DDMA Legal Whitepaper

MarTech in een privacy-first wereld

Een overzicht van alternatieven voor third-party cookies en andere nieuwe technieken

Inhoudsopgave

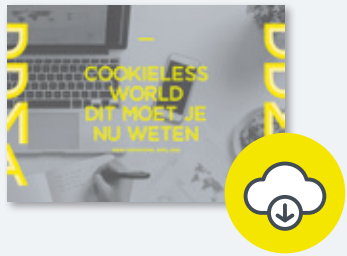
Introductie

Al enige tijd zien we in het marketinglandschap een verschuiving plaatsvinden naar een méér 'privacy-first' wereld. Deze verschuiving heeft grote impact. Zo hebben verschillende browsers en besturingssystemen het gebruik van third-party cookies en andere tracking-technieken geblokkeerd (of gaan dat in de toekomst doen). Ook zijn er (Europese) wetswijzigingen aangekondigd die het compliant gebruik van cookies juridisch moeilijk maken. Deze verschuiving vereist daarom een aanpassing van je marketingstrategie en in veel gevallen ook het implementeren van nieuwe technische oplossingen.

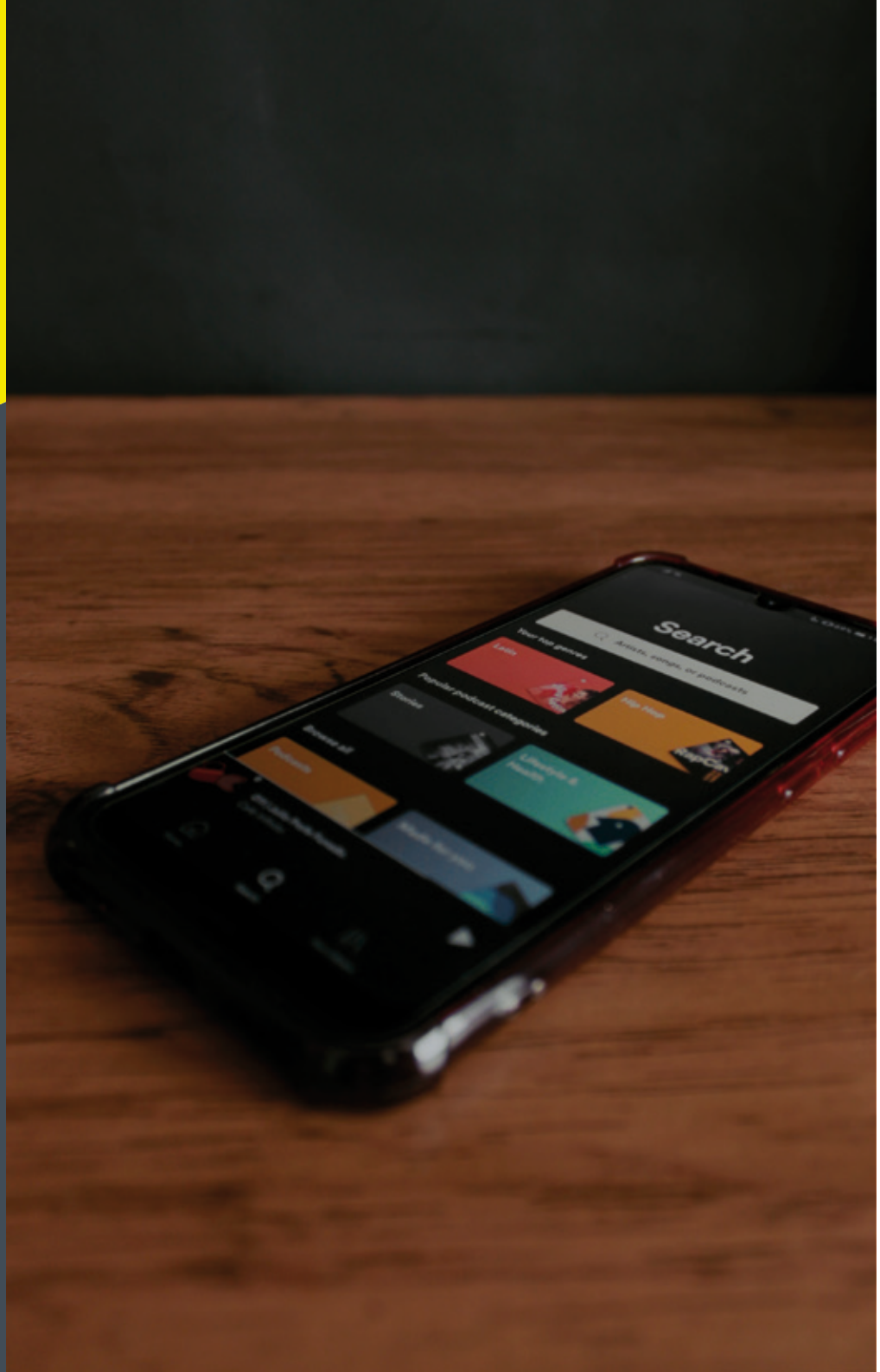
In dit whitepaper zoomen we in op nieuwe technologieën van grote tech-partijen als Google, Apple en Meta, maar ook van lokale spelers als DPG Media. Zijn dit de oplossingen die we nodig hebben? En zo ja, hoe richten we deze compliant in? Vanuit technisch en vooral juridisch perspectief werpen we een blik op de nieuwe alternatieven voor third-party cookies. Hiermee bieden we concrete handvatten om te beoordelen of én hoe je deze oplossingen zou kunnen inpassen in jouw organisatie. Dit whitepaper helpt marketeers meer inzicht te krijgen in de juridische kaders en juristen om het proces achter de techniek beter te begrijpen. We adviseren marketeers en juristen ook om samen met deze nieuwe inzichten aan de slag te gaan. Samenwerking tussen beide partijen is immers cruciaal voor succesvolle en verantwoorde data-driven marketing.

Succes!

Dit whitepaper is een uitwerking van de DDMA Legal Talk-serie over Tech in een privacy-first wereld, die plaatsvond in de eerste helft van 2023. Vorig jaar publiceerden we ook al het DDMA whitepaper: Cookieless world – dit moet je nu weten.



Als lid van DDMA heb je toegang tot onze legal helpdesk. Stuur een mailtje met je vraag naar legal@ddma.nl.



1. De privacy-first shift

1.1 Introductie

Met de opkomst en snelle ontwikkeling van het internet sinds het begin van de jaren ‘90, bood het verzamelen van data plotseling een (op het oog) onuitputtelijke bron aan mogelijkheden. Waar data tot dusver met name nuttig was voor administratieve of wetenschappelijke doeleinden, konden er nu wereldwijd bedrijfsstrategieën mee opgezet en uitgebouwd worden. Het gevolg: de eerste online ‘banner ad’ in 1994 die, in tegenstelling tot hedendaagse online advertenties, een enorme hit was.

Toch raakte de online advertising-industrie pas in een stroom-versnelling met de komst van ’s werelds grootste zoekmachine (Google, 1998) en ’s werelds grootste socialmediaplatform (Facebook, 2004). Door het groeiende gebruik van dergelijke platformen konden op grote schaal persoonsgegevens verzameld worden waarmee online (zoek)gedrag kon worden geanalyseerd en advertenties en content worden gepersonaliseerd (zoals met Google AdWords, 2000).

Om in de grootschalige verzameling het bos te kunnen blijven zien, werden analytische tools (zoals Google Analytics, 2005) ontwikkeld om de data te ordenen en inzichtelijk te maken. Tel daar het explosieve gebruik van smartphones (iPhone, 2007), de ontwikkeling van *Real Time Bidding* en *Programmatic*

Advertising (ca. 2010) én toenemende globalisering bij op en je hebt een goed idee van hoe het huidige landschap vorm heeft gekregen.

Los van de voordelen voor het bedrijfsleven was er ook al vroeg kritiek op de ontwikkelingen. Zo werd in een vroeg stadium de eerste adblocker gelanceerd (Internet Fast Forward, 1996) wegens zogenoemde 'Ad Fatigue', maar stond ook online privacy al snel op de agenda. In 2002 nam de Europese Unie dan ook nieuwe regels aan omtrent online privacy. Deze ePrivacy richtlijn (die overigens nog steeds van kracht is) wordt ook wel de 'cookiewet' genoemd, omdat door een aanpassing in 2009 werd vastgelegd dat toestemming nodig was om online data te verzamelen met de geboorte van de cookiebanner tot gevolg.

