MARKETING DATA LITERACY

EEN ROADMAP VAN PERSOONLIJKE DATA IN HET DIGITALE ECOSYSTEEM

Maart 2025

Voorwoord: De reis van persoonlijke data in het digitale ecosysteem

IIn de digitale wereld laat elke online-actie sporen achter. Om inzicht te geven in deze data-ecosystemen en hoe persoonlijke gegevens door verschillende 'spelers' worden verwerkt, volgen we een dag uit het leven van Peter.

Peter begint zijn ochtend, zoals velen van ons, met een snelle blik op zijn telefoon. Terwijl hij zijn favoriete sportsite bezoekt en door sociale media browset, laat hij – vaak zonder het zelf te beseffen – een pad van gegevens achter dat organisaties gebruiken om hem een op maat gemaakte digitale ervaring te bieden.

Van first-party data tot third-party data: een kijkje achter de schermen

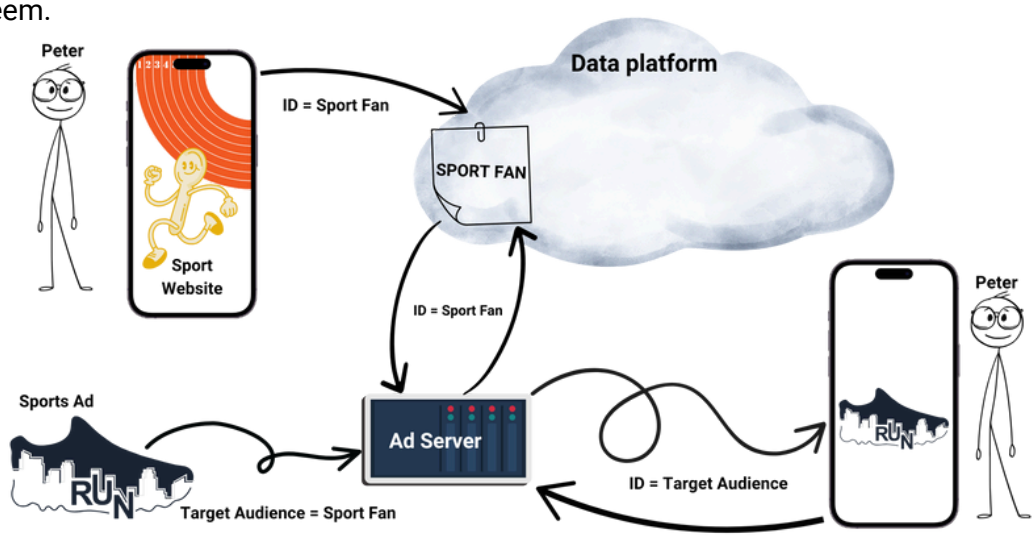
Bij zijn eerste stop verzamelt de nieuwssite first-party data, zoals Peters interesses en voorkeuren, die gebruikt worden om zijn ervaring te personaliseren. Tegelijkertijd worden echter ook third-party data door partners en advertentiebedrijven verzameld, die zijn activiteiten verder analyseren en combineren met andere informatie om een profiel op te bouwen dat buiten de nieuwssite zelf gaat. Deze gegevens creëren een breder inzicht in Peters interesses, wat leidt tot advertenties die soms verrassend nauwkeurig zijn.

Toestemming en tracking in een datagedreven ecosysteem

Als Peter doorgaat met browsen, verschijnt een toestemmingspop-up – de bekende vraag of hij cookies accepteert. Vaak zonder er veel over na te denken, klikt hij op "Accepteren", waardoor hij zijn gegevens voor verschillende doeleinden beschikbaar stelt: van gepersonaliseerde advertenties tot diepgaande analyses die zijn digitale ervaring verder vormgeven. Wat hij zich misschien niet volledig realiseert, is dat hij door deze actie zijn gegevens beschikbaar stelt aan een netwerk van partijen die zijn online gedrag blijven volgen.

