DATA DRIVEN MARKETING ASSOCIATION

BEACONS: HOE HEURT HET EIGENLIJK?

8 DECEMBER 2016

In deze beknopte handleiding legt DDMA aan de hand van de huidige stand van de wet uit waar je rekening mee moet houden bij het gebruik van beacons. Omdat elke beacon techniek zijn eigen juridische haken en ogen heeft is gekozen om dit document te beperken tot bluetooth beacons. Deze beacons worden in toenemende mate ingezet voor marketing en zijn nog niet inhoudelijk beoordeeld door de toezichthouder. Let er bij het lezen van dit document dus op dat wanneer er over 'beacons' wordt gesproken, het alleen over beacons gaat die hun locatie via bluetooth doorsturen naar een mobiele applicatie (app).

Wat zijn beacons en waar worden ze voor gebruikt?

Beacons zijn kleine bakens die bluetooth signalen uitzenden binnen een straal van ongeveer dertig meter. Deze signalen zijn éénrichtingsverkeer. De beacons zelf zijn niet aangesloten op internet en sturen een eenvoudig signaal: 'ik ben hier!' Mobiele devices die de app van de winkel of het evenement geïnstalleerd hebben weten hierdoor dat de gebruiker zich bevindt op een bepaalde locatie in het meetgebied. De marketeer kan met deze informatie een actie verbinden aan een bepaalde locatie. Een aantal voorbeelden zijn:

- Het in kaart brengen van de looproutes binnen een winkel, welke producten worden veel bekeken, worden deze producten ook door deze winkelbezoekers gekocht?
- Wanneer een webshop bezoeker een winkel binnenstapt kan hij herkend worden en vervolgens een aanbieding op maat ontvangen via een pushbericht van de app
- Het pushen van informatie over producten of aanbiedingen op het moment dat iemand een winkel binnenstapt of voorbij loopt

Je kunt het dus vergelijken met Analytics op een website, maar dan in de fysieke winkelruimte.

Welke gegevens worden toegevoegd door het gebruik van beacons?

Beacons geven apps de mogelijkheid om de locatie van de gebruiker te bepalen. Deze locatiegegevens zijn persoonsgegevens in de zin van de Wbp. Meestal zullen dit niet de enige persoonsgegevens zijn die een app verwerkt. Consumenten installeren dagelijks apps die toegang vragen tot verschillende onderdelen van de telefoon. Apps vragen (en krijgen) bijvoorbeeld toegang tot de contactenlijst, de fotoalbums of zelfs de berichten van het apparaat. Door beacons kan er een nauwkeurige locatie van de gebruiker bepaald worden. Deze informatie kan, vooral in gebouwen, een veel nauwkeurige plaatsbepaling bieden dan GPS. De app weet door de beacons waar en wanneer de gebruiker in het meetgebied is.

Toezicht van de ACM of de AP?

Locatiegegevens die via bluetooth worden verzameld vallen niet onder de Telecommunicatiewet. Omdat het om persoonsgegevens gaat is de toepasselijke wetgeving de Wet Bescherming Persoonsgegevens (Wbp). Daarvoor is de Autoriteit Persoonsgegevens de bevoegde toezichthouder.
Het installeren van een app valt onder de Telecommunicatiewet, Daardoor is de manier waarop bij het installeren van de app toestemming wordt gegeven een onderwerp waarover de ACM bevoegd is als toezichthouder[1].
Omdat we hier ingaan op locatiegegevens zal vooral naar de Wbp verwezen worden.

Privacyregel I. De grondslag

Voor de verwerking van persoonsgegevens heb je altijd een grondslag nodig. Het gerechtvaardigd belang is door de toezichthouder beoordeeld in een toepassing van WiFi-tracking, een andere beacon

[1] Artikel 11.7a Telecommunicatiewet

technologie. Het tracken van bezoekers buiten de winkelruimte op basis van deze grondslag werd in deze uitspraak verboden. Met dit verbod blijkt in de praktijk erg lastig te werken, omdat de straling zich niet beperkt tot de muren van een winkel. Daarnaast moet elke bezoeker worden geïnformeerd over de tracking voordat hij het meetgebied binnengaat, bijvoorbeeld door informatieborden bij de deur, of grote raamstickers.

Omdat de tracking moeilijk is te beperken tot een bepaalde ruimte, en je de locatiegegevens wil gebruiken om individuen te benaderen, is (voorafgaande) ondubbelzinnige toestemming de meest voor de hand liggende optie. De Wbp definieert toestemming als "elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt". Het belangrijkste hierbij is dat het voor de gebruiker duidelijk is waarvoor hij toestemming geeft, en wat hij kan verwachten. Eerder dan dit moment mogen geen locatiegegevens worden verwerkt.

Hoe verkrijg je ondubbelzinnige toestemming?

In het geval van beacons gebeurt dit door (potentiële) bezoekers een app te laten downloaden waarin de gebruiker om toestemming wordt gevraagd. Deze opt-in voor het verzamelen en verwerken van locatiegegevens wordt meestal gevraagd in combinatie met het vooruitzicht dat de gebruiker korting zal ontvangen op bepaalde producten of diensten.

