COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag **BEZOEKADRES** Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 **FAX** 070 - 88 88 501 **INTERNET** www.cbpweb.nl

College bescherming persoonsgegevens

Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace

z2014-00944

Rapport definitieve bevindingen

Openbare Versie

13 oktober 2015

INHOUDSOPGAVE

SAMENVATTING **1**

1. Inleiding **4**

2. Procedure **8**

3. Feitelijke bevindingen **10**
3.1 Organisatie en werkwijze Bluetrace 10
3.2 Middelen voor wifi-tracking 11
3.3 De inzet van middelen en de reikwijdte van metingen 12
3.4 Verzamelen van ruwe meetgegevens 12
3.5 Analyse van gegevens uit wifi-tracking in en rondom winkels 13
3.6 Verantwoordelijkheid voor gegevensverwerking 17
3.7 Informatie door Bluetrace 19
3.8 Bewaren van gegevens 20

4. Wettelijk kader **21**
4.1 Verwerking van persoonsgegevens 21
4.2 Verantwoordelijkheid voor de verwerking van persoonsgegevens 22
4.3 Grondslagen voor de verwerking van persoonsgegevens in de Wbp 23
4.4 Informatieplicht 24
4.5 Bewaren van gegevens 26

5. Beoordeling **28**
5.1 Verwerking van persoonsgegevens 28
5.2 Verantwoordelijke en bewerker 35
5.3 Grondslagen voor de verwerking van persoonsgegevens 39
5.3.1 Gerechtvaardigd belang voor wifi-tracking door Bluetrace in winkels 40
5.3.2 Gerechtvaardigd belang voor wifi-tracking door Bluetrace buiten winkels 43
5.4 Informatieverstrekking aan de betrokkene 48
5.5 Bewaren van gegevens 52

6. Conclusies **55**

SAMENVATTING

Het College bescherming persoonsgegevens (CBP) heeft onderzoek gedaan naar Bluetrace, een bedrijf dat technologie voor wifi-tracking levert en installeert in en rondom winkels in Nederland. Met de technologie van Bluetrace kunnen de wifi-signalen van mobiele apparaten, zoals telefoons, worden opvangen. Zo kan geteld worden hoeveel smartphones – en daarmee personen – er binnen een bepaald bereik zijn en hoe die zich verplaatsen. Door middel van wifi-tracking registreert Bluetrace unieke mac-adressen van mobiele apparatuur in combinatie met gegevens over de locatie, de datum en het tijdstip van registratie. Daarmee verzamelt en verwerkt Bluetrace persoonsgegevens. Dit levert bedrijfseconomische informatie op, zoals: hoeveel mensen passeren de winkels, hoeveel bezoekers gaan de winkel in, hoe lang blijven zij vervolgens op een bepaalde plaats? Bluetrace verzamelt en analyseert meetgegevens uit wifi-tracking met het doel om bedrijfseconomische informatie aan winkeliers te bieden.

In tientallen grote en middelgrote steden in Nederland is wifi-tracking van Bluetrace uitgerold. De metingen van Bluetrace raken daarmee een groot aantal Nederlanders. De wifi-sensoren van Bluetrace meten niet alleen in de winkels zelf, maar hebben bereik tot buiten de winkels op de openbare weg. Hierdoor verzamelt Bluetrace informatie over zowel winkelbezoekers als (toevallige) voorbijgangers en mensen die in het winkelgebied wonen.

Informatie aan het publiek
Bluetrace heeft geen privacybeleid en ook geen andere informatiebronnen bedoeld voor betrokkenen waarin mensen kunnen lezen wat voor gegevens Bluetrace verwerkt, voor welke doelen het bedrijf dat doet en in welke gebieden er wifi-tracking is. Het CBP concludeert dat Bluetrace de wet overtreedt doordat het bedrijf geen informatie verstrekt aan het publiek over de verwerking van persoonsgegevens via wifi-tracking.

Wettelijke grondslag
Bedrijven en organisaties die persoonsgegevens gebruiken, moeten hiervoor een zogeheten wettelijke grondslag hebben. Zonder zo'n grondslag mag een bedrijf of organisatie geen persoonsgegevens verwerken. Bluetrace geeft aan dat het bedrijf de gegevens van winkelbezoekers en -passanten verwerkt omdat dit noodzakelijk is voor een gerechtvaardigd belang (bedrijfsbelang) van de Bluetrace, namelijk het verzamelen en leveren van bedrijfseconomische informatie. Andere mogelijkheden zijn bijvoorbeeld een wettelijke taak of een overeenkomst met, of toestemming van, de betrokkene, maar deze zijn niet aan de orde in deze zaak.

Wifi-tracking in winkels
Het verzamelen van gegevens over drukte en bezoekersgedrag in winkels kan inderdaad een gerechtvaardigd belang zijn voor Bluetrace. Voorwaarde hierbij is wel dat Bluetrace de betrokkenen (de mensen van wie de persoonsgegevens verwerkt worden) goed informeert en dat de verwerking van persoonsgegevens noodzakelijk is om dit doel te bereiken. Verder moet Bluetrace zorgen dat er voldoende waarborgen zijn voor de bescherming van de privésfeer van betrokkenen.

Het CBP concludeert dat de huidige werkwijze van Bluetrace niet voldoet aan de wettelijke vereisten van proportionaliteit (de privacyinbreuk moet evenredig zijn aan het nagestreefde doel) en subsidiariteit (Bluetrace had het doel op een andere, minder ingrijpende manier kunnen bereiken).
De gegevens die Bluetrace over mensen verzamelt, zijn gevoelig van aard. Het gaat om locatiegegevens, waarmee een beeld te krijgen is van iemands verblijfplaats en (winkel)gedrag. Bovendien verzamelt Bluetrace de gegevens op een manier die meebrengt dat personen kunnen worden gevolgd door de tijd heen.
Bluetrace meet namelijk 24 uur per dag, zeven dagen per week en bewaart de gegevens onbeperkt. Volgens het CBP kan Bluetrace het gestelde doel ook bereiken door op een beperktere schaal te meten en minder gegevens te verwerken, gedurende een kortere periode. Het CBP oordeelt ook dat er – gelet op de belangen van betrokkenen en de gevoelige aard van de locatiegegevens – meer waarborgen voor de belangen van de winkelbezoekers noodzakelijk zijn. Wanneer Bluetrace de meetgegevens zo snel mogelijk, binnen maximaal 24 uur, anonimiseert of verwijdert, wordt de mogelijkheid om een beeld van een winkelbezoeker door de tijd heen te vormen beperkt.
Dit houdt in dat Bluetrace géén geldige grondslag heeft voor het verwerken van persoonsgegevens via wifi-tracking in winkels. Daarmee overtreedt Bluetrace de wet.

Wifi-tracking buiten winkels
Het CBP overweegt dat zodra wifi-tracking verder reikt dan de winkel, de belangen van betrokkenen op bescherming van de persoonlijke levenssfeer extra zwaar wegen. Dit geldt bijvoorbeeld voor voorbijgangers op straat en omwonenden van de winkels met wifi-tracking. Het is daarom niet snel gerechtvaardigd om aan wifi-tracking buiten winkels te doen, waarbij gegevens van voorbijgangers en omwonenden worden verwerkt, zeker niet wanneer hierover geen informatie wordt gegeven.
Bluetrace heeft de noodzaak om mensen buiten de winkel te registreren onvoldoende onderbouwd. Bovendien verwerkt Bluetrace meer gegevens dan nodig en kunnen de metingen qua tijdsduur beperkt worden. Bluetrace zou er voor kunnen kiezen om het bereik van de metingen te beperken tot de winkel zelf. Op die manier registreert het bedrijf de aanwezigheid van voorbijgangers op de openbare weg of bewoners van aangrenzende panden niet, of althans zo min mogelijk. De huidige werkwijze van het bedrijf voldoet niet aan de wettelijke vereisten van proportionaliteit en subsidiariteit.
Indien Bluetrace de noodzaak van deze gegevensverwerking al zou kunnen onderbouwen – en voor zover het bedrijf zou voldoen aan de vereisten van proportionaliteit en subsidiariteit – zou Bluetrace de persoonsgegevens onmiddellijk, dan wel in ieder geval zo snel mogelijk na de eerste vastlegging, onomkeerbaar moeten anonimiseren. Tot slot weegt het belang van Bluetrace niet op tegen de privacyrechten van betrokkenen omdat Bluetrace hen geen mogelijkheid biedt om zich aan wifi-tracking te onttrekken.
Dit alles houdt in dat Bluetrace ook géén geldige grondslag heeft voor het verwerken van persoonsgegevens via wifi-tracking buiten winkels. Dit is een overtreding van de wet.

Bewaartermijn
Bluetrace heeft geen bewaartermijnen vastgesteld. Het bedrijf bewaart gegevens voor onbepaalde tijd. Daarnaast anonimiseert Bluetrace de gegevens niet, maar bewaart ze in een vorm die het mogelijk maakt om betrokkenen te identificeren.
Uit het onderzoek van het CBP is niet gebleken dat het noodzakelijk is om de gegevens onbeperkt te bewaren voor het doel van de gegevensverwerking. Bluetrace handelt hierdoor ook op dit punt in strijd met de wet.

Nadat Bluetrace het rapport voorlopige bevindingen van het CBP heeft ontvangen heeft het bedrijf een zienswijze gegeven. De zienswijze bevat een plan van aanpak met daarin voorstellen voor toekomstige maatregelen en nader onderzoek naar de werkwijze van Bluetrace met betrekking tot wifi-tracking. De zienswijze van Bluetrace heeft niet geleid tot aanpassing van de conclusies van het onderzoek omdat de voorgestelde aanpak, naar het oordeel van het CBP, te weinig concreet zicht biedt op de beëindiging van de geconstateerde overtredingen.

1. INLEIDING

Het College bescherming persoonsgegevens (CBP) heeft op grond van artikel 60 van de Wet bescherming persoonsgegevens (Wbp) een ambtshalve onderzoek ingesteld naar de gegevensverwerking die plaatsvindt bij het inzetten van wifi-trackingtechnologie in winkels en rondom winkels op de openbare weg door Bluetrace B.V., statutair gevestigd in Amsterdam (hierna: Bluetrace). Bluetrace heeft vestigingen in Amsterdam en Velsen-Zuid.[1]

Bluetrace biedt wifi- en bluetooth-technologie aan waarmee het mogelijk is om mobiele apparaten als smartphones, laptops, tablets en carkits te registreren en te volgen en/of bewegingspatronen in kaart te brengen op basis van radiosignalen. Een praktisch voorbeeld hiervan is het tellen van apparaten – en daarmee van de personen die de apparaten bij zich dragen – in bijvoorbeeld winkels en tijdens evenementen. Bluetrace verwerkt en bewaart deze meetgegevens en voorziet zijn klanten van data-analyses. Bluetrace verzorgt ook service en onderhoud aan de technische installaties en installeert deze zelf op de locatie van de klant.

Wifi-tracking is een relatief nieuw fenomeen. Consumenten zullen zich vaak niet bewust zijn van het feit dat er kan worden 'meegekeken' met hun verplaatsingsgedrag. De introductie van wifi- en bluetooth-functionaliteiten en daarop gebaseerde trackingtechnologie betekent dat mobiele apparatuur met andere apparaten kan communiceren zonder dat de gebruiker daarvan iets merkt. Er vindt via deze technologie voortdurend communicatie plaats waaraan de betrokkene zelf niet of nauwelijks deelneemt.

Technisch werkt tracking als volgt. De apparaten zenden voortdurend signalen uit waarmee zij hun aanwezigheid kenbaar maken. Deze signalen bevatten een uniek identificatiekenmerk, het Media Access Control-adres (hierna: mac-adres). Mac-adressen zijn de unieke nummers die door de fabrikant zijn vastgelegd in de hardware van apparatuur, zoals op geheugenchips en/of netwerkkaarten in computers, telefoons, laptops of routers. Omdat elk mobiel apparaat een uniek bluetooth- en een uniek wifi-mac-adres heeft, kunnen apparaten door de tijd heen op specifieke locaties herkend worden.

Driekwart van de Nederlanders heeft een smartphone.[2] Het aantal telefonieklanten met een mobiele bundel voor data en spraak is het afgelopen jaar gestegen met 8,9% tot 10,6 miljoen aansluitingen.[3] De meeste mensen zijn onafscheidelijk van hun

[1] Bluetrace B.V. is sinds september 2010 geregistreerd bij de Kamer van Koophandel onder nr. 50918397. Sinds 29 juni 2015 is de locatie in Velsen-Zuid de hoofdvestiging van het bedrijf. Bron: Kamer van Koophandel, laatst geraadpleegd door het CBP 8 juli 2015

[2] Bron: Telecompaper, 'Bijna driekwart Nederlanders bezit een smartphone', 7 december 2014, URL: http://www.telecompaper.com/nieuws/bijna-driekwart-nederlanders-bezit-een-smartphone--1053583. Vergelijk ook persbericht onderzoeksbureau GFK, 'Nieuwe meting GFK trends in digitale media', 12 december 2014, URL: http://www.gfk.com/nl/news-and-events/press-room/press-releases/paginas/evenveel-nederlanders-met-tablet-als-vaste-computer.aspx. GFK schrijft: *"Bijna 10 miljoen Nederlanders (76%) is op dit moment in het bezit van een smartphone."*

[3] Bron: ACM Telecommonitor vierde kwartaal 2014, p. 4. Te raadplegen via: URL https://www.acm.nl/nl/download/publicatie/?id=14303.

smartphone. Ze dragen het apparaat dag en nacht bij zich en nemen het overal mee naar toe.[4] In Nederland wordt steeds meer mobiel internet gebruikt. In een periode van drie jaar is dit zelfs verdriedubbeld.[5] Naar verwachting zullen consumenten binnenkort net zo vaak mobiel internet gaan gebruiken als internet via een desktop computer.[6] Mensen gebruiken hun smartphone gedurende de hele dag en voor steeds meer verschillende doelen, zoals navigatie, betalen, bellen, e-mailen, spelletjes spelen of een hardlooproute bijhouden. Recent onderzoek wijst uit dat smartphonegebruikers gemiddeld 3,6 uur per dag actief bezig zijn met hun telefoon.[7] Onderweg maken smartphone-gebruikers gebruik van wifi-gastnetwerken, met name om kosten voor mobiel internetgebruik via de telefoonaanbieder te vermijden of omdat de internetverbinding via het wifi-gastnetwerk soms beter of sneller is. Daarom staat wifi op de meeste smartphones ingeschakeld. Ook de bluetooth-verbinding wordt voor uiteenlopende functies gebruikt, bijvoorbeeld om apparaten te kunnen gebruiken als fitnesstrackers, smartwatches en luidsprekers en om te kunnen bellen of navigeren in de auto.[8]
Door deze ontwikkeling worden mobiele apparaten in toenemende mate geschikt om de houder ervan te volgen en diens gedrag in beeld te brengen.

Het uitrollen van wifi-trackingtechnologie gaat gepaard met risico's voor de persoonlijke levenssfeer van de betrokkenen. De Artikel 29-werkgroep van de Europese gegevensbeschermingsautoriteiten signaleert in zijn opinie over geolocatiefuncties van slimme mobiele apparaten dat het bijhouden van locatiegegevens van mobiele apparatuur het mogelijk maakt om een indringend beeld te verkrijgen van iemands persoonlijke leven. De aanbieder van de trackingdienst of diens klant krijgt de mogelijkheid om 'terug te kijken' in de geschiedenis van een persoon, waar het gaat om (veel)bezochte locaties of afgelegde routes op specifieke tijdstippen. Uit geolocatiedata kan worden afgeleid waar iemand woont, waar iemand slaapt, waar iemand werkt en welke andere plaatsen een individu regelmatig bezoekt.

De locatiegegevens kunnen worden gebruikt om een persoon individueel te benaderen of om bepaalde besluiten te nemen of acties te ondernemen die iemand

[4] Zie bijvoorbeeld: FormexMedical, 30 april 2015, 'Is uw smartphone een hygiënerisico?', URL: http://blog.formex-medical.nl/is-jouw-smartphone-een-hygienerisico/.
[5] In het derde kwartaal van 2012 werd er in Nederland in een kwartaal nog 5,9 Petabyte aan mobiel internet verbruikt, in het derde kwartaal van 2014 was dat al 17,6 Petabyte per kwartaal. Bron: ACM Telecommonitor derde kwartaal 2014. URL: https://www.acm.nl/nl/publicaties/publicatie/13836/Gebruik-mobiel-internet-is-verdubbeld/
[6] Bron: Adformatie, 25 juni 2015, URL http://www.adformatie.nl/nieuws/mensen-browsen-over-twee-jaar-evenveel-op-hun-mobiel-als-op-desktop. Zie ook ACM Telecommonitor eerste kwartaal 2014, Te raadplegen via: URL https://www.acm.nl/nl/publicaties/publicatie/13136/ Telecommonitor-eerste-kwartaal-2014/. Zie ook: CBS webmagazine, 8 juli 2013, 'Mobiel online vooral met smartphone', URL: http://www.cbs.nl/nl-NL/menu/themas/vrije-tijd-cultuur/publicaties/artikelen/archief/2013/2013-3851-wm.htm
[7] The Guardian, 4 maart 2015, 'Smartphones are addictive and should carry health warning, say academics'. Geraadpleegd 5 juni 2015, URL: http://www.theguardian.com/technology/2015/mar/04/smartphones-addictive-make-people-narcissistic-say-academics
[8] Op iPhones staat bluetooth standaard 'aan' en wordt ook na elke software-update weer 'aan' gezet. Bron: De Morgen, 13 maart 2014, 'Waarom zet Apple stiekem bluetooth op iPhones aan na laatste iOS-update?', URL: http://www.demorgen.be/economie/waarom-zet-apple-stiekem-bluetooth-op-iphones-aan-na-laatste-ios-update-a1811034/.

persoonlijk raken. Dit kan bijvoorbeeld als historische meetgegevens uit wifi- of bluetooth-tracking worden opgevraagd door opsporingsautoriteiten.[9]

Het is lastig voor betrokkenen om zich te onttrekken aan wifi-tracking. De meeste trackingactiviteiten zijn immers niet kenbaar. Een manier om aan wifi-tracking te ontsnappen is om de wifi-functie van een apparaat uit te schakelen. Men kan de smartphone uiteraard ook helemaal uit zetten. Wanneer (de wifi-functie van) een apparaat is uitgeschakeld, kan het geen onderwerp van wifi-tracking meer zijn. Het (deels) uitschakelen van mobiele apparaten gaat echter gepaard met een verlies aan functionaliteit. Het uitschakelen van een telefoon beperkt niet alleen de telefonische bereikbaarheid, maar ook betalingsmogelijkheden, e-mailfuncties, gebruik van radio, muziekspelers, camera, en apps zoals *quantified self*-toepassingen et cetera.[10]

Gelet op de voornoemde omstandigheden heeft het CBP besloten om een onderzoek in te stellen naar wifi-tracking. Dit onderzoek valt binnen de onderzoeksprioriteiten van het CBP in 2014 en 2015.[11]

Het CBP heeft specifiek onderzoek ingesteld naar de verwerking van persoonsgegevens bij Bluetrace omdat de technologie van Bluetrace in gebruik is bij een aantal klanten met veel winkels in Nederlandse steden. De technologie wordt ook afgenomen door [vertrouwelijk], waardoor de activiteiten van Bluetrace in potentie een groot aantal Nederlanders raken.

Het bedrijf kwam in januari 2014 in het nieuws, toen bekend werd dat de BAS Group – al dan niet samen met Bluetrace – wifi-trackingtechnologie van Bluetrace toepaste in alle 160 winkels van MyCom, Dixons en iCentre, zonder dat het publiek hiervan op de hoogte was. Er werden Kamervragen gesteld over de grondslag voor deze gegevensverwerking.[12] Het CBP heeft eind 2014 vastgesteld dat Bluetrace ondanks deze ontwikkelingen geen privacybeleid had ontwikkeld.[13] Begin juni 2015 bevatte de vernieuwde website van Bluetrace nog steeds geen privacybeleid of andere informatie over de verwerking van persoonsgegevens.[14] Het CBP heeft gedurende 2014 signalen van het publiek ontvangen over wifi-tracking door Bluetrace.

---

[9] Zie bijvoorbeeld: Gerechtshof Arnhem/Leeuwarden, 27 november 2014, zaaknummer KS 21-000096-14 (medeplichtigheid aan moord op sportschoolhouder Almere).
[10] Vergelijk bijvoorbeeld: Whizpr.nl, 25 september 2012, 'Onderzoek PayPal: Jong volwassene hecht meer waarde aan smartphone dan aan portemonnee', URL: http://www.whizpr.nl/persberichten/onderzoek-paypal-jong-volwassene-hecht-meer-waarde-aan-smartphone-dan-aan-portemonnee.
[11] Bron: Toezichtagenda CBP 2015, URL: https://cbpweb.nl/nl/nieuws/cbp-presenteert-toezichtagenda-voor-2015.
[12] Kamerstukken II 2013-2014, Aanhangsel Handelingen, 2014Z01179, Vragen van de leden Oosenbrug (PvdA) en De Liefde (VVD) aan de ministers van Economische Zaken en van Veiligheid en Justitie over wifi-tracking door winkels (ingezonden 24 januari 2014) nr. 1811 en document 2014Z04895: Vragen van het lid Oosenbrug (PvdA) aan de ministers van Veiligheid en Justitie en van Economische Zaken over wifi- en bluetooth tracking (ingezonden 17 maart 2014) nr. 1696, met Antwoord van Staatssecretaris Teeven (Veiligheid en Justitie) mede namens de Minister van Economische Zaken (ontvangen 25 april 2014). Aanhangsel Handelingen Tweede kamer, 2013-2014-1811. Zie ook: Tweakers, 23 januari 2014, 'Winkels volgen je voetsporen - De opkomst van tracking via wifi-signalen', URL: http://tweakers.net/reviews/3385/3/wifi--tracking-winkels-volgen-je-voetsporen-dixons-mycom-en-icentre.html.
[13] Website Bluetrace, URL: http://www.bluetrace.nl, forensisch vastgelegd door het CBP op 10 december 2014.
[14] Website Bluetrace, URL: http://www.bluetrace.eu forensisch vastgelegd door het CBP op 8 juni 2015.

Afbakening en onderzoeksvragen

Het CBP heeft dit onderzoek beperkt tot wifi-tracking in en rond winkels door Bluetrace in Nederland met als doel het genereren van bedrijfseconomische informatie.[15] De keuze om bluetooth-tracking op dit moment buiten het onderzoek te laten is mede gebaseerd op verklaringen van Bluetrace waaruit blijkt dat het overgrote deel van de huidige metingen van Bluetrace in Nederland wifi-waarnemingen betreft. Zowel bij wifi- als bij bluetooth-tracking is het mac-adres het essentiële element waarmee tellingen en metingen kunnen worden verricht.

Het CBP heeft vanuit zijn toezichthoudende rol en naar aanleiding van het bovenstaande onderzoek ingesteld. Het onderzoek heeft zich geconcentreerd op de volgende vragen:

- Worden er persoonsgegevens verwerkt bij het toepassen van wifi-trackingtechnologie van Bluetrace?
- Is Bluetrace de verantwoordelijke in de zin van de Wbp voor de verwerking van persoonsgegevens via wifi-tracking?
- Heeft Bluetrace een grondslag voor het verwerken van persoonsgegevens voor bedrijfseconomische doeleinden? Het onderzoek ziet op zowel tracking in een winkel als het volgen van betrokkenen in de openbare ruimte, zoals buiten een winkel.
- Informeert Bluetrace het publiek op adequate wijze over de persoonsgegevens die via wifi-tracking worden verzameld en verwerkt voor bedrijfseconomische doeleinden?
- Worden de meetgegevens niet langer bewaard dan noodzakelijk is voor de beoogde doelen?

Het onderzoek richt zich aldus op toetsing aan de artikelen 1, onder a, b en d, van de Wbp (definitie persoonsgegeven, verwerking van persoonsgegevens, verantwoordelijkheid voor de gegevensverwerking), artikel 8 van de Wbp (grondslag in de Wbp), de artikelen 33 en 34 van de Wbp (informatieplicht), in combinatie met artikel 6 (zorgvuldige verwerking) en artikel 10 van de Wbp (bewaartermijn).