Tegen de tijd dat Peter zijn ochtend heeft afgerond, heeft hij – zoals velen – ongemerkt deelgenomen aan een complex data-ecosysteem. Zijn activiteiten worden opgeslagen, geanalyseerd, en gebruikt om zowel zijn ervaring te personaliseren als waardevolle inzichten te genereren voor bedrijven.

In de volgende hoofdstukken van deze whitepaper verkennen we in detail de verschillende fasen die persoonlijke data zoals die van Peter doorloopt en de rol van de spelers binnen dit ecosysteem.



INDEX

PETERS DATA VERZAMELEN EN BEHEREN VANUIT EEN ADVERTEERDERSPERSPECTIEF

1. Peters data verzamelen en beheren vanuit een adverteerdersperspectief

Elke interactie die Peter heeft met een site of advertentie levert waardevolle informatie op, die zorgvuldig wordt vastgelegd in een complex ecosysteem. Dit systeem is ontworpen om marketinginspanningen te verfijnen, content te personaliseren en het conversiepad te optimaliseren. Het verzamelen van Peters data gebeurt op verschillende manieren en via diverse technieken.

Wanneer Peter bijvoorbeeld op een advertentie klikt of producten browset, vangt de adverteerder first-party data op, zoals klikgedrag, sessieduur en productinteresses. Deze gegevens vormen de basis voor realtime personalisatie, waarbij inhoud en aanbiedingen dynamisch worden aangepast aan Peters interesses. Naast first-party data worden er ook third-party data verzameld, afkomstig van externe bronnen zoals gegevensuitwisselingen, DSP's en sociale media-API's. Deze third-party data voegen cross-platform inzichten toe die een breder profiel van Peters interesses bieden, zodat adverteerders hem nog relevanter kunnen benaderen.

Technische analyse: datatypes

Om data effectief te verzamelen en in te zetten, moeten adverteerders onderscheid maken tussen verschillende datatypes, elk met eigen bronnen, gebruiksrechten en toepassingen:

1. First-party data

- **Definitie:** Gegevens die rechtstreeks door de adverteerder worden verzameld, bijvoorbeeld via Peters interacties op hun eigen website of app.
- **Voorbeelden:** Klikgedrag, aankoopgeschiedenis, en ingevulde formulieren zoals e-mails.
- **Voordelen:** Hoge relevantie en nauwkeurigheid, doordat de data direct van de gebruiker komt. Ook eenvoudig te beheren binnen privacyregels, omdat de data in eigen beheer is.
- **Uitdagingen:** Het vereist vaak technologische investering (zoals CRM-systemen) om deze data te verzamelen en beheren, en het bereik is beperkt tot bestaande klanten.

2. **Second-party data**

- **Definitie:** First-party data van een partnerorganisatie, gedeeld op basis van een directe samenwerking.
- **Voorbeelden:** Gegevens die tussen een retailer en een merk worden gedeeld.
- **Voordelen:** Betrouwbaar en van hoge kwaliteit, omdat het van een vertrouwde bron komt met een vergelijkbare doelgroep.
- **Uitdagingen:** Afhankelijk van partnerschappen, wat juridische overeenkomsten en technische integraties vereist. Ook moet er zorgvuldig omgegaan worden met de privacy van gedeelde data.

3. **Third-party data**

- **Definitie:** Gegevens die door een externe partij zijn verzameld zonder directe relatie met de gebruiker.
- **Voorbeelden:** Demografische gegevens die zijn ingekocht via gegevensbrokers, of doelgroepsegmenten van advertentienetwerken.
- **Voordelen:** Grootschalig en helpt nieuwe doelgroepen te bereiken.
- **Uitdagingen:** Toegenomen privacyzorgen en minder nauwkeurigheid door de afstand tot de bron, en regelgevende beperkingen zoals GDPR.

