet immers duidelijk zijn waarvoor de gebruiker toestemming geeft. Welke methode in de praktijk het meeste geschikt is om toestemming van uw websitegebruikers te verkrijgen is afhankelijk van wat het doel is van de cookies, hoe privacygevoelig de data is en wat de relatie is met uw websitebezoekers.

Er zijn verschillende methodes om bezoekers te wijzen op de aanwezigheid van de cookies en ze op een transparante manier te informeren. Hieronder wordt een aantal voorbeelden opgesomd:

FEATURE LED

Bij feature-led methode wordt de bezoeker gevraagd toestemming te geven wanneer hij of zij van een bepaalde 'feature' gebruik wil gaan maken. De bezoeker kan voorafgaand aan het gebruik van een bepaald gedeelte van de website (waarvoor cookies geplaatst dienen te worden) geïnformeerd worden en om toestemming worden gevraagd, in plaats van direct bij het aankomen bij de website toestemming te vragen voor alle cookies op de gehele website.

INLOGGEN

Voorafgaand aan het inloggen op een gedeelte van de website kunt u aangeven dat u van plan bent cookies te gaan plaatsen. U kunt voor het inloggen de bezoeker informeren over het gebruik van bepaalde cookies zodat deze een geïnformeerd besluit kan nemen en al dan niet toestemming kan geven.

Let op:

- U mag de vinkjes onder geen beding al vast op 'aan' zetten. Dit wordt namelijk niet gezien als opt-in door de wetgever, maar als opt-out. Hiermee zult u dus niet voldoen aan de vereisten van de cookiebepaling.
- Zorg ervoor dat uw gebruikers de informatie zien en dat u op transparante wijze kenbaar maakt waarvoor u van deze cookies gebruik maakt.

DIALOOGVENSTER

Door middel van een dialoogvenster dwingt u de bezoeker eerst een keuze te maken alvorens de website – die achter het venster besloten ligt – te kunnen bezoeken. In dit venster informeert u de bezoeker en verwijst u naar de privacy policy.

STATUSBALK

U kunt gebruik maken van de statusbalk om de bezoeker op de hoogte te stellen. Dit kan zowel bovenaan als onderaan de pagina. Deze statusbalk informeert de gebruikers over de cookies die u wilt gaan plaatsen, geeft toegang tot de privacy policy en laat bezoekers op basis van de informatie het gebruik van de cookies accepteren. Aangezien bij deze manier van informeren niet noodzakelijk een keuze afgedwongen wordt voordat de consument verder kan, moet u erop letten dat u de statusbalk op een plek zet waar de balk goed zichtbaar is voor de gebruiker. Let erop dat u geen cookies gebruikt totdat de gebruiker daadwerkelijk expliciet zijn toestemming hiervoor heeft gegeven

WAARSCHUWINGSBALK

Een soortgelijke methode als de statusbalkmethode, maar deze is indringender aanwezig op uw website. Elke keer dat de website een cookie wil plaatsen, verschijnt de waarschuwingsbalk. Informeer op deze manier de bezoeker, link naar het privacy beleid en zorg dat bezoekers de cookies kunnen accepteren of weigeren.

SETTING LED

Indien de website mogelijkheden heeft voor de gebruiker om instellingen te kiezen, kunt u van deze instellingen ook gebruik maken om bepaalde functionaliteiten die cookies nodig hebben aan of uit te zetten. Bezoekers kunnen dan bij de instellingen een geïnformeerd besluit nemen om gebruik te maken van de functionaliteiten en toestemming te geven om de cookies te plaatsen. Aangezien bij deze manier van informeren geen voorafgaande keuze afgedwongen wordt, moet u de gebruiker duidelijk uitleggen hoe hij toestemming kan geven via zijn instellingen.

Aandachtspunten

Bewijs dat u toestemming heeft verkregen

U heeft toestemming nodig om een cookie te kunnen plaatsen. Denk eraan dat u ook moet kunnen aantonen dat u deze toestemming heeft verkregen. Zorg ervoor dat u hiervoor een procedure heeft en vastlegt van wie u de toestemming heeft gekregen. Let wel: de meest gebruiksvriendelijke manier om verkregen toestemming vast te leggen is middels een cookie!