Toch is de echte focus vanuit het bedrijfsleven op privacy pas gekomen met het in werking treden van de Algemene Verordening Gegevensbescherming (AVG) in 2018. Naast dat het de toezichthouders de mogelijkheid bood om fikse boetes op te leggen (4% van de wereldwijde jaaromzet), is het met name het groeiende bewustzijn van de consument dat voor een omschakeling heeft gezorgd. Zo is er meer aandacht voor (online) privacy en is men zich beter bewust van de rechten die zij daadwerkelijk hebben (DDMA Privacy Monitor, 2023). Ook is er door verscheidene incidenten (denk aan Cambridge Analytica) afbreuk gedaan aan het vertrouwen van de consument.

Ingegeven door bovengenoemde ontwikkelingen zien we sinds enkele jaren een verschuiving plaatsvinden in het bedrijfsleven naar een privacyvriendelijkere werkwijze: de 'Privacy-First Shift'. Organisaties nemen privacyvriendelijke maatregelen en steken meer energie in een privacy vriendelijk imago. Daarbij worden ook in rap tempo alternatieve technieken ontwikkelt om privacy van online gebruikers te waarborgen en tegelijkertijd een verlies aan inkomsten te beperken.

In dit whitepaper gaan we vanuit een juridisch perspectief dieper in op deze alternatieve technieken. We beginnen steeds met een korte technische toelichting, maar de focus ligt met name op de vraag of én hoe deze technieken in lijn met de geldende wetgeving ingezet kunnen worden. Aangezien we ons begeven in een dynamisch en innovatief vakgebied, zijn veel vragen (nog) niet concreet te beantwoorden en is er tot dusver weinig duiding vanuit toezichthouders of rechtspraak. Om die reden proberen we juridische handvatten te bieden waarmee jouw organisatie toch aan de slag kan.

1.2 Maatregelen Big Tech

De Privacy-First Shift laat zich waarschijnlijk het beste zien bij maatregelen die worden genomen door de tech-reuzen. Zo zijn basisbeginselen als transparantie, controle en beveiliging opgenomen in de bedrijfsprocessen én wordt er meer aandacht aan besteed in de communicatie (zoals deze spot van Apple).

Maar ook op technisch vlak doen de bedrijven hun best om te laten zien dat ze online privacy hoog in het vaandel hebben staan. Zo worden er organisatiebreed *Privacy Enhancing Techniques* (PET's) ontwikkeld en geïmplementeerd om privacy beter te waarborgen. Een voorbeeld hiervan is *differentiële privacy* waarbij willekeurige gegevens worden toegevoegd aan een dataset om ervoor te zorgen dat gegevens niet meer herleidbaar zijn naar een individu.

Dit soort maatregelen roepen daarnaast ook vragen op vanuit adverteerders, bijvoorbeeld over het verlies aan data of de betrouwbaarheid van de uitkomsten. Een tweetal maatregelen zijn daarbij kenmerkend voor de privacy-first shift omdat zij een grote impact hebben op de werking van de online advertising-industrie. Het is daarom de moeite waard om deze hieronder kort individueel te benoemen.

1.2.1 Uitfaseren Third-Party Cookies

Een belangrijk onderdeel van het systeem voor online advertising zijn de *third-party cookies* waarmee het mogelijk is om surf-gedrag van internetgebruikers te volgen over meerdere websites en domeinen. Op basis daarvan bouwen advertentiebedrijven gedetailleerde gebruikersprofielen waarmee ze gericht gepersonaliseerde advertenties kunnen tonen.

In navolging van Apple (Safari) en Mozilla (Firefox), kondigde Google in 2020 aan third-party cookies vanaf 2022 uit te gaan faseren in Chrome. Met een marktaandeel tussen de 60-80% voor Chrome was dit de meest impactvolle aankondiging. Al snel werd er gesproken over een leven in de 'cookieless world' en werden alternatieve oplossingen/technieken bedacht en ontwikkeld voor dataverzameling. Zo kwam Google zelf ook met alternatieve technieken in de vorm van de *privacy sandbox* (hierover later meer).

Overigens weten we inmiddels dat de soep minder heet gegeten dient te worden dan destijds werd gedacht. Google stelde de uitfasering namelijk meerdere keren uit, mogelijk vanwege de gestage ontwikkeling van de privacy sandbox. De uitfasering start nu in 2024, waarbij in het eerste kwartaal wordt getest met een blokkade bij 1% van de Chrome-gebruikers.

1.2.2 Apple App Tracking Transparency

Met het blokkeren van third-party cookies in browser Safari was Apple al een voorloper, maar de meest impactvolle wijziging van de tech-reus kwam in april 2021. Met een update van het besturingssysteem voor iPhones en iPads (iOS 14.5) wordt tracking geblokkeerd, tenzij gebruikers hiervoor toestemming geven middels de (inmiddels bekende) 'vraag app om niet te tracken' pop-up. Deze update staat ook wel bekend onder de naam App Tracking Transparency (ATT).

Met meer dan 1,8 miljard iOS gebruikers wereldwijd resulteert dit in een aanzienlijk verlies van het aantal datapunten die waardevol zijn voor het inzetten van online advertising. Het ligt dan ook voor de hand dat organisaties op zoek zijn naar nieuwe manieren om toch toestemming te verkrijgen, zoals het tonen van een extra scherm met informatie vóórdat de pop-up van Apple wordt getoond. Wereldwijd zouden iPhone-gebruikers in circa 25% van de gevallen toestemming verlenen voor het 'tracken' van hun app-gebruik.

1.3 Juridisch kader en ontwikkelingen

Om de toelichting bij de alternatieve technieken voldoende te kunnen begrijpen, is basiskennis van het juridisch kader van belang. Daarom vind je hieronder een beknopt overzicht van de meest relevante wet- en regelgeving. Ook huidige ontwikkelingen en voorstellen die op de plank liggen, passeren de revue. Voor meer gedetailleerde informatie, verwijzen we naar onze al bestaande informatiepagina's of -documenten.

1.3.1 Algemene Verordening Gegevensbescherming (AVG)

Bij vrijwel alle marketingactiviteiten in onze sector ontkom je er niet aan: het verwerken van persoonsgegevens. Dit is informatie die wat zegt óver en terug te leiden is tót een persoon. Daarbij weten we inmiddels door rechtspraak dat dit breed moet worden opgevat, waardoor het vaak gaat om persoonsgegevens.

Wanneer je bij het implementeren van alternatieve technieken persoonsgegevens gebruikt, moet je voldaan aan de basis-beginselen uit de Algemene Verordening Gegevensbescherming (AVG). De volgende uitgangspunten zijn daarbij van belang:

1. **Je moet een 'grondslag' (juridische basis) hebben voor de verwerking.**
2. **Je moet een duidelijk doel hebben voor waarom je de persoonsgegevens verwerkt.**
3. **Je moet informatie verstrekken aan de persoon van wie je persoonsgegevens verwerkt (de 'betrokkene').**

Daarnaast is het ook van belang dat je nooit meer persoons-gegevens gebruikt dan nodig is, dat je persoonsgegevens verwijdert die je niet meer nodig hebt én dat je persoons-gegevens altijd 'passend' beveiligt. Later in dit whitepaper gaan we dieper in op de verhouding tussen de AVG en de alternatieve technieken.

Meer weten over de AVG? Bekijk onze dossierpagina over de AVG.

1.3.2 ePrivacy richtlijn

Het tweede belangrijke kader waarmee we rekening moeten houden, is de ePrivacy richtlijn. Een richtlijn is een ander soort wetgeving vanuit Europa dan een verordening. Waar een verordening namelijk direct geldt in ieder lidstaat, moet een richtlijn worden omgezet in nationale wetgeving. Daarbij hebben de lidstaten nog een bepaalde vorm van vrijheid, wat betekent dat er tussen lidstaten verschillen bestaan. In Nederland is de ePrivacy richtlijn verwerkt in de Telecommunicatiewet (Tw).

Hoewel de wet ook bekendstaat als de 'cookiewet', ziet deze richtlijn niet specifiek toe op cookies. Het bevat wel een definitie waar cookies onder vallen, namelijk:

'' ...het via een elektronisch communicatienetwerk ***opslaan van of toegang*** verkrijgen tot ***informatie*** in de randapparatuur van een gebruiker...''

Zoals je kunt zien, is de definitie breder en kunnen ook andere technieken (zoals pixels of device fingerprinting) hieronder vallen. Dit zorgt ervoor dat de richtlijn 'techniekneutraal' is en al meer dan twintig jaar dienst kan doen. Maar het brengt ook onzekerheid met zich mee, omdat het niet duidelijk is welke technieken hier precies onder gevat kunnen worden.