Tools voor gegevensverzameling: cookies en tags

Data wordt verzameld via twee belangrijke technieken: cookies en tags. Een eenvoudige analogie verduidelijkt het verschil tussen cookies en tags. Stel je voor dat Peter een kroegentocht maakt:

Bij de eerste kroeg krijgt hij een stempel op zijn pols (cookie) die zijn bezoek vastlegt. Als hij drankjes bestelt, ontvangt hij een bon (tag) met details over zijn bestelling. Bij elke kroeg die hij bezoekt, krijgt hij een nieuwe bon, maar de stempel blijft hetzelfde en identificeert hem bij terugkeer in eerdere kroegen. Hierdoor herkennen de kroegen hem, en kan de uitsmijter op basis van de bonnen zien dat Peter een frequente klant is, wat hem extra voordelen oplevert.

Samengevat:

- Een **cookie** (stempel) onthoudt wie Peter is en wanneer hij eerder is geweest.
- Een **tag** (bon) registreert details over zijn acties tijdens zijn bezoek.

Een meer technische omschrijving van beide technieken:

- **Tags** zijn stukjes code die specifieke acties en gedragingen registreren.
  - **Analysetags:** Volgen gebruikersgedrag en interacties, zoals met Google Analytics.
  - **Conversietags:** Meten de effectiviteit van advertenties door conversies te volgen.
  - **Remarketingtags:** Targeten gebruikers met advertenties nadat ze een site hebben bezocht, zoals met de Facebook Pixel.
  - **Tag Management Systems (TMS):** Tools zoals Google Tag Manager helpen bij het beheren en implementeren van tags zonder directe wijziging aan de websitecode.

- **Cookies** zijn kleine tekstbestanden die door de website op Peters apparaat worden geplaatst om informatie over zijn sessie en voorkeuren op te slaan.
  - **Verschillende soorten cookies:**
    - **Functionele en prestatiecookies:** Deze onthouden sessies en voorkeuren om de gebruikservaring te verbeteren.
    - **Advertentie- en trackingcookies:** Bevatten first-party en third-party cookies die nodig zijn voor personalisatie en targeting.
    - **Beveiligingscookies:** Versterken de beveiliging, zoals ‘HTTP-only’ cookies.
    - **Historische cookies:** Zoals Flash cookies en zombie cookies, die steeds minder vaak voorkomen.
  - **Meest gebruikte cookies:**
    - **First-party cookies:** Ingesteld door de website zelf om gebruikersinstellingen en sessies te beheren.
    - **Third-party cookies:** Ingesteld door externe partijen om gebruikersgedrag over meerdere sites te volgen en een profiel op te bouwen.

Een meer technische omschrijving van beide technieken:

Cookies zijn vaak onderwerp van privacydiscussies, vooral in het kader van GDPR en andere wetgeving. Hoewel sommige cookies essentieel zijn voor een prettige online ervaring, zoals first-party cookies die voorkeuren en inlogstatussen onthouden, is er veel kritiek op third-party cookies vanwege hun vermogen om gebruikers over meerdere websites te volgen.

2

PRIVACY EN TOESTEMMINGSMECHANISMEN IN HET DIGITALE LANDSCHAP

Terwijl adverteerders zich richten op het verzamelen en benutten van gegevens zoals die van Peter, zijn er specifieke rechten die Peter als gebruiker beschermen. Tegelijkertijd moeten bedrijven zich houden aan wet- en regelgeving om te waarborgen dat de gegevens van individuen op een veilige en transparante manier worden beheerd. Dit hoofdstuk beschrijft Peters rechten onder de huidige wetgeving en de kaders waaraan adverteerders moeten voldoen.