Third party cookies

In principe moet iedere partij die gegevens plaatst de bezoeker informeren en toestemming verkrijgen, ook de derde partijen. In plaats van afzonderlijke toestemming te krijgen (uw cookies apart van third party cookies), kunt u ook afspreken met de derde partij om in de informatievoorziening een verwijzing op te nemen naar de privacy informatie van de derde partij. Dit scheelt de bezoeker een extra pop-up. Daarnaast kunt u de gebruiker informeren hoe third party cookies uit te schakelen in de browser.

Een cookie voor meerdere websites

Gebruikt u een cookie voor meerdere websites? Heeft u verschillende websites met elkaar verbonden en gebruikt u daarvoor dezelfde cookies? Om voor alle websites tegelijk toestemming te ontvangen, moet u ervoor zorgen dat u de bezoeker duidelijk informeert voor welke websites u toestemming wenst te verkrijgen.

Verandering nadat cookies toestemming is verkregen

Wanneer u nadat u toestemming hebt verkregen, wijzigingen aanbrengt in de te gebruiken cookies, of nieuwe cookiediensten afneemt van andere partijen, zal u mogelijk opnieuw toestemming moeten hebben van de bezoeker. U zult opnieuw toestemming moeten vragen indien u wijzigingen aanbrengt in:

1. Het doel van de geplaatste cookie;
2. Door wie de cookie wordt geplaatst;
3. Hoe lang de cookie wordt bewaard;
4. Wie toegang krijgt tot de gegevens;
5. Of de cookie wordt hergebruikt en door wie.

Toestemming intrekken

Een eenmaal gekregen toestemming kan altijd worden ingetrokken.
Denk eraan om de bezoekers de mogelijkheid te bieden om deze toestemming op een eenvoudige wijze in te trekken.

4. Toon aan dat u geen persoonsgegevens verwerkt

Vanaf 1 januari 2013 zal de nieuwe cookiebepaling gehandhaafd worden waarin het gebruik van 'commerciële' cookies (een cookie dat tot doel heeft gegevens over het gebruik van verschillende diensten van de informatiemaatschappij door de gebruiker of de abonnee te verzamelen, combineren of analyseren voor commerciële, charitatieve of ideële doeleinden) wordt gezien als het verwerken van persoonsgegevens waardoor de privacywetgeving van toepassing wordt. Hierbij heeft de wetgever gebruik gemaakt van het middel rechtsvermoeden: ú wordt vermoed persoonsgegevens te verwerken, ténzij u kunt aantonen dat dit niet zo is. Zie appendix E voor het geval het vermoeden dat u persoonsgegevens verwerkt gerechtvaardigd is, en u hier nog niets voor geregeld hebt. Indien u vindt dat dit vermoeden niet gerechtvaardigd is en u van mening bent dat u geen persoonsgegevens verwerkt, wordt in dit hoofdstuk beschreven wat u moet doen.

Het aantonen dat u geen persoonsgegevens verwerkt is niet eenvoudig. Een goede voorbereiding is belangrijk, zodat u op het moment dat u het bewijs dient te leveren niet met lege handen staat maar proactief kan handelen. Door het volgen van de volgende stappen krijgt u een goed beeld van het datagebruik binnen de organisatie, en heeft u uw dossier met bewijsmateriaal klaarliggen om aan te kunnen tonen dat u geen persoonsgegevens verwerkt.

Stap 1. Leg vast in een managementverklaring waarom u geen persoonsgegevens verwerkt

Weet wat u aan wilt tonen. Stel (management)verklaringen op waarin u aangeeft waarom u geen persoonsgegevens verwerkt. En waarin staat welke maatregelen u hebt genomen om data anoniem te houden.

U KUNT BIJVOORBEELD VERKLAREN:

- De door [uw organisatie] verzamelde, opgeslagen en bewerkte data kan niet worden herleid naar de individuele internetgebruiker of computer van waar de gegevens vandaan komen;

'Door het volgen van de volgende stappen krijgt u een goed beeld van het datagebruik binnen de organisatie, en heeft u uw dossier met bewijsmateriaal klaarliggen om aan te kunnen tonen dat u geen persoonsgegevens verwerkt.'

Stap 2. Breng processen en informatiestromen in kaart

Breng de relevante processen en informatiestromen in kaart in relatie tot het gebruik van de cookies.