[15] [vertrouwelijk]

2. PROCEDURE

Het verloop van de procedure is als volgt:

- Op 10 december 2014 heeft het CBP telefonisch en per e-mail aangekondigd dat het voornemens was om ambtshalve onderzoek in te stellen naar bepaalde gegevensverwerkingen bij Bluetrace.
- Op 10 december 2014 heeft Bluetrace per e-mail de ontvangst van het e-mailbericht van het CBP bevestigd.
- Bij brief van 11 december 2014 heeft het CBP formeel aangekondigd ambtshalve onderzoek in te stellen naar bepaalde gegevensverwerkingen bij Bluetrace en gevraagd om inlichtingen. In de brief is tevens een onderzoek ter plaatse aangekondigd.
- Op 2 januari 2015 heeft Bluetrace per e-mail de ontvangst van de brief van 11 december 2014 bevestigd.
- Bluetrace heeft per e-mail van 15 januari 2015 uitstel gevraagd voor het beantwoorden van de schriftelijke vragen.
- Op 15 januari 2015 heeft het CBP uitstel verleend tot en met 22 januari 2015.
- Op 22 januari 2015 heeft Bluetrace per fax voldaan aan het verzoek om inlichtingen en bescheiden. Niet alle vragen zijn op dat moment echter voldoende inhoudelijk beantwoord.
- Op 3 februari 2015 heeft het CBP een onderzoek ter plaatse ingesteld bij Bluetrace te Amsterdam.
- Op 12 februari 2015 heeft een vertegenwoordiger van Bluetrace een aanvullende toelichting op een aantal technische zaken gegeven ten kantore van het CBP. Het ging deels om het beantwoorden van vragen die tijdens het onderzoek ter plaatse niet beantwoord waren.
- Op 24 februari 2015 heeft het CBP per brief verzocht om aanvullende inlichtingen.
- Op 26 februari 2015 heeft Bluetrace per brief de vragen van 24 februari 2015 beantwoord en de gevraagde bescheiden verstrekt.
- Bij brief van 27 februari 2015 heeft het CBP een schriftelijke weergave van de verklaringen van Bluetrace ten tijde van het bedrijfsbezoek van 3 februari 2015 toegezonden aan Bluetrace. In deze brief heeft het CBP aangegeven dat Bluetrace de gelegenheid had om te reageren op de brief en om aan te geven of het bedrijf zich herkende in de weergave van verklaringen. Het CBP verleende een reactietermijn tot en met 13 maart 2015.
- Bluetrace heeft niet gereageerd op de brief van 27 februari 2015. Het CBP gaat er daarom vanuit dat de verklaringen zoals opgetekend in de brief van 27 februari 2015 juist zijn.
- Bluetrace heeft per e-mail op 27 maart 2015 nadere technische gegevens over antennes toegezonden aan het CBP.
- Op 21 juli 2015 heeft het CBP een rapport van voorlopige bevindingen vastgesteld en verzonden aan Bluetrace. In de begeleidende brief is aangegeven dat Bluetrace in de gelegenheid is gesteld om een zienswijze op het rapport in te dienen en om aan te geven welke onderdelen van het rapport, naar het oordeel van Bluetrace, bedrijfsvertrouwelijk zijn.
- Bij brief van 26 augustus 2015 heeft Bluetrace gereageerd op de voorlopige bevindingen van het CBP met een zienswijze en een plan van aanpak. Het

plan van aanpak bevat voorstellen voor het nemen van maatregelen en voor het starten van onderzoeken naar de overtredingen die het CBP heeft gesignaleerd in het rapport van voorlopige bevindingen. Bluetrace heeft in haar zienswijze niet aangegeven in hoeverre het rapport van voorlopige bevindingen bedrijfsvertrouwelijke passages bevat.

3. FEITELIJKE BEVINDINGEN

3.1 Organisatie en werkwijze Bluetrace

Bluetrace levert wifi- en bluetooth-technologie voor tracking van mobiele apparatuur in winkels, in winkelgebieden, op stations en langs snelwegen.[16] Wifi-tracking en bluetooth-tracking worden met name gebruikt om drukte en menselijke verplaatsingen te meten. De wifi- en bluetooth-trackingtechnologie van Bluetrace maakt gebruik van het feit dat smartphones en andere mobiele apparatuur hun unieke mac-adressen uitzenden om verbindingen tot stand te kunnen brengen. Door deze signalen op te vangen met sensoren is tracking mogelijk: het registreren van de aanwezigheid van een – nieuw of eerder waargenomen – apparaat in de buurt van de sensor op een bepaald moment.

Volgens de KvK-registratie zijn de hoofdactiviteiten van Bluetrace B.V. het *"beheer van computerfaciliteiten"*, *"overige dienstverlenende activiteiten op het gebied van informatietechnologie"*, *"het verrichten van diensten en activiteiten op het gebied van meetbare mobiele oplossingen"* en het *"leveren en onderhouden van wifi-netwerken."*[17] Praktisch betekent dit dat Bluetrace ook wifi-gastnetwerken levert en dat het bedrijf daaraan diverse diensten kan koppelen, zoals het faciliteren van direct-marketingactiviteiten. Deze dienstverlening op het terrein van wifi-gastnetwerken en daaraan gekoppelde activiteiten valt buiten het bereik van dit onderzoek.[18]

Bluetrace is in 2008 begonnen om bluetooth-tracking in te zetten op evenementen. In 2010 is het bedrijf begonnen met de ontwikkeling en uitrol van tracking op basis van wifi-signalen. Bluetrace bediende begin 2015 circa [vertrouwelijk] klanten in Nederland op het gebied van wifi- en bluetooth-tracking. Het CBP heeft vastgesteld dat Bluetrace betrokken is bij trackingactiviteiten op ten minste [vertrouwelijk] locaties in Nederland.[19] Het gaat daarbij om tracking in winkelgebieden, in en rond winkels en [vertrouwelijk].
Het registreren, volgen en in kaart brengen van wifi- en bluetooth-signalen van mobiele apparatuur levert een schat aan informatie op die voor uiteenlopende doelen relevant kan zijn. Informatie over de locatie en beweging van klanten is bijvoorbeeld waardevol voor bedrijfseconomische doeleinden, zoals het bepalen van de ideale personeelsplanning, het bepalen van de aantrekkelijkheid van een winkel voor langslopend publiek of het meten van drukte op een bepaalde plaats. Het toepassen van wifi-tracking in winkelgebieden kan ook voordelen met zich meebrengen voor de consument. Wanneer de hoeveelheid personeel goed is afgestemd op de drukte in een winkel, hoeft een klant wellicht minder lang te wachten. Een consument heeft ook baat bij de optimalisering van looproutes door een winkel. Er zijn dan minder knelpunten waar mensen elkaar lastig kunnen passeren en/of de uitgangen zijn beter bereikbaar. Dit laatste gebeurt bijvoorbeeld op [vertrouwelijk].[20] Meetgegevens over

[16] Bluetrace is onderdeel van de Moreless Group. De activiteiten van het bedrijf Moreless bestaan onder meer uit de verkoop van en service aan draadloze betaalautomaten. Moreless B.V is ingeschreven bij de Kamer van Koophandel onder nummer 34231107.
[17] Bron: Uittreksel handelsregister Kamer van Koophandel. Geraadpleegd op 12 november 2014, op 3 juni 2015 en op 8 juli 2015.
[18] Dat Bluetrace ook wifi-gastnetwerken levert, blijkt uit de website www.bluetrace.eu. Bluetrace heeft dit ook bevestigd tijdens het onderzoek ter plaatse door het CBP op 3 februari 2015.
[19] Bluetrace levert op dit moment wifi- en bluetooth-tracking aan [vertrouwelijk].
[20] [vertrouwelijk].

drukte en bewegingen van het publiek blijken in de praktijk ook gebruikt te kunnen worden voor het beheersen van grote groepen mensen tijdens evenementen of het bepalen van de geschiktste inrichting van een terrein met het oog op de openbare orde of de veiligheid van het publiek.[21]

Bluetrace verricht deze activiteiten voor bedrijfseconomische doelen, zoals het meten van 'retail performance'. Bluetrace werkt ook mee aan tracking voor [vertrouwelijk]. Bluetrace is actief (voor klanten) in België, Italië, Ierland, Duitsland, Zwitserland, Dubai en Canada.[22] De activiteiten buiten Nederland vallen buiten het bereik van dit onderzoek. Bluetrace richt zich in Nederland met name op de volgende activiteiten:[23]

- Verkoop van sensoren en installaties voor wifi- en bluetooth-tracking, alsmede uitgifte van licenties voor het gebruik van technieken en software.
- Trackingdienstverlening, bestaande uit het plaatsen en onderhouden van sensoren op locatie, het verrichten van data-analyse van de meetgegevens en visualisatie van de metingen via een *user interface* voor de klant, het 'Dashboard'.
- Servicecontracten en technische ondersteuning voor tracking.

3.2 Middelen voor wifi-tracking

Bluetrace gebruikt sensoren die zowel wifi- als bluetooth-signalen kunnen meten voor trackingdiensten. Bluetrace heeft tijdens het onderzoek ter plaatse door het CBP op 3 februari 2015 een voorbeeld van de apparatuur getoond, die gebruikt wordt door de klanten van Bluetrace. Het gaat om een sensor [vertrouwelijk] die werkt op basis van [vertrouwelijk] software.

De getoonde sensor beschikt over twee antennes: een bluetooth-antenne en een wifi-antenne. De apparatuur bevat [vertrouwelijk].[24] Er kunnen meer antennes voor het opvangen van signalen op een sensor aangesloten worden, bijvoorbeeld om twee verschillende gebieden in of rond een winkel in kaart te brengen. Dit wordt de *multi zone*-optie genoemd.[25]

Het opvangen van een mac-adres met de wifi-antenne, zoals door Bluetrace is geïmplementeerd, is een passieve handeling: de apparaten binnen het bereik van de antenne zenden het adres zelf uit, de antenne vangt dit slechts op. Op basis van een [vertrouwelijk] wordt geluisterd naar het netwerkverkeer. Uit dit netwerkverkeer worden mac-adressen en data over signaalsterkte gefilterd. Deze gegevens worden

[21] Verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace van 27 februari 2015 (bijlage).
[22] Bron: (oude) website Bluetrace, URL: http://www.bluetrace.nl. Deze informatie blijkt tevens uit interne documenten, onder meer [vertrouwelijk].
[23] Voor zover relevant voor dit onderzoek. Bron: verklaringen tijdens het bedrijfsbezoek op 3 februari 2015 zoals weergegeven in de brief van het CBP aan Bluetrace van 27 februari 2015.
[24] Verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace d.d. 27 februari 2015, bijlage, onder meer punten 6 en 7.
[25] [handleiding].

naar een server verstuurd. De onderzochte apparatuur van Bluetrace kan [vertrouwelijk] mac-adressen per minuut verwerken.[26]

3.3 De inzet van middelen en de reikwijdte van metingen

De apparatuur wordt door Bluetrace per klant en per locatie handmatig ingesteld.[27] Bluetrace plaatst steeds één sensor per winkel. Een monteur van Bluetrace bepaalt de ideale positie voor het plaatsen van de sensor in een winkel. Om de sensor goed af te stellen, meet de monteur op een aantal plaatsen rondom de sensor, aan de hand van het signaal van een telefoon. Hierbij loopt de monteur ook buiten de winkel en naar de overkant van de straat. De monteur meet met de apparatuur de grenswaarde van de signaalsterkte, zodat duidelijk is of een bezoeker in de winkel of een voorbijganger buiten de winkel wordt geregistreerd. In beginsel wordt de sensor voor een zo goed mogelijke ontvangst midden in de winkel, boven (aan) het plafond bevestigd. [28] In de installatiehandleidingen wordt bovendien aanbevolen om de sensor dicht bij een verkooppunt (kassa) te plaatsen.[29]

Afbeelding 1: Kastje met sensor en wifi-antenne

[afbeelding vertrouwelijk]

Omgevingsfactoren spelen een rol bij het vaststellen van de ideale instellingen van de sensoren. Signalen uit langsrijdende trams en bussen kunnen bijvoorbeeld de metingen beïnvloeden. Signaalsterkte is een belangrijk gegeven om afstand tot een sensor te bepalen en ook om het onderscheid tussen een winkelbezoeker en een passant op straat te maken.

3.4 Verzamelen van ruwe meetgegevens

Het belangrijkste aspect dat wordt gemeten is de aanwezigheid van een apparaat met een actieve wifi-functie binnen het bereik van de sensoren. Deze aanwezigheid wordt vastgesteld door het waarnemen van het wifi-mac-adres van dat apparaat.

In winkelgebieden kan Bluetrace met één sensor per winkel vaststellen of een bezoeker binnen of buiten de winkel is, en hoe lang een bezoeker in – of buiten – het pand verblijft. Het element signaalsterkte is daarvoor van grote betekenis. Hoe dichter het apparaat bij de sensor is, hoe sterker het signaal. Bluetrace doet in Nederland niet aan nauwkeurige plaatsbepaling via triangulatie.[30]

---

[26] De getoonde sensor is van het type [vertrouwelijk]. Bron: verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace d.d. 27 februari 2015.

[27] Verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace d.d. 27 februari 2015 (bijlage). De standaardwerkwijze staat in de handleiding voor monteurs: [handleiding].

[28] Zie [handleiding]. Zie ook: [handleiding]. Verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace van 27 februari 2015 (bijlage).

[29] Bron: [handleiding].

[30] Triangulatie werkt met een combinatie van meetgegevens vanuit drie sensoren. Verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace d.d. 27 februari 2015 (bijlage). Verklaringen betreffen de activiteiten in Nederland, op het moment van het onderzoek ter plaatse, februari 2015.

Het CBP heeft tijdens het onderzoek ter plaatse vastgesteld dat Bluetrace een standaardformule gebruikt om de afstand tussen het gemeten apparaat en de sensor te berekenen op basis van de signaalsterkte.[31]

Het aantal detecties van een bepaald mac-adres door dezelfde sensor is van belang om waar te nemen hoe lang een bezoeker op ongeveer dezelfde plaats blijft en ook om een winkelbezoeker van een passant te onderscheiden. Iedere [vertrouwelijk] seconden zendt de sensor meetgegevens van de op dat moment waargenomen apparaten naar de servers van Bluetrace. Zo ontstaat er een serie momentopnames (samples) in de tijd, waarmee een gedetailleerd beeld gevormd kan worden over aanwezigheid en verplaatsing van unieke mobiele apparaten. Zodra een mac-adres in meerdere samples achter elkaar voorkomt, is dit een indicatie dat een apparaat gedurende langere tijd wordt waargenomen bij dezelfde sensor. In dat geval gaat Bluetrace ervan uit dat de persoon die het apparaat bij zich heeft gedurende een bepaalde tijd in de buurt van de sensor is gebleven of is blijven staan. Dit wordt *dwell time* genoemd. Wanneer er gebruik wordt gemaakt van de *multi zone*-optie, dus het installeren van één sensor met meerdere antennes die elk gericht zijn op een eigen gebied, kan het aantal winkelbezoekers ook op een andere manier vastgesteld worden. Wanneer de ene antenne voornamelijk is gericht op het gebied buiten de winkel en de andere voornamelijk binnen de winkel meet, kan een beeld gevormd worden van inkomende en uitgaande bezoekers.[32]

Samenvattend genereert Bluetrace de volgende ruwe meetgegevens bij wifi-tracking in en rondom winkels.[33]

- Het mac-adres van (mobiele) apparaten.
- De signaalsterkte van het geregistreerde wifi- signaal van de apparaten.
- Het serienummer van de sensor.
- Datum en tijdstip van de meting.

3.5 Analyse van gegevens uit wifi-tracking in en rondom winkels

Uit de ruwe meetgegevens (mac-adres, signaalsterkte, sensornummer, datum en tijdstip van meting) kan Bluetrace een aantal geavanceerdere meetresultaten genereren voor zijn klanten, door het analyseren van de data.[34]

Afbeelding 2: Schermafbeelding vastgelegde gegevensverwerking

[afbeelding vertrouwelijk]

Deze analyse levert de volgende soorten informatie op:

- Tellingen: het tellen van het aantal unieke apparaten (personen) dat langs een sensor komt.[35]

[31] Bedrijfsbezoek CBP op 3 februari 2015.
[32] [handleiding].
[33] Verklaringen tijdens het bedrijfsbezoek op 3 februari 2015 zoals weergegeven in de brief van het CBP aan Bluetrace d.d. 27 februari 2015, bijlage, onder meer paragraaf 30.
[34] Verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace d.d. 27 februari 2015 (bijlage); [handleiding].
[35] Bluetrace schrijft hierover: "*Counting of all visitors entering and walking along venue. Determine shopper and window conversion and recognize peak hours for staff planning. Maybe change opening hours? Staff can*

- Mobiliteit: het analyseren van de bewegingen van apparaten binnen het bereik van de sensoren. Daarin wordt inbegrepen het bijhouden waar mensen pauzeren, vastlopen, versnellen et cetera, alsmede het onderscheid tussen een winkelbezoeker en een passant.[36] De mogelijkheden van trajectmetingen vallen buiten het bereik van dit onderzoek.[37]
- Bezoekfrequentie: het registreren hoe vaak een bepaald apparaat binnen het bereik van de sensoren is geweest, om zo het onderscheid mogelijk te maken tussen 'unieke' en 'terugkerende' apparaten, alsmede tussen nieuwe bezoekers en vaste klanten.[38]

Bluetrace meet sinds het vierde kwartaal van 2013 continu, dat wil zeggen: 24 uur per dag en zeven dagen per week, hoeveel mensen er langs winkels van zijn klanten lopen, hoeveel mensen er binnenkomen en vervolgens hoe lang klanten gemiddeld in de buurt blijven (*dwell time*). [39] Daarmee weet de klant bijvoorbeeld hoeveel personeel er nodig is in de winkel. Bij benadering weten Bluetrace en zijn opdrachtgevers ook hoeveel voorbijgangers er in een openbaarvervoermiddel of een auto langs de winkel kwamen in een bepaalde periode.[40] Een overzicht van de meetresultaten die Bluetrace verzorgt met tracking is weergegeven in de afbeelding hieronder.[41]

Afbeelding 3: Meetresultaten wifi-tracking in en rondom winkels door Bluetrace

Ruwe meetgegevens worden omgezet in de volgende meetresultaten
Verblijftijd mac-adres nabij een sensor
Aantal mac-adressen per uur, per dag
Aantal unieke mac-adressen per uur, per dag
Meten bezoekfrequentie
Aantal winkelpassanten per uur, per dag
Aantal unieke winkelpassanten per uur, per dag
Aantal winkelbezoekers per uur, per dag
Aantal unieke winkelbezoekers per uur, per dag
Aantal winkelcentrumbezoekers per uur, per dag

be excluded from counting by wearing Bluetrace Staff Tags", URL: www.bluetrace.nl/#wifi-tracking (URL forensisch vastgelegd door het CBP op 10 december 2014).

[2] Bluetrace schrijft hierover:"*Where are they moving to or pausing? Where are 'hot zones'? Do we need more staff? Are people queuing at the checkout? Analyze, compare and improve the store layout and design: facilitate the shopper's path to purchase.*", URL: http://www.bluetrace.nl/#Wi-Fi Tracking (URL forensisch vastgelegd door het CBP op 10 december 2014).

[37] Bluetrace kan metingen doen met meer dan één sensor om apparaten over een bepaald traject te registreren, bijvoorbeeld tijdens een evenement. Daarmee kan de verplaatsingsroute van personen op een bepaald traject worden geregistreerd. Zoals aangegeven in de inleiding van dit rapport, richt dit onderzoek zich uitsluitend op wifi-tracking in en rond winkels, mede omdat Bluetrace heeft verklaard dat het bedrijf op het moment van onderzoek, begin 2015, geen (traject)metingen met meer dan één sensor verricht in winkelgebieden in Nederland.

[38] Bluetrace schrijft:"*How many of your visitors are new? How many are loyal or cross store visitors? How often do they visit the store? Design and assortment need to be adjusted to the kind of crowd: tourists and day trippers for instance need different service and assortment then local costumers. Analyze and follow all trends in real time on the clear, easy to use Bluetrace dashboard. All data is collected and stored, ready to be integrated into any BI system. This Wi-Fi driven solution is remarkably more affordable and sophisticated than any other existing tracking systems working with cameras or sensors*". Website Bluetrace, door het CBP vastgelegd op 10 december 2014. (URL: http://www.bluetrace.nl/#Wi-Fi Tracking)

[39] Verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace van 27 februari 2015 (bijlage). Dit doen zij in elk geval voor [afnemer].

[40] Zie [handleiding]. Door de samplefrequentie van [vertrouwelijk] seconden betreft dit een minder nauwkeurige meting dan van bezoekers in de winkel.

[41] Brief van Bluetrace aan het CBP van 22 januari 2015, met antwoorden op de vragen van het CBP.

Aantal unieke winkelcentrumbezoekers per uur, per dag

Aanvullende gegevens
Bluetrace heeft verklaard dat er in sommige gevallen aanvullende gegevens worden verwerkt om de meetresultaten zoals opgesomd in afbeelding 3 meer nauwkeurigheid te geven. Het gebruik van aanvullende gegevens verschilt per opdrachtgever. Het CBP heeft vastgesteld dat Bluetrace en haar klanten in sommige gevallen gebruik maken van camera's om de gegevens over het aantal waargenomen apparaten te corrigeren naar het aantal personen. Het gaat hier om camera's waarmee wordt waargenomen hoeveel mensen zich ergens bevinden, of hoeveel mensen een poortje passeren. Er wordt geen visueel beeld van personen vastgelegd, maar de camera herkent contouren van mensen en telt deze. Het gaat daarbij vaak om eigen apparatuur van de klant, maar Bluetrace kan deze apparatuur ook leveren en installeren bij de klant.[42] Cameragegevens die worden verwerkt zijn in dat geval getallen over het aantal personen dat een ruimte inloopt en het aantal personen dat een ruimte verlaat. Met deze getallen kunnen meetgegevens over het aantal waargenomen apparaten worden gecorrigeerd indien gewenst. Aanvullende gegevens zijn echter niet vereist om wifi-tracking te kunnen doen voor bedrijfseconomische doeleinden.[43]

Bluetrace heeft verklaard dat het bedrijf alleen klantspecifieke rapportages produceert. Dat wil zeggen dat Bluetrace geen data-analyse doet op basis van gegevens van meerdere klanten of alle klanten. Bluetrace berekent alleen rapportages per klant en per filiaal. Er worden geen rapportages van alle filialen in een winkelketen samen of van meerdere klanten gemaakt. [Vertrouwelijk].[44]

Hashing
Hashen is een wiskundige bewerking die informatie (bijvoorbeeld een mac-adres) omzet in een hashwaarde die altijd even lang is (bijvoorbeeld in het geval van SHA1, 160 bits). Het maakt daarbij niet uit hoe groot de ingevoerde informatie is. Het CBP heeft vastgesteld dat Bluetrace als hashingmethode [vertrouwelijk] toepast.[45] [Beschrijving hashing methode].[46] Het CBP heeft vastgesteld dat de datum die meegenomen wordt in de hashing standaard een nauwkeurigheid van één dag heeft.[47] Hierdoor zal de waarneming van het zelfde mac-adres op twee verschillende dagen leiden tot een andere hashwaarde. Klanten van Bluetrace kunnen er voor kiezen om de periode die is aangegeven in het hashing algoritme aan te (laten) passen.[48] Het geheel van de hierboven omschreven bewerkingen wordt hierna hashing genoemd.

[42] Zie [handleiding]. Zie ook de overeenkomst tussen [afnemer] en Bluetrace.
[43] Het onderhavige onderzoek is beperkt tot de toetsing van de verwerking van mac-adressen, signaalsterkte, sensornummer en datum en tijdstip van meting, omdat dit de set gegevens is bij alle opdrachten verwerkt wordt door Bluetrace. Deze set gegevens is elk geval minimaal vereist voor Bluetrace om via wifi-tracking bedrijfseconomische gegevens te leveren aan klanten. Nader onderzoek naar aanvullende gegevens vereist onderzoek bij opdrachtgevers en dat valt buiten de omvang van dit onderzoek naar Bluetrace.
[44] Zie: [handleiding], pagina 15-18. Zie ook: [handleiding] .
[45] [vertrouwelijk]
[46] Zie [handleiding].
[47] Uit [handleiding] blijkt dat Bluetrace de volgende hashfunctie gebruikt voor [hashing]: [vertrouwelijk].
[48] Uit [handleiding] blijkt dat Bluetrace de volgende hashfunctie gebruikt voor [hashing]: [vertrouwelijk]

Bluetrace heeft verklaard dat zij op verschillende momenten hashing toepast. Hashing kan plaatsvinden op de sensor (bij het verzamelen van gegevens) of op de server (bij het opslaan of bewerken van gegevens). Normaal gesproken slaat Bluetrace meetgegevens op en vervangt hierin de mac-adressen na drie weken met de gehashte waarden. Bluetrace kan de gegevens op verzoek van een klant ook eerder hashen, op de sensoren vlak nadat de mac-adressen zijn vastgelegd, maar het bedrijf heeft verklaard dat dit niet de standaardinstelling van de apparatuur en de software is. [Afnemer] heeft gevraagd om hashing op de sensoren toe te passen.[49]

3.6 Onderzoeken naar het aanpassen van de werkwijze

Naar aanleiding van het rapport voorlopige bevindingen van het CBP heeft Bluetrace in zijn brief van 27 augustus 2015 voorgesteld om onderzoek te doen naar mogelijkheden om zijn werkwijze aan te passen. Hiervoor heeft Bluetrace een beknopt plan van aanpak opgesteld. Bluetrace stelt hierin voor om nader onderzoek te doen naar pseudonimisering, anonimisering, het beperken van metingen in plaats en tijd en opt-out-mogelijkheden. Bluetrace geeft in het plan van aanpak geen concrete inschatting van de maatregelen die eventueel kunnen worden ontwikkeld naar aanleiding van deze onderzoeken en de opleverdatum van een eventueel onderzoeksrapport.