Peters rechten: toestemming en Privacy by Default

De invoering van de GDPR (General Data Protection Regulation) in 2018 heeft de privacyrechten van individuen zoals Peter aanzienlijk versterkt. Hij heeft hierdoor de volgende rechten met betrekking tot zijn gegevens:

- **Toestemming:** Voordat persoonlijke gegevens verwerkt mogen worden, moet expliciete toestemming worden verkregen. Dit betekent dat adverteerders geen toestemming kunnen verstoppen in lange, complexe voorwaarden. Toestemming moet vrij, specifiek en geïnformeerd zijn, en Peter kan deze op elk moment intrekken
- **Privacy by Default:** Onder de GDPR geldt dat privacy de standaardinstelling is. Dit betekent dat diensten en producten standaard met de hoogste privacybescherming moeten zijn ingericht, zonder dat de gebruiker hiervoor iets hoeft in te stellen. Data wordt beperkt verzameld en uitsluitend gebruikt voor noodzakelijke doeleinden, en bedrijven moeten zorgen voor veilige opslag van gegevens.

Naast deze basisrechten heeft Peter ook andere rechten, waaronder:

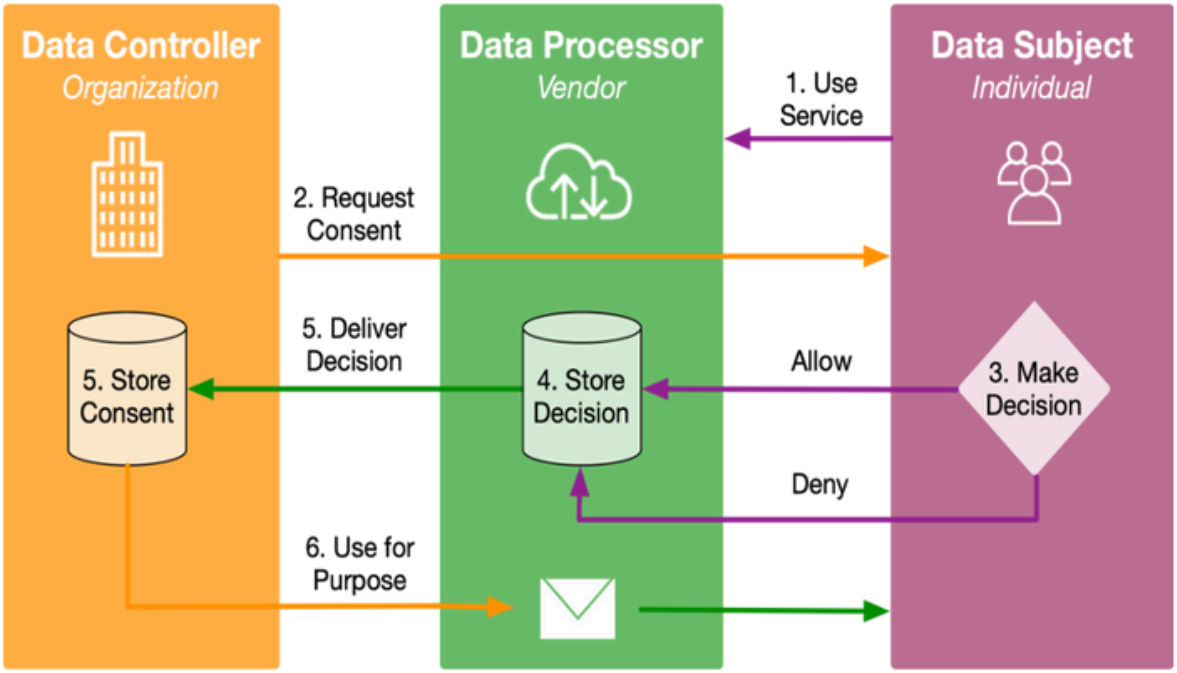
- **Het recht om vergeten te worden:** Hiermee kan Peter verzoeken om verwijdering van zijn gegevens.
- **Het recht op gegevensoverdraagbaarheid:** Dit stelt Peter in staat zijn gegevens naar een andere dienstverlener over te dragen.
- **Het recht op inzage:** Peter kan opvragen welke gegevens zijn verzameld en hoe deze worden gebruikt.