- Welke cookies gebruikt u?
- Waar gaat alle informatie naartoe?
- Wat voor informatie wordt verzameld?
- Wie maakt gebruik van deze informatie?

Door het in kaart brengen van de processen en informatiestromen krijgt u zelf een goed beeld van de informatiehuishouding. Hierdoor zorgt u ervoor dat u zeker weet dat u met alle informatieverzamelingen rekening heeft gehouden.

Stap 3. Stel vast hoe u aan kunt tonen dat het geen persoonsgegevens zijn

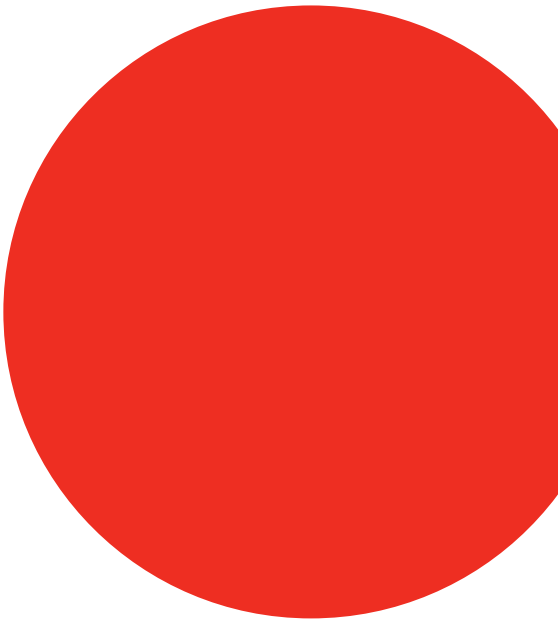
Wat kunt u laten zien zodat u kunt aantonen dat u geen persoonsgegevens verwerkt? Laat bijvoorbeeld zien welke gegevens u verzamelt, welke maatregelen u hebt genomen om gegevens te anonimiseren en wat voor gebruik u van de gegevens maakt (bijvoorbeeld alleen voor statistische doeleinden).

Stap 4. Voer een 'gap-analyse' uit

Een gap analyse is een methode om een vergelijking te maken tussen een bestaande en een gewenste situatie. Controleer of u niet onverhoopt toch data verzamelt die terug kan worden geleid naar de internetgebruiker of computer. Gebruik de in stap 2 in kaart gebrachte informatiestromen en processen. Probeer aan de hand van de reeds verzamelde gegevens of deze te herleiden zijn naar een computer of persoon.

Stap 5. Wanneer van toepassing: repareer de gevonden 'gaps' en rapporteer het werkelijke datagebruik

Mocht u hebben geconstateerd in de vorige stap dat er nog zogeheten 'gaps' zijn, probeer deze dan te repareren. Anonimiseer waar nodig gegevens of neem andere maatregelen om ervoor te zorgen dat u aan de gewenste situatie voldoet. Rapporteer uiteindelijk over het werkelijke datagebruik binnen uw organisatie zodat u aan kunt tonen dat u – wanneer van toepassing - geen persoonsgegevens verwerkt en dus wat deze gegevens betreft niet aan de Wet bescherming persoonsgegevens hoeft te voldoen.



Appendix A.
De nieuwe ‘cookieregels’

De wetswijziging in het kort

Op grond van de nieuwe cookiebepaling in de Telecommunicatiewet, dient men alvorens men cookies op de computer wil plaatsen (of toegang daartoe te verkrijgen) eerst toestemming van de gebruiker te verkrijgen.

Informatieplicht

Men dient de gebruiker vooraf van duidelijke en volledige informatie te voorzien over de doeleinden waarvoor men de cookies wil gaan plaatsen of uitlezen.

Toestemming

De toestemming dient vooraf plaats te vinden, en te voldoen aan het begrip ‘toestemming’ zoals deze is beschreven in artikel 1 van de Wet bescherming persoonsgegevens: het dient te gaan om een vrije, specifieke en op informatie berustende wilsuiting. Toestemming hoeft niet voor iedere individuele cookie apart te worden gegeven door de verschillende partijen. De gebruikers moeten deze toestemming te allen tijden kunnen intrekken.