Valt een techniek wel onder de regels? Dan is het uitgangspunt dat toestemming vereist is om hiervan gebruik te kunnen maken. Let daarbij op: het inzetten van de techniek wordt geregeld door de ePrivacy richtlijn, maar het verzamelen van de gegevens valt onder de AVG. Wanneer je dan ook toestemming uitvraagt voor het inzetten van de techniek, is de AVG dus je juridische basis.

Overigens zijn er in Nederland, in tegenstelling tot veel andere EU-landen, twee uitzonderingen opgenomen die van belang zijn:

1. **Noodzakelijke en functionele technieken:** dit zijn technieken die noodzakelijk zijn om een website te laten werken. Denk daarbij aan een cookie voor het onthouden van je winkelwagen in een webshop.

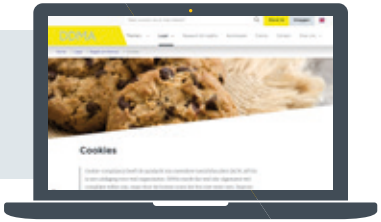
2. **Analytische technieken:** dit zijn technieken waarmee de kwaliteit of effectiviteit kan worden gemeten van de geleverde dienst. Denk daarbij aan een cookie die het aantal bezoekers op een website bijhoudt. Voor analytische technieken geldt overigens een aanvullende voorwaarde: er mogen geen (of slechts geringe) gevolgen zijn voor de privacy van de betrokkene.

   Hoe je precies aan deze voorwaarde kunt voldoen, is vrij onduidelijk. Toezichthouders en rechters zijn hier tot dusver niet heel concreet in geworden. Wél kunnen we met zekerheid stellen dat data die is verzameld voor analytische doeleinden niet zonder toestemming voor marketingactiviteiten ingezet mag worden.

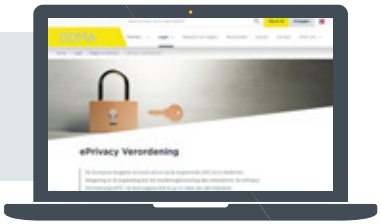
ePrivacy Verordening en de Cookiepledge

De ePrivacy richtlijn houdt het al sinds 2002 vol. Dit is opmerkelijk gezien de wetgeving gaat over een vakgebied met razendsnelle technische ontwikkelingen. Juist om die reden kwam er in 2017 een voorstel voor nieuwe regels: de ePrivacy Verordening. De onderhandelingen zitten daarentegen al jaren muurvast en het lijkt er zelfs op dat het voorstel in de prullenbak wordt gegooid.

Meer weten over de ePrivacy Richtlijn? Bekijk onze dossierpagina over cookies.



Meer weten over de ePrivacy Verordening? Bekijk onze dossierpagina over deze wet.



Meer weten over de cookiepledge? Lees dit artikel

Aangezien nieuwe Europabrede regels voor cookies en soortgelijke technieken ver weg lijken, is er inmiddels een nieuw initiatief opgestart vanuit de Europese Commissie om problemen zoals overmatige cookiebanners en onduidelijke regels op te lossen. Deze 'cookiepledge' is daarentegen op vrijwillige basis en zal geen rechtskracht hebben, waardoor het nog de vraag is wat de effect ervan zal zijn in de praktijk.

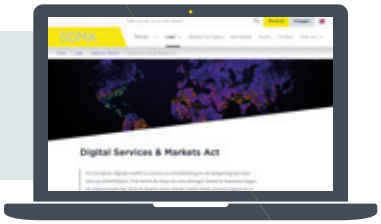
1.3.3 DSA & DMA

De nieuwste set aan regels die we in het overzicht mee moeten nemen, zijn de Digital Services Act (DSA) en de Digital Markets Act (DMA). Na een pakketvoorstel in december 2020 werden beide stukken wetgeving 'razendsnel' aangenomen door de Europese organen in het voorjaar van 2022. Inmiddels zijn de regels zelfs officieel van kracht, maar wordt er pas gehandhaafd op de verplichtingen vanaf het voorjaar van 2024.

Beide wetten worden vaak in één adem genoemd worden omdat ze beiden (voornamelijk) bedoeld zijn om Big Tech te temmen. De DSA heeft tot doel om de digitale diensten die worden aangeboden aan consumenten beter te reguleren. Het gaat dan met name om internetaanbieders, hostingbedrijven, online platformen, zoekmachines en marktplaatsen. Voor veel organisaties zal de DSA niet direct impact hebben, maar mogelijk wel indirect. Zo moeten de zogenoemde Very Large Online Platforms (VLOPs) een register van advertenties op hun platform bijhouden en voorkomen dat er gepersonaliseerde advertenties getoond worden aan kinderen of op basis van bijzondere persoonsgegevens.

De DMA ziet toe op het reguleren van concurrentie op de Europese markt (ook wel mededinging genoemd). Om een meer level *playing field* te creëren, krijgen zogenoemde 'Gatekeepers van het internet' maatregelen opgelegd. Voor deze grote impactvolle partijen geldt dat zij zichzelf niet mogen voortrekken door bijvoorbeeld enkel hun eigen diensten bruikbaar te maken binnen een platform, het verplichten om gebruik te maken van de eigen diensten óf eigen advertenties hoger te plaatsen dan die van derden.

Meer weten over de DSA en DMA? Bekijk onze dossierpagina over deze wetten



1.3.4 AI Act

Tot slot wetgeving die nog in de pijpleiding zit, maar al wel veel tongen los heeft gemaakt: de AI Act. Zoals ook bij de AVG het geval was, proberen de Europese organen het voortouw te nemen en voor het eerst concrete regels vast te stellen voor het inzetten van Artificial Intelligence (AI). Na een voorstel vanuit de Europese Commissie in het voorjaar van 2021 is het wetgevingstraject in de volgende fase beland en zijn de Europese organen aan het onderhandelen. Ondanks dat het traject in een stroomversnelling is geraakt door de opkomst van generatieve AI, zullen concrete regels op z'n vroegst pas gaan gelden vanaf 2026.

Toch zie je dat veel partijen al aan het voorsorteren zijn op deze mogelijke verordening door processen in te richten en daarbij de voorgestelde regels mee te nemen. Afhankelijk van de rol die jouw organisatie heeft bij het inzetten van AI én de risico's die eraan wordt toegekend, zijn er verplichtingen waaraan voldaan moet worden. Zo moet je duidelijk aan een consument laten weten dat deze interacteert met een AI-systeem, maar zijn er ook administratieve verplichtingen (zoals een register) om de kwaliteit te kunnen waarborgen.

Meer weten over de AI Act? Bekijk onze dossierpagina over de AI Act

2 Alternatieve technieken

Nu we de belangrijkste juridische kaders hebben aangestipt, kunnen we wat dieper de inhoud induiken. Daarbij is nogmaals belangrijk om te benoemen dat we ons begeven in een dynamisch vakgebied waarin technologieën snel ontwikkelen. Dit maakt dat in veel gevallen rechters, toezichthouders en wetgevers nog geen duidelijke kaders hebben kunnen stellen.

Om in het bos van juridische bomen toch grip te houden op compliance, hanteren we bij DDMA zes vaste stappen om een nieuwe techniek juridisch te kunnen analyseren. Door middel van die stappen kunnen we hieronder per techniek de juridisch 'knelpunten' uitlichten én bespreken welke keuzes je hierin zelf kunt maken. De stappen zijn als volgt:

1. Is er sprake van een verwerking van persoonsgegevens?
2. Op welke juridische basis?
3. Welke rol heeft jouw organisatie?
4. Op welke wijze wordt er geïnformeerd?
5. Wordt er een opt-out aangeboden?
6. Is de inzet verantwoord?

We hebben de alternatieve technieken in dit whitepaper opgedeeld in drie categorieën: collectie, analyse en activatie van data. Hoewel sommige technieken overlap hebben in de functies die zij vervullen, helpt deze categorisering bij het begrijpen van de techniek en de juridische benadering daarbij. We beginnen steeds met een kleine omschrijving van het doel van de techniek, maar verwijzen voor meer specifieke uitleg door naar externe bronnen.

2.1 Technieken voor collectie

In deze eerste paragraaf gaan we in op de technieken die de manier waarop persoonsgegevens worden verzameld ingrijpend hebben gewijzigd. Daarbij letten we met name op de daadwerkelijke gevolgen die dit heeft op de verwerking van persoonsgegevens en de rol die jouw organisatie hierbij speelt.