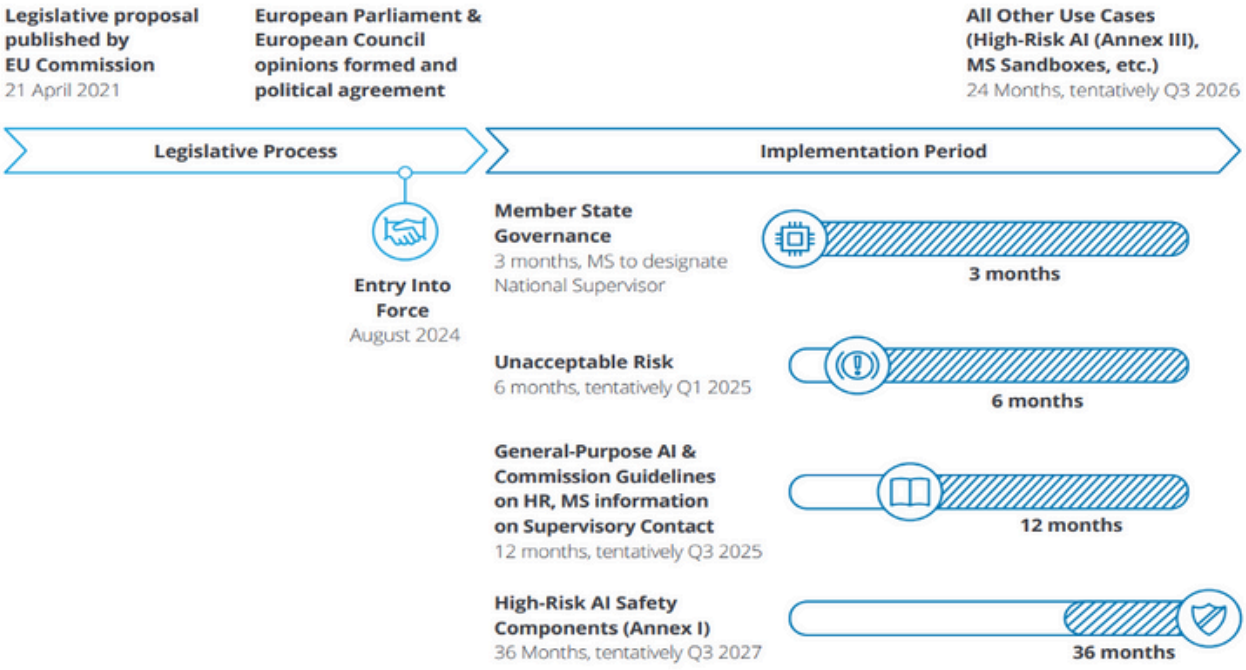
Wet- en regelgeving voor bedrijven

Adverteerders en andere bedrijven die met data werken, moeten zich houden aan meerdere regelgevingen om te waarborgen dat de rechten van gebruikers zoals Peter worden gerespecteerd. De belangrijkste wettelijke kaders zijn:

- **·GDPR (2018):** Deze Europese regelgeving stelt strikte eisen aan het verzamelen, opslaan en verwerken van persoonlijke gegevens. Bedrijven die binnen de EU opereren of data verwerken van EU-burgers, moeten zich houden aan principes zoals rechtmatigheid, eerlijkheid, transparantie en gegevensminimalisatie. GDPR dwingt bedrijven tot transparantie over hun datapraktijken, geeft gebruikers controle over hun eigen data en stelt hoge boetes voor inbreuken.
- **·Digital Services Act (DSA, 2022):** De DSA richt zich op het reguleren van online-platforms en heeft als doel een veilig en transparant digitaal landschap te creëren. Het reguleert onder andere de verantwoordelijkheid van platforms om illegale inhoud en schadelijke praktijken aan te pakken, wat de privacy en veiligheid van gebruikers verder ondersteunt.
- **·Digital Markets Act (DMA):** De DMA richt zich specifiek op grote online-platforms (de “poortwachters”) om eerlijke concurrentie te bevorderen en misbruik van marktmacht te voorkomen.