Hoe vrij is vrij? Als je de opt-in meeneemt als voorwaarde voor deelname of als voorwaarde bij het ontvangen van gratis content, dan kun je je afvragen of deze toestemming 'vrij' is. Je kunt dan natuurlijk bepleiten dat het nog steeds vrij is omdat men er ook voor kan kiezen om de gratis content niet te ontvangen. Iemand kan ook zonder de app de ruimte betreden en ondervindt daar ook geen hinder of schade door.

Je kan een opt-in voor gratis content als voorwaarde stellen, maar het moet wel duidelijk zijn. De meest verantwoorde oplossing is om het delen van locatiegegevens niet te verplichten voor het gebruik van de app.

Voorbeeld: De ondubbelzinnige toestemming kan gevraagd worden door bij het eerste gebruik van de app een leeg keuze hokje op te nemen waarin staat: *"Ik geef toestemming aan [bedrijf] om mijn locatie in de winkel te bepalen door middel van bluetooth beacons, om mij tijdens mijn winkelbezoek via de [bedrijf] app van gepersonaliseerde aanbiedingen te voorzien. Lees hier meer over hoe [bedrijf] omgaat met je gegevens: [link naar privacy statement]"*

Toestemming voor het verwerken van locatiegegevens moet altijd ingetrokken kunnen worden. Zorg ervoor dat daarvoor altijd een gebruiksvriendelijke mogelijkheid beschikbaar is, waar nodig met waarschuwing dat de app daardoor niet volledig meer zal functioneren. Zie voor meer informatie Privacyregel III.

Hoe zit het met de verschillen tussen besturingssystemen?

Per mobiel besturingssysteem ziet de toestemming voor het inschakelen van bluetooth er anders uit. Wees voorzichtig met aannemen dat de toestemming die gevraagd wordt voor *toegang* tot bluetooth gelijk staat aan toestemming in de zin van de Wet bescherming persoonsgegevens (Wbp). De toestemming moet gebaseerd zijn op voldoende informatie, zodat de gebruiker voorafgaand aan de toestemming weet wat er met de gegevens zal gebeuren. Kijk dus goed per besturingssysteem hoe je er voor kan zorgen dat deze informatie wordt verstrekt voordat de gegevens worden verzameld. Zie voor meer uitleg over toestemming pagina 8-11 van de DDMA handleiding over mobiele apps: https://ddma.nl/juridisch/archief/praktische-juridische-tips-mobile/

Privacyregel II. Informeer helder en volledig

Een van de belangrijkste uitgangspunten van de Wbp is transparantie. Als je persoonsgegevens verwerkt behoor je de gebruikers daarover zo eenvoudig en helder mogelijk te informeren. Zowel op het moment van verzamelen als daarna. Vermeld het feit dat je beacons gebruikt om bezoekers te volgen dan ook zeker in het privacy statement van je website en app. Wees zo specifiek mogelijk in je informatievoorziening, zodat de consument weet wat hij kan verwachten:

- Welke informatie wordt verzameld?
- Waarvoor wordt deze informatie gebruikt?
- Met wie wordt deze informatie gedeeld?
- Hoe lang wordt de informatie bewaard?

Er worden met deze technologie alleen gegevens verwerkt van bezoekers die hiervoor (geïnformeerde) toestemming hebben gegeven via de app. Daarom zou je kunnen stellen dat het voldoende is om te informeren via die app. Uiteraard is meer informatie altijd beter. Zo zou je flyers

kunnen neerleggen in de winkel, waar men meer kan lezen over het gebruik van beacons.

Privacyregel III. Respecteer de rechten van de gebruikers

Gebruikers moeten altijd de mogelijkheid hebben zich eenvoudig en kosteloos af te melden voor tracking door middel van beacons. Je moet de gebruiker informeren over de wijze waarop hij zich kan afmelden. Bluetooth tracking volgt alleen de bezoekers die de app geïnstalleerd hebben en in de app toestemming hebben gegeven voor het volgen door middel van bluetooth signalen. Afmelden voor bluetooth tracking kan op de volgende manieren:

- Het meetgebied betreden met bluetooth uitgeschakeld
- De app toegang tot bluetooth ontzeggen

De gebruiksvriendelijkere optie is om de app zo te bouwen dat deze nog steeds functioneert wanneer men de toestemming intrekt om het bluetooth signaal te gebruiken. Zorg ervoor dat de aanwezigen correct geïnformeerd worden met een gebruiksvriendelijke instructie.