“Toestemming: een vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt ”

Uitzondering op de regel: strikt noodzakelijke cookies

De informatieplicht en het toestemmingsvereiste van de cookiebepaling zijn niet van toepassing indien de cookies strikt noodzakelijk zijn. U moet hierbij redeneren vanuit cookies die strikt noodzakelijk zijn voor de websitegebruiker en niet voor u als website verantwoordelijke.

Artikel 11.7a

1. Onverminderd de Wet bescherming persoonsgegevens dient een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een gebruiker dan wel gegevens wenst op te slaan in de randapparatuur van de gebruiker: a. de gebruiker duidelijke en volledige informatie te verstrekken overeenkomstig de Wet bescherming persoonsgegevens, en in ieder geval omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en b. van de gebruiker toestemming te hebben verkregen voor de desbetreffende handeling. Een handeling als bedoeld in de aanhef, 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 voor commerciële, charitatieve of ideële doeleinden, wordt vermoed een verwerking van persoonsgegevens te zijn, als bedoeld in artikel 1, onderdeel b, van de Wet bescherming persoonsgegevens.
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 gegevens worden opgeslagen of toegang wordt verleend tot op het randapparaat opgeslagen gegevens.3. Het bepaalde in het eerste en tweede lid is niet van toepassing, voor zover het de technische opslag of toegang tot gegevens betreft met als uitsluitend doel: a. de communicatie over een elektronisch communicatienetwerk uit te voeren, of b. de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren en de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is. 4. Bij 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. Het College bescherming persoonsgegevens wordt om advies gevraagd over een ontwerp van bedoelde algemene maatregel van bestuur.

Appendix B.
Wat als u niet aan deze regels voldoet?

Handhaving OPTA

OPTA kan een maximale boete opleggen van €450.000,- per overtreding van de Telecommunicatiewet en besluiten tot het opleggen van een last onder dwangsom.

Handhaving CBP

Wanneer met de te plaatsen of uit te lezen tekstbestandjes persoonsgegevens worden verwerkt, dan heeft u tevens te maken met de Wet bescherming persoonsgegevens waarbij het College Bescherming Persoonsgegevens de handhavingsautoriteit is.

Bestuurlijke boetes

Wanneer u bijvoorbeeld een gegevensverwerking niet meldt bij het CBP of bij een functionaris voor de gegevensbescherming, kan het College een bestuurlijke boete opleggen van ten hoogste €4500,-. Bij het bepalen van de hoogte van de boete wordt mede rekening gehouden met de verwijtbaarheid, de ernst en de duur van de overtreding.

Dwangsommen en bestuursdwang

Wanneer naar het oordeel van het CBP in strijd wordt gehandeld met de in de Wbp gestelde verplichtingen, kan het CBP besluiten tot het opleggen van een last onder bestuursdwang of dwangsom. Eerst zal een voorafgaand onderzoek door het CBP moeten plaatsvinden. De overtreder zal wel een termijn worden gegund om de betreffende overtreding ongedaan te maken voordat overgegaan wordt tot het toekennen van een last onder bestuursdwang of een dwangsom.

Appendix C.
Voor wie is de cookiebepaling van belang?

Het is van belang dat alle stakeholders op de hoogte zijn van de nieuwe verplichtingen en een strategie bepalen voor hoe ze compliant kunnen worden.

De nieuwe cookie verplichtingen zullen in ieder geval van belang zijn voor de volgende stakeholders:

- Ad network providers;
- Publishers;
- Social media
- Adverteerders
- Digitale media ontwikkelaars en ad serving technology;
- Affiliates en affiliate networks;
- Data providers;
- Online ad traders;
- Media bureaus

De nieuwe regels zijn overigens van toepassing voor iedere partij die informatie wil opslaan of zich toegang wil verschaffen tot informatie die beschikbaar is op randapparatuur van iedere Nederlandse internetgebruiker. Kortom, ook de websites van buitenlandse partijen die bezocht worden door Nederlandse websitegebruikers, dienen te voldoen aan de verplichtingen uit de cookiebepaling.

