AUTORITEIT
PERSOONSGEGEVENS

**Autoriteit Persoonsgegevens**
Postbus 93374, 2509 AJ Den Haag
Prins Clauslaan 60, 2595 AJ Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

AANGETEKEND
Detailhandel Nederland
Aan het bestuur
Postbus 262
2260 AG LEIDSCHENDAM

Datum
15 juni 2016

Ons kenmerk
z2016-00087

Onderwerp
Wifi-tracking en de Wet bescherming persoonsgegevens

Geacht bestuur,

De Autoriteit Persoonsgegevens vraagt bij deze graag uw aandacht voor het volgende. Vandaag is aan diverse bedrijven en gemeenten een brief gestuurd over de toepasselijkheid van de Wet bescherming persoonsgegevens (Wbp) op wifi-trackingtechnologie waarmee signalen van mobiele telefoons geregistreerd kunnen worden.

De Autoriteit Persoonsgegevens ontvangt regelmatig signalen van het publiek waaruit blijkt dat er zorgen zijn over de impact van wifi-trackingtechnologie op de privacy van betrokken die daaraan –dikwijls ongemerkt- worden blootgesteld.

Wifi-tracking wordt op grote schaal toegepast in en rond winkels in Nederland. Deze technologie wordt, onder meer, ingezet om bezoekersaantallen van winkels en passanten te tellen en hun bewegingen in kaart te brengen. Naar aanleiding daarvan heeft de Autoriteit Persoonsgegevens onderzoek gedaan naar een Nederlandse aanbieder van wifi-trackingtechnologie. De resultaten van dat onderzoek zijn op 1 december 2015 gepubliceerd op de website van de Autoriteit Persoonsgegevens.[1] Detailhandel Nederland heeft hier vervolgens op 3 december 2015 aandacht aan besteed op haar website.

Ik wil u vragen uw leden te informeren over de eisen die de Wbp stelt aan de inzet van wifi-tracking (en vergelijkbare) technologie. In de bijlage zijn de eisen die aan bod kwamen in het hierboven genoemde onderzoek kort samengevat.

[1] Zie: Rapport definitieve bevindingen inzake Bluetrace, zaak z2014-00994

Datum
15 juni 2016

Ons kenmerk
z2016-00087

**Eerder onderzoek**
Het eerder onderzochte bedrijf gebruikt wifi-tracking met als doel het tellen van bezoekers en passanten, om de commerciële prestaties van winkels te kunnen meten. In dit onderzoek naar wifi-tracking is gebleken dat de verzamelde meetgegevens persoonsgegevens zijn, waarop de Wet bescherming persoonsgegevens van toepassing is. De technologieleverancier en de afnemer van de technologie kunnen beide verantwoordelijke zijn – medeverantwoordelijke - voor de gegevensverwerking wanneer zij beide mede bepalen voor welke doelen en met welke middelen de gegevens verwerkt worden.

De Autoriteit Persoonsgegevens heeft in dit onderzoek vastgesteld dat de informatievoorziening aan het publiek tekort schoot en dat een wettelijke grondslag voor metingen/tellingen, zowel binnen als buiten de winkel, ontbrak. De metingen werden 24 uur per dag verricht en daarnaast werden de gegevens langer bewaard dan strikt noodzakelijk voor het verzameldoel. Het registreren of volgen van bewegingen van individuen – waaronder voorbijgangers op de openbare weg - door middel van wifi-tracking heeft een grote impact op de persoonlijke levenssfeer van betrokkenen.[2]
In dit geval weegt dit niet op tegen de bedrijfseconomische doeleinden waarvoor de technologie wordt ingezet door deze verantwoordelijke. Uit het onderzoek van de Autoriteit Persoonsgegevens volgt dat wifi-tracking niet onbeperkt mag worden ingezet.

**Eisen en waarborgen**
Met de brief die vandaag is verstuurd informeert de Autoriteit Persoonsgegevens onder meer diverse gemeenten die wifi-tracking gebruik(t)en, dat het toepassen van wifi-tracking of vergelijkbare technologie slechts is toegestaan binnen de kaders van de Wet bescherming persoonsgegevens.[3] Deze wetgeving brengt mee dat de verantwoordelijke moet zorgen voor voldoende informatie aan het publiek over de inzet van wifi-tracking. Daarnaast moeten er waarborgen zijn voor de bescherming van de persoonlijke levenssfeer van personen die zich binnen het bereik van de meetapparatuur bevinden.