- **Artificial Intelligence Act (AI Act):** Hoewel deze wet zich richt op AI-systemen, is hij relevant voor bedrijven die AI inzetten voor dataverzameling en analyse. De AI Act verplicht organisaties om ethisch met AI om te gaan en beperkt het gebruik van AI met een hoog risico voor de privacy van gebruikers.





Wat gebeurt er zodra Peter toestemming geeft?

Wanneer Peter toestemming geeft via een Consent Management Platform (CMP) op een website of app, zoals door op "Ik ga akkoord" te klikken, start hij een reeks gegevensverwerkingsactiviteiten. Hoewel dit een eenvoudige handeling lijkt, geeft Peter feitelijk toestemming aan de website of dienst om specifieke informatie over hem te verzamelen. Afhankelijk van het platform kan deze informatie variëren van zijn IP-adres en locatie tot zijn browsegedrag en persoonlijke voorkeuren.

Websites maken vaak gebruik van trackingtechnologieën zoals cookies en tags om Peters activiteit over verschillende websites en appsessies te monitoren. Met zijn toestemming kunnen deze gegevens worden verzameld en gebruikt voor uiteenlopende doeleinden, zoals het verbeteren van de gebruikerservaring of het tonen van gerichte advertenties. In sommige gevallen worden Peters gegevens zelfs gedeeld met derde partijen, zoals advertentienetwerken (bijv. Meta, Spotify, Google) of analyseproviders (bijv. Google, Adobe, Comscore).

Verantwoordelijkheid bedrijfsleven

Zodra toestemming is verleend, ligt de verantwoordelijkheid bij de organisatie om Peters gegevens op een verantwoorde manier te beheren. Onder de GDPR moeten bedrijven:

- **duidelijke en wettige redenen** hebben voor de gegevensverwerking en gebruikers informeren over de specifieke doeleinden van gegevensverzameling;
- **transparantie** bieden om het vertrouwen van gebruikers te behouden, door helder te communiceren welke gegevens worden verzameld en waarom;
- **beschermende maatregelen** implementeren, zoals versleuteling en anonimisering, om persoonlijke gegevens te beveiligen en het risico op inbreuken te minimaliseren.

Het is belangrijk op te merken dat toestemming geen blanco goedkeuring is. Peter behoudt het recht om op elk moment zijn toestemming in te trekken. Zodra hij dit doet, is de organisatie verplicht om te stoppen met het verwerken van zijn gegevens en deze, indien gevraagd, te verwijderen. Bovendien stelt GDPR dat bedrijven de kwaliteit van hun dienstverlening niet mogen verminderen voor gebruikers die toestemming weigeren, waardoor Peter meer controle behoudt over zijn privacy.

Naast deze basisrechten heeft Peter ook andere rechten, waaronder:

De GDPR en andere regels benadrukken het belang van transparantie en naleving voor adverteerders en platforms. Om in lijn te blijven met deze wetgeving, moeten adverteerders:

- **transparantie bieden:** gebruikers moeten altijd duidelijk en begrijpelijk worden geïnformeerd over welke data wordt verzameld, voor welk doel en hoe lang deze bewaard wordt;
- **toestemming verkrijgen:** het gebruik van data, vooral door middel van c ookies en trackingmethoden, vereist expliciete toestemming van de gebruiker, die op elk moment moet kunnen worden aangepast of ingetrokken;
- **gegevenskwaliteit en -veiligheid waarborgen:** het gebruik van high-quality first-party data is doorgaans de meest privacy-vriendelijke optie, maar bedrijven moeten ervoor zorgen dat alle verzamelde gegevens veilig worden opgeslagen en alleen worden gebruikt voor de gespecificeerde doeleinden.