Reikwijdte van het meetgebied

Voor marketeers zal het verleidelijk zijn om met de push melding voorbijgangers die de app geïnstalleerd hebben te attenderen op aanbiedingen van nabijgelegen winkels. De AP heeft hierover nog geen uitspraak gedaan in het geval van bluetooth tracking. Het is momenteel dan ook niet zeker wat haar standpunt hierin is. Uit de gekozen lijn in de uitspraak over WiFi-tracking kan wel worden opgemaakt dat de Autoriteit Persoonsgegevens geen voorstander is van tracking in de openbare ruimte. Daar zou men zich 'onbespied' moeten kunnen voortbewegen. Of het standpunt hetzelfde is in het geval van een opt-in voor zowel bluetooth tracking als push notificaties is momenteel niet duidelijk. Wie zekerheid wil kan er dan ook beter voor kiezen om het meetgebied zoveel mogelijk te beperken tot de ruimte die bij de opdrachtgever hoort. Om te weten hoe ver je mag gaan moet je een inschatting maken van de verwachtingen van de consument op het moment dat toestemming werd gegeven.

Privacyregel IV. Heldere afspraken over verantwoordelijkheden.

De inzet van beacons is meestal een samenwerking tussen de opdrachtgever, een mobile/digital bureau, de beacon-aanbieder. DDMA adviseert om er goed op te letten dat locatiegegevens niet gebruikt worden voor andere doeleinden dan waarvoor ze zijn verzameld. De toestemming vervalt wanneer de verwerking niet meer 'verenigbaar' is met het oorspronkelijk gecommuniceerde doel. De DDMA raadt daarom aan om heldere schriftelijke afspraken te maken met de betrokken partijen over:

- Het doel van de verwerking;
- welke soort gegevens worden verwerkt;
- de bewaartermijnen;
- het gebruik van de gegevens alsmede eventuele verstrekking aan derden;
- de (eventuele) zeggenschap van de beacons-aanbieder;
- de technische en organisatorische maatregelen die de dienst neemt om de data te beveiligen; en,
- de plicht om de data te vernietigen na afloop van de campagne.

Door antwoord te geven op deze vragen kan aan het licht worden gebracht wat de juridische rollen zijn van partijen. In de meeste gevallen zal de opdrachtgever verantwoordelijke zijn, en de aanbieder van de beacon technologie de bewerker. Dit is alleen het geval wanneer de opdrachtgever het doel van de verwerking en de inzet van (financiële) middelen bepaalt. Het is verstandig om de afspraken vast te leggen in een bewerkersovereenkomst met de aanbieder. Let wel op: het afsluiten van een bewerkersovereenkomst sluit niet uit dat de aanbieder toch verantwoordelijke is in de zin van de Wbp. De werkelijke situatie is hiervoor bepalend. Per proces kunnen de verhoudingen anders liggen, wat op zijn beurt weer gevolgen heeft voor de juridische rollen.

DDMA heeft voor haar leden een template bewerkersovereenkomst. Deze wordt regelmatig bijgewerkt naar de stand van de wet en is op aanvraag beschikbaar.

Gebruik van beacon data voor push berichten

Locatiegegevens die via beacons verzameld worden zullen in de praktijk veelal ingezet worden voor het verzenden van pushberichten met de app. In tegenstelling tot locatiegegevens vallen pushberichten onder de Telecommunicatiewet. Kijk voor volledig juridisch kader over de verwerking van persoonsgegevens in apps naar de DDMA handleiding op de volgende pagina: https://ddma.nl/juridisch/archief/praktische-juridische-tips-mobile/ Pagina 12 en 13 van deze

handleiding gaan dieper in op de regelgeving over pushberichten.

Wat betekent de nieuwe Europese Privacywet voor het gebruik van beacons?

Onder de nieuwe wet die in mei 2018 in werking treedt komt meer nadruk op *'privacy by design'*. Dit principe verplicht organisaties om gedurende het hele proces actief bezig te zijn met impact op de privacy van de betrokkene. Bij projecten die de privacy raken is het verstandig om vooraf een *Privacy Impact Assessment* uit te voeren; een handige tool waarmee kan worden blootgelegd wat de impact is op de privacy van de betrokkene. Met deze informatie kun je vervolgens in een vroeg stadium bekijken hoe je op een verantwoorde manier het gewenste resultaat kunt behalen. Houd hierbij goed het principe van dataminimalisatie in de gaten: kan ik dit doel ook bereiken met minder persoonsgegevens? Andere voorbeelden van nuttige privacy bevorderende maatregelen zijn pseudonimiseren, aggregeren of het hashen van gegevens.

Je kunt je bijvoorbeeld afvragen hoe lang na een winkelbezoek de locatiegegevens van de klant nog nodig zijn. Als er al een aankoop heeft plaatsgevonden kun je ervoor kiezen om de gegevens te aggregeren tot statistieken die niet meer te herleiden zijn tot een individu.

DDMA bereidt haar leden in 2017 voor op de nieuwe Europese Privacywetgeving. Lid en geïnteresseerd? Laat DDMA dit dan weten.

Heb je meer juridische vragen over de inzet van Beacons of andere marketingkanalen? Neem dan contact op DDMA via 020-45 284 13 of met sannemulder@ddma.nl/ matthiasdebruyne@ddma.nl

Technologie loopt op wetgeving vooruit. DDMA (branchevereniging voor data driven marketing) ziet het als haar taken het juridisch kader te schetsen voor het gebruik van nieuwe technologie voor marketingdoeleinden, zoals de inzet van beacons in de openbare ruimte.