2.1.1 Server-side Google Tag Management (sGTM)

Met de livegang van sGTM was een veel gelezen bericht dat hiermee 'alle juridische problemen' opgelost zouden zijn. sGTM kent namelijk een nieuwe manier van dataverzameling waarbij verzamelde data niet gelijk door wordt geschoten naar Google maar eerst op een server in eigen beheer wordt geplaatst, in tegenstelling tot client-side Google Tag Management waarbij de data rechtstreeks vanuit de browser naar Google of een andere ad vendor gaat.

Eén van de grote voordelen van sGTM is dat je meer in controle bent over welke datapunten je deelt met ad vendors en andere derden, zoals analytics-partijen. De data die je uiteindelijk deelt zal ruw geschat nog steeds hetzelfde zijn als bij de client-side tag, maar er is dus wel de mogelijkheid om bepaalde informatie eruit te filteren. Denk bijvoorbeeld aan een IBAN of e-mailadres dat standaard wel met Google Analytics 4 wordt gedeeld. Met de komst van sGTM kun je dit er eenvoudiger uit uitfilteren (of maskeren). Ook kan webactiviteit juist worden verrijkt met informatie uit een andere bron, zoals een CRM of datawarehouse.

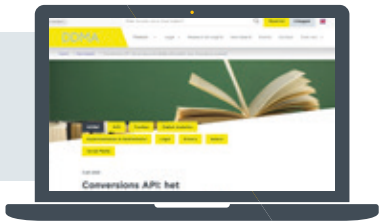
In praktijk is er bij sGTM snel sprake van een verwerking van persoonsgegevens. Dit betekent dat de AVG van toepassing is. Bij het gebruik van sGTM is het verder vaak zo dat er maar één stroom van data vanaf de website naar de sGTM server is. Dit is anders dan bij het gebruik van client-side tagging, want dan zijn er meerdere gegevensstromen naar verschillende ad vendors of derden. Toch is dit juridisch niet wezenlijk anders, want de gegevens zijn nog steeds afkomstig van een apparaat. Dit betekent dat ook zal moeten worden voldaan aan de cookiewet. Kortom, dit betekent dat er toestemming moet zijn voor personalisatie en ad tracking, wanneer dit (ook) gebeurt op basis van web- en app activiteiten. Daarnaast heb je bij sGTM zelf een grotere rol in de manier waarop de verwerking plaatsvindt door middel van de instellingen die je kiest.

2.1.2 Conversions API

De meeste ad vendors hebben ondertussen ook een eigen Conversions API. De meest bekende is wellicht die van Meta (Facebook). Met deze techniek kan je gegevens rechtstreeks met Meta en andere ad vendors delen, maar wel via een eigen server. De API wordt in feite beschikbaar gesteld als alternatief voor de Facebook-pixel, die client-side wordt gedraaid. In feite gelden dan dezelfde regels als bij sGTM, wat betekent dat toestemming vereist is.

Maar er kunnen ook andere gegevens dan webevents worden gedeeld, zoals CRM-informatie in het geval van een conversie. In zo'n situatie is de cookiewet niet direct van toepassing en zit je dus niet vast aan toestemming. De juiste grondslag moet je dan vaststellen aan de hand van de AVG, waarbij je al snel uitkomt op het gerechtvaardigd belang of het uitvoering geven aan een overeenkomst.

Meer weten over de Conversions API? Bekijk dit artikel: Conversions API: het privacyvriendelijke alternatief voor third-party cookies?



2.2 Technieken voor analyse

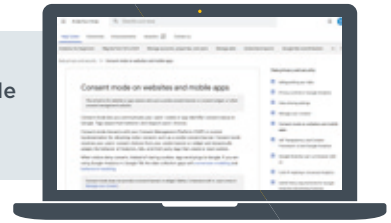
Onder deze noemer vatten we de alternatieve technieken die tot doel hebben om het verlies van datapunten op te vangen, waardoor relevante inzichten behouden blijven. Belangrijke punten hier zijn met name de vraag of het om persoonsgegevens gaat en op welke juridische basis deze verzameld worden.

2.2.1 Consent Mode

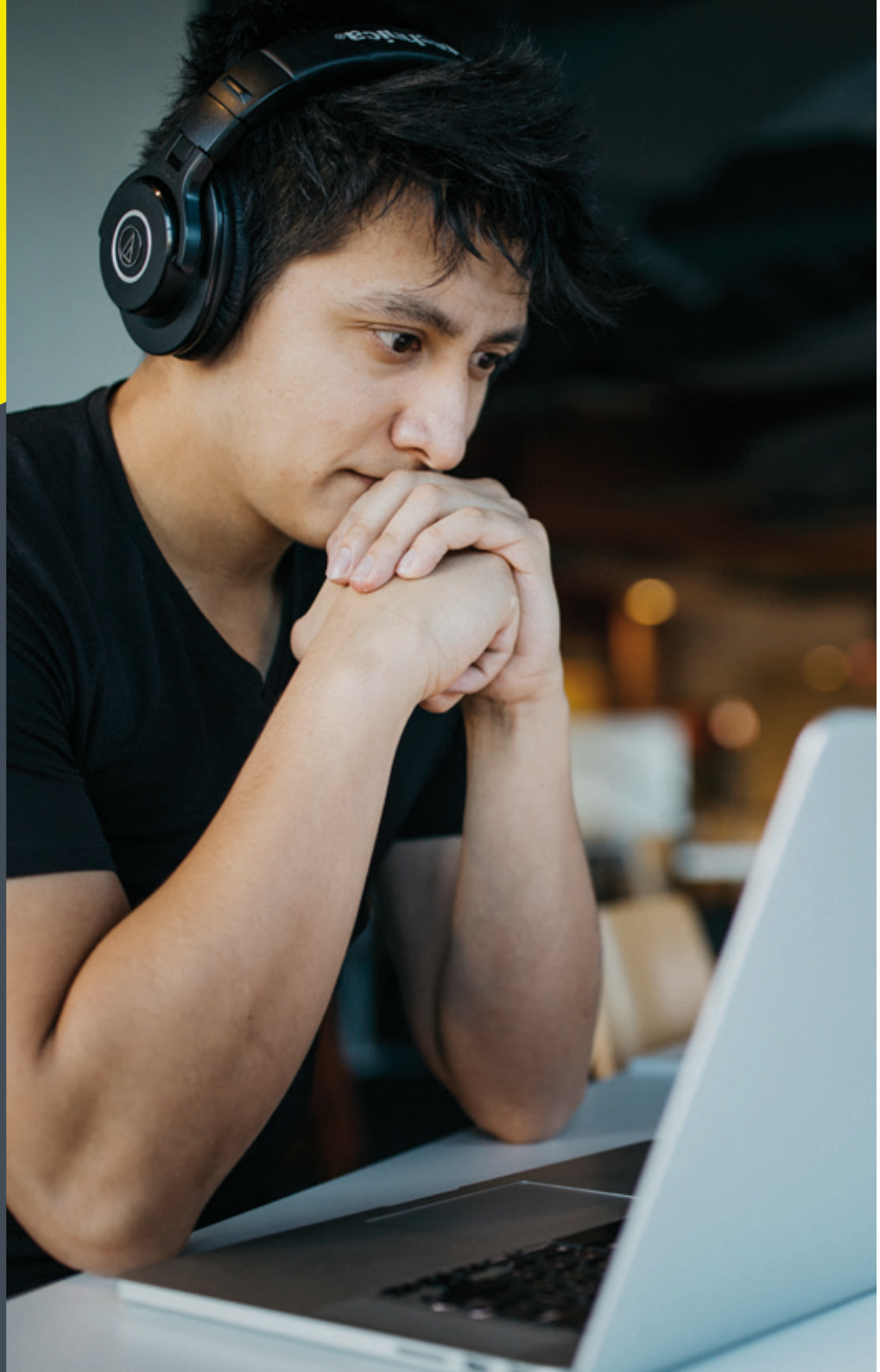
Alhoewel de naam doet vermoeden dat het om een consent-managementsysteem gaat, is Google's Consent Mode een techniek die voornamelijk ontwikkeld is om relevante inzichten te kunnen verkrijgen ondanks dat een gebruiker geen toestemming geeft. Daarbij wordt de techniek vaak wel actief gezet in een consentmanagementsysteem, zoals Cookiebot of Onetrust.

