Tot op de bodem

Komst Google Consent Modus V2

Waarom de Google Consent Mode V2?

De regelgeving rondom het gebruik van cookies en het verzamelen en gebruiken van persoonsgegevens wordt steeds strenger. Daarnaast wordt er steeds beter gehandhaafd en zijn er al de nodige boetes uitgedeeld. Google moest dan ook wel iets doen aan het huidige systeem om aan de wetgeving te voldoen en boetes te voorkomen. Google hoopt dat de nieuwe consentmodus hen hierbij gaat helpen.

Waar wordt het voor gebruikt?

In principe is het een mechanisme van Google. Het wordt gebruikt om de privacyaspecten van de Google tools in goede banen te lijden. Denk aan Google Ads, Google Analytics en het Google marketing platform. In principe kunnen andere tools ook gebruik maken van dit mechanisme maar wij zijn nog niet op de hoogte dat dit al gebeurt. Denk bijvoorbeeld aan Facebook advertising, Hotjar, Hubspot, Clarity en alle andere marketing- en advertising tools. Voor deze tools zal je dus vooralsnog ook nog iets moeten inregelen om de privacy te waarborgen.

Wat is Google Consent Mode V2

In wezen is het vrij eenvoudig, Google heeft een aantal onderdelen[1] [Bron 6] vastgelegd waar de bezoeker van jouw website toestemming voor kan geven. Dit zijn de meest relevante:

1. Analytics_storage: Verzamelen van data en gebruik van cookies voor niet-anonieme statistieken
2. Ad_storage: Verzamelen van data en gebruik van cookies voor advertenties
3. Ad_user_data: Gebruiken van gebruikersdata voor Advertising
4. Ad_personalisation: Gebruiken van gebruikersdata voor gepersonaliseerde advertenties

Jouw website moet deze waarden doorgeven aan alle Google tools die op jouw website staan, anders werken deze tools vanaf 1 maart 2024 niet meer. Google belooft deze waarden te respecteren.

Of een bezoeker van jouw website toestemming geeft heeft impact op de effectiviteit van jouw (marketing)tooling. Als een bezoeker bijvoorbeeld geen toestemming geeft voor gepersonaliseerde advertenties, dan kan je deze bezoeker (later) niet targetten met een gepersonaliseerde advertentie via Google Ads.

[1] Het is iets complexer dan hoe het in dit artikel beschreven wordt, maar voor de leesbaarheid zijn een aantal zaken vereenvoudigd weergeven.

Hoe werkt het geven van toestemming nu eigenlijk?

Er zijn een aantal manieren hoe je hiermee om kan gaan, het basismechanisme werkt(e) meestal als volgt:

1. Een bezoeker opent een pagina op jouw website.

2. De website plaatst de Google TAG manager (GTM) op deze pagina. GTM verzamelt geen persoonsgegevens en plaatst geen “verboden” cookies. Het kan zijn dat GTM al enkele scripts plaatst waar geen toestemming voor nodig is.

3. De website vraagt aan de bezoeker of deze toestemming geeft voor de hiervoor benoemde aspecten. Dit is de befaamde cookie-banner. Deze cookiebanner wordt ook wel het Consent Management Platform (CMP) genoemd. Denk bijvoorbeeld aan Cookiebot, Cookie First, maar dit kan ook een CMP zijn dat in het CMS is ingebouwd.

4. Als de bezoeker op het CMP heeft aangegeven waarvoor wel en geen toestemming is gegeven dan worden deze waarden doorgestuurd naar de Google Tag Manager.

5. Afhankelijk van de gegeven toestemmingen plaatst de Google Tag Manager alle tools die toegestaan zijn. Daarnaast stuurt de GTM de hiervoor genoemde waarden door naar de geplaatste tools, zodat deze precies weten wat ze wel en niet mogen doen.

6. De gegeven toestemmingen worden bewaard op de computer van de bezoeker en als deze een volgende pagina van jouw website gaat bezoeken, dan worden deze waarden direct gebruikt en zo hoeft er niet op iedere pagina opnieuw om toestemming gevraagd te worden.

De hierboven beschreven werkwijze wordt toegepast op alle tools, dus niet alleen die van Google, maar bv ook voor Facebook-pixels en Hotjar.