Pseudonimisering
Bluetrace heeft voorgesteld om in kaart te brengen hoe het mac-adres kan worden gemaskeerd dan wel omgezet kan worden naar een ander uniek identificatie(kenmerk). Op deze wijze zou dan het mac-adres als middel om personen te identificeren weggenomen kunnen worden. Bluetrace stelt voor het proces van pseudonimisering onder te brengen bij een derde partij (outsourcing) zodat Bluetrace zelf (en zijn klanten) nog slechts gebruik maakt van deze afgeleide gegevens en er in mindere mate mac-adressen verwerkt worden.

Anonimiseren van mac-adressen
In de zienswijze van 27 augustus 2015 heeft Bluetrace eveneens voorgesteld om onderzoek te doen naar mogelijkheden om mac-adressen te anonimiseren. Bluetrace heeft aangegeven dat het bedrijf gaat onderzoeken wat de consequenties zijn van het anonimiseren van mac-adressen binnen een bepaalde tijd na de eerste vastlegging van de gegevens (bijvoorbeeld 24 uur). Dit onderzoek kan, aldus Bluetrace, worden voltooid op [datum].

Beperking van de reikwijdte van metingen in plaats en tijd
Bluetrace stelt voor om te onderzoeken welke consequenties voor de eigen bedrijfsvoering, lopende contractuele verplichtingen en het zakelijke bedrijfsmodel van Bluetrace het beperken van wifi-tracking tot binnen de winkels zou hebben. Dit onderzoek kan, conform het bijbehorende plan van aanpak, voltooid zijn binnen [periode].
Tevens heeft Bluetrace voorgesteld aan het CBP om onderzoek te doen naar de consequenties van het beperken van wifi-tracking in tijd, bijvoorbeeld tot binnen de

[49] Verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace d.d. 27 februari 2015 (bijlage). Paragraaf 20-21.

winkelopeningstijden. Dit onderzoek kan, conform het plan van aanpak, voltooid zijn binnen [periode].

Opt-out mogelijkheden
Bluetrace stelt in zijn brief van 26 augustus 2015 tot slot voor om technisch te onderzoeken in hoeverre opt-out mogelijkheden kunnen worden ingezet. Dit onderzoek kan binnen [periode] worden voltooid, volgens het bijgeleverde plan van aanpak.

3.7 Verantwoordelijkheid voor gegevensverwerking

Bluetrace schrijft in de brief van 22 januari 2015 dat het bedrijf verantwoordelijk is voor de verwerking van ruwe meetgegevens uit wifi-tracking, zoals mac-adressen en signaalsterkten. Ook neemt Bluetrace opslag en beheer van data voor zijn rekening.[50] Het CBP heeft, onder meer tijdens het bedrijfsbezoek, zelfstandig vastgesteld dat Bluetrace feitelijk beschikt over alle gegevens zoals genoemd in paragrafen 3.4. en 3.5 van dit rapport en dat het bedrijf zeggenschap heeft over de toegang tot deze gegevens.[51]

Bluetrace heeft verklaard dat de ruwe meetgegevens in principe niet worden verstrekt aan derden. Bluetrace heeft een verzoek van een van zijn klanten afgewezen om meetgegevens te mogen inzien naar aanleiding van een winkeldiefstal.[52] Bluetrace is met een van zijn klanten specifiek overeengekomen dat hij deze klant wel de ruwe meetgegevens, waaronder de mac-adressen, ter beschikking stelt.[53] Bluetrace heeft verklaard dat hij zelf gegevens heeft verstrekt aan autoriteiten voor een opsporingsonderzoek.[54]

Bluetrace heeft verklaard dat het bedrijf afspraken maakt met zakelijke partners over het eigendom van en/of de verantwoordelijkheid voor data. Tijdens het ambtshalve onderzoek heeft het CBP de overeenkomsten tussen Bluetrace en zijn klanten opgevraagd. Uit deze overeenkomsten blijkt dat partijen geen schriftelijke afspraken hebben gemaakt over het eigendom van en de verantwoordelijkheid voor meetgegevens en gerelateerde data.

Er is bij Bluetrace eind 2013, begin 2014 een interne inventarisatie en evaluatie geweest naar dataverwerking en beveiliging. In deze evaluatie van de IT-systemen is gekeken naar onder andere privacyaspecten van de dataverwerking en de beveiliging van gegevens.[55]

In de rapportage wordt geconcludeerd dat mac-adressen niet herleidbaar zijn tot IMEI-nummers[56], telefoonnummers of andere gegevens die personen identificeren. In de brief van 22 januari 2015 heeft Bluetrace aan het CBP verklaard dat het bedrijf zich

[50] Brief Bluetrace van 22 januari 2015.
[51] Bedrijfsbezoek CBP, gesprek met Bluetrace, screenshots gemaakt tijdens het bedrijfsbezoek.
[52] In verband met een diefstal in een winkel van een klant van Bluetrace, in 2008. De klant heeft toen gevraagd om de mac-adressen. Bluetrace heeft deze gegevens niet verstrekt.
[53] Overeenkomst met [vertrouwelijk]
[54] Bij ongeregeldheden rondom [vertrouwelijk]. De politie [regio] heeft toen gevraagd om de meetgegevens, inclusief mac-adressen van Bluetrace. Bluetrace heeft de gegevens verstrekt.
[55] [Intern rapport van Bluetrace].
[56] IMEI staat voor International Mobile Equipment Identity. Dit is een (meestal 15-cijferig) nummer dat een mobiele telefoon identificeert.

op het standpunt stelt dat er bij wifi-tracking geen *persoons*gegevens worden verwerkt.[57] Bluetrace baseert deze conclusie voor een belangrijk deel op resultaten van het interne auditrapport.[58] Specifieke verantwoordelijkheden inzake de verwerking van *persoons*gegevens zijn niet vastgelegd binnen het bedrijf.

In de brief van 22 januari 2015 is Bluetrace echter, omwille van het onderzoek en in het geval het CBP anders oordeelt over deze kwestie, beknopt ingegaan op de vraag welke grondslagen voor de verwerking van persoonsgegevens mogelijk van toepassing zijn op de verwerking van meetgegevens uit wifi-tracking in en buiten winkels door Bluetrace. Bluetrace beroept zich op artikel 8 onder f, van de Wbp en wijst erop dat de verwerking van ruwe meetgegevens uit wifi-tracking in en rond winkels noodzakelijk is voor het genereren van bedrijfseconomische informatie over de commerciële prestatie van winkels. Bluetrace is van mening dat dit een gerechtvaardigd belang van Bluetrace en zijn opdrachtgevers is.

In zijn zienswijze op het rapport voorlopige bevindingen van 21 juli 2015 heeft Bluetrace voorgesteld om in overleg met zijn klanten nadere (contractuele) afspraken te maken over bewaartermijnen en eigendom van gegevens. Bluetrace geeft tevens aan dat deze afspraken kunnen leiden tot technische aanpassingen. Bluetrace heeft aangegevens dat deze maatregel voltooid kan zijn op [datum].

[57] Verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace van 27 februari 2015, (bijlage); Brief van Bluetrace aan het CBP van 22 januari 2015.
[58] Zie: [Intern rapport van Bluetrace].

3.8 Informatie door Bluetrace

Bluetrace heeft tijdens het onderzoek ter plaatse door het CBP op 3 februari 2015 verklaard dat het bedrijf zelf geen informatie aan het publiek verstrekt over wifi-tracking op of rond de plaatsen waar de sensoren van Bluetrace hangen.

Het bedrijf heeft voorts verklaard dat de klanten van Bluetrace dit in sommige gevallen wel doen, door stickers op de winkelruiten te plakken.[59] In januari 2014 heeft een woordvoerder van BAS Group verklaard in de media dat de winkelketens Dixons, MyCom en iCentre hun klanten zullen informeren over de aanwezigheid van wifi-tracking.[60] Het CBP heeft op 20 maart 2015 vastgelegd dat [afnemer] stickers op de winkelruiten heeft geplakt met de volgende tekst: "WIFI BT TELLER".[61] Op de sticker is – naast de tekst – ook een afbeelding van een hangslot te zien, een wifi-logo en een bluetooth-logo, zie afbeelding 4.[62]

Afbeelding 4: Informatiesticker over wifi-tracking

[afbeelding van situatie bij afnemer]

Er vindt geen melding (optisch of akoestisch) plaats op het apparaat wanneer het apparaat wordt waargenomen door de trackingsensoren. De aanwezigheid van wifi-tracking is voor een winkelbezoeker of voorbijganger ook niet op een andere wijze merkbaar. De sensoren voor wifi-tracking worden door Bluetrace geïnstalleerd op plaatsen die voor het publiek doorgaans niet zichtbaar zijn. De sensoren worden bijvoorbeeld boven de plafonds van een winkelruimte geplaatst of in een meterkast.[63]

Het CBP stelt vast dat Bluetrace, ondanks de aandacht van politiek en media begin 2014 voor dit onderwerp, geen voorlichtingsmateriaal voor het publiek of een kenbaar privacybeleid heeft ontwikkeld.[64]

In het voorjaar van 2015 heeft Bluetrace zijn website vernieuwd. Ook op deze website, www.bluetrace.eu, heeft het CBP geen informatie voor het publiek aangetroffen over de gegevensverwerking. [65]

---

[59] Verklaring van Bluetrace tijdens het onderzoek ter plaatse van 3 februari 2015, zoals weergegeven in de brief van het CBP van 27 februari 2015, bijlage, m.n. paragraaf 42.
[60] Bron: Tweakers.net, "Dixons, MyCom en iCentre gaan klanten informeren over wifi-tracking" (laatst geraadpleegd op 8 mei 2015)
[61] Forensisch vastgelegd door het CBP op 20 maart 2015, bij [afnemer].
[62] Idem.
[63] Verklaring Bluetrace tijdens het bedrijfsbezoek d.d. 3 februari 2015, zoals weergegeven in de brief van het CBP d.d. 28 februari 2015, bijlage, onder nummers 10 en 36.
[64] Zie in dit kader *Kamerstukken II* 2013–2014, Aanhangsel Handelingen, nr. 1696 (21 februari 2014) en nr. 1811 (24 april 2014) 2014Z04895 met het antwoord op Kamervragen van Kamerlid Oosenbrug aan de ministers van Veiligheid en Justitie en van Economische Zaken over wifi- en bluetooth-tracking. Bluetrace heeft geen meldingen gedaan in het meldingenregister van het CBP.
[65] Website door het CBP forensisch vastgelegd op 10 december 2014, 25 maart 2015 en 8 juni 2015. Medio mei 2015 heeft het CBP geconstateerd dat de website van Bluetrace vernieuwd is. Het CBP heeft op 8 juni 2015 op de nieuwe website geen privacybeleid of andere informatie voor het publiek over de privacyaspecten van wifi-tracking aangetroffen. Een zoekopdracht binnen de site naar het trefwoord 'privacy' leverde nul resultaten op. Ook een zoekopdracht in een zoekmachine naar de combinatie 'bluetrace' en 'privacy' leverde geen verwijzingen op naar privacybeleid van Bluetrace.

Uit de overeenkomsten die Bluetrace met zijn klanten heeft gesloten, blijkt dat partijen geen afspraken hebben gemaakt over informatieverstrekking aan het algemene publiek en/of aan winkelbezoekers over de tracking van hun mobiele apparatuur. Bluetrace voorziet op dit moment niet in opt-outmogelijkheden voor het publiek.[66]

Ontwikkeling van privacybeleid
In zijn zienswijze op het rapport voorlopige bevindingen van het CBP heeft Bluetrace voorgesteld om voor [datum] een privacybeleid op te stellen en informatie over het privacybeleid op zijn website te plaatsen. Bluetrace is daarnaast voornemens om zijn klanten op de hoogte te stellen van het privacybeleid en hen aan te sporen dit te delen en te communiceren aan hun eigen klanten, dat wil zeggen, het winkelende publiek.

Bluetrace heeft naar aanleiding van het rapport voorlopige bevindingen van het CBP voorgesteld om onderzoek te doen naar de uitingen over wifi-tracking in winkels. Bluetrace zal in het kader van het onderzoek in overleg met klanten bepalen welke uitingen in winkels gedaan moeten worden over wifi-tracking. De afspraken daarover zullen worden vastgelegd in overeenkomsten. Bluetrace schetst in zijn brief van 26 augustus 2015 de verwachting dat deze maatregel kan worden voltooid per [datum].

3.9 Bewaren van gegevens

In de database waaruit rapportages worden gegenereerd, worden de ruwe meetgegevens met mac-adressen maximaal drie weken bewaard in hun originele vorm. Daarna worden de mac-adressen gehasht. De gehashte gegevens worden voor onbepaalde tijd bewaard in backupbestanden die te bereiken zijn via [vertrouwelijk]. Bluetrace beschikt over servers in Nederland, [vertrouwelijk] en [vertrouwelijk.] Om veiligheidsredenen heeft Bluetrace een backup-opslagfaciliteit voor data in [vertrouwelijk].[67] Bluetrace beschikt daarmee over een archief met alle meetgegevens.

Bluetrace heeft verklaard dat het bedrijf geen bewaartermijnen heeft bepaald of ingesteld voor de verzamelde meetgegevens. Er is ook geen beleid ontwikkeld voor het bepalen van redelijke bewaartermijnen per doel van de meting en voor hoe de verwijdering van bepaalde resultaten technisch vorm krijgt wanneer de gegevens van het ene event wel bewaard mogen blijven en gegevens van het andere event niet.[68]

---

[66] Er zijn initiatieven in Nederland om een dergelijk gemeenschappelijk opt-outregister op te zetten, maar Bluetrace is daarbij niet aangesloten. Zie bijvoorbeeld: Privacy Special Interest Group, URL: http:/www.privacysig.org. Zie ook: URL http://bluemark-innovations.com/nl/2014/06/special-interest-group-founded-on-privacy-of-retail-customers/. De Privacy Special Interest Group heeft een privacyhandleiding ontwikkeld voor de deelnemende bedrijven. Een dergelijk document zou doorontwikkeld kunnen worden tot een gedragscode die aan het CBP kan worden voorgelegd ter goedkeuring, conform artikel 25 van de Wbp. Andere voorbeelden van opt-out-initiatieven in het buitenland zijn: Smartstoreprivacy: URL: http://www.smartstoreprivacy.org, Smart Place Privacy, URL: https://optout.smart-places.org/. Zie ook: ZDNet, 19 februari 2014, 'New website helps user opt-out of smartphone tracking', URL: http://www.zdnet.com/article/new-website-helps-users-opt-out-of-smartphone-tracking/, vastgelegd door het CBP op 5 juni 2015. De kwaliteit van de hier genoemde opt-out initiatieven is niet beoordeeld door het CBP.
[67] Bron: [Interne rapportage Bluetrace].
[68] Bluetrace geeft aan dat de verzamelde data kan worden gebruikt voor "*Gathering data for predictive analysis of costumer and crowd behavior*".Bron: (oude) website Bluetrace, zoals vastgelegd door het CBP op 10 december 2014.

Bluetrace heeft verklaard dat het bedrijf meetgegevens voorhanden heeft vanaf het moment dat met wifi-tracking is begonnen.[69] Bluetrace heeft tevens verklaringen afgelegd [over de huidige wijze van dataopslag]. [Vertrouwelijk].[70]

Uit de overeenkomsten die Bluetrace met zijn klanten heeft gesloten, blijkt dat partijen geen schriftelijke afspraken hebben gemaakt over het bewaren van gegevens en de bewaartermijnen die in acht moeten worden genomen.

In de zienswijze op de voorlopige bevindingen van het CBP d.d. 21 juli 2015 heeft Bluetrace voorgesteld om om (in samenspraak met klanten) bewaartermijnen vast te stellen. Bluetrace heeft in zijn brief van 26 augustus 2015 de verwachting uitgesproken dat dit traject op [datum] voltooid kan zijn.

4. WETTELIJK KADER

4.1 Verwerking van persoonsgegevens

Volgens artikel 1, aanhef en onder a, van de Wbp wordt onder een 'persoonsgegeven' verstaan: "*elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*".

'Verwerking van persoonsgegevens' is gedefinieerd in artikel 1, aanhef en onder b, van de Wbp en omvat onder meer het verzamelen, vastleggen, bewaren, gebruiken, samenbrengen en met elkaar in verband brengen van persoonsgegevens.[71]

Artikel 1, aanhef en onder a, van de Wbp vormt een implementatie van artikel 2, aanhef en onder a, van de Europese Privacyrichtlijn:

> *"In de zin van deze richtlijn wordt verstaan onder (…) 'persoonsgegevens', iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit."*

Overweging 26 van de Privacyrichtlijn[72] luidt in dit verband:

"*Overwegende dat de beschermingsbeginselen moeten gelden voor elk gegeven betreffende een geïdentificeerde of identificeerbare persoon; dat, om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij*

[69] Verklaringen van Bluetrace tijdens het bedrijfsbezoek van 3 februari 2015, zoals weergegeven in de brief van het CBP van 28 februari 2015, bijlage, onder nummers 30-34.
[70] [vertrouwelijk].
[71] Artikel 1, aanhef en onder b, van de Wbp verstaat – voluit – onder 'verwerking van persoonsgegevens': "*elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens*".
[72] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, Publicatieblad Nr. L 281 van 23 november 1995, p. 0031 - 0050.

redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren; dat de beschermingsbeginselen niet van toepassing zijn op gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is (…)."

Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon moeten als persoonsgegevens worden beschouwd.[73] Het CBP verwijst in dit verband ook naar de adviezen 5/2014 (over anonimiseringsmethoden[74]) en 13/2011 (over geolocatiefuncties op mobiele apparaten[75]) van de Artikel 29 werkgroep, het samenwerkingsverband van Europese toezichthouders op basis van artikel 29 van de ePrivacy Richtlijn. In de laatstgenoemde opinie zijn locatiegegevens (van mobiele telefoons) door de Europese privacytoezichthouders aangemerkt als persoonsgegevens van gevoelige aard: *"Omdat smartphones en tabletcomputers onlosmakelijk verbonden zijn met hun eigenaren, leveren de verplaatsingen van de apparaten een zeer intieme inkijk in het leven van hun eigenaren."*[76]

4.2 Verantwoordelijkheid voor de verwerking van persoonsgegevens

> Het begrip 'verantwoordelijke' is gedefinieerd in artikel 1, aanhef en onder d. De verantwoordelijke is de (…) rechtspersoon (…) die (…), alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[77]

Uit dit wetsartikel blijkt dat er meer dan een verantwoordelijke voor de verwerking van persoonsgegevens kan zijn. Bij de beantwoording van de vraag wie de verantwoordelijke is, moet volgens de wetsgeschiedenis enerzijds worden uitgegaan van de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen en anderzijds van een functionele benadering. Het laatste criterium betekent dat gekeken moet worden naar wat er feitelijk gebeurt tussen partijen. Dit speelt met name een rol als er verschillende actoren bij de gegevensverwerking betrokken zijn en de juridische bevoegdheid onvoldoende helder is geregeld om te kunnen bepalen wie van de betrokken actoren als verantwoordelijke in de zin van de wet moet worden aangemerkt.[78]

Het Hof van Justitie van de EU heeft in een recent arrest bevestigd dat eventuele gezamenlijke verantwoordelijkheid voor bepaalde gegevensverwerkingen niets afdoet aan de eigen verantwoordelijkheid van een van de (gezamenlijke)

[73] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 46.
[74] Artikel 29-werkgroep, WP 216, Advies 5/2014 over anonimiseringstechnieken, 10 April 2014.
[75] Artikel 29-werkgroep, WP 185, Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten, 16 mei 2011.
[76] Idem. Zie ook persbericht CBP van 18 mei 2011 over deze opinie, URL: https://cbpweb.nl/nl/nieuws/gemeenschappelijk-standpunt-europese-privacytoezichthouders-over-geolocatiediensten.
[77] Artikel 1, aanhef en onder d, van de Wbp.
[78] Gelet op de wetsgeschiedenis is niet zozeer de juridische constellatie tussen partijen bepalend, maar is de feitelijke situatie doorslaggevend. Is er zelfs weinig of niets geregeld in overeenkomsten, dan zal aan de hand van algemeen in het maatschappelijk verkeer geldende maatstaven moeten worden bezien aan welke natuurlijke persoon, rechtspersoon of bestuursorgaan de betreffende verwerking moet worden toegerekend. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 16 en p. 55.

verantwoordelijken.[79] Het CBP betrekt bij de toepassing van deze bepaling Advies 1/2010 van de Artikel 29-werkgroep over de verantwoordelijke en de bewerker.[80]

4.3 Grondslagen voor de verwerking van persoonsgegevens in de Wbp

Voor het verwerken van persoonsgegevens is een grondslag (rechtvaardigingsgrond) vereist als opgesomd in artikel 8 van de Wbp.

> Artikel 8 van de Wbp bepaalt dat persoonsgegevens slechts mogen worden verwerkt indien*:*
> *a. de betrokkene voor de verwerking zijn ondubbelzinnige* ***toestemming*** *heeft verleend;*
> *b. de gegevensverwerking noodzakelijk is voor de uitvoering van een* ***overeenkomst waarbij de betrokkene partij is****, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;*
> *c. de gegevensverwerking noodzakelijk is om een* ***wettelijke verplichting na te komen*** *(…)*
> *d. de gegevensverwerking noodzakelijk is voor de vrijwaring van een* ***vitaal belang*** *van de betrokkene;*
> *e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een* ***publiekrechtelijke taak*** *door het bestuursorgaan (…)*
> *f. de gegevensverwerking noodzakelijk is voor de behartiging van* ***het gerechtvaardigde belang van de verantwoordelijke*** *of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.*

Ten aanzien van de grondslag gerechtvaardigd belang (artikel 8, aanhef en onder f, van de Wbp) geldt het volgende. Deze grondslag kan worden toegepast indien de verwerking noodzakelijk is (proportionaliteitstoets: de inbreuk op de belangen van de bij de verwerking betrokkene mag niet onevenredig zijn in verhouding tot het doel van de verwerking) en het doeleinde mag niet op een andere wijze of met minder ingrijpende middelen kunnen worden bereikt (subsidiariteitstoets).[81] De toepassing van de grondslag uit artikel 8, onder f, van de Wbp vereist een zorgvuldige belangenafweging. De Artikel 29-werkgroep geeft een nadere uitwerking van deze afweging, met praktische voorbeelden, in Opinion 6/2014 over het gerechtvaardigde belang.[82]

In aanvulling op de eerste afweging (noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke), waarbij mogelijk de belangen van de betrokkene als onderdeel van een veelheid van belangen al onder ogen zijn gezien, is er nog een tweede toets.[83] Deze tweede toets (privacytoets) vergt een nadere afweging, waarbij de belangen van de betrokkene een zelfstandig gewicht in de schaal leggen tegenover het belang van de verantwoordelijke. In het geval dat het belang van bescherming van de

[79] HvJ EU van 13 mei 2014, zaak 131/12 (Google Spain SL and Google Inc vs Agencia Española de Protección de Datos), r.o. 40: "*Deze omstandigheid doet immers niet af aan het feit dat het doel van en de middelen voor deze verwerking door deze exploitant worden vastgesteld. Bovendien doet, gesteld al dat deze mogelijkheid voor de webredacteurs betekent dat zij samen met deze exploitant de middelen voor deze verwerking vaststellen, deze vaststelling niets af aan de verantwoordelijkheid van laatstgenoemde, daar artikel 2, sub d, van richtlijn 95/46 uitdrukkelijk bepaalt dat dit doel en deze middelen 'alleen of tezamen met anderen' kunnen worden vastgesteld*."
[80] Artikel 29-werkgroep, WP 169, Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en de 'verwerker', 16 februari 2010.
[81] Vgl. de proportionaliteits- en subsidiariteitstoets uit artikel 8 EVRM. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 80. Zie ook idem, p. 8 en idem, nr. 92c, p. 6.
[82] Artikel 29-werkgroep, WP 217, Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 april 2014.
[83] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 87.

persoonlijke levenssfeer van de betrokkene doorslaggevend is, dient de verantwoordelijke af te zien van de gegevensverwerking.[84]

Bij de in artikel 8, onder f, van de Wbp voorgeschreven afweging speelt de mate van gevoeligheid van de gegevens die de verantwoordelijke wil verwerken een rol, evenals de maatregelen die de verantwoordelijke heeft genomen om rekening te houden met de belangen van de betrokkene. De belangen van de betrokkene zullen in mindere mate gewicht in de schaal leggen naarmate er meer waarborgen voor een zorgvuldig gebruik van de gegevens zijn.[85]

Het CBP toetst de gegevensverwerkingen ambtshalve aan het gehele artikel 8 van de Wbp. Het CBP stelt zelfstandig vast op welke grondslagen een rechtsgeldig beroep gedaan kan worden in een concreet geval en welke partij(en) daarvoor, gelet op artikel 15 van de Wbp, zorg moet(en) dragen.