Appendix D.
Wettelijke definities

Gebruiker:

een natuurlijk persoon die gebruik maakt van een openbare elektronische communicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd;

Eindgebruiker:

een natuurlijk persoon of rechtspersoon die van een openbare elektronische communicatiedienst gebruik maakt of wil gaan maken en die niet tevens openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten aanbiedt;

Communicatie:

informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronische communicatiedienst; dit omvat niet de informatie die via een omroepdienst over een elektronisch communicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gerelateerd aan de identificeerbare abonnee of gebruiker die de informatie ontvangt;

Toestemming van een gebruiker of abonnee:

toestemming van een betrokkene als bedoeld in artikel 1, onder i, van de Wet bescherming persoonsgegevens, met dien verstande dat de toestemming mede betrekking kan hebben op gegevens van abonnees die geen natuurlijke personen zijn;

Appendix E.
Wet bescherming persoonsgegevens

Het kan zijn dat u persoonsgegevens verwerkt door het plaatsen of uitlezen van cookies. In dat geval is de Wet bescherming persoonsgegevens van toepassing (Wbp). Voor de Wbp geldt een strenger regime dan voor cookies zonder persoonsgegevens. Indien u tevens cookies verwerkt, dan zult u de volgende stappen moeten doorlopen om te voldoen aan de Wbp.

Stap 1 Worden er persoonsgegevens verwerkt?

Stel vast of u persoonsgegevens opslaat of uitleest. Dit is het geval wanneer de informatie die u in een cookie opslaat of uitleest informatie betreft over een natuurlijke persoon, ook wanneer deze niet direct betrekking hebben op deze persoon maar uit deze informatie wel een persoon uit af te leiden is. Bijvoorbeeld NAW-gegevens of een IP-adres.

Stap 2 Meld de verwerking van persoonsgegevens bij het College Bescherming Persoonsgegevens.

Indien is vastgesteld dat er persoonsgegevens worden verwerkt zoals u in 'Stap 1' hebt vastgesteld, dient u dit kenbaar te maken bij het College Bescherming Persoonsgegevens (CBP), tenzij het een verwerking betreft welke van de meldplicht is vrijgesteld.

Stap 3 Informeer de persoon van wie u gegevens verzamelt

Een doel van de privacywetgeving is het zorgen voor transparantie over de verwerking van persoonsgegevens. U dient uw websitebezoekers op begrijpelijke wijze duidelijk te maken wat u gaat doen met de gegevens, waarvoor u deze gegevens nodig heeft en of u de persoonsgegevens doorgeeft aan andere partijen. Ook moet u uw eigen identiteit kenbaar maken.

Stap 4 Voor welk doeleinde heeft u de persoonsgegevens nodig?

De persoonsgegevens mogen slechts voor een vooraf bepaald doel worden verwerkt. Daarom is het belangrijk dat u vooraf goed nadenkt waarvoor u de gegevens nodig heeft, en of u niet meer gegevens verzamelt dan nodig zijn om dit doel te behalen. Dit doel moet u kenbaar maken aan zowel het CBP als aan de betrokkene van wie u de persoonsgegevens verzamelt.

Belangrijk is dat u de gegevens die voor het bepaalde doel zijn verzameld niet langer mag bewaren dan nodig is voor de verwezenlijking van deze doeleinden. Wat u kunt doen is deze gegevens in een geanonimiseerde vorm bewaren, zodat u deze toch kunt gebruiken voor bijvoorbeeld statistische doeleinden.

Stap 5 Zorg ervoor dat u alleen gegevens verwerkt op basis van een van de grondslagen uit de Wbp

U kunt niet zomaar persoonsgegevens van iemand verzamelen, dit is alleen toegestaan wanneer er een grondslag kan worden gevonden in de Wet bescherming persoonsgegevens.

In de wet wordt een zestal grondslagen genoemd, waarvan een van de belangrijkste het verkrijgen van ondubbelzinnige toestemming van de betrokkene is. In de wet wordt deze toestemming omschreven als een 'vrije, specifieke en op informatie berustende wilsuiting', ofwel de betrokkene is vooraf goed geïnformeerd over de verzameling van persoonsgegevens, en heeft hiervoor expliciet zijn of haar toestemming gegeven.

Dit kunt u bijvoorbeeld combineren met de al bestaande informatieplicht op grond van de Cookiebepaling, al gelden hiervoor strengere regels!

Stap 6 Voldoet u aan de kwaliteitseisen?

De Wbp heeft een aantal kwaliteitseisen opgesteld die ervoor moeten zorgen dat de persoonsgegevens juist en nauwkeurig zijn. Oftewel: niet meer gegevens dan nodig is, maar ook zeker niet minder!