Wat moet er veranderen? De eenvoudige (basic) werkwijze.

Google verplicht alle websites om per 1 maart 2024 de hiervoor benoemde toestemmingen door te geven aan de Google tools. Hiervoor moeten de volgende zaken aangepast worden:

1. Als de Google Tag Manager op de website geplaatst wordt (stap 2 uit de vorige paragraaf) dan geef je aan wat de basis-toestemmingen zijn, **voordat** de bezoeker toestemming gegeven. In de regel zet je alles op “geen toestemming” (denied).

2. De toestemmingen die de website aan de bezoeker vraagt via het CMP (stap 3 uit de vorige paragraaf) moeten aansluiten bij de toestemmingen die Google wil hebben. Deze kunnen al overeenkomen maar mogelijk ook niet.

3. De toestemmingen die de bezoeker gegeven heeft moeten worden doorgeven aan de Google Tag Manager. De Google Tag Manager plaatst alleen de tools op jouw website waarvoor toestemming is gegeven én de gegeven toestemmingen worden doorgestuurd naar de tools die geplaatst mogen worden. De basis-toestemmingen uit stap 1 worden overschreven door de gegeven toestemming.

In stap 3 staat meer informatie verstopt dan je waarschijnlijk in eerste instantie denkt. Wat hierboven beschreven is, is de **eenvoudige manier**, deze **sluit het beste aan bij hoe het altijd al werkte** en is **vanuit de AVG ook de meest veilig manier.**

Het kan ook anders en Google geeft de voorkeur aan een complexer mechanisme.

Hoe het ook kan, de geavanceerde (advanced) werkwijze.

Het mechanisme wat in de eenvoudige werkwijze beschrijven is, is heel veilig. Als een bezoeker geen toestemming geeft voor bijvoorbeeld marketing cookies dan wordt Google Ads niet op de website geplaats. Het is onmogelijk voor Google Ads om persoonsgegevens te verzamelen.

Wat Google nu bedacht heeft is een geavanceerd mechanisme om tóch de tools op de website te plaatsen, altijd, dus ook als er geen toestemming is gegeven en dat deze tools dan op basis van de meegestuurde toestemmingen zelf bepalen welke persoonsgegevens er gebruikt mogen worden.

Het idee hierachter is, dat de Google tools wel degelijk wat kunnen met de niet-gebruiker gerelateerde data die zij zo ontvangen. Het is niet helemaal duidelijk wat Google exact met deze data doet maar het ligt voor de hand dat deze geanonimiseerd wordt en dat Google deze gebruikt voor verdere optimalisatie van haar tooling en analyses van het gedrag van websitebezoekers.

Het voordeel voor jou, de eigenaar van de website, is dat Google aangeeft dat ze deze data gebruikt om de data van de bezoekers die wél toestemming hebben gegeven aan te vullen. Google doet dit door het gedrag van de niet-toestemmers te analyseren en te gebruiken om het gedrag van de wel-toestemmers te extrapoleren (Google noemt dit Behavioral modeling [Bron 4]). Dit is ingewikkeld, maar waar het op neerkomt is dat bijvoorbeeld de statistieken in Google Analytics hier beter van worden.

Om gebruik te maken van de geavanceerde methode moeten de volgende zaken aangepast worden:

1. Als de Google Tag Manager op de website geplaatst wordt (stap 2 uit de vorige paragraaf) dan geef je aan wat de basis-toestemmingen zijn, **voordat** de bezoeker toestemming gegeven. In de regel zet je alles op “geen toestemming” (denied).

2. Alle Google tools worden direct, nog voordat de bezoeker toestemming heeft gegeven op de website geplaatst en de basis-toestemmingen worden meegestuurd.

3. De toestemmingen die de website aan de bezoeker vraagt via het CMP (stap 3 uit de vorige paragraaf) moeten aansluiten bij de toestemmingen die Google wil hebben. Deze kunnen al overeenkomen maar mogelijk ook niet.