4.4 Informatieplicht

De informatieplicht houdt in dat de verantwoordelijke transparant moet zijn over de redenen waarom hij persoonsgegevens van de betrokkene verwerkt. Artikel 33 van de Wbp beschrijft de situatie dat de gegevens worden verkregen bij of van de betrokkene zelf, bijvoorbeeld wanneer hij aan de hand van een formulier gegevens over zichzelf moet invullen voor een bepaald doel. Artikel 34 regelt de informatieverplichting in overige situaties.[86]

De artikelen 33 en 34 van de Wbp bepalen dat de verantwoordelijke vóór het moment van de verkrijging van persoonsgegevens aan de betrokkene informatie moet verstrekken, tenzij de betrokkene daarvan reeds op de hoogte is.
De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, mede.
De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen, tenzij de betrokkene daarvan reeds op de hoogte is (artikel 33 en artikel 34, eerste tot en met derde lid, van de Wbp).
Het eerste lid van artikel 34 is niet van toepassing indien mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast (artikel 34, vierde lid van de Wbp).

Hoewel artikel 33 vereist dat verstrekking van gegevens aan de verantwoordelijke moet zijn beoogd door de betrokkene, hoeft er geen sprake te zijn van een direct contact tussen de betrokkene en de verantwoordelijke.[87] In de memorie van toelichting bij de Wbp wordt het voorbeeld gegeven van cameratoezicht. Als dat heimelijk geschiedt, is artikel 34 Wbp van toepassing. De gegevensvergaring met videocamera's kan onder artikel 33 worden geschaard indien het geen geheime observatie betreft.

[84] Idem.
[85] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 88.
[86] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 149. Bijvoorbeeld als onopgemerkt gegevens omtrent betrokkenen worden verzameld en verwerkt, met behulp van automatische procedures voor gegevensvergaring. Vgl. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 78.
[87] Mr. drs. T.F.M. Hooghiemstra en mr. dr. S. Nouwt, Sdu Commentaar Wet bescherming persoonsgegevens, 2014, p. 155.

Indien de betrokkene op de hoogte is van de aanwezigheid van camera's en hij eveneens weet voor welk doel deze gebruikt worden, is hij zich bewust van de gegevensverwerking en heeft hij de mogelijkheid zich hieraan te onttrekken. Doet hij dat niet, dan kan gesteld worden dat hij zijn persoonsgegevens voor het desbetreffende doel bewust ter beschikking heeft gesteld.[88]

De wet schrijft voor dat er ten minste informatie verstrekt moet worden over de doeleinden waarvoor persoonsgegevens worden verwerkt en om welke (categorieën van) gegevens het gaat.[89] Ook moet duidelijk zijn welke (rechts)persoon verantwoordelijk is voor de dataverwerking. Op basis van deze verplichting moet daarnaast zo veel aanvullende informatie worden geboden aan de betrokkene als nodig is voor een behoorlijke en zorgvuldige verwerking, oftewel, een eerlijke gang van zaken. Te denken valt aan de bewaartermijn,[90] een specificatie van de soorten persoonsgegevens die worden verwerkt, een verwijzing naar de mogelijkheden om inzage, verwijdering of correctie van gegevens te vragen, informatie over de koppeling van gegevensbestanden of een overzicht van de eventuele andere organisaties die toegang hebben tot de gegevens en/of andere informatie over de omstandigheden rond de verwerking die redelijkerwijs relevant zijn voor de betrokkene.[91] De ratio van de informatieverplichting is dat de betrokkene in staat moet zijn te volgen hoe gegevens over hem worden verwerkt en zich moet kunnen verzetten tegen of onttrekken aan bepaalde vormen van dataverwerking of onrechtmatig gedrag van de verantwoordelijke. Het is evenzeer van belang dat de betrokkene zelf zijn rechten kan uitoefenen op inzage, correctie, verzet en/of verwijdering, zodra hij weet welke partij verantwoordelijk is voor de verwerking van zijn persoonsgegevens. De wijze van informatieverstrekking is in principe vormvrij, maar er moet wel gekozen worden voor een methode die de betrokkene daadwerkelijk op het juiste moment (voor aanvang van de verwerkingen) bereikt.[92]

De uitzondering die in het vierde lid van artikel 34 van de Wbp wordt gemaakt (dat een verantwoordelijke niet hoeft te informeren als dat onmogelijk blijkt of een onevenredige inspanning kost) is breder dan de uitzondering die Richtlijn 95/46/EC beschrijft in artikel 11, tweede lid. Daarin wordt de uitzondering beperkt tot gegevensverwerking voor statistische doeleinden of voor historische of wetenschappelijke onderzoeksdoeleinden. Lidstaten moeten in die gevallen bij wet adequate waarborgen bieden voor betrokkenen. De Nederlandse wetgever heeft als waarborg gekozen dat verantwoordelijken bij een beroep op deze uitzondering de herkomst van gegevens moeten vastleggen. De Nederlandse wetgever heeft in artikel 34 van de Wbp geen aanvullende waarborgen beschreven voor de verwerking van gegevens van personen die niet (meer) achterhaald kunnen worden, maar in artikel 31, eerste lid, onder b, van de Wbp, is voorgeschreven dat voor heimelijke vastlegging van persoonsgegevens een voorafgaand onderzoek van het CBP vereist is.

Het staat buiten kijf dat de wetgever, door het opnemen van een uitzondering op de informatieplicht als gegevens niet rechtstreeks van betrokkenen worden verzameld,

[88] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 155-157.
[89] Vgl. ook artikel 11, eerste lid, onder c, van de Privacyrichtlijn.
[90] Vgl. Last onder dwangsom NS Groep N.V. CBP 9 juni 2011, z2011-00057. URL: https://cbpweb.nl/sites/default/files/downloads/pb/pb_20110726_ov-chip_lod_ns.pdf.
[91] *Kamerstukken II* 1997/98, 25 892, nr. 3, p 154-155.
[92] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 155.

niet heeft willen aanmoedigen dat persoonsgegevens op heimelijke wijze worden vergaard. Dit blijkt bijvoorbeeld uit de strafbaarstelling van heimelijke waarneming in de artikelen 139f en 441b van het Wetboek van Strafrecht.[93] De uitzondering in artikel 34, vierde lid, van de Wbp beoogt derhalve niet om heimelijke gegevensvergaring goed te keuren wanneer de gekozen werkwijze meebrengt dat betrokkenen niet kunnen worden geïnformeerd, maar dient gelezen te worden in de context van het statistische, historische en wetenschappelijke onderzoek waar de richtlijn naar verwijst. De uitzondering om betrokkenen niet te hoeven informeren moet zeer beperkt worden geïnterpreteerd en omvat slechts vormen van (verdere) verwerking (meestal door andere verantwoordelijken) in een statistische, historische of wetenschappelijke context waarbij het een onevenredige inspanning kost om betrokkenen te achterhalen en hen achteraf te informeren over deze verdere verwerking, bijvoorbeeld omdat er geen actuele contactgegevens meer beschikbaar zijn.

Deze bepalingen vormen een uitwerking van het transparantiebeginsel en het in artikel 6 van de Wbp neergelegde beginsel van 'fair processing' uit de Europese Privacyrichtlijn. Dit heeft tot gevolg dat overtreding van de informatieplicht zal leiden tot onrechtmatige verwerking(en).[94] Artikel 33 en 34 van de Wbp gaan ervan uit dat er geen onderzoeksplicht van de betrokkene is.[95]

4.5 Bewaren van gegevens

Artikel 10 van de Wbp bepaalt:
1. Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.
2. Persoonsgegevens mogen langer worden bewaard dan bepaald in het eerste lid voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

Artikel 10 Wbp brengt in de praktijk mee dat de verantwoordelijke zich dient zich af te vragen of hij gegevens daadwerkelijk moet bewaren en hoe lang hij de gegevens dan nodig heeft om de activiteit te kunnen verrichten waarvoor hij de data heeft verzameld. De verantwoordelijke moet namelijk op grond van artikel 15 van de Wbp zorg dragen voor het naleven van de eisen aan het bewaren van persoonsgegevens. Zijn er voldoende redenen om gegevens te bewaren, dan moet hij bepalen welke bewaartermijnen gelden. Dit alles kan worden vastgelegd in intern beleid voor bewaartermijnen. Zijn die termijnen verlopen, dan zal hij de gegevens niet meer mogen verwerken, tenzij voor een ander, daarmee verenigbaar doel.[96]

De verantwoordelijke is niet geheel vrij om elke willekeurige termijn te stellen die denkbaar is. De term *noodzakelijk* in artikel 10 is een belangrijke waarborg die ervoor

[93] Deze waarborg geldt sinds 1 januari 2004.
[94] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 149. Voor een nadere toelichting, zie Mr. drs. T.F.M. Hooghiemstra en mr. dr. S. Nouwt, Sdu Commentaar Wet bescherming persoonsgegevens, 2014, p. 151.
[95] *Kamerstukken II* 1997/98, 25 892,nr. 3, p. 150-151.
[96] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 95.

zorgt dat de verantwoordelijke aannemelijk moet maken waarom het bewaren van gegevens gedurende de door hem gestelde termijn noodzakelijk is voor het verwezenlijken van het verwerkingsdoel. Artikel 10 stelt hiermee een zelfstandige norm voor die bedoeld is om de betrokkene te beschermen tegen verwerkingen van persoonsgegevens die hem buitenproportioneel langdurig kunnen achtervolgen.

Het CBP betrekt bij de toepassing van deze bepaling de Opinies van de Artikel 29-werkgroep over geolocatiefuncties op mobiele apparaten[97] en over anonimiseringsmethoden.[98]

[97] Artikel 29-werkgroep, WP 185, Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten, 16 mei 2011.
[98] Artikel 29-werkgroep, WP 216, Advies 5/2014 over anonimiseringstechnieken, 10 april 2014.

5. BEOORDELING

5.1 Verwerking van persoonsgegevens

Het CBP heeft in paragraaf 3.4 van dit rapport vastgesteld dat Bluetrace ten minste de onderstaande gegevens genereert en verzamelt (en heeft verzameld) met wifi-tracking.

- Het mac-adres van mobiele apparaten, met name telefoons;
- De signaalsterkte van het geregistreerde wifi- signaal van de apparaten;
- Het serienummer van de sensor;
- Het tijdstip van de meting.

Op basis van deze vier kenmerken verricht Bluetrace wifi-tracking in winkels en wifi-tracking buiten winkels op de openbare weg
Het gebruik van deze combinatie van gegevens is een verwerking van persoonsgegevens, omdat daarmee individuele betrokkenen, namelijk houders van de betreffende apparaten, identificeerbaar zijn.

Volgens artikel 1, aanhef en onder a, Wbp wordt onder een persoonsgegeven verstaan: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.[99] Gegevens moeten geschikt zijn om een persoon te identificeren of althans direct of indirect identificeerbaar zijn om te kunnen spreken van persoonsgegevens.

Direct indentificerende gegevens
Van direct identificerende gegevens is in dit geval geen sprake. Het gaat hier niet om gegevens als namen, adressen en telefoonnummers. Er bestaat ook geen opzoektabel van mac-adressen en het eigendom van de betreffende apparatuur.

Indirect identificerende gegevens
Er kan wel sprake zijn van indirect identificeerbare gegevens, indien gegevens, zonder dat zij namen bevatten, door combinatie met elkaar of met andere gegevens teruggebracht kunnen worden tot een bepaalde persoon. Een persoon is identificeerbaar indien zijn identiteit – direct of via nadere stappen, door gegevens die alleen of in combinatie met andere gegevens zo kenmerkend zijn voor zijn persoon[100] – redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.[101] Om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke

[99] 'Verwerking' van persoonsgegevens is gedefinieerd in artikel 1, onder b, Wbp en omvat onder meer het vastleggen, verzamelen en bewaren van persoonsgegevens. Zie paragraaf 4.1.
[100] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48. Bijvoorbeeld "gevallen (…) waarbij gegevens niet direct op naam zijn terug te vinden, doch de betrokken persoon met aanwending van beschikbare middelen alsnog kan worden achterhaald, bijvoorbeeld aan de hand van een nummer. Te denken valt aan een situatie waarbij een lijst van nummers met bijbehorende namen beschikbaar is, hetzij via openbare bron, (bijvoorbeeld het telefoonboek), hetzij via een bron die slechts raadpleegbaar is voor een bepaalde categorie van personen (bijvoorbeeld het kentekenregister door de politie of het nummer van een rekening door bankemployés). De met die nummers verbonden gegevens zijn – hoewel niet op naam – persoonsgegevens wegens de beschikbare mogelijkheid om met behulp van de nummers de identiteit van de betrokken personen te achterhalen." Lijst van vragen en antwoorden, 13 juli 1999, Kamerstukken II 1998/99, 25 892, nr. 13, p. 2.
[101] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 47-49. In de wetsgeschiedenis bij de Wbp wordt over het begrip 'onevenredige inspanning' opgemerkt: *"Dit doet zich bijvoorbeeld voor indien identificatie van personen door de computer vele dagen in beslag zou nemen."* Kamerstukken II 1998/99, 25 892, nr. 13, p. 2.

dan wel enig ander persoon zijn in te zetten om die persoon te identificeren.[102] Er moet worden uitgegaan van een redelijk toegeruste verantwoordelijke.[103] In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise en technische faciliteiten van de verantwoordelijke.[104]

In de Wbp is rekening gehouden met de voortdurende innovatie in de informatietechnologie: "*Bij het voortschrijden van informatietechnologie moet rekening worden gehouden met het feit dat waar voorheen wellicht nog sprake was van een onevenredige inspanning (en dus niet van een persoonsgegeven), deze inspanning geringer wordt met het beschikbaar komen van nieuwe technieken. Wat dus bij een bepaalde stand van de techniek als anoniem, want redelijkerwijs niet op een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding.*"[105]

Identificatie zonder naam

Identificatie kan ook plaatsvinden zonder dat de naam van de persoon wordt achterhaald. Vereist is slechts dat de gegevens ervoor zorgen dat een bepaald persoon kan worden onderscheiden van anderen. In de opinie van de Artikel 29-werkgroep over het begrip persoonsgegeven is hierover opgemerkt: *"(…) dat hoewel identificatie door middel van de naam in de praktijk het meest voorkomt, de naam niet in alle gevallen noodzakelijk is om een persoon te identificeren. Dit is het geval wanneer andere identificatiemiddelen worden gebruikt om iemand van anderen te onderscheiden. In computerbestanden waarin persoonsgegevens zijn opgenomen, wordt aan de geregistreerde personen doorgaans een unieke identificatiecode toegewezen om verwisseling van personen in het bestand te voorkomen. Op het world wide web is het met behulp van bewakingsinstrumenten voor het webverkeer eenvoudig om het gedrag van een machine te identificeren en daarmee ook van de gebruiker ervan. (…) Met andere woorden, de identificatie van een persoon vereist niet langer het vermogen zijn of haar naam te achterhalen. De definitie van 'persoonsgegeven' weerspiegelt ook dit feit."* [onderstrepingen toegevoegd door het CBP].[106]

Als de gegevens niet direct tot identificatie van een bepaald persoon leiden maar de gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon, betreft het indirect identificerende persoonsgegevens. De memorie van toelichting van de Wbp schrijft hierover: "*Zij kunnen zijn ontdaan van de naam, doch onder omstandigheden door combinatie met andere gegevens weer worden teruggebracht tot een bepaalde persoon.*[107]

Identificatie door combinatie van objectgegevens en andere gegevens

De memorie van toelichting bij de Wbp beschrijft dat als persoonsgegevens worden beschouwd "alle gegevens die informatie kunnen verschaffen over een

[102] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48. Vergelijk ook Opinie 4/2009 van de Artikel 29-werkgroep over de definitie van persoonsgegevens (WP 136), p. 16: "*Daarbij moet rekening worden gehouden met alle relevante factoren, zoals de kosten van identificatie, het beoogde doel van de verwerking, de wijze waarop de verwerking is gestructureerd, het voordeel dat de voor de verwerking verantwoordelijke ervan verwacht, de belangen die voor de betrokken personen op het spel staan, het risico op organisatorische tekortkomingen (bijvoorbeeld inbreuken op de vertrouwelijkheidsplicht) en technische storingen.*"
[103] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48-49.
[104] Idem, p. 49. Registratiekamer 27 maart 1995, 95.V.029.
[105] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 49.
[106] Artikel 29-werkgroep, WP 136, Advies 4/2007 over het begrip persoonsgegeven, p. 14-15.
[107] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 49.

identificeerbare natuurlijke persoon". Ook gegevens die niet direct betrekking hebben op een bepaalde persoon, maar bijvoorbeeld op een product of een proces, kunnen soms informatie verschaffen over een bepaalde persoon, bijvoorbeeld wanneer daarmee de arbeidsproductiviteit van een werknemer gemakkelijk in kaart kan worden gebracht.[108]
In dit verband is het van belang om persoonsgegevens te onderscheiden van "objectgegevens". De wetsgeschiedenis schrijft hier over: *"Gegevens die uitsluitend voorwerpen aanduiden, (…) zijn geen persoonsgegevens indien deze geen informatie bevatten met behulp waarvan personen in hun maatschappelijke positie kunnen worden geraakt. Het gaat dan om zuivere objectgegevens."* Wanneer een objectgegeven wordt gecombineerd met andere informatie kan er een set gegevens ontstaan die informatie betreffende een persoon kan verschaffen.[109]

Locatiegegevens
Locatiegegevens (van mobiele telefoons) zijn door de Europese privacytoezichthouders aangemerkt als persoonsgegevens van gevoelige aard: *"Omdat smartphones en tabletcomputers onlosmakelijk verbonden zijn met hun eigenaren, leveren de verplaatsingen van de apparaten een zeer intieme inkijk in het leven van hun eigenaren."*[110]

Identificeerbaarheid meetgegevens wifi-tracking van Bluetrace
Hoewel Bluetrace de naam van de betrokkene alleen kan achterhalen met aanvullende data, bijvoorbeeld door ten tijde van de detectie van het mac-adres door de sensoren de betrokkene aan te spreken in of bij een winkel, is het niet cruciaal voor de definitie van persoonsgegevens of een verantwoordelijke de naam van een betrokkene kan achterhalen.

Het mac-adres van een mobiel apparaat is een identificerend kenmerk van dat apparaat, in die zin dat het mobiele apparaat altijd hetzelfde mac-adres uitzendt en de aanwezigheid van een apparaat in de buurt van een sensor vergeleken kan worden met eerder opgeslagen waarnemingen van dat mac-adres en met het mac-adres in het apparaat zelf. (bijvoorbeeld de mobiele telefoon)

Het zijn feiten van algemene bekendheid dat smartphones zeer persoonlijke apparaten zijn, dat zij zelden gedeeld worden met meerdere personen en dat de locatie van een telefoon gedurende het grootste gedeelte van een dag overeenkomt met de verblijfplaats van de eigenaar.[111] Het CBP gaat er daarom van uit dat de exacte locatie van een smartphone in onze huidige maatschappij onmiskenbaar informatie over de verblijfplaats van diens eigenaar geeft. Bluetrace combineert een objectgegeven (mac-adres) met aanvullende informatie over de datum, het tijdstip en de plaats waar het mac-adres is waargenomen. Daarbij is van belang dat mac-adressen unieke apparaten onderscheiden en dat die apparaten, in de context van geolocatiediensten, rechtstreeks

[108] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 46
[109] Vergelijk: Onderzoek CBP naar de verzameling van wifi-gegevens met Street View-auto's door Google, Rapport definitieve bevindingen, z2010-00582, 7 december 2010, p. 29 e.v. url: https://cbpweb.nl/sites/default/files/downloads/rapporten/rap_2011_google.pdf
[110] Artikel 29-werkgroep, WP 185, Opinion 13/2011 on geolocation services on smart mobile devices
[111] Scholieren.com, 25 maart 2014, Jongeren nemen mobiel mee naar bed', URL: http://www.scholieren.com/blog/4275/jongeren-nemen-mobiel-mee-naar-bed. Zie ook: 1V Jongerenpanel, Onderzoek "Connected met je mobiel" van maart 2015, URL: http://www.eenvandaag.nl/uploads/doc/Rapport%20connected%20met%20je%20mobiel.pdf

verbonden zijn met de locatie van een houder. Daarmee is er sprake van een set gegevens die informatie kan verschaffen over een persoon.[112]

Bluetrace heeft er tijdens het onderzoek meerdere malen op gewezen dat het bedrijf ervan uitgaat dat herleidbaarheid van meetgegevens uit wifi-tracking naar personen een zuiver theoretische mogelijkheid is. Bluetrace stelt onder andere dat deze gegevens voor het bedrijf redelijkerwijs niet herleidbaar zijn naar individuele personen. Om deze reden gaat Bluetrace ervan uit dat het bedrijf geen persoonsgegevens verwerkt. Bluetrace heeft daarnaast verklaard dat identificatie van personen ook niet het doel is van de gegevensverwerkingen.[113]

Niet *iedere* mogelijkheid om de gegevens voor de herleiding van personen te gebruiken moet zijn uitgesloten, om te mogen concluderen dat er geen sprake is van persoonsgegevens. De memorie van toelichting bij de Wbp geeft aan dat wanneer deze mogelijkheid weliswaar theoretisch aanwezig is, maar het ondenkbaar is dat dit ook daadwerkelijk gebeurt, men ervan uit kan gaan dat de gegevens niet als persoonsgegevens worden aangemerkt. De memorie van toelichting bij de Wbp bepaalt in dit verband echter ook dat: *"uitgegaan moet worden van een redelijk toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening gehouden worden met de bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke."* [114]

Het CBP acht van belang dat Bluetrace zelf de sensoren installeert ter plaatse. Bluetrace weet dus exact welke sensor op welke fysieke locatie staat. De combinatie van het sensornummer met de gegevens over de signaalsterkte maakt het voor Bluetrace eenvoudig om de locatie van het geregistreerde apparaat vast te stellen. Wanneer er een aantal mac-adressen geregistreerd wordt op een bepaalde plek en op een bepaald tijdstip, dan is tegelijkertijd ook fysiek waar te nemen welke mensen daar op dat moment lopen. Dit kan door een mens, bijvoorbeeld een medewerker van Bluetrace of van een winkel, op de locatie waargenomen worden.[115] De betrokkene kan op dat moment persoonlijk benaderd worden.

De herleidbaarheid naar personen is geen strikt theoretische mogelijkheid. Zoals toegelicht in paragraaf 3.2 van dit rapport, heeft Bluetrace tijdens het onderzoek van het CBP verklaard dat het voor is gekomen dat de politie meetgegevens heeft opgevraagd bij Bluetrace voor opsporingsonderzoeken. Het is ook voorgekomen dat een klant van Bluetrace gegevens heeft opgevraagd in verband met winkeldiefstal, om de dader op te kunnen sporen.