IEDERS ROL IN DE TOEKOMST

De informatie die we tot nu toe hebben behandeld, laat zien hoe belangrijk het is dat Peter en andere gebruikers controle behouden over hun gegevens, en welke verantwoordelijkheden bedrijven dragen om die privacy te waarborgen. In de kern komt dit neer op een "gegevensafweging": de impliciete of expliciete overeenkomst tussen gebruikers en dienstverleners, waarbij gebruikers hun persoonlijke informatie delen in ruil voor toegang tot diensten, functies of inhoud.

Deze gegevensafweging vormt de basis van de moderne internet-economie. Toegang tot veel van de gratis diensten die we dagelijks gebruiken — sociale media, zoekmachines, nieuwssites — wordt vaak gefinancierd door gerichte advertenties die afhankelijk zijn van het verzamelen van gebruikersdata. De vraag blijft echter of gebruikers, zoals Peter, zich volledig bewust zijn van de gegevens die ze opgeven en of de waarde die zij hiervoor terugkrijgen in verhouding staat tot de prijs die ze betalen in termen van privacy.

Hoewel gegevensverzameling veel voordelen biedt, zoals gepersonaliseerde ervaringen en gebruiksgemak, gaat dit altijd gepaard met privacyrisico's. Gegevensinbreuken, ongeoorloofde gegevensdeling en de creatie van gedetailleerde gebruikersprofielen kunnen het vertrouwen van gebruikers schaden. Regelgeving zoals de GDPR probeert dit evenwicht te herstellen door gebruikersrechten te versterken en bedrijven verantwoordelijk te houden voor transparantie en ethisch gegevensbeheer.

De uitdaging voor de toekomst is duidelijk: adverteerders en dienstverleners moeten blijven zoeken naar een manier om gegevens op een ethisch verantwoorde manier te benutten, waarbij de privacy van gebruikers altijd gewaarborgd blijft. In dit hoofdstuk kijken we vooruit en verkennen we de stappen die bedrijven kunnen nemen om deze balans te vinden en het vertrouwen van hun gebruikers te behouden.

De rol van de adverteerder

Adverteerders moeten zorgvuldig blijven omgaan met verschillende technische aspecten van gegevensbeheer. Gegevensprivacy en naleving zijn niet-onderhandelbaar. Hoewel Peter mogelijk snel heeft ingestemd met cookietracking, moeten adverteerders ervoor zorgen dat ze zich houden aan privacykaders zoals GDPR en CCPA. Dit omvat het handhaven van transparantie over gegevensgebruik en het implementeren van mechanismen voor de rechten van betrokkenen, zoals het intrekken van toestemming of het verwijderen van gegevens.

Een ander cruciaal element is gegevensintegratie en -hygiëne. Adverteerders hebben vaak te maken met meerdere gegevensbronnen. Een goede integratie via CDP's (Customer Data Platforms) of DMP's (Data Management Platforms) zorgt ervoor dat Peters gegevens worden opgeslagen in een uniek profiel, waardoor silo's worden geminimaliseerd en de nauwkeurigheid van personalisatie-algoritmen wordt gemaximaliseerd.

Ten slotte zijn frequentiecap en cross-channel optimalisatie essentieel om advertentiemoeheid te voorkomen. Met geavanceerde programmatic ad serving en tracking over kanalen heen, moeten adverteerders intelligente limieten op advertentieblootstelling toepassen, terwijl ze ervoor zorgen dat Peter een gebalanceerd, samenhangend verhaal ervaart. Overmatige blootstelling aan identieke advertenties kan leiden tot afnemende rendementen, dus het implementeren van AI-gestuurd frequentiebeheer is de sleutel tot het behouden van betrokkenheid zonder oververzadiging.