Kort samengevat: wanneer een websitegebruiker besluit de cookies (gedeeltelijk) te weigeren, wordt er informatie afgevangen uit de communicatie die standaard plaatsvindt tijdens een websitebezoek. Deze informatie wordt middels een zogenoemde 'ping' doorgeschoten naar Google en vervolgens aangevuld door middel van een voorspellend AI-model. Aan de hand van deze informatie kunnen vervolgens alsnog inzichten worden verzameld, zoals conversies.

Meer over de techniek achter Consent Mode weten? Bekijk deze uitleg van Google.



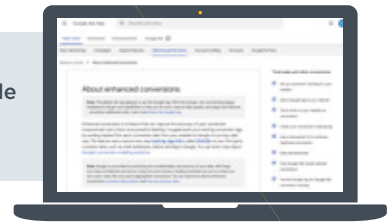
Het lastige juridische aspect waar discussie over bestaat bij Consent Mode, is de vraag of het doorsturen van de 'ping' binnen de cookiewetgeving valt. Als dat het geval is, is de volgende vraag namelijk of één van de uitzonderingen van toepassing is waardoor geen toestemming vereist is. Ondanks dat Google zelf geen specifieke toelichting geeft over het juridische perspectief, zou je uit de werking van de techniek kunnen afleiden dat toestemming in ieder geval niet vereist is. Je verzamelt immers de gegevens juist nadat expliciet géén toestemming is gegeven. De 'geest' van de ePrivacy-richtlijn is dat de privacy van gebruikers beschermd wordt, waardoor je niet zomaar gegevens kunt verzamelen vanuit een apparaat of browser. Op basis van die gedachte zouden we kunnen concluderen dat je bij het gebruik van Consent Mode rekening moet houden met deze regels, omdat er browser- of websitegegevens worden verzameld.



De vervolgvraag is of je een beroep kan doen op de uitzonderingen. Gezien het doel van de techniek is het lastig om te onderbouwen dat Consent Mode noodzakelijk is. Zonder de techniek zou de functionaliteit van de website namelijk niet (substantieel) worden aangetast. Voor de analytische uitzondering valt daarentegen al meer te zeggen, aangezien de data die wordt verzameld lastig herleidbaar is.

Daarbij speel je, net als bij sGTM, zelf een grote rol in dit proces door middel van de keuzes die je maakt bij de instellingen. Verzamel je zoveel mogelijk data? Of maak je bewuste keuzes in welke data wordt verzameld? Je doet er goed aan om kritisch door de standaardinstellingen heen te lopen én alles wat overbodig is, uit te schakelen. Op die manier kun je beter onderbouwen dat Consent Mode binnen de kaders van de wetgeving past.

Meer over de techniek achter Consent Mode weten? Bekijk deze uitleg van Google



2.2.2 Enhanced Conversions

Google Ads maakt het sinds enige tijd ook mogelijk om conversies meer accuraat te meten met Enhanced Conversions. Deze techniek kan zowel client-side met een tag of via een API worden gebruikt en maakt het mogelijk om je first party data (e-mail, naam, adres etc.) met Google te delen om deze te matchen aan Google-accounts. Daarmee kun je inzichten vergaren over aankopen of andere interacties zoals ad clicks of betekenisvolle conversies. De first-party data wordt vóór het versturen gehasht (met het SHA-256 algoritme) en is daardoor niet direct herleidbaar.

Juridisch gezien zijn een aantal elementen van belang als je Enhanced Conversions in gaat zetten.

1. **Allereerst moet je *nadenken over de manier waarop de data verzameld wordt*. Als dit rechtstreeks van een website (bijvoorbeeld middels een API-koppeling) komt, dan gelden de dezelfde regels zoals deze hierboven beschreven zijn voor sGTM en Conversion API's. Laad je de data zelf achteraf in? Dan moet je kijken of het doorsturen en matchen van de data past binnen de grondslag en het doel waarmee de gegevens in eerste instantie verzameld zijn. Dit wordt ook wel de verenigbaarheidstoets genoemd.**

2. **Ten tweede is de manier *hoe je informeert* over het inzetten van de techniek ook van belang. Daarbij vereist de AVG dat de techniek zelf wordt benoemd, maar moet wel duidelijk zijn waarom deze gegevens worden verzameld, door-gestuurd en gematcht én naar welke partijen de data gaat. Daarnaast moet je een mogelijkheid tot verzet aanbieden op het moment dat je de persoonsgegevens doorstuurt op grond van het gerechtvaardigd belang**

3. **Tot slot is het ook verstandig om *jouw AVG-rol goed in de gaten te houden*. Je bent zelf verwerkingsverantwoordelijke voor de persoonsgegevens die je verzamelt en doorstuurt. Google is verantwoordelijk voor de persoonsgegevens die zij van hun gebruikers verzamelen. Daarnaast zou het ook kunnen zijn dat zowel jouw organisatie als Google gezamenlijk verantwoordelijk is voor het matchingsproces. Hierover bestaan nog veel onduidelijkheden in het juridische landschap, maar je doet er goed aan om de gemaakte afspraken met Google te documenteren evenals de interne overwegingen om de tooling in te zetten.**

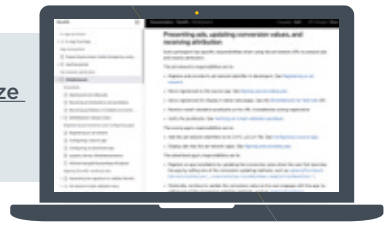
2.2.3 SKAdNetwork

Een enigszins onderbelichte techniek die wel degelijk binnen het kader van dit whitepaper past, is het SKAdNetwork van Apple. De attributietechniek werd in eerste instantie als extra optie gelanceerd om conversies binnen het Apple-ecosysteem privacyvriendelijker te meten. Daarentegen is het sinds de lancering van het eerdergenoemde ATT door Apple nog de enige manier om attributie te meten binnen het ecosysteem zelf. Daarbij is de techniek meerdere keren geüpdatet met nieuwe features en zitten we inmiddels in versie 4.0.

Het systeem werkt op basis van drie factoren:
1. Een aangemeld advertentienetwerk van een adverteerder;
2. Een plek waar de advertentie wordt getoond (in app of in de browser)
3. De app waarover is geadverteerd.

Wanneer een gebruiker op een advertentie klikt, wordt een code gekoppeld aan deze klik (en niet aan de gebruiker). Als de app waarover is geadverteerd binnen een bepaald timewindow wordt gedownload, ontvangt de adverteerder hierover informatie. Daarbij werkt Apple met verschillende fases van *crowd anonymity*. Dit houdt in dat hoe meer interactie er is met de campagne, hoe meer data geaggregeerd kan worden getoond.

Meer weten over SKAdNetwork? Bekijk deze uitleg van Apple.



Het lastige bij SKAdNetwork is dat het moeilijk inzichtelijk is welke data precies wordt verzameld. Vanuit de beschikbare documentatie lijkt het erop dat er weinig tot geen data wordt verzameld over de gebruiker of uit het device van de gebruiker, maar alleen over de advertentie zelf. In dat geval ben je niet aan de slag met persoonsgegevens en kun je deze techniek zonder juridische haken en ogen toepassen. In sommige gevallen kan er echter ook gebruik worden gemaakt van gegevens die op het apparaat gegenereerd worden. In dat geval heb je te maken met de cookieregels, maar zou je mogelijk een beroep kunnen doen op één van de uitzonderingen.

2.3 Technieken voor activatie

In deze laatste paragraaf komen de technieken aan bod die in ontwikkeling zijn om doelgroepen te bereiken met minder data óf met minder impact op de privacy van de betrokkene. Ook hier gaat het vaak over de vraag of het persoonsgegevens betreft en welke grondslag je kunt gebruiken, maar ook welke rol jouw organisatie heeft wanneer je samenwerkt met een derde partij. Daarnaast is het goed om te benoemen dat veel van deze technieken ook een analytisch onderdeel bevatten. Voor dat gedeelte kun je de kaders toepassen die in het voorgaande hoofdstuk zijn besproken.

2.3.1 First-party data matching

Misschien wel de meest geprezen techniek is het matchen van je eigen data met die van een derde partij óf kortgezegd: first-party data matching. De techniek bestaat al enige tijd in de markt, maar met de aangekondigde uitfasering van third-party cookies heeft het zeker een boost gekregen en wordt door veel partijen een first-party-datastrategie als een no-brainer gezien. Deze manier om je doelgroepen te bereiken óf juist uit te sluiten wordt inmiddels dan ook door meerdere partijen aangeboden en onder verschillende namen. De meest gebruikte oplossingen die we binnen DDMA hebben bekeken, zijn:

- Customer Match van Google
- Custom Audiences van Meta
- CRM-Matching door DPG
- LiveRamp ID

Daarnaast gaan we ook in op de zogenoemde ‘Clean Rooms’ waarbij persoonsgegevens via een tussenpersoon met elkaar worden gematcht in plaats van rechtstreeks bij een derde partij.