De wetgever merkt in de memorie van toelichting bij de Wbp expliciet op: "*Indien het (…) mogelijk is de gegevens te gebruiken om fraude op te sporen, dan is sprake van een persoonsgegeven. Daarbij is niet relevant of de bedoeling om de gegevens voor dat doel te*

[112] Vergelijk: Onderzoek CBP naar de verzameling van wifi-gegevens met Street View-auto's door Google, Rapport definitieve bevindingen, z2010-00582, 7 december 2010, p. 29 e.v. URL: https://cbpweb.nl/sites/default/files/downloads/rapporten/rap_2011_google.pdf
[113] Brief van Bluetrace van 22 januari 2015.
[114] *Kamerstukken II* 1997/98, 25 892, nr. 3, vanaf p. 47.
[115] Zie: M. Cunche, 'I know your MAC address, targeted tracking of individuals using Wi-Fi', Journal of Computer Virology and Hacking Techniques, November 2014, Volume 10, Issue 4, pp 219-227, 27 december 2013, URL: http://link.springer.com/article/10.1007/s11416-013-0196-1#page-1.

gebruiken ook aanwezig is. Er is reeds sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel, kan worden gebruikt."[116]

Zowel uit de praktijk bij Bluetrace als uit recente rechtspraak is duidelijk geworden dat de gegevens zich lenen voor toepassing van een dergelijk op de persoon gericht doel. Het CBP verwijst naar een uitspraak van het Gerechtshof Arnhem-Leeuwarden van 27 november 2014. Deze uitspraak heeft betrekking op een strafzaak waarin tijdens het opsporingsonderzoek naar strafbare feiten gebruik gemaakt is van de meetgegevens van bluetooth-trackinginstallaties van de Verkeersinformatiedienst, om te bewijzen dat de verdachte aanwezig was op bepaalde plaatsen. Mede op basis van de beschikbare gegevens over tracking van mobiele apparatuur, zoals telefoons, kon geconcludeerd worden dat de verdachte medeplichtig was aan moord.[117] Omdat het mac-adres van de telefoon van de verdachte bekend was bij de opsporingsdiensten, was eenvoudig te achterhalen waar zijn telefoon zich bevond omstreeks het tijdstip waarop het delict was gepleegd. De rechter heeft dit gebruikt als bewijsmiddel omtrent de verblijfplaats van deze persoon.

In de jurisprudentie komen daarnaast andere gevallen voor waarin sprake is van het achterhalen van een persoon die een apparaat gebruikt en/of het achterhalen van diens verblijfplaats aan de hand van het mac-adres van een telefoon, een wifi-router, een simkaart of een laptop.[118] Mac-adressen met aanvullende meetgegevens worden dus in de praktijk opgevraagd en toegepast om individuele personen – zoals daders of getuigen van strafbare feiten – op te sporen.

Het CBP heeft in eerder onderzoek eveneens vastgesteld dat het genereren en gebruiken van de combinatie van (a) mac-adressen en (b) de berekende locatie van een wifi-router aan te merken is als een verwerking van gegevens over identificeerbare personen.[119]

Hashing

Bluetrace wijst er in zijn brief van 22 januari 2015 op dat de mac-adressen gehasht worden. Op verzoek van klanten kan Bluetrace dit kort na de vastlegging van de gegevens doen. Zonder dergelijk verzoek worden de waargenomen mac-adressen na drie weken gehasht, alvorens zij voor langere tijd bewaard worden. Bluetrace schrijft dat in het geval het CBP meent dat mac-adressen herleidbaar zijn tot personen, de hashing deze herleidbaarheid definitief wegneemt, zodat er geen sprake meer kan zijn van persoonsgegevens. [120]

---

[116] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 47. Artikel 29 Werkgroep, Opinie 4/2007 over het begrip persoonsgegevens, blz. 18. Zie ook: Rechtbank 's-Gravenhage, 2 april 2010, LJN BM1481.
[117] Bron: Gerechtshof Arnhem/Leeuwarden, 27 november 2014, zaaknummer KS 21-000096-14, ECLI:NL:GHARL:2014:9050 (medeplichtigheid aan moord op sportschoolhouder Almere).
[118] Bronnen: Rechtbank Midden-Nederland, Afdeling Strafrecht, Zittingslocatie Lelystad, 17 december 2013, Parketnummer: 07.662349-12 (P), ECLI:NL:RBMNE:2013:7281; Gerechtshof Den Haag, 14 oktober 2013, zaaknummer 22001690-13, ECLI:NL:GHDHA:2013:3871; Gerechtshof Den Haag, 9 maart 2011, zaaknummer 22002281-10, ECLI:NL:GHSGR:2011:BP7080.
[119] CBP, zaak z2010-00582, Rapport Definitieve bevindingen inzake Google Street View, 7 december 2010, p. 29 e.v. URL: https://cbpweb.nl/sites/default/files/downloads/rapporten/rap_2011_google.pdf
[120] Het CBP merkt hierbij subsidiair op dat Bluetrace de hashingmaatregel niet standaard onmiddellijk bij het verzamelen van de gegevens neemt, maar na drie weken, of, op verzoek van klanten, op de sensor circa [vertrouwelijk] seconden na eerste detectie van het mac-adres. Zelfs wanneer hashing ervoor zou zorgen dat de gegevens niet meer herleidbaar zijn tot personen,

Hashen is naar zijn aard echter niet bedoeld om gegevens te anonimiseren. Om te bereiken dat geen sprake meer is van persoonsgegevens, moeten gegevens zijn ontdaan van identificerende kenmerken die het mogelijk maken om die gegevens te herleiden naar een individuele natuurlijke persoon. Na verwijdering van deze identificerende gegevens, mag identificatie ook op andere wijze redelijkerwijs niet (meer) mogelijk zijn. Pas dan worden er geen persoonsgegevens meer verwerkt en is de Wbp niet (meer) van toepassing. Dit betekent dat het loskoppelen van (in)direct identificerende elementen en de overige gegevens onomkeerbaar moet zijn en dat deze gegevens ook in een later stadium - eventueel met behulp van andere (bijkomende of nieuwe) gegevens of technieken - niet alsnog aan elkaar kunnen worden gekoppeld waardoor wederom personen kunnen worden geïdentificeerd. Indien er een reële mogelijkheid op heridentificatie blijft bestaan, dan dienen verantwoordelijken technische en organisatorische maatregelen te treffen om dit risico te beheersen. De Wbp blijft in dat geval dus van toepassing op de set gegevens.[121]

In bepaalde gevallen en onder bepaalde voorwaarden kan het hashen van persoonsgegevens, in combinatie met andere maatregelen en waarborgen, leiden tot anonimiseren. Hashen kan in dat verband bijvoorbeeld meerwaarde hebben als tussenstap in een anonimiseringsproces.[122]

Of sprake is van anonimiseren hangt sterk af van de concrete omstandigheden van het geval. Van anonimiseren door middel van hashen is in elk geval geen sprake als op basis van een hash de originele waarde is te achterhalen. Juist omdat de verantwoordelijke doorgaans de beschikking heeft over de hashing formule, is het in de meeste gevallen mogelijk voor de verantwoordelijke om de hash opnieuw te berekenen met het oorspronkelijke gegeven.[123]

Het CBP heeft in paragraaf 3.5 van dit rapport vastgesteld dat Bluetrace zelf de hashing algoritmen heeft die binnen het bedrijf gebruikt worden. Daarmee heeft Bluetrace de sleutel in handen om de hashwaarden terug te rekenen naar de originele waarden. Hoewel [vertrouwelijk: hashing methode], leidt dit niet tot een zodanig informatieverlies dat ervoor zorgt dat hashwaarden niet meer uniek terug te leiden zijn tot de oorspronkelijke waarde. Het verwachte aantal verschillende mac-adressen dat tot de zelfde hashwaarde leidt (hash colissions) is bij de door Bluetrace toegepaste hashing methode verwaarloosbaar klein. Het CBP heeft vastgesteld dat er mogelijk

---

hetgeen het CBP bestrijdt, dan zou dit er, gezien de werkwijze van Bluetrace, ten hoogste toe kunnen leiden dat de verwerking van persoonsgegevens korter duurt en niet tot de conclusie dat er in het geheel geen persoonsgegevens zijn verwerkt.

[121] Zie ook CBP Onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door Tele2 Nederland B.V., z2011-00462, Rapport definitieve bevindingen. Mei 2013. URL: https://cbpweb.nl/sites/default/files/downloads/rapporten/rap_2013-analyse-gegevens-mobiel-dataverkeer-tele2.pdf

[122] Zie bijvoorbeeld CBP, Ambtshalve onderzoek naar de verwerking van geolocatiegegevens door TomTom N.V., Rapport van definitieve bevindingen. December 2011. URL: https://cbpweb.nl/sites/default/files/downloads/mijn_privacy/pb_20120112_tomtom-geolocatie-persoonsgegevens-definitieve-bevindingen.pdf.

[123] Zie ook CBP, Ambtshalve Onderzoek naar de verwerking van persoonsgegevens in het kader van de mobiele applicatie Whatsapp door WhatsApp Inc, z2011-00987, Rapport definitieve bevindingen. Mei 2013. URL: https://cbpweb.nl/sites/default/files/downloads/rapporten/rap_2013-whatsapp-cbp-definitieve-bevindingen-nl.pdf

hash collissions optreden bij een zeer groot aantal waarnemingen.[124] Omdat het aantal mac-adressen dat door één sensor in een winkel verzameld wordt op een dag naar verwachting vele malen kleiner is, is het aantal te verwachten dubbelingen verwaarloosbaar. Daarom is het mogelijk om een bekend mac-adres te hashen voor een specifieke dag om te zien of - en zo ja, bij welke sensor - dat mac-adres in gehashte vorm voorkomt in de historische meetgegevens, en dus gemeten is op die dag.

De door Bluetrace toegepaste hashing van de mac-adressen leidt derhalve niet tot de conclusie dat geen sprake meer is van de verwerking van persoonsgegevens.

Onderzoek naar pseudonimisering
Het CBP acht het onderzoek naar maskering van mac-adressen, dat Bluetrace heeft voorgesteld naar aanleiding van het rapport voorlopige bevindingen te onbepaald om te kunnen inschatten voor welke van de geconstateerde overtredingen dit een concrete uitkomst biedt. Met het voltooien van dit onderzoek is er in elk geval nog geen concrete maatregel getroffen die in de praktijk leidt tot een aanpassing van de werkwijze van Bluetrace.

Het CBP wijst in dit verband op de opinie van de Artikel 29-werkgroep over anonimiseringstechnieken.[125] Pseudonimisering is geen vorm van anonimisering. Pseudonimisering vermindert de relateerbaarheid van gegevens aan de identiteit van betrokkenen, en/of vereist daarvoor een extra tussenstap. Daardoor kan het een nuttige beveiligingsmaatregel zijn, omdat in geval van verlies of diefstal minder snel een verband met de individuele betrokkene kan worden gelegd door een derde die zich toegang verschaft tot de gepseudonimiseerde data. Het toepassen van pseudonimisering door de verantwoordelijke leidt echter niet tot de conclusie dat er geen sprake meer is van persoonsgegevens. Voor de verantwoordelijke zelf is immers te achterhalen hoe de pseudonieme gegevens zich verhouden tot c.q. zijn afgeleid uit de oorspronkelijke gegevens. [126] Voor zover Bluetrace gegevens zou willen pseudonimiseren (in plaats van verwijderen of onomkeerbaar anonimiseren) dient Bluetrace er ook dan rekening mee te houden dat er nog sprake is van gegevens die een persoon direct of indirect kunnen identificeren. Daarom gelden ook ten aanzien van pseudonieme gegevens de verplichtingen uit de Wbp, zoals onder meer informatievoorziening aan de betrokkene, een beleid inzake bewaartermijnen, en een grondslag voor de verwerking van gepseudonimiseerde gegevens.

Onderzoek naar anonimisering
Het volledig en onomkeerbaar anonimiseren van mac-adressen zou ertoe kunnen leiden dat er geen sprake meer is van de verwerking van persoonsgegevens, omdat de gegevens dan niet meer herleidbaar zijn tot een identificeerbare persoon. Ten aanzien van anonimisering wijst het CBP op het advies over anonimiseringstechnieken en het

[124] Stel dat er 17 miljoen maal een mac-adres plus tijdstempel wordt waargenomen op een dag (de bevolking van heel Nederland) dan is het verwachte aantal hash colissions bij benadering 0,51. Zie voor berekening: URL: http://www.wolframalpha.com/input/?i=k%5E2%2F%282N%29%2C+N%3D2%5E48%2C+k%3D17000000.
[125] Artikel 29-werkgroep, WP 216, Advies 5/2014 over anonimiseringstechnieken, 10 April 2014.
[126] Zie ook het Rapport definitieve bevindingen van het CBP in zaak z2011-00462 d.d. 29 mei 2013 (Tele2) p.43. 67, 103, 108 en de bijlage bij dit rapport.

advies over geolocatiefuncties op mobiele apparaten van de Artikel 29-werkgroep.[127] In deze adviezen is aangegeven dat het binnen 24 uur anonimiseren van mac-adressen een maatregel is die een belangrijke waarborg biedt voor de belangen van de betrokkene op bescherming van de persoonlijke levenssfeer.

Het CBP acht het voorgestelde plan echter te onbepaald om te kunnen inschatten of het voorgestelde onderzoek van Bluetrace binnen een redelijke termijn zal leiden tot een (technische) wijziging van de huidige werkwijze. Met het louter voltooien van dit onderzoek is er in elk geval nog geen concrete aanpassing van de werkwijze van Bluetrace die aanleiding geeft voor een andere beoordeling van de vraag of er sprake is van de verwerking van persoonsgegevens.

De verzamelde wifi-mac-adressen van mobiele apparaten, in combinatie met de datum en het tijdstip van registratie en de (berekende locatie op basis van de) signaalsterkte en het serienummer van de sensor, zijn in deze context persoonsgegevens in de zin van artikel 1, onder a, van de Wbp, omdat het unieke identificerende nummers zijn van mobiele apparaten, waarmee aan de hand van locatie en tijdstip van waarneming individuele houders identificeerbaar zijn.

5.2 Verantwoordelijke en bewerker

De ontwikkeling en het gebruik van nieuwe ICT-producten en -diensten zorgen voor nieuwe rollen en verantwoordelijkheden, waarbij het niet altijd duidelijk is wie de verantwoordelijke is en wie eventueel een bewerker. Het eerste doel van het dataprotectierecht is om betrokkenen te beschermen bij de verwerking van hun persoonsgegevens. Als niet helder is op wie de belangrijkste verplichtingen rusten, als er geen verantwoordelijke is of een heel groot aantal mogelijke verantwoordelijken, dan is onvoldoende duidelijk welke organisatie aanspreekbaar is voor de verwerking van persoonsgegevens.[128] Voor de betrokkene is het dan bijvoorbeeld niet goed mogelijk om het recht op inzage, correctie en/of verwijdering van persoonsgegevens uit te oefenen.
Bluetrace werkt bij het leveren van de wifi-trackingdienstverlening in en rondom winkels nauw samen met zijn opdrachtgevers. Bij het dagelijks functioneren van deze dienst is er sprake van verwevenheid tussen de rol van de klant en de rol van Bluetrace.[129]
In het advies van de Artikel 29-werkgroep over de begrippen 'verantwoordelijke' en 'bewerker' wordt nader ingegaan op situaties waarin activiteiten van verschillende partijen met elkaar verweven zijn. De gezamenlijke toezichthouders lichten in deze opinie toe dat de partij die bepaalt welke gegevens worden verwerkt, de duur van de opslag van de gegevens vaststelt en zeggenschap heeft over de toegang tot de

[127] Artikel 29-werkgroep, WP 216, Advies 5/2014 over anonimiseringstechnieken, 10 April 2014 en Artikel 29-werkgroep, WP 185, Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten, 16 mei 2011
[128] Artikel 29-werkgroep, WP 169, Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", 16 februari 2010, p. 6. Zie ook de conclusies van het CBP over de verantwoordelijkheid van het Landelijk Schakelpunt in 2005, z2005-0505, URL: https://cbpweb.nl/sites/default/files/downloads/uit/z2005-0505.pdf.
[129] Gelet op de wetsgeschiedenis is niet zozeer de juridische constellatie tussen partijen bepalend, maar is de feitelijke situatie doorslaggevend. Is er zelfs weinig of niets geregeld in overeenkomsten, dan zal aan de hand van algemeen in het maatschappelijk verkeer geldende maatstaven moeten worden bezien aan welke natuurlijke persoon, rechtspersoon of bestuursorgaan de betreffende verwerking moet worden toegerekend. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 16 en p. 55.

gegevens als verantwoordelijke wordt aangemerkt. Dit zijn elementen van wezenlijk belang voor de gegevensverwerking.[130]

In de praktijk komt het veel voor dat een verantwoordelijke organisatie bepaalde aspecten van gegevensverwerking delegeert aan andere partijen, bijvoorbeeld omdat expertise of faciliteiten ontbreken om dat onderdeel zelf te regelen. Met name technische of organisatorische aangelegenheden kunnen worden gedelegeerd zonder af te doen aan de juridische status van drager van verantwoordelijkheid. De bovengenoemde punten van wezenlijk belang zijn echter essentiële elementen van verantwoordelijkheid, dat wil zeggen dat deze niet zomaar gedelegeerd kunnen worden.[131] Praktische indicaties van verantwoordelijkheid van een partij zijn:

- het bepalen van de doeleinden voor de gegevensverwerking;
- het bepalen van de middelen die aangewend worden voor de verwerking;
- het bepalen welke gegevens worden verwerkt;
- het bepalen van de bewaartermijnen;
- zeggenschap over de toegang tot de gegevens;
- zeggenschap over de informatie die wordt verstrekt aan de betrokkene;
- zeggenschap over het verstrekken van gegevens aan derden en/of naar partijen in landen buiten de EU;
- de contractuele afspraken over gegevensverwerking tussen partijen.

Contracten en andere formeel-juridische bronnen zijn niet allesbepalend. Uiteraard is uit (contractuele) afspraken tussen partijen af te leiden hoe de verantwoordelijkheden voor gegevensverwerking zijn verdeeld over de partijen, maar de juridische allocatie van verantwoordelijkheden die partijen zelf voor ogen hadden is niet doorslaggevend wanneer er in de praktijk feitelijk niet naar gehandeld wordt.[132] Overeenkomsten zijn wel een goed aanknopingspunt om te beginnen wanneer de verantwoordelijkheid voor gegevensverwerking moet worden vastgesteld.

Bij Bluetrace is sprake van een relatie tussen opdrachtgever en opdrachtnemer. De klanten van Bluetrace huren het bedrijf in om voor hen een wifi-trackingsysteem op te zetten en daaraan gerelateerde diensten te leveren. De dienstverlening van Bluetrace bestaat daarmee niet primair uit het verwerken van gegevens.[133] De verwerking van gegevens is een uitvloeisel van de dienst waarvoor het bedrijf ingehuurd wordt door klanten, namelijk het installeren van wifi-trackingsystemen in en rond winkels, het genereren van meetgegevens en het analyseren, beheren en opslaan daarvan. Bluetrace levert daarvoor de technologie, plaatst deze bij de klant en onderhoudt deze ook. Daarnaast worden de meetgegevens verwerkt en in een voor de klant begrijpelijke rapportage opgeleverd. Volgens de memorie van toelichting op de Wbp is de omstandigheid dat de gegevensverwerking meer een uitvloeisel van de

[130] Artikel 29-werkgroep, WP 169, Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", 16 februari 2010, p. 15-17, 32 en 37.
[131] Artikel 29-werkgroep, Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", m.n. p. 14 van de Engelstalige versie en p. 16 e.v. van de Nederlandstalige versie.
[132] Idem, voorbeeld van de SWIFT-zaak, p 11.
[133] Voor de beoordeling van de vraag naar verantwoordelijkheid is van belang of de diensten die verleend worden primair bestaan uit dataverwerking. Wanneer dit namelijk het geval is, kan er sprake zijn van een bewerkersopdracht waarbij de ene partij een bepaalde verwerking van gegevens uitbesteedt aan de andere partij.

dienstverlening is dan een primaire activiteit, een indicatie dat er geen sprake is van bewerkerschap in de zin van de Wbp.[134]

Bluetrace bepaalt wezenlijke aspecten van de gegevensverwerking bij wifi-tracking. Het feit dat er in deze zaak sprake is van een opdrachtgever-opdrachtnemerrelatie lijkt erop te wijzen dat de verantwoordelijkheid voor dataverwerking ligt bij de opdrachtgevende partij die het initiatief neemt. Maar omdat Bluetrace zelf bepaalt welke soort gegevens het bedrijf verwerkt, hoe lang en met welke technische middelen, ligt de verantwoordelijkheid primair bij Bluetrace. [135] Bluetrace heeft bovendien het feitelijk beheer over alle opgeslagen gegevens uit de trackingactiviteiten en de zeggenschap over eventueel te hanteren bewaartermijnen. Bluetrace verwerkt meetgegevens met als doel het leveren van bedrijfseconomische data aan de klant. Dit is een eigen doel, bepaald door Bluetrace, waarmee het bedrijf een dienst met toegevoegde waarde levert aan zijn klanten. Zonder de data-analyse zou Bluetrace slechts ruwe meetgegevens kunnen overleggen aan de klant en is er nauwelijks sprake van bedrijfseconomische informatie.[136] Hieraan doet niet af dat het bedrijf daarmee opdrachtgevers van dienst wil zijn. De opdrachtgever bepaalt vervolgens op welke manier de door Bluetrace geleverde bedrijfseconomische informatie wordt toegepast in het bedrijf. Tot slot is van belang dat Bluetrace zelfstandig besluiten heeft genomen over het wel of niet verstrekken van gegevens aan derden en/of opsporingsdiensten.

Gelet op het bovenstaande is Bluetrace de verantwoordelijke in de zin van artikel 1, onder d, van de Wbp. Het overgrote deel van de essentiële elementen van verantwoordelijkheid voor de gegevensverwerking in de zin van de Wbp ligt feitelijk bij Bluetrace.

Niettemin is er sprake van verwevenheid tussen de activiteiten van Bluetrace en de activiteiten van zijn klanten. De Wbp en de richtlijn gaan ervan uit dat de zeggenschap en bevoegdheden ten aanzien van de belangrijkste aspecten van dataverwerking in de regel in dezelfde hand liggen. Is dit niet het geval, dan kan er sprake zijn van gezamenlijke verantwoordelijkheid. Hoewel de wetgever en ook de Europese richtlijnen rekening houden met deze mogelijkheid, is niet concreet uitgewerkt welke vormen van gezamenlijke verantwoordelijkheid mogelijk zijn en welke gevolgen dit heeft voor aansprakelijkheid. De memorie van toelichting bij de Wbp geeft drie basisvarianten aan die in elk geval mogelijk zijn, te weten 'gemeenschappelijke verantwoordelijkheid', 'afzonderlijke verantwoordelijkheid' en 'gezamenlijke verantwoordelijkheid'.[137]

---

[134] Het bewerkersbegrip is in principe van toepassing op verschillende vormen van dienstverlening. Uitgangspunt is daarbij dat de dienstverlening betrekking heeft op het verwerken van persoonsgegevens. Zodra de gegevensverwerking een uitvloeisel is van een andere vorm van dienstverlening, is de dienstverlener daarvoor zelf verantwoordelijk. Een advocaat die namens een cliënt optreedt of een telemarketingbedrijf dat in opdracht van een derde onderzoek verricht, is bijvoorbeeld zelf verantwoordelijk voor de verwerking van persoonsgegevens die bij uitvoering van zijn taak plaatsvindt. Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3 p. 62.

[135] Bluetrace is als rechtspersoon niet ondergeschikt aan (een van) zijn klanten.

[136] Bluetrace geeft aan dat de verzamelde data kan worden gebruikt voor *"Gathering data for predictive analysis of costumer and crowd behavior"*. Website Bluetrace, zoals vastgelegd op 10 december 2014. (www.bluetrace.nl)

[137] Gemeenschappelijke verantwoordelijkheid: Aan de verwerkingen nemen verschillende organisaties deel, er is echter één gemeenschappelijke verantwoordelijke. Deze is aansprakelijk voor de verwerkingen als geheel. Daarnaast zijn de deelnemende organisaties aansprakelijk voor de

Bluetrace heeft verschillende samenwerkingsafspraken gemaakt met zijn verschillende klanten. Daarbij zijn de verantwoordelijkheden niet gelijk verdeeld. Zo ligt het initiatief voor het inzetten van wifi-tracking bij de klanten en nemen de klanten besluiten over waar, waarom en hoe lang zij wifi-tracking willen inzetten en welke financiële middelen daarvoor beschikbaar zijn. Aan de andere kant heeft Bluetrace belangrijke verantwoordelijkheden en feitelijke zeggenschap over de gegevensverwerking, zoals hierboven toegelicht. De vorm waarin Bluetrace zijn meetresultaten uiteindelijk ontsluit aan de klanten varieert. Zo kan de ene klant wel ruwe meetgegevens inzien en de andere klant niet. De Artikel 29-werkgroep heeft in Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'bewerker' aangegeven dat gezamenlijke verantwoordelijkheid ook kan bestaan wanneer de taken ongelijk verdeeld zijn over meerdere organisaties of afdelingen.[138]

In deze casus is sprake van gezamenlijke verantwoordelijkheid, omdat de verschillende gegevensverwerkingen geïntegreerd zijn. Het is niet zo dat de klant verwerkingen doet in het kader van wifi-tracking die losstaan van andere verwerkingen die Bluetrace doet. Dit betekent dat zowel Bluetrace als zijn klanten verantwoordelijk zijn voor het geheel van de gegevensverwerkingen in het kader van wifi-tracking. Bluetrace kan als medeverantwoordelijke worden aangesproken voor alle handelingen die in het kader van de gegevensverwerking plaatsvinden, zoals het daadwerkelijk verwerken van persoonsgegevens (in de vorm van verzamelen, beheren, data-analyse), de keuze welke gegevens worden verwerkt en met welk doel[139], de inzet van technische middelen, de informatievoorziening aan het publiek, het vaststellen van de plaatsen waar gemeten moet worden, de duur van metingen en doelen voor de uiteindelijke toepassing van de bedrijfseconomische informatie, die via wifi-tracking is verkregen, in de organisatie van de klant.