De rol van de overheid

In de nasleep van GDPR hebben we een golf van nieuwe regelgeving over de hele wereld zien ontstaan, van de CCPA in Californië tot de LGPD in Brazilië, die allemaal de nadruk leggen op de noodzaak van meer transparantie en controle over persoonlijke gegevens. Technologische innovatie, met name op gebieden zoals kunstmatige intelligentie (AI) en machine learning, zal een belangrijke rol spelen bij het vormgeven van de toekomst van privacy. Deze technologieën zijn sterk afhankelijk van gegevens om te functioneren, wat vragen oproept over hoe privacy kan worden gehandhaafd in een tijdperk van big data. Privacy-verhogende technologieën (PET's), zoals differentiële privacy en (homomorfe) versleuteling, zullen waarschijnlijk prominenter worden naarmate bedrijven proberen de bruikbaarheid van gegevens in balans te brengen met gebruikersprivacy.

Tegelijkertijd kunnen we een voortdurende push verwachten voor meer gebruikerssoevereiniteit over gegevens. Concepten zoals gegevensbezit en gegevensoverdraagbaarheid zullen waarschijnlijk aan kracht winnen, waardoor individuen kunnen beslissen hoe hun gegevens worden gebruikt en gemonetariseerd.

Overheden zouden scholen kunnen stimuleren en subsidiëren om kinderen al vroeg het concept van digitale tracking en de resultaten van privacybewust gedrag bij te brengen. Ook de controle en handhaving door overheden is nog in ontwikkeling, en we hebben nog niet gezien hoe dit zich in de toekomst zal ontwikkelen. Er is niet veel transparantie en duidelijkheid over de manier waarop overheden de naleving van gegevensbeschermingswetten controleren en boetes opleggen bij overtredingen.

De rol van de overheid

Laten we ten slotte niet vergeten dat al deze inspanningen van organisaties en overheden niets waard zijn zonder Peters eigen bewustzijn en bereidheid om zijn rechten op gegevensprivacy uit te oefenen. Hoewel bedrijven en wetgevers het kader kunnen bieden, ligt de uiteindelijke keuze bij gebruikers zoals Peter. Door zich bewust te zijn van wat hij deelt en zijn opties zorgvuldig te overwegen, kan hij een actieve bijdrage leveren aan een verantwoorde datacultuur.

Bij het inzetten van data speelt ook de verantwoordelijkheid van de gebruiker een rol. Gebruikers zoals Peter moeten zich bewust zijn van de waarde van hun gegevens en de implicaties van het delen ervan. Vaak geven consumenten informatie weg zonder zich bewust te zijn van de mogelijke gevolgen. Zo zou Peter kunnen besluiten zijn gegevens te delen met een weerapplicatie, in ruil voor gratis toegang. Zolang hij weet dat deze keuze betekent dat hij later nogmaals kan worden getarget, is dit een eerlijke afweging. Mocht Peter echter liever betalen voor een advertentievrije ervaring, dan moet dit tegen een redelijk bedrag toegankelijk zijn. Het lastige hier is dat er geen eenduidige standaard bestaat voor wat een eerlijke prijs is, omdat dit afhankelijk is van markt, locatie en andere factoren.

Conclusie

Hoewel de weg vooruit onzeker is, is één ding duidelijk: privacy- en toestemmingsmechanismen zullen centraal blijven staan in discussies over de toekomst van het internet. Organisaties die erin slagen de juiste balans te vinden tussen datagestuurde innovatie en gebruikersprivacy, zullen beter gepositioneerd zijn om te gedijen in het digitale tijdperk. Overheden met een vooruitziende blik op het gebied van onderwijs, regelgeving en transparantie in de handhaving van die regels, zullen voorop lopen in de ontwikkeling. Uiteindelijk vereist de toekomst van gegevensbeheer een gezamenlijke inspanning, waarin adverteerders, overheden en gebruikers samen streven naar een digitale omgeving die zowel waardevol als respectvol is.