Customer Matching, Custom Audiences en CRM-Matching

Hoewel het om verschillende partijen gaat, kunnen we overkoepelend het juridisch kader schetsen bij deze technieken. Als er verschillen bestaan tussen de technieken, benoemen we deze. Daarbij gaan we ervanuit dat het in de meeste gevallen gaat om een verwerking van persoonsgegevens (hierover later meer). We kunnen hierin twee situaties van elkaar onderscheiden:

1. *Je wil first-party data matchen die nog verzameld moet worden*

Vanuit juridisch oogpunt is het startpunt hier de plek waarop je de informatie gaat verzamelen. Een account dat wordt aangemaakt, een bestelformulier of een API-koppeling: hier maak je de keuze voor de grondslag waarmee je de gegevens wil gaan

matchen én de informatie die je beschikbaar stelt. Ondanks dat dit in de praktijk vaak niet gebeurt, leeft de gedachte dat toestemming is vereist voor het matchen van third-party data. Dit zou je kunnen doen door een simpel aanvinkbaar hokje met daarbij de benodigde informatie waarvoor deze persoon toestemming geeft.

Toch is het niet altijd noodzakelijk om toestemming uit te vragen. Gegevensverzameling kan ook op de grondslag gerechtvaardigd belang. De Europese koepel van privacytoezichthouders (EDPB) heeft dit bevestigd in een richtlijn. Hierin staat aan de hand van voorbeelden beschreven wanneer geen toestemming is vereist en samengevat is dit mogelijk op basis van de volgende voorwaarden:

- Er moet een relatie zijn met de betrokkene.
- Er moet bij de verzameling duidelijk geïnformeerd zijn over het doorsturen en matchen van de data.
- Er moet bij de verzameling de mogelijkheid zijn geboden tot verzet tegen deze verwerking.
- Het mag enkel gaan om gelijksoortige producten/diensten.

Uiteindelijk is de hamvraag hier: verwacht de betrokkene dat diens gegevens worden ingezet voor deze doeleinden? Daarbij is het goed om op te merken dat de toezichthouders niet duidelijk uitleggen hoe de mogelijkheid tot verzet moet worden aangeboden. Dit zou bijvoorbeeld in een tweede laag kunnen, maar als je het privacyvriendelijker wil inrichten, bied je de mogelijkheid aan met een duidelijke keuze-optie (zoals een hokje).

2. Je wil first-party data matchen die je al hebt verzameld

Bij het matchen van data die je al eerder hebt verzameld en bijvoorbeeld hebt opgeslagen in een CRM-systeem, is het juridisch veel lastiger te onderbouwen dat je deze kunt matchen met een derde partij.

Het probleem is hierbij namelijk dat je de data eerder hebt verzameld op een andere grondslag en (hoogstwaarschijnlijk) niet hebt geïnformeerd over het doorsturen en matchen van de data.

De AVG kent een uitzondering voor deze situaties waarin je data 'verder verwerkt': **de verenigbaarheidstoets**. Als je kunt onderbouwen dat het doorsturen en matchen te rijmen valt met het eerdere doel van de verzameling, kun je dit op dezelfde grondslag doen. Daarbij moet je rekening houden met de volgende voorwaarden.

1. De oorspronkelijke verwerking is gebaseerd op het *gerechtvaardigd belang* óf de *uitvoering van een overeenkomst*. Immers: om deze verwerking op basis van toestemming te kunnen doen, had je deze al duidelijk moeten uitvragen op het moment van verzamelen.
2. Je moet kunnen onderbouwen dat de betrokkene verwacht dat diens gegevens voor deze doeleinden worden gebruikt op basis van de volgende factoren:
   a. ieder verband met het doel van verzamelen;
   b. het kader waarin de persoonsgegevens zijn verzameld (verhouding betrokkenen en verwerkingsverantwoordelijke);
   c. de aard van de gegevens (bijzondere persoonsgegevens en/of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten);

d. de (mogelijke) gevolgen van een verstrekking;
e. het bestaan van passende waarborgen (o.a. versleuteling of pseudonimisering);
f. de verwachtingen van de betrokkene (degene van wie een organisatie persoonsgegevens gebruikt).

Je kunt je voorstellen dat het vrijwel onmogelijk is om te onderbouwen dat een betrokkene verwacht dat diens gegevens worden ingezet voor matching als je hier niet over hebt geïnformeerd en het afwijkt van de oorspronkelijke verzameling (zoals het aanmaken van een account of het bestellen van een product). Voor reeds verzamelde data moet je daarom kijken of je het hele proces opnieuw kan doorlopen, waarbij je de stappen kunt doorlopen die in de paragraaf hiervoor zijn benoemd.

Denk na over je rol als organisatie

Zoals eerder genoemd bij Enhanced Conversions, is het belangrijk om goed in de gaten te houden wat de rol is van jouw organisatie wanneer je first-party data gaat matchen. In principe ben je zelf verwerkingsverantwoordelijke voor de persoonsgegevens die je verzameld en doorstuurt én is de derde partij verantwoordelijk voor de persoonsgegevens die zij van hun gebruikers verzamelen.

Daarnaast zou het ook kunnen zijn dat zowel jouw organisatie als de derde partij gezamenlijk verantwoordelijk is voor het matchingsproces. Hierover bestaan nog veel onduidelijkheden in het juridische landschap, maar je doet er goed aan om de gemaakte afspraken met de derde partij te documenteren evenals de interne overwegingen om de tooling in te zetten. Daarbij kunnen er verschillen zijn op de manier waarop je met deze partijen samenwerkt. Zo zul je bij Big Tech snel tegen standaardafspraken aanlopen, maar heb je bij een lokale partij als DPG Media vaak de mogelijkheid om afspraken te maken die meer passend zijn.

First-party data anoniem inzetten

Een ander veel gehoorde aanname in dit kader is dat gehashte data anoniem is, dus niet onder de AVG valt. Een gedeelte hiervan klopt: wanneer data anoniem is, hoeft geen rekening meer worden gehouden met de AVG. Het gedeelte dat niet klopt is dat hashing altijd zorgt voor anonimiteit. Over het algemeen wordt namelijk aangenomen dat ook gehashte data nog herleidbaar is naar een persoon en de AVG dus wel degelijk van toepassing is.

Wel is door een recente uitspraak van het Europees Hof (waarbij het hoger beroep nog loopt) de discussie over anonieme data opnieuw opgelaaid, maar voor de praktijk zal dit alleen impact hebben op het doorsturen van de data en niet hoe het proces aan de voorkant is ingeregeld. Immers: om de data mogelijk te kunnen anonimiseren moet het in eerste instantie verzameld worden waardoor de AVG daar wel van toepassing is.

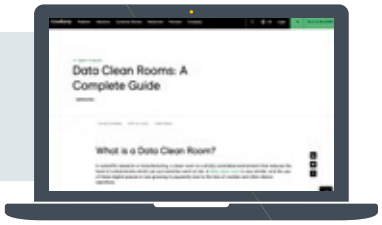
Meer informatie over de huidige status over anonieme data kun je vinden in dit artikel.

Data Clean Rooms

Een oplossing die meelift op de boost voor first-party datastrategieën, zijn de zogenaamde *Data Clean Rooms*. Dit is een digitale omgeving bij een (onafhankelijke) derde partij waarin first-party data van verschillende organisaties wordt samengebracht, ook wel *data collabaration* genoemd. Daarbij is het idee dat door *privacy enhancing techniques* (PET's, zoals encryptietechnieken en aggregatie) partijen niet van elkaar weten welke data er is ingeladen. Hiervoor wordt vaak een identificatienummer gebruikt (zoals de Ramp ID van LiveRamp) die door geen van de deelnemende partijen kan worden ontsleuteld. Vervolgens kun je alsnog inzichten opdoen of doelgroepen bereiken waarmee het verlies van datapunten met third-party cookies kan worden opgevangen. Voorbeelden van partijen die Data Clean Rooms aanbieden:

- Facebook
- Google
- Amazon
- Salesforce
- Adobe
- LiveRamp
- Snowflake
- Neustar
- InfoSum

Meer weten over Data Clean Rooms? Bekijk deze uitleg van LiveRamp.