Gelet op het bovenstaande is Bluetrace gezamenlijk met zijn opdrachtgevers (mede-) verantwoordelijke in de zin van de Wbp.

De omvang van de (gezamenlijke) verantwoordelijkheid van de opdrachtgevers van Bluetrace (de exploitanten van de winkels waar wifi-tracking uitgerold is) en de vraag in hoeverre deze verantwoordelijken handelen in overeenstemming met de Wbp, vallen buiten het bereik van dit onderzoek, nu dit onderzoek zich richt op Bluetrace en

---

aangeleverde gegevens. De verantwoordelijke is voor de inhoud daarvan slechts verantwoordelijk naar de mate waarop hij daarover juridische zeggenschap heeft. [...] Afzonderlijke verantwoordelijkheid: Verschillende verwerkingen zijn min of meer geïntegreerd zonder dat een gemeenschappelijke verantwoordelijke aanwezig is. Er is sprake van afzonderlijke verantwoordelijkheid per (deel-)verwerking. De betrokkene kan slechts een van de afzonderlijke verantwoordelijken aanspreken voor het aandeel van die partij in de dataverwerking. Gezamenlijke verantwoordelijkheid: Verschillende verwerkingen zijn geïntegreerd zonder dat een gemeenschappelijke verantwoordelijke aanwezig is. Er is sprake van gezamenlijke verantwoordelijkheid. Elk van de verantwoordelijken is aansprakelijk voor het geheel van verwerkingen. *Kamerstukken II* 1997/98, 25 892, nr. 3.p. 55 e.v.

[138] Zie artikel 15 van de Wbp. Zie ook Artikel 29 werkgroep, Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'bewerker', 16 februari 2010, p. 37-38.

[139] Dat wil zeggen doelen die onderbouwd moeten worden met een grondslag uit artikel 8 van de Wbp.

het CBP heeft vastgesteld dat in ieder geval Bluetrace op het moment van onderzoek de verantwoordelijke is voor de onderzochte gegevensverwerkingen.[140]

5.3 Grondslagen voor de verwerking van persoonsgegevens

Gelet op de wetssystematiek, hangt het vaststellen van de mogelijke grondslagen waarop een verantwoordelijke zich in een bepaald geval kan beroepen samen met het doel waarvoor gegevens worden verwerkt. In deze zaak heeft het CBP twee gegevensverwerkingen onderzocht, te weten de verwerking in het kader van wifi-tracking in winkels en de verwerking in het kader van wifi-tracking van passanten buiten de winkels, beide met als doel het genereren van bedrijfseconomische informatie. Managementinformatie over aantallen winkelbezoekers, aantallen passanten en verblijftijden en het aanbieden van data-analyses op basis van meetgegevens uit wifi-tracking zijn voorbeelden van bedrijfseconomische informatie in dit verband.
Het CBP heeft in paragraaf 3.3 van dit rapport vastgesteld dat de onderzochte werkwijze van gegevensverwerking bestaat uit het plaatsen van één sensor in een winkel met een bereik dat tot buiten de winkel reikt. Daardoor worden niet alleen gegevens van bezoekers van de winkel verwerkt, maar ook gegevens van personen die zich buiten de winkel bevinden, bijvoorbeeld voorbijgangers die langs het pand op straat lopen.

De Wbp bepaalt in artikel 8 dat persoonsgegevens alleen verwerkt mogen worden wanneer daarvoor een wettelijke grondslag is. Artikel 8 bevat een limitatieve opsomming van gronden (a tot en met f) die een gegevensverwerking rechtvaardigen. Bluetrace is van mening dat het bedrijf een gerechtvaardigd belang heeft, in de zin van onderdeel f van dit artikel, om wifi-tracking in en rond winkels toe te passen voor bedrijfseconomische doeleinden. Het CBP beoordeelt ambtshalve eerst of een van de andere grondslagen van toepassing kan zijn.

Beoordeling grondslagen uit artikel 8 van de Wbp

<u>Artikel 8, aanhef en onder a, van de Wbp – ondubbelzinnige toestemming</u>
Bluetrace vraagt betrokkenen die winkels betreden of passeren waar wifi-tracking actief is niet om toestemming en verkrijgt deze ook niet op een andere wijze. Er wordt bovendien niet of nauwelijks aan informatievoorziening over wifi-tracking gedaan, waardoor er geen sprake kan zijn van een op informatie berustende keuze van de betrokkene om het gebied met wifi-tracking wel of niet te betreden. Een beroep op de grondslag uit artikel 8, onder a, van de Wbp is dus in dit geval niet mogelijk.

<u>Artikel 8, aanhef en onder b, van de Wbp – ter uitvoering van een overeenkomst</u>
Onderdeel b biedt een grondslag voor de verwerking van persoonsgegevens als die noodzakelijk is om een overeenkomst uit te voeren waarbij de betrokkene partij is. Hoewel het denkbaar is dat wifi-tracking plaatsvindt op grond van een overeenkomst, is een beroep op deze grondslag in deze zaak niet mogelijk. Bluetrace sluit weliswaar overeenkomsten met zijn zakelijke klanten, maar dit zijn geen overeenkomsten

[140] Zie ook HvJ EU 13 mei 2014, C-131/12 (Google Spain SL, Google Inc / Agencia Española de Protección de Datos), r.o. 40, en gelet op artikel 15 van de Wbp.

waarbij de betrokkenen partij zijn.[141] De gegevensverwerkingen van Bluetrace kunnen daarom niet gebaseerd worden op de grondslag uit artikel 8 onder b van de Wbp.

Artikel 8, aanhef en onder c, d, en e, van de Wbp – wettelijke plicht, vitaal belang of publiekrechtelijke taak

Ten overvloede vult het CBP aan dat Bluetrace niet met publieke taken is belast. Bluetrace is evenmin onderworpen aan wettelijke verplichtingen die meebrengen dat het bedrijf bedrijfseconomische informatie moet leveren met wifi-tracking. Door wifi-tracking in winkelgebieden worden ten slotte ook geen handelingen verricht die van levensreddende aard zijn voor betrokkenen. Bluetrace kan daarom geen beroep doen op de grondslagen uit artikel 8, onder c, d, en e, van de Wbp.

Artikel 8, aanhef en onder f, van de Wbp – noodzakelijk voor de behartiging van een gerechtvaardigd belang

Voor de beoordeling of Bluetrace de gegevensverwerkingen in het kader van wifi-tracking in en buiten winkels kan baseren op de grondslag uit artikel 8, aanhef en onder f, van de Wbp is een belangenafweging nodig.
In lijn met de memorie van toelichting bij artikel 8, onderdeel f, van de Wbp en Opinie 6/2014 van de Artikel 29-werkgroep over het gerechtvaardigd belang beoordeelt het CBP eerst of de belangen van Bluetrace gerechtvaardigd kunnen zijn.[142] De volgende stap is de beoordeling of de gegevensverwerking noodzakelijk is om de nagestreefde belangen van de verantwoordelijke te verwezenlijken. Tot slot beoordeelt het CBP, voor zover relevant, welk gewicht toegekend kan worden aan de diverse belangen, waaronder het belang van betrokkenen op bescherming van de persoonlijke levenssfeer, en in hoeverre de verantwoordelijke waarborgen in acht neemt om de belangen van de betrokkenen te beschermen. Hierover gaat de volgende paragraaf.

5.3.1 Gerechtvaardigd belang voor wifi-tracking door Bluetrace in winkels

Het belang van Bluetrace bij wifi-tracking in winkels

Het verzamelen van informatie over aantallen winkelbezoekers, drukte op bepaalde tijden en bijvoorbeeld de route die het publiek loopt door een winkel, door middel van wifi-tracking, kan op zichzelf een gerechtvaardigd commerciëel belang zijn van de winkeliers en Bluetrace. Bluetrace levert de technologie en data-analysediensten om dit mogelijk te maken en is gezamenlijk met de winkeliers verantwoordelijk voor het geheel van gegevensverwerkingen dat dit met zich meebrengt, zoals vastgesteld in paragraaf 5.2.
De Minister van veiligheid en justitie bevestigde dit in antwoord op Kamervragen:
"Eigenaren van winkels zijn vrij in het vaststellen van voorwaarden waaronder het publiek gerechtigd is de winkel te betreden, zo lang die voorwaarden redelijk zijn. Tegen deze achtergrond moet ook de verzameling van gegevens door middel van wifi-trackers worden gezien. Op grond van artikel 8, onder f, van de Wet bescherming persoonsgegevens (Wbp) kan de eigenaar van de winkel het verzamelen van deze gegevens aanmerken als een gerechtvaardigd eigen belang, wanneer dit belang opweegt tegen het belang of de fundamentele rechten en vrijheden van de betrokkene, waaronder het belang bij de bescherming van de persoonlijke levenssfeer. Indien het belang van de winkeleigenaar is gelegen in het vaststellen van het aantal

[141] Er is ook geen sprake van een gegevensverwerking op verzoek van de betrokkene of van een precontractuele fase, zoals bedoeld in artikel 8, onder b van de Wbp.
[142] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 86 e.v., en Artikel 29-Werkgroep, WP 217, Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC. 9 april 2014. Annex I, p. 55 e.v. (alleen Engelstalig).

bezoekers en het vaststellen van hun verplaatsingsgedrag in de winkel, zonder dat in combinatie daarmee andere persoonsgegevens worden verwerkt, is voorstelbaar dat dit belang in concreto als redelijk kan worden aangemerkt. Daarbij geldt overigens dat ingevolge de artikelen 33 en 34 van de Wbp kenbaarheid aan de verwerking van persoonsgegevens moet worden gegeven."[143]

Noodzakelijkheid

Los van de eerste toets of er sprake is van een belang dat zich leent voor een beroep op artikel 8, aanhef en onder f, van de Wbp, moet de verwerking ook *noodzakelijk* zijn voor het nagestreefde belang, wil een beroep op deze grondslag slagen.[144] Aan dit noodzakelijkheidsvereiste wordt voldaan als het nagestreefde belang niet op een andere, minder vergaande manier of met minder ingrijpende middelen kan worden gediend. Het CBP toetst de gegevensverwerking in het kader van wifi-tracking in winkels daarom aan de vereisten van proportionaliteit en subsidiariteit.

De staatssecretaris van veiligheid en justitie zei hierover tegen de Tweede Kamer: *"Verantwoordelijke en betrokkene kunnen immers een onderling tegengesteld belang bij de verwerking van gegevens hebben. Maar ook de aard van de gegevens en van de verwerking, de verwachtingen die betrokkenen redelijkerwijs kunnen hebben, de waarborgen die zijn getroffen bij de verwerking van deze gegevens, en andere relevante omstandigheden behoren bij de afweging te worden betrokken.(…) Een voorbeeld van een dergelijke waarborg is het onmiddellijk en onomkeerbaar anonimiseren en aggregeren van de gegevens die met wifi-tracking worden verzameld (bijvoorbeeld door de identificerende kenmerken van de telefoons of andere apparaten van de betrokkenen direct te verwijderen), op zodanige wijze dat individuele gebruikers niet door de tijd heen kunnen worden herkend of onderscheiden.*[145]

Het CBP heeft in paragraaf 3.5. van dit rapport vastgesteld dat Bluetrace 24 uur per dag, zeven dagen per week metingen verricht in de winkels, dus ook als de winkels gesloten zijn. Het CBP merkt in het kader van proportionaliteit en subsidiariteit op dat het mogelijk is om metingen in winkels te beperken in tijd en ruimte. Het is bijvoorbeeld mogelijk om de metingen te beperken tot de reguliere openingstijden van winkels, of een andere afgebakende tijdsperiode, in plaats van 24 uur per dag en zeven dagen per week. Bluetrace licht het publiek niet in over de aanwezigheid van wifi-trackingtechnologie, de gegevens die daarmee worden verwerkt, de redenen voor de metingen in winkels en welke organisatie(s) daarvoor verantwoordelijk zijn. Bluetrace heeft geen bewaartermijn bepaald voor de (gehashte) gegevens. Daarnaast

[143] Vragen van de leden Oosenbrug (PvdA) en De Liefde (VVD) aan de ministers van Economische Zaken en van Veiligheid en Justitie over wifi-tracking door winkels, kenmerk 2014Z01179 (ingezonden 24 januari 2014) met antwoorden, 21 februari 2014, URL http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/02/22/antwoorden-kamervragen-ove-wifi-tracking-door-winkels.html.

[144] Het Hof van Justitie van de Europese Unie vult het begrip noodzakelijkheid op een strikte wijze in: Zie HvJ EU 16 december 2008, zaak C-524/06 (*Huber*), r.o. 52: *"Gelet op het doel, een gelijkwaardige bescherming te bieden in alle lidstaten, kan het begrip noodzakelijkheid zoals dit naar voren komt uit artikel 7, sub e, van richtlijn 95/46, dat een nauwkeurige afbakening wil geven voor een van de gevallen waarin de verwerking van persoonsgegevens geoorloofd is, dus niet een inhoud hebben die verschilt van lidstaat tot lidstaat. Het gaat bijgevolg om een autonoom begrip van het gemeenschapsrecht, dat moet worden uitgelegd op een wijze die volledig beantwoordt aan het doel van de richtlijn zoals omschreven in artikel 1, lid 1."*

[145] Vragen van het lid Oosenbrug (PvdA) aan de ministers van Veiligheid en Justitie en van Economische Zaken over wifi- en bluetooth tracking, kenmerk 2014Z04895 (ingezonden 17 maart 2014) met antwoorden van staatssecretaris Teeven, 24 april 2014. http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/04/25/antwoorden-kamervragen-over-wifi-en-bluetooth-tracking.html

geldt dat Bluetrace méér persoonsgegevens verwerkt dan strikt noodzakelijk is voor het omschreven doel, omdat de gegevens in beginsel voor onbeperkte tijd bewaard worden.

Gelet hierop is het CBP van oordeel dat het meten van bezoekersaantallen en verblijftijden uitvoerbaar is op een minder ingrijpende wijze. De werkwijze van Bluetrace voldoet derhalve niet aan het noodzakelijkheidsvereiste uit artikel 8, onder f van de Wbp.

Bescherming van de persoonlijke levenssfeer van de betrokkene

De aard van de verwerkte gegevens speelt een belangrijke rol in de afweging van de belangen van betrokkenen bij de bescherming van hun persoonlijke levenssfeer enerzijds, en de belangen van de verantwoordelijke anderzijds. Deze belangenafweging schetst het CBP hier ten overvloede, nu de verwerking van persoonsgegevens door Bluetrace in het kader van wifi-tracking in winkels niet voldoet aan de eisen van proportionaliteit en subsidiareit.
Er is sprake van de verwerking van locatiegegevens. Locatiegegevens zijn door de Artikel 29-werkgroep aangemerkt als gegevens met een hoog privacyrisico.[146] Het bedrijf biedt geen (informatie over) opt-outmogelijkheden aan.[147] Daardoor heeft de bezoeker van de winkel geen realistische mogelijkheid om zich te onttrekken aan de tracking in de winkel, anders dan het uitschakelen van de (wifi-functie van) mobiele apparatuur, of het volledig mijden van de betreffende winkel.

Bluetrace verwijdert de mac-adressen niet op het moment dat hetzelfde mac-adres voor een tweede maal wordt waargenomen. De werkwijze van Bluetrace leidt ertoe dat individuele winkelbezoekers door tijd de heen kunnen worden herkend of onderscheiden.[148] Gezien de invloed die dit heeft op de persoonlijke levenssfeer van de betrokkenen is er een beperking van de bewaartermijnen nodig als waarborg voor de belangen van de betrokkenen. Bluetrace biedt zijn opdrachtgevers weliswaar de mogelijkheid om de opgeslagen meetgegevens na korte tijd te (laten) hashen. In elk geval hasht Bluetrace de bewaarde gegevens na drie weken. Echter, de hashing maatregel neemt niet weg dat er persoonsgegevens lang bewaard worden. De wijze van hashing die Bluetrace toepast ziet het CBP als een beveiligingswaarborg, omdat het de gegevens beschermt tegen kennisname door derden die niet bekend zijn met de toegepaste hashing methode, bijvoorbeeld in geval van een datalek. Het is echter geen anonimiseringsmethode.
Het verwijderen van mac-adressen binnen een periode van maximaal 24 uur zou wel een extra waarborg kunnen zijn, indien het om een of andere reden niet mogelijk of niet haalbaar zou zijn om de persoonsgegevens na de vastlegging onomkeerbaar te anonimiseren.
Bluetrace heeft geen verklaringen of stukken overlegd waaruit af te leiden is dat het bedrijf een eigen interne belangenafweging heeft verricht om in te schatten in hoeverre het voldoende rekening houdt met de belangen van winkelbezoekers in zijn

[146] Zie de toelichting op het wettelijk kader in paragraaf 5.1 van dit rapport.
[147] Er zijn overigens ook geen opt-outmogelijkheden overwogen, terwijl andere bedrijven in de sector dit wel doen, zoals toegelicht in paragraaf 3.7 van dit rapport.
[148] Zie: Artikel 29-werkgroep, WP 185, Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten. Zie ook: Vragen van het lid Oosenbrug (PvdA) aan de ministers van Veiligheid en Justitie en van Economische Zaken over wifi- en bluetooth tracking, kenmerk 2014Z04895 (ingezonden 17 maart 2014) met antwoorden van Staatssecretaris Teeven, 24 april 2014.

huidige werkwijze.[149] Bluetrace adviseert opdrachtgevers ook niet over de privacyaspecten van de inzet van wifi-tracking.

Gelet op het voorgaande weegt het belang van Bluetrace thans niet op tegen het recht van de winkelbezoekers op eerbiediging van hun persoonlijke levenssfeer. Een geslaagd beroep op een gerechtvaardigd belang van Bluetrace als grondslag voor wifi-tracking in winkels is onder de gegeven omstandigheden niet mogelijk.

Naar aanleiding van het rapport voorlopige bevindingen heeft Bluetrace voorgesteld om onderzoek te doen naar de gevolgen die het afbakenen van wifi-tracking tot alleen winkelopeningstijden zou hebben voor Bluetrace als bedrijf en diens verplichtingen jegens anderen. Het beperken van de tijden waarop wordt gemeten kan worden gezien als een waarborg voor personen die langs de winkel komen, bijvoorbeeld voorbijgangers. De beperking van de meettijden zou bovendien leiden tot het verminderen van de hoeveelheid gegevens die wordt verwerkt, waarmee meer recht gedaan wordt aan het beginsel van subsidiariteit.

Echter, het enkel voltooien van een onderzoek is, zonder dat daaraan concrete acties zijn gekoppeld die in de praktijk leiden tot een aanpassing van de werkwijze van Bluetrace, niet voldoende concreet om te beschouwen als waarborg voor de belangen van de betrokkene. Bovendien is in dit hoofdstuk aangegeven dat er meer waarborgen voor de belangen van de betrokkene vereist zijn voor een geslaagd beroep op artikel 8 sub f van de Wbp.

Door het verwerken van persoonsgegevens met het doel het genereren van bedrijfseconomische informatie door wifi-tracking *in* winkels zonder geldige grondslag, handelt Bluetrace in strijd met artikel 8 van de Wbp.

5.3.2 Gerechtvaardigd belang voor wifi-tracking door Bluetrace buiten winkels

Het belang van Bluetrace bij wifi-tracking buiten winkels
Het genereren van bedrijfseconomische informatie door wifi-tracking van passanten op de openbare weg, op een wijze die naar zijn aard verborgen blijft voor het publiek, is, mede gelet op het voorgaande, geen belang dat in aanmerking komt voor een beroep op de grondslag 'gerechtvaardigd belang van de verantwoordelijke' zoals bedoeld in artikel 8, onder f, van de Wbp.[150] Aan de afweging tussen het belang van de verantwoordelijke en de belangen van de betrokkenen komt men dan niet toe.
Het CBP wijst erop dat de verwerking van persoonsgegevens via wifi-tracking in de openbare ruimte, zoals in casu buiten de winkels, op een wijze die verborgen blijft voor het publiek niet toegestaan is zonder een voorafgaand onderzoek van het CBP, omdat deze vorm van heimelijke waarneming valt onder artikel 31, eerste lid, onder b, van de Wbp.

[149] Vergelijk: Onderzoek CBP naar de verwerking van persoonsgegevens door Snappet, Rapport definitieve bevindingen, 14 juli 2014, z2013-00795, p. 51-52. URL: https://cbpweb.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf
[150] Voor het verrichten van wifi-tracking op de openbare weg met het voornemen om dit verborgen te houden voor de betrokkenen is een voorafgaand onderzoek van het CBP vereist, als bedoeld in artikel 31 lid 1, onder b, van de Wbp.

Het CBP heeft echter niet vastgesteld dat Bluetrace daadwerkelijk de keuze heeft gemaakt om wifi-tracking buiten winkels te realiseren op een wijze die geheel verborgen moet blijven voor het publiek. Bluetrace heeft namelijk verklaard dat een van zijn klanten het publiek wel –zij het summier – informeert met een sticker op de winkelruit en dat hij daartegen geen bezwaar heeft gemaakt.[151] Hierdoor gaat het CBP er van uit dat heimelijke waarneming niet het oogmerk van Bluetrace is.

Wanneer de betrokkenen op een op andere wijze op de hoogte zijn van deze gegevensverwerking, dan is een beroep op een gerechtvaardigd belang onder omstandigheden mogelijk, mits de voorgenomen verwerking noodzakelijk is voor het nagestreefde belang en er voldoende rekening gehouden wordt met het recht op bescherming van de persoonlijke levensfeer van betrokkenen.

In dat geval moet bij het beoordelen van de noodzakelijkheid en de impact van de verwerking van persoonsgegevens via wifi-tracking op de persoonslijke levenssfeer van de betrokkenen meegenomen worden dat er een belangrijk verschil is tussen het registreren van winkelbezoekers enerzijds en het registreren van winkel*passanten* anderzijds. Wifi-tracking op de openbare weg, of anderzins buiten de winkel, heeft een grotere impact op de persoonlijke levenssfeer dan wifi-tracking in een winkel. Een verschil met wifi-tracking in een winkel is dat het in een winkel gaat om een afgebakende plaats waarbinnen bezoekers aan tracking onderworpen worden en waarbinnen zij hierover geïnformeerd kunnen worden. Bovendien kan de bezoeker een vrije keuze maken om een winkel wel of niet te betreden. Op de openbare weg geldt dat de partij die wifi-tracking wil toepassen rekening moet houden met de redelijke verwachting van privacy bij het passerende publiek, omdat die er niet op bedacht hoeft te zijn om in de openbare ruimte gevolgd te worden. De staatssecretaris van veiligheid en justitie merkte daarover in de beantwoording van Kamervragen het volgende op:

"Het ligt in de rede dat de voornoemde belangenafweging anders uitpakt bij gegevens die op de openbare weg zijn verzameld dan bij gegevens die zijn verzameld in de winkel, omdat betrokkenen op de openbare weg in algemene zin vaak niet adequaat zullen kunnen worden geïnformeerd over de gegevensverwerking. Het belang van de betrokkene zou dan zwaarder kunnen wegen dan dat van de winkelier, waarbij ook meespeelt dat passanten er niet op verdacht hoeven te zijn dat zij mogelijk worden gevolgd. Door het ontbreken van de benodigde informatie kunnen deze personen ook geen maatregelen nemen om het verzamelen van de gegevens te voorkomen, zoals het uitschakelen van Bluetooth en WiFi."[152]

Gelet op het bovenstaande geldt voor wifi-tracking buiten de winkel, bijvoorbeeld op een deel van op de openbare weg, dat een hoge drempel zal moeten worden genomen alvorens het gerechtvaardigd belang in de zin van artikel 8 onder f van de Wbp als grondslag kan worden aanvaard. De belangen van de betrokkene(n) op bescherming van de persoonlijke levenssfeer zullen in dergelijke situaties snel zwaarder wegen dan de belangen van de verantwoordelijke. Het gaat echter steeds om een belangenafweging in een concreet geval. De beoordeling van de werkwijze van Bluetrace volgt hierna.

[151] Zie bevindingen in paragraaf 3.3.