[2] Het houden van toezicht op openbare wegen is bovendien in beginsel voorbehouden aan de overheid: Kamerstukken II 66-4428 (30 maart 2005), Kamerstukken I 30-1434 (28 juni 2005) en Vzr. Rb. Middelburg 9 april 2002.
[3] Afhankelijk van de gebruikte technologie, kan ook de Telecommunicatiewet van toepassing zijn.

Datum
15 juni 2016

Ons kenmerk
z2016-00087

**Handhaving**
Indien wifi-tracking of vergelijkbare technieken ingezet worden op een wijze die niet voldoet aan de in de bijlage genoemde vereisten, dan handelt de verantwoordelijke in strijd met de Wet bescherming persoonsgegevens.
De Autoriteit Persoonsgegevens kan, uit eigen beweging of bijvoorbeeld op grond van signalen, onderzoek instellen naar de verwerking van persoonsgegevens door middel van (wifi-) tracking systemen, eventueel gevolgd door handhavende maatregelen.

Ik dank u bij voorbaat voor uw inspanning om dit onderwerp onder de aandacht te brengen. Tot slot wijs ik u erop dat deze brief zal worden gepubliceerd op de website van de Autoriteit Persoonsgegevens.

Hoogachtend,

de Autoriteit Persoonsgegevens,
Voor deze,

Mr. W. B. M. Tomesen
Vicevoorzitter

Datum
15 juni 2016

Ons kenmerk
z2016-00087

**Bijlage**

**Informatie**

Op grond van artikel 34 van de Wbp moet een organisatie die op indirecte wijze gegevens verzamelt, de betrokkenen informatie verstrekken over wie hij is, en wat de doelen van de gegevensverwerking zijn. Bij wifi-tracking worden locatiegegevens verwerkt. Vanwege de gevoelige aard van deze gegevens moet de verantwoordelijke nadere informatie verstrekken, zoals een overzicht waaruit blijkt welke gegevens precies worden verwerkt, informatie over doorgifte van gegevens aan bewerkers of derden en de mogelijkheden van betrokkenen om hun rechten uit te oefenen die zij op grond van de Wbp hebben. Deze rechten omvatten bijvoorbeeld het indienen van een verzoek om inzage of verwijdering van gegevens of het recht van verzet tegen de verwerking. De informatie moet de betrokkenen in principe bereiken op het moment dat zij te maken krijgen met tracking of metingen op basis van wifi-signalen.

**Grondslag**

Artikel 8 van de Wbp schrijft voor dat de verwerking van persoonsgegevens toegestaan is wanneer dat gebaseerd is op een van de wettelijke grondslagen die zijn genoemd in dat artikel.
Voorafgaande toestemming van de betrokkenen is een van de grondslagen die genoemd is in artikel 8. Een verantwoordelijke kan ervoor kiezen om wifi-tracking, of vergelijkbare technieken, zoals bluetooth tracking, in te zetten als betrokkenen daarvoor specifieke, op informatie berustende, toestemming hebben verleend. Dat kan bijvoorbeeld via een aparte app, of met behulp van incheckmethoden in winkels zoals voorafgaand aan het gebruik van een wifi-gastnetwerk. Daarnaast kunnen organisaties met een publiekrechtelijke taak, met name overheden, persoonsgegevens verwerken als dat noodzakelijk is voor de uitvoering van die taak. Hiervoor is wel vereist dat de publieke instelling haar handelen kan baseren op een wettelijke bevoegdheid.[4] Het verwerken van persoonsgegevens door middel van wifi-tracking technologie is ook toegestaan wanneer de verantwoordelijke kan onderbouwen dat dit noodzakelijk is voor het behartigen van een gerechtvaardigd belang.[5] De gekozen werkwijze mag dan in beide gevallen (publiekrechtelijke taak of privaatrechtelijk belang) niet verder gaan dan strikt noodzakelijk is om het doel te bereiken en de verantwoordelijke moet aantonen dat dit doel niet met minder ingrijpende middelen te verwezenlijken is. Het afbakenen van gebieden en periodes waarbinnen gemeten wordt is een voorbeeld van een waarborg op het gebied van proportionaliteit. De verantwoordelijke moet daarnaast er voor zorgen dat er bij de gegevensverwerking rekening gehouden wordt met het recht van betrokkenen op bescherming van hun persoonlijke levenssfeer. Een maatregel die daaraan bijdraagt is het anonimiseren van gegevens binnen 24 uur na vastlegging.