Het juridische element zit bij deze Data Clean Rooms in de vraag of het nog om persoonsgegevens gaat wanneer je deze deelt met andere partijen. Met de huidige juridische ontwikkelingen valt er namelijk wat voor te zeggen dat er situaties zijn waarin het mogelijk niet meer om herleidbare gegevens gaat. Twee punten zijn daarbij belangrijk om mee te nemen wanneer je gebruik wil gaan maken van deze oplossingen.

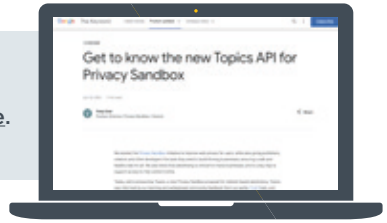
1. Om te beginnen moet het duidelijk zijn dat **er onderscheid bestaat tussen Data Clean Rooms bij de partij met wie je direct samenwerkt én Data Clean Rooms die onafhankelijk opereren van alle partijen** die samenwerken. In het eerste geval vindt de bewerking van de data namelijk vaak plaats binnen de omgeving van de andere partij waardoor moeilijker te onderbouwen is dat zij de versleutelde data niet kunnen herleiden tot een individu. Wanneer je daarentegen gebruik maakt van een onafhankelijke partij (een trusted third-party) vindt de versleuteling vaak plaats bij de organisaties zelf voordat het naar de onafhankelijke partij gaat. Hierdoor zou je kunnen stellen dat het voor de onafhankelijke partij én de partij waarmee wordt samengewerkt niet mogelijk is om de data te herleiden.

2. Vervolgens is het belangrijk om op te merken dat **ondanks dat het privacyvriendelijker is om data niet ongecontroleerd te delen met meerdere partijen, het AVG-technisch geen directe vrijwaring biedt**. Immers: voordat je de data deelt met een Data Clean Room (onafhankelijk of niet) gaat het om persoonsgegevens en moet je voldoen aan alle verplichtingen van de AVG. Vervolgens is het dus afhankelijk van de Data Clean Room die je kiest of je het verder inzetten van de data als anoniem kunt beschouwen. Is dat het geval? Dan vrijwaart het je in de praktijk met name van de administratieve plichten die de AVG kent, zoals het hebben van een verwerkersovereenkomst. Voor het voorafgaande proces blijf je verantwoordelijk en zou je bij een datalek of onjuiste verwerking een boete kunnen ontvangen.

2.3.2 Topics API

Een andere alternatieve techniek die buiten het kader van first-party data valt, is de nieuwe Topics API van Google. Deze toepassing is bedoeld om het verlies van (hyper)personalisatie door middel van third-party cookies op te vangen. Strandde het eerste initiatief van Google (FLoC) nog in schoonheid na grote kritiek, is de Topics API inmiddels al gedeeltelijk live. De insteek van de techniek is dat Chrome-gebruikers niet langer gepersonaliseerde advertenties te zien krijgen op basis van opgebouwde profielen, maar op basis van hun interesses. Deze interesses worden in maximaal 3 categorieën opgeslagen in de browser zelf. Daarbij is de context van de webpagina's die worden bezocht leidend voor welke interesses worden toegekend aan een gebruiker. Inmiddels zijn er 469 categorieën die toegekend kunnen worden en waar adverteerders hun campagnes op kunnen inrichten.

Meer weten over Topics API?
Bekijk dan deze uitleg van Google.



Vanuit juridisch perspectief oogt de Topics API als een zeer privacyvriendelijke oplossing: de categorieën worden enkel opgeslagen in de browser van de gebruiker zelf, de categorieën worden na 3 weken automatisch verwijderd én er worden controlemechanismes ingebouwd voor gebruikers om bijvoorbeeld bepaalde categorieën op voorhand te blokkeren. Daarnaast is het grote voordeel voor organisaties dat de verantwoordelijkheid voor het verzamelen van de interesses bij Google ligt, je bent zelf enkel verantwoordelijk voor de advertentie die wordt getoond.

Toch is er ook kritiek vanuit juridisch perspectief op een aantal onderdelen. Om te beginnen worden er door Google nog steeds gegevens verzameld en opgeslagen in de browser. Google deelt deze persoonsgegevens niet met andere partijen, die krijgen namelijk enkel de interesses te zien waarop ze kunnen adverteren. Ook worden deze gegevens zoveel mogelijk versleuteld door middel van Privacy Enhancing Techniques. Toch lijkt het erop dat Google op basis van browsergegevens online gedrag (websitebezoeken) kan analyseren en deze in theorie aan personen kan koppelen. De kritiek vanuit de markt daarbij is dat Google op deze manier voor zichzelf een monopolie vergaard via deze inzichten.

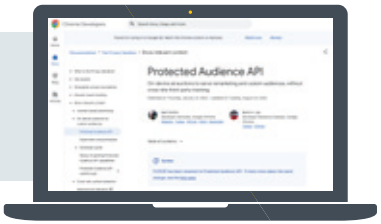
Over kritiek uit de markt gesproken: andere browsers, zoals Safari en Firefox, staan er niet om te springen om deze techniek te implementeren in hun systemen. Google leek in het begin nog in te zetten op een nieuw advertentiesysteem voor de gehele sector, maar andere partijen zijn bang voor een monopolie-positie. Daarmee lijkt het dat de Topics API enkel beschikbaar zal zijn in Chrome.

Tot slot betekent het verzamelen en opslaan van de data dat de cookiewet van toepassing is op deze data. Dat betekent dat voor het aan kunnen zetten hiervan Google, in ieder geval voor de advertentiedoeleinden, toestemming nodig heeft van de Chrome-gebruiker. Inmiddels heeft Google de Topics API-optie uitgerold onder gebruikers middels een toestemmingsscherm wanneer Chrome voor het eerst wordt ingeschakeld. Daar kwam enige kritiek op omdat het aanzetten van de techniek werd geduid als het verbeteren van je privacy, terwijl gebruikers die hun advertentievoorkeuren strikt hadden ingesteld juist een deel van hun privacy opgeven. Daarnaast vond men de informatie over de techniek en welke gegevens precies worden verzameld, lastig te achterhalen uit de documentatie. Overigens is de API achteraf ook nog in te schakelen door gebruikers via de browserinstellingen.

2.3.3 Protected Audiences API

Nog een initiatief uit de Privacy Sandbox van Google die een naamsverandering kent is de Protected Audiences API. Deze techniek, formerly known as FLEDGE, moet het proces van *Real-Time Bidding* privacyvriendelijker maken door het biedings-proces plaats te laten vinden op het apparaat zelf. Net als bij de Topics API zorgt dit ervoor dat persoonsgegevens niet meer worden gedeeld met derde partijen. Deze krijgen enkel te inzichten terug zoals of een advertentie heeft gewonnen en is geplaatst. Daarbij werkt de Protected Audiences API samen met de Topics API om advertenties te laten zien en de kwaliteit daarvan te meten gemeten van de advertentie zonder dat hierbij persoonsgegevens worden gedeeld met derde partijen. Hiervoor gelden dan ook dezelfde juridische knelpunten als hierboven zijn aangehaald.

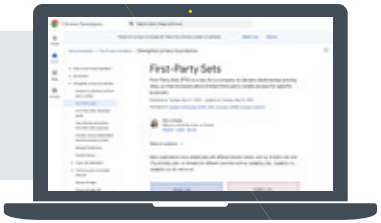
Meer weten over Protected Audiences API?
Bekijk de uitleg van Google.



2.3.4 Related Websites Sets

Dan nog een techniek uit de Privacy Sandbox die niet veel wordt besproken, maar wel interessant is: de Related Websites Sets. Deze alternatieve techniek (eerder nog bekend onder de naam First-Party Sets) moet ervoor zorgen dat partijen met brede domeinen (meerdere websites) binnen een domein data kunnen blijven delen. Nu denk je wellicht: zijn dat dan geen third-party cookies? Dat klopt: via deze techniek staat Chrome het toe dat op beperkte wijze third-party cookies ingezet kunnen worden. Op die manier kan een gebruiker bijvoorbeeld ingelogd blijven over meerdere websites, maar kan er ook gepersonaliseerd worden. Daarvoor moet wel aangetoond kunnen, aan de hand van richtlijnen, dat deze domeinen een relatie met elkaar hebben (bijvoorbeeld omdat het binnen een merk hoort) en daarmee een set vormen.

Meer weten over Related Websites Sets?
Bekijk deze uitleg van Google.