[152] Vragen van het lid Oosenbrug (PvdA) aan de ministers van Veiligheid en Justitie en van Economische Zaken over wifi- en bluetooth tracking, kenmerk 2014Z04895 (ingezonden 17 maart 2014) met antwoorden van Staatssecretaris Teeven, 24 april 2014, URL: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/04/25/antwoorden-kamervragen-over-wifi-en-bluetooth-tracking.html

Noodzakelijkheid wifi-tracking buiten de winkel voor het leveren bedrijfseconomische informatie

Het CBP stelt vast dat de huidige werkwijze van Bluetrace waarbij wifi-tracking tot buiten de winkels reikt niet voldoet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit.
Bluetrace plaatst geen sensoren in de openbare ruimte, maar doet dat binnen in een winkel en gebruikt steeds één sensor per winkel. Toch stelt Bluetrace het bereik van de sensor zodanig af dat een deel van de openbare ruimte, direct aan het eigen terrein grenzend, binnen het bereik van de sensor valt.
Het CBP stelt vast dat Bluetrace onvoldoende heeft onderbouwd wat de noodzaak is om mensen buiten de winkel (de voorbijgangers) te tracken op de wijze waarop dat gebeurd. Bluetrace is technisch in staat om het bereik van de metingen in te stellen en kan er voor kiezen om dit te beperken tot de winkel zelf, zodat aanwezigheid van voorbijgangers op de openbare weg niet, of in ieder geval zo min mogelijk, geregistreerd wordt. Het feit dat het nuttig kan zijn voor winkeliers om een vergelijking te maken tussen de aantallen passanten en het aantal mensen dat daadwerkelijk de winkel betreedt, rechtvaardigt de huidige werkwijze nog niet. Voor een rechtvaardiging is vereist dat de noodzaak van de gekozen werkwijze is aangetoond. Er zijn bovendien andere methodes beschikbaar om dergelijke getallen te produceren.[153]
Bluetrace heeft geen adequate informatie over wifi-tracking buiten winkels verstrekt aan betrokkenen.
Voorts is, net als in de beoordeling van wifi-tracking binnen winkels, van groot belang dat er 24 uur per dag, zeven dagen per week gemeten wordt. Het CBP acht wifi-tracking op een dergelijke schaal buiten de winkels niet noodzakelijk voor het effectief nastreven van de belangen van Bluetrace. Het CBP wijst erop dat het mogelijk is om gedurende kortere periodes, op sterk afgebakende plaatsen en tijdstippen (bijvoorbeeld winkelopeningstijden) aan wifi-tracking te doen met als doel het genereren van bedrijfseconomische informatie. Daarnaast geldt dat Bluetrace méér persoonsgegevens verwerkt dan strikt noodzakelijk is voor het omschreven doel, omdat de gegevens in beginsel voor onbeperkte tijd bewaard worden. Daarbij neemt het CBP in ogenschouw dat het recht op bescherming van de persoonlijke levensfeer van de betrokkenen in de openbare ruimte zwaar weegt, gelet op de redelijke verwachting van het publiek om als voorbijganger niet ongemerkt gevolgd te worden en het feit dat er systematisch gegevens vastgelegd worden.[154]

Impact van wifi-tracking buiten winkels op de persoonlijke levenssfeer van betrokkenen
Nu de werkwijze van Bluetrace ten aanzien van wifi-tracking buiten winkels de noodzakelijkheidstoets niet doorstaat, overweegt het CBP het volgende slechts ten overvloede.
Indien Bluetrace de noodzaak voor wifi-tracking met een bereik dat zich deels buiten de winkel uitstrekt al zou kunnen onderbouwen – en voor zover het bedrijf zou

[153] Bluetrace heeft hiervoor bijvoorbeeld telcamera's of aanverwante apparatuur tot zijn beschikking, zoals beschreven op pagina 14 en 15 van dit rapport. Er kan uiteraard ook door mensen geteld worden.
[154] Zie bijvoorbeeld: Europese Hof voor de Rechten van de Mens, 25 september 2001, (P.J. en J.H. vs. Verenigd Koninkrijk), r.o. 57

voldoen aan de vereisten van proportionaliteit en subsidiariteit door, onder meer, de metingen te beperken in tijd en ruimte – zal het belang van Bluetrace op moeten wegen tegen de belangen van individuele betrokkenen bij de bescherming van hun persoonlijke levenssfeer. Dit is bijvoorbeeld het geval wanneer er, mede gelet op de aard van de verwerkte gegevens, adequate waarborgen ter bescherming van de belangen van de betrokkenen zijn.

Het CBP stelt vast dat Bluetrace de opgeslagen gegevens weliswaar beveiligd (versleuteld) door middel van hashing, maar dat het bedrijf de persoonsgegevens in beginsel voor onbeperkte tijd bewaard. De werkwijze van Bluetrace leidt ertoe dat individuele winkelbezoekers door tijd de heen kunnen worden herkend of onderscheiden.[155] Gezien de invloed die dit heeft op de persoonlijke levenssfeer van de betrokkenen is er een beperking van de bewaartermijnen nodig als waarborg voor de belangen van de betrokkenen. Het CBP stelt zich op het standpunt dat Bluetrace de persoonsgegevens onmiddellijk, dan wel in ieder geval zo snel mogelijk na de eerste vastlegging, onomkeerbaar zal moeten anonimiseren om de inbreuk op de persoonlijke levenssfeer van de betrokkenen te minimaliseren.[156]

Deze waarborg acht het CBP echter op zichzelf niet toereikend om tegemoet te komen aan de belangen van voorbijgangers op de openbare weg en omwonenden die onderwerp van wifi-tracking *buiten* de winkels voor bedrijfseconomische doeleinden worden.
Net als in paragraaf 5.3.1., hiervoor, is van belang dat het hier gaat om de verwerking van lokatiegegevens. Dit zijn gegevens die naar hun aard privacy-gevoelig zijn.
Het CBP wijst in het bijzonder op het feit dat er specifieke groepen mensen zijn wiens persoonlijke levenssfeer extra onder druk komt te staan wanneer wifi-tracking zich buiten de kaders van een winkel uitstrekt. Het gaat hierbij om de omwonenden van de betreffende winkel. Wanneer een deel van de openbare weg vlak buiten de winkel binnen het bereik van wifi-tracking valt is het aannemelijk dat een omwonende het gebied waarbinnen tracking gedaan wordt relatief vaak zal passeren. Het CBP stelt daarnaast vast dat het bereik van de sensoren slechts in beperkte mate begrenst wordt door fysieke barrières zoals muren, gelet op het stralingspatroon van de antennes en de eigenschappen van wifi-radiosignalen. Dit betekent dat niet alleen een deel van de buitenruimte op de openbare weg vóór de winkel wordt meegenomen maar ook een deel van de ruimte naast, boven of onder een winkel. Daarmee vallen naastgelegen panden en mogelijk ook woningen potentieel binnen het bereik van wifi-tracking door Bluetrace. Het CBP stelt daarom dat er waarborgen moeten zijn om te voorkomen dat iemand geregistreerd, gevolgd of gecontroleerd kan worden in zijn woonruimte, wanneer deze privéruimte zich binnen het bereik van wifi-tracking bevind. Het aanbieden van een effectieve opt-out mogelijkheid aan de betrokkenen is een zeer belangrijke waarborg in dit verband, omdat het anders niet mogelijk is voor de betrokkenen om zich aan wifi-tracking in hun privéruimte te onttrekken.

[155] Zie ook de beoordeling in paragraaf 5.3.1. Zie verder: Artikel 29-werkgroep, WP 185, Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten. Zie ook: Vragen van het lid Oosenbrug (PvdA) aan de ministers van Veiligheid en Justitie en van Economische Zaken over wifi- en bluetooth tracking, kenmerk 2014Z04895 (ingezonden 17 maart 2014) met antwoorden van Staatssecretaris Teeven, 24 april 2014.
[156] Zie ook: Artikel 29-werkgroep, WP 185, Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten. Zie ook: Vragen van het lid Oosenbrug (PvdA) aan de ministers van Veiligheid en Justitie en van Economische Zaken over wifi- en bluetooth tracking, kenmerk 2014Z04895 (ingezonden 17 maart 2014) met antwoorden van Staatssecretaris Teeven, 24 april 2014.

Daarnaast acht het CBP het noodzakelijk dat de omwonenden gericht en actief worden geïnformeerd door de verantwoordelijke partij(en) over de aanwezigheid, de werking, het doel en de reikwijdte van wifi-tracking waaraan zijn in de openbare ruimte of in de privésfeer worden blootgesteld.[157]

Bluetrace heeft geen blijk gegeven van een interne belangenafweging waarin de noodzaak voor de huidige werkwijze die zich tot buiten de winkels uitstrekt en mogelijke minder inbreukmakende alternatieven aan bod zijn gekomen. Bluetrace heeft geen argumenten aangevoerd waarom een minder inbreukmakende werkwijze niet zou volstaan om zijn doelen te verwezenlijken en om zijn diensten te leveren aan klanten.

Naar aanleiding van het rapport voorlopige bevindingen van het CBP heeft Bluetrace voorgesteld om een onderzoek te doen naar de gevolgen van het beperken van wifi-tracking tot binnen de winkels en niet meer buiten de winkels. Het beperken van de reikwijdte van wifi-tracking tot binnen winkels zou de impact van wifi-tracking op de openbare ruimte en de persoonlijke levenssfeer van betrokkenen sterk verminderen. Ook zou een dergelijke maatregel kunnen zorgen dat meer recht wordt gedaan aan de beginselen van proportionaliteit en subsidiariteit. Dat wil zeggen, dat met het beperken van het gebied waarbinnen aan wifi-tracking wordt gedaan voorkomen wordt dat er meer gegevens worden verzameld dan strikt noodzakelijk is voor het doel van de verwerking. Het CBP stelt vast dat het door Bluetrace voorgestelde onderzoek een stap is die het bedrijf kan zetten om de noodzaak van gegevensverwerkingen voor wifi-tracking te bepalen en de bij deze verwerking betrokken belangen af te wegen.
Echter, het enkel voltooien van een onderzoek naar de gevolgen van het afbakenen van wifi-tracking tot alleen binnen de winkel voor Bluetrace als bedrijf, zonder dat daaraan concrete acties zijn gekoppeld die in de praktijk leiden tot een aanpassing van de werkwijze van Bluetrace, is niet voldoende om te kunnen spreken van waarborgen voor de belangen van betrokkenen.

Bluetrace heeft in de zienswijze op de voorlopige bevindingen van het CBP tevens voorgesteld om nader onderzoek te doen naar het ontwikkelen van opt-out mogelijkheden. Het aanbieden van een effectieve opt-out mogelijkheid ziet het CBP als een belangrijke waarborg, die, in combinatie met andere waarborgen, kan leiden tot de slotsom dat de verantwoordelijke voldoende rekening met de belangen van de betrokkenen heeft gehouden. Zodra Bluetrace daadwerkelijk realistische opt-out mogelijkheden voor het publiek aanbiedt, of heeft ontwikkeld, waarmee een betrokkene zich kan onttrekken aan de gegevensverwerking indien hij dat wenst, kan het CBP beoordelen of daarmee de gesignaleerde risico's voor de persoonlijke levenssfeer van de betrokkenen worden weggenomen.

Het enkel voltooien van een onderzoek, zonder dat daaraan concrete acties zijn gekoppeld die in de praktijk leiden tot een aanpassing van de werkwijze van Bluetrace is onvoldoende om de gegevensverwerking in overeenstemming met de Wbp te brengen.

[157] Zie voor een toelichting op de mogelijke (en vereiste) waarborgen voor de belangen van de betrokkene, zoals bedoeld in de Europe privacyrichtlijn: Artikel 29 werkgroep, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), p. 51 en 56

De wijze waarop Bluetrace wifi-trackingtechnologie toepast buiten de winkels voldoet daarmee niet aan de vereisten van proportionaliteit en subsidiariteit en weegt niet op tegen de inbreuk op de persoonlijke levenssfeer van betrokkenen die daarmee gepaard gaat.

Door het verwerken van persoonsgegevens met het doel het genereren van bedrijfseconomische informatie via wifi-tracking *buiten* winkels zonder geldige grondslag handelt Bluetrace in strijd met artikel 8 van de Wbp.

5.4 Informatieverstrekking aan de betrokkene

Het CBP heeft in paragraaf 5.1. van dit rapport vastgesteld dat Bluetrace via wifi-tracking in en buiten winkels persoonsgegevens verzamelt. Daarom moet Bluetrace bij wifi-tracking binnen én buiten winkels voldoen aan de informatieverplichtingen uit de Wbp.

De wijze waarop informatie wordt verstrekt is in beginsel vormvrij. Het uitgangspunt is dat de informatie zodanig moet worden verstrekt dat de betrokkene daarover daadwerkelijk beschikt voordat er persoonsgegevens worden verwerkt. Het is daarbij van belang dat uit deze informatievoorziening duidelijk blijkt wat er gemeten wordt (welke gegevens verwerkt worden), wie hiervoor verantwoordelijk is en met welke redenen (doeleinden) dit gebeurd.[158]

Gelet op de aard van de verwerkte persoonsgegevens, namelijk locatiegegevens, dient Bluetrace aanvullende informatie te verstrekken om 'een eerlijke verwerking' te waarborgen. De Europese privacyrichtlijn 95/46/EG brengt dit tot uitdrukking door de woorden 'ten minste' in de aanhef van beide artikelen over de informatieplicht.[159] Hierbij valt te denken aan informatie over de omvang van het gebied en het tijdsbestek waarin betrokkenen onderwerp van wifi-tracking kunnen worden en over de periode dat de gegevens worden verzameld en bewaard. Zodra Bluetrace en/of zijn klanten opt-outmogelijkheden aanbieden aan betrokkenen, moeten zij informatie verstrekken over de wijze waarop een betrokkene zich aan de metingen kan onttrekken.

Voor Bluetrace geldt de informatieverplichting uit artikel 34 van de Wbp.[160] Het gaat daarbij om de informatieplicht over persoonsgegevens die op indirecte wijze zijn verkregen, in casu door het uitlezen van de wifi-mac-adressen van smartphones en andere mobiele apparaten. Bluetrace heeft de gegevens over mobiele apparatuur zelf verzameld, bij de betrokkenen, door signalen op te vangen met de trackingsensoren. Omdat Bluetrace niet bekend heeft gemaakt dat er wifi-tracking plaatsvindt, is het publiek niet geïnformeerd over deze gegevensverzameling. Bluetrace stelt betrokkenen daardoor ook niet in de gelegenheid hun gedrag aan te passen, bijvoorbeeld door hun apparatuur anders in te stellen of uit te schakelen, andere

[158] Zie ook artikel 11 onder c van de Europese privacyrichtlijn 95/46/EC ('the categories of data concerned').
[159] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 149-150. Zie ook: CBP, Wbp naslag bij hoofdstuk 5 Wbp (www.cbpweb.nl).
[160] De artikelen 43 en 44 van de Wbp zijn niet van toepassing op wifi-tracking door Bluetrace.

routes te lopen of anderszins bezwaar te maken tegen opname van de hen betreffende gegevens in de bestanden van Bluetrace.
Zoals toegelicht in hoofdstuk 4 van dit rapport over het wettelijk kader, kent de Wbp twee artikelen waarin een informatieplicht voor de verantwoordelijke is neergelegd, te weten de artikelen 33 en 34. De memorie van toelichting bij de Wbp geeft – onder andere – met een voorbeeld over cameratoezicht aan welke verplichting geldt in welke situatie. Als cameratoezicht heimelijk geschiedt, is artikel 34 Wbp van toepassing; is het kenbaar voor de betrokkene, dan geldt artikel 33.
"De gegevensvergaring met behulp van videocamera's kan onder artikel 33 worden geschaard indien het geen geheime observatie betreft. Indien de betrokkene op de hoogte is van de aanwezigheid van camera's en hij eveneens weet voor welk doel deze gebruikt worden, heeft hij de mogelijkheid zich hieraan te onttrekken Doet hij dat niet dan kan gesteld worden dat hij zijn persoonsgegevens voor het desbetreffende doel bewust ter beschikking heeft gesteld."[161]

Bluetrace verstrekt in het geheel geen informatie aan het publiek over de verwerking van persoonsgegevens via wifi- tracking, niet op de meetlocaties en ook niet via zijn website.[162] Dit geldt voor zowel de metingen in winkels als de metingen van voorbijgangers op de openbare weg. Bluetrace heeft geen privacybeleid.

De werkwijze die Bluetrace verkiest, die meebrengt dat gegevens op dit moment verzamelt zonder het publiek te informeren, betekent nog niet dat informeren redelijkerwijs niet mogelijk is en ontslaat het bedrijf niet van de verplichting om op grond van artikel 34, eerste lid, onder a, Wbp betrokkenen te informeren op het moment van vastlegging van de gegevens. Bluetrace kan geen beroep doen op de uitzonderingen in het vierde lid van artikel 34 Wbp, omdat het bedrijf wel degelijk in staat is om betrokkenen te informeren op het moment van de gegevensverzameling en dit voor het bedrijf geen onevenredige inspanning inhoudt. Een toelichting op deze beoordeling volgt hieronder. Bluetrace kan geen beroep doen op de uitzondering uit het vijfde lid van artikel 34 omdat er geen sprake is van een wettelijk voorschrift, in de zin van deze uitzondering.

Geen uitzondering informatieplicht bij wifi-tracking in winkels
Het is voor Bluetrace goed mogelijk om het publiek te voorzien van informatie over wifi-tracking binnen in de winkels.[163] Er kunnen in een winkel duidelijke borden, posters of stickers opgehangen worden, waarop ruimte is voor enige uitleg. Ook kan het winkelpersoneel geïnstrueerd worden om voorlichting te geven aan het publiek en is het mogelijk om informatiebrochures voorradig te hebben in winkels.[164] Het is in het

[161] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 155-157.
[162] Verklaringen Bluetrace tijdens het bedrijfsbezoek op 3 februari 2015, zoals weergegeven in de brief van het CBP aan Bluetrace, d.d. 27 februari 2015, bijlage, paragraaf 42.
[163] Andere verantwoordelijken doen dit immers, zij het in beperkte mate, zoals toegelicht in paragraaf 3.3 van dit rapport.
[164] Informatievoorziening is in dit verband vormvrij, zolang de uitleg de doelgroep maar bereikt. Zo kan bijvoorbeeld met een QR-code op de genoemde posters of stickers worden doorverwezen naar een website met meer informatie over doelen, verantwoordelijkheden en gegevensverwerkingen bij wifi-tracking. Zie ter vergelijking ook het Protocol Collectief winkelverbod (Hoofdbedrijfschap Detailhandel, 2008). Hierbij is een sticker ontworpen die geschikt is om betrokkenen te informeren over het hanteren van een beleid van zwarte lijsten van personen met een winkelverbod. Te raadplegen via: . Zie ook: CBP, z2010-00628, Besluit geen nader onderzoek collectief winkelverbod Leeuwarden, 6 juli 2010; CBP, z2010-01438, Besluit geen nader onderzoek, Protocol collectief winkelverbod Venray centraal, 16 december 2010; CBP, z2010-01439, Besluit geen nader onderzoek, Protocol collectief winkelverbod Voorthuizen, 16 december 2010. Te raadplegen via: URL

straatbeeld gebruikelijk dat op de stoep voor winkels reclame- en informatieborden staan. Een mededeling over tracking is op een dergelijke plaats (ook) mogelijk. Daarnaast kunnen op websites of via advertenties mededelingen aan het publiek gedaan worden over wifi-tracking in winkels. Het CBP oordeelt dat het verstrekken van informatie over wifi-tracking in winkels geen onevenredige inspanning van Bluetrace vereist.

De omstandigheid dat metingen doorgaans op het terrein van de opdrachtgever van Bluetrace plaatsvinden doet hier niet aan af, omdat Bluetrace als (gezamenlijke) verantwoordelijke in ieder geval ook de verantwoordelijkheid draagt voor naleving van de informatieplicht.[165] Bluetrace kan richting zijn opdrachtgevers aangeven dat het verstrekken van informatie aan het publiek, waaronder in het bijzonder de omwonenden, een voorwaarde is voor het kunnen implementeren van wifi-tracking en hierover (contractuele) afspraken maken.

Het CBP schrijft in dit geval niet bindend voor welke vorm van communicatie aan het publiek toegepast moet worden in dit geval. Het is in eerste instantie aan de verantwoordelijke partij(en) zelf om de meest geëigende wijze van informatievoorziening aan het publiek te kiezen en zich ervan te vergewissen dat de informatie de doelgroep bereikt.

Geen uitzondering informatieplicht bij wifi-tracking buiten winkels
Bij wifi-tracking van voorbijgangers is de kans groot dat een persoon al is geregistreerd op het moment dat hij of zij een eventueel bord bij/op de deur of etalage kan lezen, omdat het bereik van de sensoren in de winkels tot (ver) voorbij de voordeur reikt. Bluetrace moet als de verantwoordelijke voor wifi-tracking in de openbare ruimte daarom communicatiemiddelen inzetten waarvan het redelijkerwijs aannemelijk is dat deze het publiek tijdig zullen bereiken op de locatie waar wifi-tracking is geïmplementeerd. Hierbij kan gedacht worden aan persberichten, openbare aanplakkingen, borden op palen bij de ingang van winkelcentra (vergelijkbaar met informatie over cameratoezicht), gerichte advertenties, herkenbaarheid van de wifi-trackingapparatuur ter plaatse en duidelijke herkenbaarheid of markering van het gebied waarbinnen wifi-tracking plaatsvindt. Het CBP stelt vast dat het informeren van betrokkenen, zoals bedoeld in het vierde lid van artikel 34 van de Wbp, niet onmogelijk is.

Het CBP wijst hier ook op de maatschappelijke context van deze gegevensverwerking. Naar mate er meer trackingtechnologie wordt ingezet, nemen de mogelijkheden toe om personen in de openbare ruimte te registreren. Er zijn steeds meer marktpartijen die diensten aanbieden op het gebied van tracking en tracing, bijvoorbeeld in het kader van 'smart cities', en er vinden overal in Nederland pilots plaats met het meten van gegevens uit smartphones. Omdat veel Nederlanders altijd een smartphone bij zich dragen, komt daardoor een steeds groter deel van onze openbare ruimte binnen het bereik van sensoren. Vrijwel ongemerkt kunnen daardoor ook steeds meer

https://cbpweb.nl/nl/zelf-doen/register-zwarte-lijsten/collectief-winkelverbod-leeuwarden-venray-en-voorthuizen.
[165] Artikel 15 van de Wbp jo. de artikelen 6 en 34 van de Wbp.

persoonlijke gegevens over bewegingen en gedrag worden vastgelegd en voor bedrijfseconomische doeleinden worden verwerkt.[166]

De activiteiten van Bluetrace moeten worden gezien in dit kader. De wijze waarop Bluetrace op dit moment wifi-tracking uitvoert, draagt bij aan het ontstaan van een openbare ruimte waarin het publiek in toenemende mate traceerbaar en volgbaar is, terwijl datzelfde publiek tegelijkertijd onwetend blijft over de aanwezigheid van sensortechnologie waarmee gegevens over hun aanwezigheid en hun gedrag worden vastgelegd. Het CBP is (mede) daarom van oordeel dat de informatieverplichting uit artikel 34 van de Wbp in dit geval van belang is en dat de inspanning die het informeren van betrokkenen vergt van Bluetrace niet snel onevenredig is.

Gelet op de omvang van de gegevensverzameling, de zwaarwegende belangen van betrokkenen om te weten dat er gegevens over hen worden verzameld in de openbare ruimte en voor welk doel, de zwaarwegende belangen van betrokkenen, met name omwonenden, om te weten hoe zij zich daaraan kunnen onttrekken en/of zich daartegen kunnen verzetten en gegeven de mogelijkheden die Bluetrace en zijn klanten ter beschikking staan voor (publieke) informatievoorziening, is het voldoen aan de informatieplicht in deze context niet een disproportionele last voor Bluetrace, zoals bedoeld met de term 'onevenredige inspanning' in het vierde lid van artikel 34 van de Wbp. Het CBP schrijft ook in dit geval niet bindend voor welke vorm van communicatie aan het publiek toegepast moet worden in dit geval. Het is in eerste instantie aan de verantwoordelijke partij(en) zelf om de meest geëigende wijze van informatievoorziening aan het publiek te kiezen en zich ervan te vergewissen dat de informatie de doelgroep bereikt.

Zienswijze Bluetrace
Naar aanleiding van de voorlopige bevindingen van het CBP heeft Bluetrace voorgesteld om onderzoek te doen naar uitingen over wifi-tracking in winkels die kunnen worden ontwikkeld. In de zienswijze op de voorlopige bevindingen stelde Bluetrace voor om in overleg met klanten te bepalen welke uitingen in winkels gedaan moeten worden over wifi-tracking. Bluetrace heeft daarnaast voorgesteld om een privacybeleid te ontwikkelen en informatie over het privacybeleid op zijn website te plaatsen. Bluetrace is daarnaast voornemens om haar klanten op de hoogte te stellen van het privacybeleid en hen aan te sporen dit te delen en te communiceren aan hun eigen klanten. Deze activiteiten kunnen volgens het verstrekte plan van aanpak voltooid zijn op [datum].