De Autoriteit Persoonsgegevens maakt onderscheid tussen het verrichten van metingen binnen in winkels, bedrijven of instellingen en metingen buiten, op de openbare weg. Het verschil is gelegen in het feit dat de impact van wifi-tracking op de persoonlijke levenssfeer van betrokkenen groter is wanneer dit

[4] Vergelijk bijvoorbeeld de bevoegdheid van cameratoezicht door gemeenten, art. 151c Gemeentewet.
[5] Het is in theorie ook mogelijk dat wifi tracking noodzakelijk is voor de uitvoering van een overeenkomstmet de betrokkene. Daarnaast wijst de Autoriteit Persoonsgegevens op artikel 11.7a van de Telecommunicatiewet. Dit artikel kan van toepassing zijn op tracking technieken waarbij gegevens worden geplaatst op het apparaat van de consument, of daarvan worden afgelezen.

plaatsvindt in de openbare ruimte dan wanneer dit plaatsvindt in de context van het bezoek aan een specifiek bedrijf of organisatie. In de openbare ruimte moeten mensen zich onbespied kunnen bewegen, zonder dat hun bewegingen in kaart worden gebracht. De belangenafweging die vereist is op basis van artikel 8 onder f van de Wbp, is afhankelijk van de context. De Autoriteit Persoonsgegevens neemt bijvoorbeeld in overweging wat het bereik van de metingen is, in hoeverre omwonenden of voorbijgangers geraakt worden door de gegevensverwerking en of zij zich hier aan kunnen onttrekken. Daarom geldt voor wifi-tracking op de openbare weg dat er meer waarborgen nodig zijn voor de persoonlijke levenssfeer dan voor wifi-tracking binnen (in) de ruimte van een organisatie.

Een belangrijke waarborg in dit verband is het onmiddellijk en onomkeerbaar anonimiseren van gegevens, zodra deze door sensoren of andere meetinstrumenten worden vastgelegd. Deze waarborg reduceert het risico voor betrokkenen. De kans dat herleidbare personen over verschillende locaties en door de tijd heen gevolgd kunnen worden en/of anders behandeld kunnen worden op basis van over hen vastgelegde informatie wordt dan namelijk kleiner.

**Bewaartermijn**

Het verwerken van gegevens door middel van wifi-tracking of vergelijkbare technieken houdtin dat er locatiegegevens van betrokkenen worden opgeslagen, samen met de unieke identifier van hun mobiele apparaat of apparaten. Zolang deze meetgegevens herleidbaar zijn naar individuele betrokkenen, mogen zij slechts gedurende een beperkte periode bewaard worden (artikel 10 van de Wbp). De verantwoordelijke moet daarom bewaartermijnen instellen en onderbouwen waarom de gekozen bewaartermijn van persoonsgegevens noodzakelijk is voor het beoogde doel van de metingen. Na afloop van de bewaartermijn moeten gegevens daadwerkelijk vernietigd of onomkeerbaar geanonimiseerd worden. Uit het genoemde onderzoek blijkt overigens dat het toepassen van een (vast) hashing algoritme op de verzamelde unieke identifiers niet altijd leidt tot anonimisering.

**Overige eisen Wbp**

Een organisatie die gebruik wil maken van wifi-tracking of vergelijkbare technieken moet, naast de bovengenoemde aspecten, ook de overige voorschriften van de Wbp in acht nemen. Voorbeelden daarvan zijn: Het melden van de gegevensverwerking aan de Autoriteit Persoonsgegevens; Het vastleggen van heldere doelen voor de gegevensverwerking en het beperken van de verwerking tot die doelen (artikelen 7 en 9 van de Wbp); Waarborgen treffen voor passende beveiliging van de gegevens, inclusief het melden van inbreuken daarop (artikelen 13 en 34a van de Wbp) en het naleven van de regels met betrekking tot het inschakelen van bewerkers of derden (onder meer artikel 14 Wbp).