- Zorg ervoor dat u dus alleen datgene verzamelt wat u nodig heeft, en dat deze gegevens ook juist en volledig zijn.
- Controleer regelmatig uw database op verouderde informatie en
- Probeer zoveel mogelijk foutieve en incomplete gegevens op te schonen.

Wanneer u de gegevens niet meer nodig heeft moet u deze verwijderen (of anonimiseren / aggregeren).

Stap 7 Stel procedures vast om de rechten van betrokkenen na te kunnen leven

In het kader van de transparantie en kwaliteit van de gegevens, hebben personen van wie u gegevens verzamelt een aantal rechten toebedeeld gekregen.
Wanneer een persoon graag wil weten welke gegevens u van deze persoon heeft, kan diegene bij u een verzoek tot inzage versturen. Hiervoor heeft de wet een aantal vereisten voor opgesteld, zoals de plicht om de betrokkene binnen vier weken te informeren of over hem persoonsgegevens worden verwerkt. Wanneer de persoon op basis van de inzage fouten constateert, kan diegene verzoeken deze fout te corrigeren.

- Zorg ervoor dat de betrokkene weet bij wie ze terecht kunnen om hun rechten te kunnen uitoefenen.
- Stel een procedure op om aan de uitoefening van deze rechten te kunnen voldoen.

Stap 8 Neem passende organisatorische en technische beveiligingsmaatregelen

Stel vast dat er maatregelen zijn genomen om de persoonsgegevens te beschermen tegen verlies of enige vorm van onrechtmatige verwerking. Afhangende van de gevoeligheid van de gegevens wordt het beschermingsniveau bepaald. Gaat het bijvoorbeeld om hele gevoelige medische gegevens, dan dient u zwaardere maatregelen te nemen dan wanneer u bijvoorbeeld alleen IP-adressen verzamelt.

- Zorg ervoor dat kwaadwillenden niet bij de persoonsgegevens kunnen komen, of dat onbevoegden (zowel intern als extern) niet bij de gegevens kunnen komen.
- Laat u desgewenst informeren door beveiligingsexperts om tot een 'passend beschermingsniveau' te komen.

Stap 9 Besteed u het verwerken van persoonsgegevens uit aan een derde partij?

Wanneer u een andere partij de gegevens laat opslaan, dient u over deze verwerking goede afspraken te maken. Door middel van een overeenkomst moet u afspreken dat de derde partij zich aan de vereisten van de Wbp houdt, zoals het nemen van passende organisatorische en technische maatregelen.

- Zorg er voor dat u de naleving van de overeenkomst en de daaruit voortvloeiende verplichtingen periodiek controleert.

Stap 10 Brengt u de gegevens buiten de EU? Neem dan extra maatregelen.

Controleer of het om een niet EU- land gaat dat een zogeheten 'passend beschermingsniveau' biedt. Hierover kunt u te rade gaan bij de website van het CBP (www.cbpweb.nl). Mocht dit niet het geval zijn, dan krijgt u te maken met aanvullende vereisten vanuit de Wbp.

Appendix F.
SOLV Factsheet – 'New Cookie Rules'

WHAT

Late 2009 the European legislator introduced new, stricter legislation with regard to behavioral targeting and the use of cookies. This legislation is laid down in the amended ePrivacy Directive of 25 November 2009 and should have been implemented in the laws of the Member States by 25 May 2011.

On 8 May 2012 the Dutch passed a Bill to amend the Dutch Telecommunications Act (Telecommunicatiewet, hereinafter 'DTA'). This introduces a legal regime governing the use of cookies which is stricter than the ePrivacy Directive prescribes. The new regime for the use of cookies boils down to the requirement of informed consent based on an opt-in system:

- Prior to installing or reading cookies on the terminal equipment of the end user, the end user should be informed, and consent of the end user should be obtained.
- If the cookies are used to collect, combine or analyze information on the use of different services of the information society by the end user for commercial, charitable or non-profit purposes, this is presumed to be a procession of personal data. That means the Dutch Data Protection Act is applicable.
- Functional cookies are exempted.

Principal rule: prior informed consent

TECHNOLOGY

The new legislation doesn't specifically apply to cookies. It applies to any technology

- by which information is stored on the terminal equipment of a user, or
- by which information already stored is being accessed.