4. De toestemmingen van de bezoekers worden doorgeven aan de Google Tag Manager. De Google Tag Manager plaatst de niet-Google tools op jouw website waarvoor toestemming is gegeven. De Google tools die in stap 2 zijn geplaatst blijven geplaatst, ongeacht of de bezoeker wel of geen toestemming heeft gegeven. De gegeven toestemmingen worden doorgestuurd naar de Google tools.

Wat is wijsheid? Niets doen, de basis- of toch de geavanceerde methode?

Nietsdoen is eigenlijk geen optie. Je zult op zijn minst de nieuwe toestemmingswaarden moeten doorgeven aan de Google Tag Manager en de andere Google tools anders werken deze tools niet meer vanaf 1 maart 2024[2].

Dan blijft de vraag over of je voor de basismethode gaat of voor de geavanceerde methode. Een belangrijke overweging is het aantal bezoekers dat jouw website per dag heeft. Google heeft aangegeven dat ze Behavioral modeling alleen toepassen als jouw website meer dan 1000 bezoekers per dag heeft die wél toestemming hebben gegeven en meer dan 1000 bezoekers die géén toestemming hebben gegeven [Bron 4]. Is dit niet het geval, dan heeft de geavanceerde methode geen toegevoegde waarde voor jouw website.

Heeft jouw website meer dan 1000 bezoekers mét toestemming en meer dan 1000 bezoekers zónder toestemming per dag? Dan is het een optie om voor de geavanceerde methode te kiezen. Hier zitten mogelijk privacyrisico's aan en je zult heel zorgvuldig naar de inrichting van de GTM en het CMP moeten kijken. Maar als je aan marketing en advertising doet dan kunnen de voordelen opwegen tegen de nadelen.

Als je twijfelt dan neem gerust contact op met een van onze business consultants om samen te kijken wat de beste keuze is.

Nog geavanceerdere instellingen

Google biedt nog complexere mechanismen om het toestemmingsbeheer verder te optimaliseren. Zo is het bijvoorbeeld mogelijk om te detecteren uit welk land een bezoeker komt en afhankelijk van de afkomst het toestemmingsbeheer anders in te richten. Zo kunnen de basis-toestemmingen voor landen waarde de AVG van toepassing is anders ingesteld worden dan voor landen waar minder strenge regels gelden.

Deze zaken gaan echter te ver voor dit artikel en mocht je daar meer over willen weten, neem dan contact op met een van onze consultants die je hier graag meer over vertellen en kunnen aangeven of dit iets is voor jouw website.

Hoe nu verder?

Als je nog niets gedaan hebt zal je voor 1 maart 2024 actie moeten ondernemen. In de meeste gevallen betekent dit het implementeren van de basis werkwijze. Heb je een extern marketingbureau die voor jou het toestemmingsbeheer en de markting tools beheert, neem dan contact op met hen om samen te bespreken wat er moet gebeuren. Je kan ook altijd contact opnemen met een van onze consultants die jou hier verder bij kan helpen.

---

[2] Het is overigens niet helemaal duidelijk wat "niet meer werken" precies inhoud. Google is hier onduidelijk over maar het ligt in de lijn der verwachting dat alle Google tools dan zullen opereren alsof er geen toestemming is gegeven. Als dit zo is, dan is dat heel vervelend voor jullie marketingafdeling maar wordt er in principe wel voldaan aan de AVG. Google heeft echter ook aangegeven dat zij er dan mogelijk van uitgaan dat juist volledige toestemming is gegeven. Dit houdt mijn inziens geen stand t.o.v. de wet- en regelgeving dus vermoedelijk zal dit niet gebeuren.

Handige tools:

1. https://tagassistant.google.com

Bronnen:

1. https://www.markus-baersch.de/blog/consent-mode-2-0-faq/#Check_in_Tag_Assistant_4
2. https://www.markus-baersch.de/consent-checkliste-buch/
3. https://www.youtube.com/watch?v=zyz4weLD5f4
4. https://support.google.com/analytics/answer/11161109
5. https://support.google.com/analytics/answer/9976101?hl=en
6. https://support.google.com/tagmanager/answer/13802165
7. https://www.simoahava.com/analytics/consent-mode-v2-google-tags/#what-if-consent-mode-isnt-implemented-by-march-2024
8. https://developers.google.com/tag-platform/security/guides/consent?consentmode=advanced#upgrade-consent-v2