Voor het juridische perspectief kunnen we grotendeels terug-verwijzen naar wat we eerder hebben gezegd in de paragraaf over het inzetten en verzamelen van first-party data. Er is een grondslag vereist voor het verzamelen van de websitegegevens waarbij je aan moet sluiten bij de cookiewet. Ook moet er duidelijke informatie beschikbaar zijn over het onderling delen van de data tussen de websites binnen het domein.

Een interessanter vraagstuk is hier misschien meer van ethische aard. Zo wordt dit initiatief onder andere gesteund door de W3C, de wereldwijde organisatie voor webstandaarden. Op zich is dit verklaarbaar omdat het inzetten ervan ook in het voordeel van de gebruiker werkt. Zonder een dergelijke oplossing zou een gebruiker ook op iedere pagina en in elk land binnen hetzelfde domein opnieuw een cookiebanner krijgen óf moeten inloggen. Daarbij is het wel van belang dat gewaarborgd wordt dat het gaat om websites die een duidelijke relatie met elkaar hebben.

Daarnaast laat deze techniek toch een kleine opening voor grote merken om cross site of zelfs cross device (app/web) te tracken wat een gebruiker aan het doen is en de cookiebanners een relevant topic blijven.

2.3.5 Contextual Advertising

Tot slot dan nog de techniek die aan een tweede leven bezig lijkt: Contextual Advertising. Hierbij worden de getoonde advertenties gekoppeld aan de context van de webpagina die wordt bezocht. Hierbij worden geen extra persoonsgegevens verwerkt en worden enkel de advertenties zelf gemeten. Dit maakt ook dat het door sommigen wordt gezien als de meest privacyvriendelijke oplossing. Toch doe je er goed aan om ook bij contextual kritisch te blijven kijken naar hoe de techniek werkt. Hoe meer parameters worden gebruikt, hoe je dichter je bij een mogelijk omslagpunt voor persoonsgegevens komt. Daarbij moet je namelijk ook meenemen dat je als website vaak nog wel andere gegevens verzamelt. Bijvoorbeeld voor analytische doeleinden of als iemand is ingelogd. De combinatie van parameters plus andere gegevens maakt dat je met contextual mogelijk alsnog persoonsgegevens aan het verzamelen bent.

Zoals gezegd is de techniek weer in opkomst, mede dankzij de resultaten die de STER (het reclamebedrijf van de publieke omroepen) deelde. Volgens STER was hun contextual advertising-strategie minstens net zo effectief als adverteren op basis van third-party cookies. En ondanks dat het door velen wordt beschouwd als een stap terug in de tijd, wordt de techniek nu flink doorontwikkeld, bijvoorbeeld door DPG Media.

Het is goed om je realiseren dat adverteerders sterk afhankelijk zijn van de mogelijkheden die mediapartners bieden. Op dit moment zijn er maar een beperkt aantal netwerken volledig op contextueel adverteren gebaseerd. Eén voorbeeld daarvan is STER, maar denk ook aan de New York Times. Andere in het oog springende netwerken zijn schaars. Google AdSense begon bijvoorbeeld jaren terug als contextueel advertentienetwerk, maar nu worden advertentieruimtes óók verkocht op basis van gebruikersprofielen. Dus los van de wil om contextueel te adverteren moet er ook een netwerk worden gevonden waarmee dit mogelijk is.

2.4 Privacy Enhancing Techniques

Eerder in dit whitepaper haalden we Privacy Enhancing Techniques (PET's) al even aan. Dit zijn technieken die ontwikkeld worden om persoonsgegevens of het proces van de verwerking zo te bewerken dat de privacy beter wordt gewaarborgd. Ondanks dat de term privacy er vrij duidelijk in staat, zijn PET's over het algemeen eigenlijk een beveiligings-maatregel. Door het bewerken van de persoonsgegevens wordt het namelijk lastiger om te de data te herleiden en hier bijvoorbeeld onjuiste dingen mee te doen. Er wordt door veel partijen hard gewerkt aan nieuwe vormen van PET's die er mogelijk voor zorgen dat data in de toekomst als niet herleidbaar kan worden beschouwd.

Voorbeelden van PET's zijn:

1. **Versleuteling**
   a. Technieken, zoals end-to-end encryptie waarbij de data alleen beschikbaar is voor de verzender en de ontvanger.

2. **Transport Layer Security (TLS)**
   a. Dit beveiligt de verbinding tussen de browser van een gebruiker en de website die ze bezoeken.

3. **Anonimisering**
   a. Masking: Vervangt, verbergt of vervormt oorspronkelijke gegevens om gevoelige informatie te beschermen terwijl de bruikbaarheid behouden blijft.
   b. Pseudonimisering: Vervangt of verwijdert directe identificatoren, zoals namen, door pseudoniemen om de identiteit van individuen te beschermen.

4. **Differentiële Privacy**
   a. Deze statistische techniek voegt ruis of verstoring toe aan gegevens op een manier zonder dat de uitkomst wordt beïnvloed.

5. **Proxy-servers**
   a. Deze fungeren als tussenpersonen tussen het apparaat van een gebruiker en het internet, waardoor hun IP-adres en locatie worden geanonimiseerd.

6. **Multi-Party Computation**
   a. Hiermee kunnen meerdere partijen gezamenlijk een berekening maken, terwijl de invoer privé blijft.

7. **Tokenisatie**
   a. Vervangt gevoelige gegevens door tokens of symbolen. Bijvoorbeeld, in betalingsverwerking worden creditcard-nummers vervangen door tokens.

3 Een blik op de toekomst

In de ondertitel van dit whitepaper beloven we het meest complete overzicht van alternatieven voor third-party cookies van juridisch perspectief te tonen. We hopen dat we die belofte waar hebben kunnen maken. Tegelijkertijd verandert ons vakgebied elke dag en kan deze publicatie alweer snel achterhaald zijn. Daarom hebben we onze juridische uitleg, net als de ePrivacy richtlijn, zoveel mogelijk techniekneutraal gemaakt. Mochten er in de toekomst nieuwe technieken opkomen of ontwikkeld worden, dan kun je aan de hand van dit whitepaper zélf tot een compliant inzet te komen. Uiteraard blijft het vervolgens altijd de vraag hoe een toezichthouder of een rechter hier naar kijkt. Bij grote ontwikkelingen of veranderingen zullen we dit whitepaper updaten.

Daarnaast zien we een duidelijke verschuiving naar méér privacyvriendelijke oplossingen. Dat betekent dat we ook in de nabije toekomst nieuwe maatregelen vanuit Big Tech, nieuwe technieken én nieuwe wetgeving kunnen verwachten. Ook zien we ook dat consumenten zich steeds bewuster worden van hun recht op privacy en hoe hier mogelijk een inbreuk op wordt gemaakt. Wil je jouw doelgroep blijven bereiken, dan moet je mee in deze ontwikkelingen. Dat begint bij het inrichten van interne processen en zorgen voor een goede samenwerking tussen legal, marketing, data en IT. Alleen zo kun je nieuwe technieken succesvol en verantwoord toepassen en de privacy van jouw klanten waarborgen.

Uiteraard volgen we bij DDMA deze ontwikkelingen op de voet om onze leden te kunnen voorzien van een waardevol advies over verantwoord gebruik van data en technologie voor marketingdoeleinden. Mocht je een vraag hebben over de implementatie van nieuwe technologieën of andere juridische vraagstukken, neem dan contact op met onze legal counsels via legal@ddma.nl.

Colofon

Uitgever

DDMA
WG Plein 185
1054 SC Amsterdam
T: 020 4528413
E: info@ddma.nl
W: www.ddma.nl

Heb je vragen of opmerkingen over dit whitepaper? Stuur dan een e-mail naar legal@ddma.nl.

Eindredactie
Erik Molkenboer
Teamlead Content & Community bij DDMA

Auteurs

Romar van der Leij
Legal Counsel
DDMA

Frank de Vries
Senior legal counsel
DDMA

OVER DDMA

DDMA is de grootste brancheverenigingen voor marketing en data. Wij zijn een netwerk van ruim 360 merken, non-profits, uitgevers, bureaus en tech-leveranciers die data succesvol en verantwoord willen inzetten voor marketingdoeleinden. Wij duiden ontwikkelingen op het gebied van technologie, regelgeving en ethiek en brengen marketeers, dataspecialisten en juristen bij elkaar om hen te helpen groeien in hun vak. Ook bevorderen we zelfregulering en zijn we gesprekspartner van beleidsmakers en toezichthouders.

Ga voor alle DDMA-publicaties naar: ddma.nl/kennisbank