It concerns not only personal computers,
but also mobile phones and other mobile devices.

Examples of cookies that fall within the exemption are cookies that are stored and read to remember the personal settings and preferences of a user, such as the preferred language, cookies used for the processing of online orders and the execution of transactions.

The new rules do apply to any other cookies, flash-cookies, Java-scripts, web taps and spyware or similar software such as dialler programmes. Device fingerprinting and digital television are also covered.

The Bill makes no distinctions between first party or third party cookies.

PRIOR INFORMATION

The information that has to be provided prior to placing or reading the cookie, needs to be 'clear and comprehensive'. It needs to inform the end user of the purpose of the cookie and the further processing of the data collected by the cookie.
This means that the end user should at least be provided with the following information:

- the identity of the user of the cookie technology;
- the fact that the cookie is being stored on the terminal equipment;
- the purpose of the cookie;
- the period it remains active;
- if the cookie is being used to track online behaviour for targeted advertising this should be mentioned too, including with whom the information is being shared.

The information has to be easily accessible and understandable to the users.

PRIOR CONSENT

There has been a lot of debate about the question how consent can be obtained. The legal requirement is that consent has to be free, specific and informed. Unambiguous consent is not a requirement, although some parties argue the law has to be interpreted as such. The preamble of the ePrivacy Directive it is made clear that browser settings may possibly be an adequate means of giving consent. Dutch government has confirmed that the present browsers are insufficient, mainly because they are set to accept cookies by default.

In line with the European Commission, the Dutch government is in favor of a Do-Not-Track standard as a means to obtain prior consent. However, the current standard, implemented in www.youronlinechoices.eu is deemed to be insufficient.

Dutch data protection act (Wet bescherming persoonsgegevens)

The requirement of obtaining informed consent before placing or further accessing cookies is in line with the ePrivacy Directive.

However, the adopted Dutch Bill goes considerably further and introduces an additional legal regime for the use of cookies. Any cookie used to collect, combine or analyze information of the user with regard to his online surfing behaviour, is presumed to involve personal data. As a consequence, the Dutch Data Protection Act is applicable to many different cookies, entailing an even stricter legal regime to the use of cookies.

This 'cookie plus' regime is applicable to all cookies used for behavioural targeting, but may also apply to analytics cookies such as Google Analytics.

WHO

Any party that places cookies on the terminal equipment of the user or accesses information already stored on this equipment should comply with the new rules. The regulatory authorities have stressed that there can be a shared responsibility, imposing at least some responsibly for the publishers.

The new rules are applicable to anyone who wants to store information or access information already stored on the terminal equipment of internet users in the Netherlands. Thus, also companies established outside the Netherlands are governed by the Dutch rules for the use of cookies.

WHEN

The new rules have come into effect as of 5 June 2012. The Dutch government has stated that it wants to await further developments of a Do-Not-Track standard within the European Union. For this reason it said that the new rules with respect to the consent requirement shall not be enforced before 1 January 2013. However, the responsible regulatory authority, OPTA, is an independent authority and therefore may enforce despite such promises of the government.

HOW

The information that needs to be provided prior to placing the cookies has to be easily accessible and understandable to the users. This implies that a clearly visible link to the information most likely does suffice, however, a privacy policy as sole source of information is insufficient.

It is obvious that publishers and users of the cookie technology have to work together on this since the most logical place to provide information is on the website the consumer is visiting when the cookie is dropped. The consent of the user must be a clear indication of his wishes. A pop-up screen with clear and comprehensive information and a tick-box stating "I accept" seems at present the only way to comply to the new cookie rules.

The regulatory authorities have expressed that consent is not required for each individual cookie. Once the user has agreed to cookies of a specific ad network provider, this ad network provider doesn't need to obtain additional consent for cookies serving the same purpose.

Users should always be given to possibility to opt-out.

Please note that at present it is still unclear how parties should comply to the consent requirement. The responsible regulatory authority OPTA has not given any guidelines, opinions or such on this subject yet. The responsible Minister has only expressed that browsers are currently not sufficient. Other than that he confirms there is no consensus in the EU and that therefore he cannot give any indication on how to practically obtain adequate consent.

IAB Nederland
Prins Hendriklaan 29
1075 AZ Amsterdam
T: +31 85 401 08 02