In het licht van de informatieplicht van artikel 34 van de Wbp is het ontwikkelen van privacybeleid en informatiemateriaal voor in de winkel een nuttige maatregel. Meer informatievoorziening in en rondom de winkel die de betrokkene daadwerkelijk bereikt en voorziet van eenvoudig te begrijpen informatie over het doel en de omvang van de gegevensverwerking draagt bij aan het voldoet van de informatieplicht van artikel 34 van de Wbp. Het CBP acht het van groot belang dat Bluetrace voorstelt om dit in samenwerking met haar (mede-verantwoordelijke) klanten te doen. Als verantwoordelijke partij is Bluetrace ook verplicht om te informeren over zijn eigen rol

[166] Zie bijvoorbeeld: Emerce, 11 mei 2015, 'Hoe offline cookies fashion retail gaan veranderen', URL: http://www.emerce.nl/interviews/emerce-efashion-hoe-offline-cookies-fashion-retail-gaat-veranderen.

bij wifi-tracking. Een privacybeleid is hiervoor een geschikt instrument en de eigen bedrijfswebsite is hiervoor een geschikt medium. Het CBP kan de kwaliteit van het privacybeleid pas beoordelen als daarvan documenten beschikbaar zijn.

Het voorgestelde onderzoek naar uitingen die in winkels kunnen worden gedaan laat onverlet dat er zeer weinig informatie wordt verstrekt aan betrokkenen die zich bevinden in een gebied waar Bluetrace wifi-tracking uit heeft gerold. Het plan van aanpak bevat geen concrete voorstellen van uitingen, zodat het CBP niet kan beoordelen in hoeverre er daadwerkelijk communicatie-uitingen zullen worden gedaan, in winkels, in welke vorm of omvang dat voorzien is en met welke inhoud. Het CBP wijst er in dit verband op dat informatie in ieder geval voldoende specifiek en begrijpelijk moet zijn met betrekking tot de (soorten) gegevens die met wifi-tracking verwerkt worden, waar en met welke reden dat gebeurt en welke organisatie(s) daarvoor verantwoordelijk zijn.

Geen 'fair processing'

Door het niet naleven van de plicht om betrokkenen in Nederland te informeren over het verzamelen en verwerken van gegevens over wifi-tracking in en buiten winkels handelt Bluetrace in strijd met artikel 34 Wbp. Omdat de informatieplicht van artikel 34 Wbp een uitwerking is van het beginsel van 'fair processing' uit artikel 6 van de Wbp, handelt Bluetrace zowel ten opzichte van de bezoekers van winkels als van voorbijgangers die onderworpen worden aan wifi-tracking daardoor ook in strijd met het bepaalde in artikel 6 van de Wbp.

5.5 Bewaren van gegevens

Artikel 10 van de Wbp schrijft voor dat persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.

Dit betekent dat Bluetrace de database met daarin de gemeten mac-adressen, signaalsterkte, datum en tijdstip en sensorkenmerk niet langer mag bewaren dan redelijkerwijs noodzakelijk is voor het genereren van bedrijfseconomische informatie over bezoekers en passanten van winkels, onder meer door data-analyse uit te voeren voor de klant.

Bluetrace heeft verklaard de verzamelde mac-adressen drie weken te bewaren en deze daarna te hashen. Bluetrace bewaart de mac-adressen daarmee enige tijd in de originele vorm. Hashing leidt in dit geval echter niet tot anonimisering, omdat Bluetrace zelf over de toegepaste hashfunctie beschikt, zoals beoordeeld in paragraaf 5.1 van dit rapport. De toegepaste hashingmethode vermindert de mate waarin gegevens herleidbaar zijn tot de betrokkenen niet, omdat de bewerking door Bluetrace ongedaan gemaakt kan worden. Er is daarmee ook na drie weken nog sprake van een verschijningsvorm die het *mogelijk* maakt om betrokkenen te identificeren.[167]

Uit de Nederlandse wetsgeschiedenis en de wetsuitleg van de Europese gegevensbeschermingsautoriteiten blijkt dat van Bluetrace in dit geval gevraagd mag worden om strikte – en dus zeer beperkte – bewaartermijnen in acht te nemen, tenzij

[167] Zie paragraaf 5.1 van dit rapport over hashing door Bluetrace.

het aannemelijk is dat het voor het verwezenlijken van gerechtvaardigde verwerkingsdoelen noodzakelijk is om de persoonsgegevens onbeperkt te bewaren.

Volgens het advies van de Artikel 29-werkgroep over geolocatiefuncties op slimme mobiele apparaten vormen locatiegegevens van mobiele apparatuur namelijk een bijzonder privacyrisico voor de betrokkenen. De Europese toezichthouders stellen in hun opinie dat voor het bewaren van mac-adressen uit wifi-tracking een maximale bewaartermijn van 24 uur passend is, wanneer deze opslag nodig is voor het functioneren van de trackingdienst.[168] Het opslaan van mac-adressen voor gerechtvaardigde bedrijfseconomische doelen zou volgens de werkgroep nog verder beperkt moeten zijn. Dit geldt met name wanneer het gaat om het registreren van de apparaten van personen over *meerdere* locaties en tijdstippen, zoals dat bijvoorbeeld het geval is wanneer Bluetrace meet in hoeverre er sprake is van een *unieke* bezoeker of voorbijganger van een winkel en in de situatie waarin er routering wordt gemeten.[169]

Het CBP heeft geconstateerd dat Bluetrace alle met wifi-tracking gegenereerde data sinds het begin van de metingen heeft bewaard. Bluetrace heeft niet gesteld, of op een andere wijze aannemelijk gemaakt, dat het voor het verwezenlijken van de aangegeven verwerkingsdoelen noodzakelijk is om gegevens zonder beperking te bewaren. Gelet op het voorgaande had Bluetrace bewaartermijnen moeten vaststellen en had Bluetrace aan het einde van de gestelde bewaartermijnen zijn meetgegevens uit wifi-tracking volledig moeten anonimiseren (bewaren in een vorm die identificatie onmogelijk maakt) of daadwerkelijk moeten verwijderen.[170]

Bluetrace kan geen beroep doen op de uitzondering op de regels voor bewaartermijnen voor statistische, historische of wetenschappelijke doeleinden in het tweede lid van artikel 10 van de Wbp, nu het bedrijf heeft aangegeven – en het CBP heeft vastgesteld– dat de onderzochte verwerkingen worden verricht voor bedrijfseconomische doeleinden. Uit de jurisprudentie blijkt overigens dat er geen *noodzaak* is om oorspronkelijke gegevens te bewaren als de verwerking een louter statistisch doeleinde zou dienen.[171]

---

[168] Artikel 29-werkgroep, WP 185, Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten, 13 mei 2011, p. 18-19. De werkgroep van Europese toezichthouders past hierin artikel 6 lid 1(e) van Richtlijn 95/46/EG, over het bewaren van persoonsgegevens, toe op wifi-tracking. Artikel 10 Wbp is de implementatie van de bewaartermijn uit Richtlijn 95/46/EG in Nederlands recht.

[169] Volgens de Artikel 29-werkgroep zou dan bij de vastlegging van de locatie waarop een bepaald mac-adres wordt waargenomen de vorige waargenomen locatie direct gewist moeten worden. Artikel 29-werkgroep, WP 185, Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten, 13 mei 2011, p. 19.

[170] Zie bijvoorbeeld: CBP, 24 mei 2012, z2011-00057, persbericht CBP 13 juni 2012 inzake last onder dwangsom Nederlandse Spoorwegen, URL: https://cbpweb.nl/nl/nieuws/cbp-vordert-dwangsom-ns-wegens-bewaren-reisgegevens-studenten; CBP 15 juni 2012, z2011-00987, persbericht CBP 16 augustus 2012 inzake last onder dwangsom RET, URL: https://cbpweb.nl/nl/nieuws/cbp-vordert-dwangsom-ret-wegens-bewaren-reisgegevens-studenten.

[171] HvJ EU 16 december 2008, zaak C-524/06 (*Huber*), r.o. 64-65 en 68: "*Evenzo gaat verordening nr. 862/2007, die de verstrekking regelt van statistische gegevens over de migratiebewegingen op het grondgebied van de lidstaten, ervan uit dat de lidstaten de informatie verzamelen op basis waarvan die statistieken kunnen worden opgesteld. De uitoefening van die bevoegdheid maakt echter niet het verzamelen en bewaren van gegevens op naam zoals plaatsvindt in het kader van een register als het AZR, noodzakelijk in de zin van artikel 7, sub e, van richtlijn 95/46. Zoals de advocaat-generaal in punt 23 van zijn conclusie heeft aangegeven, is voor een dergelijk doel alleen de verwerking van anonieme gegevens noodzakelijk. (…) In geen geval kunnen als noodzakelijk in de zin van artikel 7, sub e, van richtlijn 95/46 worden beschouwd de bewaring en de*

In zijn zienswijze op het rapport voorlopige bevindingen van het CBP heeft Bluetrace voorgesteld om in overleg te gaan met klanten over het bepalen van geschikte bewaartermijnen. Bluetrace geeft ook aan dat dit aanleiding zal zijn voor het maken van contractuele afspraken over het bewaren en de eigendom van gegevens. Bluetrace heeft daarbij aangegeven dat dit per [datum] gerealiseerd zou kunnen worden. Het CBP heeft echter in het onderzoek vastgesteld dat Bluetrace (nog) geen bewaartermijn heeft ingesteld voor de gegevens terwijl die reeds via wifi-tracking verzameld worden. Daarnaast is met deze maatregel niet gemotiveerd wat dan de noodzaak is van de in te voeren bewaartermijnen en voor welke gegevens die geldt. Dit is de kern van artikel 10 van de Wbp (noodzaak bewaartermijnen). De voorgestelde maatregel is niet concreet genoeg om op kortere termijn te waarborgen dat de gegevensverwerking voldoet aan artikel 10 van de Wbp. Het CBP overweegt hierbij in het bijzonder de belangen van betrokkenen en de gevoelige aard van de locatiegegevens van mobiele apparatuur.

Omdat Bluetrace zijn meetgegevens, zij het met gehashte mac-adressen, in de praktijk onbeperkt bewaart en omdat het bedrijf niet heeft vastgesteld en vastgelegd hoe lang het voor het verrichten van de normale werkzaamheden op het gebied van wifi-tracking noodzakelijk is om te kunnen beschikken over (historische) meetgegevens, handelt Bluetrace in strijd met artikel 10 van de Wbp.

verwerking van persoonsgegevens op naam in het kader van een register als het AZR, voor statistiekdoeleinden." Vgl. AG HvJ EU 3 april 2008, zaak C-524/06 (Huber), r.o. 23: *"Statistieken zijn per definitie anoniem en niet persoonsgebonden."*

6. CONCLUSIES

Het College bescherming persoonsgegevens (CBP) heeft op grond van artikel 60 van de Wet bescherming persoonsgegevens (Wbp) ambtshalve onderzoek ingesteld naar de verwerking van persoonsgegevens door het bedrijf Bluetrace B.V., statutair gevestigd te Amsterdam (hierna: Bluetrace) door het gebruik van wifi-trackingtechnologie in winkels en rondom winkels op de openbare weg.

Bluetrace biedt winkeliers wifi-sensortechnologie aan waarmee het mogelijk is om mobiele apparaten te registreren. De technologie van Bluetrace maakt gebruik van het feit dat smartphones automatisch hun unieke wifi-mac-adres uitzenden. Door deze signalen op te vangen kunnen apparaten worden geteld en kan hun verplaatsingsgedrag in kaart worden gebracht. Omdat de locatie van een smartphone gedurende het grootste deel van de dag, en zelfs in de nacht, overeen komt met de locatie van de eigenaar ervan en omdat het apparaat in de praktijk bijna altijd aan staat, wordt met wifi-tracking *de facto* de gebruiker van het apparaat geregistreerd en gevolgd. Het gaat daarbij niet alleen om mensen die een winkel bezoeken, maar ook om mensen buiten winkels, zoals voorbijgangers op de openbare weg.

Bluetrace verzamelt met wifi-tracking gegevens over de aantallen mensen die de winkels bezoeken en/of passeren en over hoe lang mensen op bepaalde plaatsen verblijven. De metingen van Bluetrace raken een groot aantal Nederlanders. Sensoren van Bluetrace bevinden zich in winkels in tientallen grote en middelgrote steden in Nederland. Bluetrace plaatst steeds één sensor per winkel, maar de sensoren hebben bereik tot op de openbare weg buiten de winkel. Hierdoor verzamelt Bluetrace informatie over zowel winkelbezoekers als voorbijgangers. Bluetrace informeert betrokkenen niet over het feit dat zij op deze manier via hun mobiele apparatuur ongemerkt worden geregistreerd en geteld. Bluetrace verwerkt de gegevens met als doel om (locatiegebaseerde) data-analysediensten te verlenen aan zijn klanten en om relevante managementinformatie te genereren voor zijn klanten.

Persoonsgegevens
Met wifi-tracking registreert Bluetrace unieke mac-adressen van mobiele apparatuur in combinatie met gegevens over de locatie, de datum en het tijdstip van registratie. Daarmee verzamelt en verwerkt Bluetrace persoonsgegevens als bedoeld in artikel 1, onder a, van de Wbp. Bij wifi-tracking worden gegevens verwerkt die naar hun aard gevoelig zijn, namelijk locatiegegevens van personen. Daarmee kan een beeld van het winkelgedrag van betrokkenen worden opgebouwd. De door Bluetrace toegepaste *hashing* van de mac-adressen na een periode van drie weken leidt niet tot de conclusie dat geen sprake meer is van de verwerking van persoonsgegevens.

Verantwoordelijkheid
Bluetrace werkt intensief samen met opdrachtgevers het implementeren van wifi-tracking. Binnen de samenwerking met afnemers bepaalt Bluetrace wezenlijke aspecten van de gegevensverwerkingen in het kader van wifi-tracking. Bluetrace bepaalt, onder meer, welke soort gegevens verwerkt worden, hoe lang en met welke middelen. Bluetrace heeft bovendien het feitelijk beheer over alle opgeslagen data uit de trackingactiviteiten en de zeggenschap over eventueel te hanteren bewaartermijnen en over het verstrekken van gegevens aan derden. Bluetrace kan daarom niet als

bewerker worden aangemerkt maar is een verantwoordelijke in de zin van de Wbp. Niettemin is er sprake van verwevenheid tussen de activiteiten van Bluetrace en die van zijn klanten. In deze casus is sprake van gezamenlijke verantwoordelijkheid, omdat de verschillende gegevensverwerkingen geïntegreerd zijn. Dit betekent dat zowel Bluetrace als zijn klanten verantwoordelijk zijn voor het geheel van de gegevensverwerkingen in het kader van wifi-tracking. Bluetrace kan als medeverantwoordelijke worden aangesproken voor zowel handelingen die feitelijk in zijn macht liggen als voor aspecten van gegevensverwerking die in meer of mindere mate samenhangen met wat klanten bepalen binnen het samenwerkingsverband. Het gaat daarbij om informatievoorziening aan het publiek, het vaststellen van de plaatsen waar gemeten moet worden, de duur van metingen en doelen voor de uiteindelijke toepassing van de bedrijfseconomische informatie (die via wifi-tracking is verkregen) in de organisatie van de klant.

Grondslag
Bluetrace sluit geen overeenkomsten met betrokkenen en vraagt hen ook geen toestemming. Bluetrace kan geen beroep doen op de grondslagen uit artikel 8, onder c, d, en e, van de Wbp (een wettelijk voorschrift, een vitaal belang of de uitoefening van een publieke taak). Bluetrace heeft verklaard dat het bedrijf gegevens over winkelbezoekers en winkelpassanten verwerkt op basis van de grondslag van artikel 8, aanhef en onder f, van de Wbp (noodzakelijk voor de behartiging van een gerechtvaardigd belang).

<u>Rechtmatigheid van wifi-tracking in de winkels</u>
Bij het verwerken van gegevens van bezoekers in en rondom een winkel geldt dat het belang van winkeliers bij het verkrijgen van informatie over drukte en bezoekersgedrag in winkels op zichzelf een gerechtvaardigd belang kan dienen, mits Bluetrace betrokkenen adequaat informeert en de verwerking van persoonsgegevens noodzakelijk is voor het verwezenlijken van de gestelde doelen.

De huidige, door het CBP onderzochte, werkwijze van Bluetrace voldoet echter niet aan de vereisten van proportionaliteit en subsidiariteit. Het bedrijf kan de gestelde doelen bereiken op een wijze waarbij het op een beperktere schaal meet en waarbij het minder gegevens verwerkt, gedurende een kortere periode. Er zijn, gelet op de belangen van betrokkenen en de gevoelige aard van de locatiegegevens, minder ingrijpende wijzen zijn waarop Bluetrace wifi-tracking in de praktijk kan brengen voor de gestelde doelen. Wifi-tracking in winkels wordt bijvoorbeeld minder ingrijpend wanneer de persoonsgegevens die daarbij verwerkt worden zo snel mogelijk, dan wel binnen maximaal 24 uur, anoniem worden gemaakt.

Door het verwerken van persoonsgegevens met het doel bedrijfseconomische informatie te genereren door wifi-tracking *in* winkels zonder geldige grondslag, handelt Bluetrace in strijd met artikel 8 van de Wbp.

<u>Rechtmatigheid van wifi-tracking buiten de winkels</u>
Het genereren van bedrijfseconomische informatie door wifi-tracking buiten de winkels op een wijze die naar zijn aard verborgen blijft voor de betrokkenen kan niet gelden als een belang wat zich leent voor een beroep op artikel 8, aanhef en onder f, van de Wbp. Is deze verwerking kenbaar voor betrokkenen dan is een beroep op deze grondslag mogelijk als de verwerking noodzakelijk is en opweegt tegen de

individuele belangen van betrokkenen, met name de bescherming van de persoonlijke levenssfeer.
Bluetrace heeft geen blijk gegeven van een keuze voor een werkwijze die wifi-tracking buiten de winkels verborgen houdt. Het CBP stelt wel vast dat er een sterk gebrek aan transparantie is. De huidige werkwijze van Bluetrace voldoet niet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Er wordt 24 uur per dag en zeven dagen per week gemeten en Bluetrace bewaart de gegevens onbeperkt. Bluetrace heeft de noodzaak om mensen buiten de winkel (zoals passanten en omwonenden) te tracken onvoldoende onderbouwd in het licht van hun recht op bescherming van de persoonlijke levenssfeer. Bluetrace kan ervoor kiezen om het bereik van de metingen te beperken tot de winkel zelf, zodat aanwezigheid van voorbijgangers op de openbare weg of van bewoners van aangrenzende panden niet, of althans zo min mogelijk, geregistreerd wordt. Indien Bluetrace de noodzaak van deze gegevensverwerking al zou kunnen onderbouwen – en voor zover het bedrijf zou voldoen aan de vereisten van proportionaliteit en subsidiariteit – zou Bluetrace de persoonsgegevens onmiddellijk, dan wel in ieder geval zo snel mogelijk na de eerste vastlegging, onomkeerbaar moeten anonimiseren.
Ten slotte weegt het belang van Bluetrace niet op tegen het recht op bescherming van de persoonlijke levenssfeer van betrokkenen door het ontbreken van een effectieve en realistische manier om zich te kunnen onttrekken aan wifi-tracking.

Door het verwerken van persoonsgegevens met het doel het genereren van bedrijfseconomische informatie door wifi-tracking *buiten* winkels zonder geldige grondslag handelt Bluetrace in strijd met artikel 8 van de Wbp.

Informatie
Het CBP stelt vast dat Bluetrace geen informatie aan het publiek verstrekt over de verwerking van persoonsgegevens door wifi-tracking in en buiten winkels. Hoewel Bluetrace mede in opdracht van klanten aan wifi-tracking doet en dit feitelijk plaatsvindt op de locaties van zijn klanten, moet Bluetrace, als medeverantwoordelijke voor de gegevensverwerking, zelf ook informatie hierover (laten) verstrekken. Omdat Bluetrace niet informeert over de gegevens die het bedrijf verwerkt met wifi-tracking, handelt Bluetrace in strijd met artikel 34 van de Wbp. Omdat het voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens vereist is om de informatievoorschriften uit de Wbp in acht te nemen, handelt Bluetrace ook in strijd met artikel 6 van de Wbp.

Bewaartermijn
Bluetrace heeft geen beleid voor bewaartermijnen vastgesteld en bewaart in de praktijk alle gegevens voor onbepaalde tijd in een vorm die het mogelijk maakt om betrokkenen te identificeren. Uit het onderzoek is niet gebleken dat het voor het bereiken van de doelen waarvoor gegevens worden verwerkt noodzakelijk is om gegevens onbeperkt te bewaren. Bluetrace handelt hierdoor in strijd met artikel 10 van de Wbp.

Nadat Bluetrace het rapport voorlopige bevindingen van het CBP heeft ontvangen heeft het bedrijf een zienswijze gegeven. De zienswijze bevat een plan van aanpak met daarin voorstellen voor toekomstige maatregelen en nader onderzoek naar de werkwijze van Bluetrace met betrekking tot wifi-tracking. De zienswijze van Bluetrace heeft niet geleid tot aanpassing van de conclusies van het onderzoek reeds omdat de voorgestelde aanpak, naar het oordeel van het CBP, te weinig concreet zicht biedt op de beëindiging van de geconstateerde overtredingen.

BIJLAGE: ZIENSWIJZE BLUETRACE OP DE VOORLOPIGE BEVINDINGEN VAN HET CBP

In een brief van 26 augustus 2015 (door het CBP ontvangen op 2 september 2015, hierna te noemen "zienswijze") heeft Bluetrace zijn zienswijze op het rapport voorlopige bevindingen (d.d. 21 juli 2015) van het CBP kenbaar gemaakt.

Bluetrace heeft verklaard dat de voorlopige bevindingen van het CBP in goede orde zijn ontvangen en gelezen. Bluetrace heeft aangegeven dat het de bevindingen en conclusies van het rapport niet in twijfel trekt. Bluetrace heeft geen correctieverzoeken, of aanvullingen aangedragen.

Dit betekent dat de zienswijze van Bluetrace niet zal leiden tot aanpassingen van de conclusies in het rapport met voorlopige bevindingen van het CBP dat is opgesteld naar aanleiding van het ambtshalve onderzoek.

Bluetrace geeft in de zienswijze aan dat het bereid is om de maatregelen te nemen die noodzakelijk zijn om de geconstateerde overtredingen te beëindigen. Bluetrace heeft na ontvangst van het rapport voorlopige bevindingen gewerkt aan een plan van aanpak om haar werkwijze aan te passen, zodat het bedrijf in de toekomst kan voldoen aan de Wbp. In het plan van aanpak worden acht maatregelen voorgesteld om de overtredingen te beeïndigen. Bluetrace heeft de maatregelen toegelicht en voorzien van een indicatie van de benodigde tijd om de acties door te voeren, zodat het CBP een indruk heeft van de termijn waarop de door het CBP gesignaleerde problemen te verhelpen zijn.

De inhoud van het plan van aanpak wordt hieronder per maatregel behandeld door het CBP. Het plan van aanpak in de zienswijze heeft geleid tot enkele aanvullingen van de feitelijke bevindingen in het rapport voorlopige bevindingen. De voorgestelde maatregelen worden vervolgens beoordeeld. Geen van de maatregelen is op dit moment voltooid of van start gegaan. Het CBP geeft in deze bijlage per maatregel aan in hoeverre dit mogelijk leidt tot of bijdraagt aan de beëindiging van de overtredingen van de Wet berscherming persoonsgegevens, zoals die zijn geconstateerd in het rapport voorlopige bevindingen. De zienswijze heeft derhalve geleid tot aanvullingen van de feitelijke bevindingen en de beoordeling. De zienswijze heeft niet geleid tot aanpassing van de conclusies van het CBP in dit onderzoek.

Overzicht voorgenomen maatregelen door Bluetrace

1. Onderzoek naar de mogelijkheden om mac-adressen te maskeren.
2. Het ontwikkelen van een privacybeleid
3. Onderzoek naar de consequenties van het anonimiseren van mac-adressen
4. Onderzoek naar gevolgen van beperking wifi-tracking tot binnen de winkel
5. Onderzoek naar gevolgen van het beperken van wifi-tracking tot gezette tijden
6. Onderzoek naar mogelijke aanpassingen in contracten met klanten
7. Onderzoek naar het ontwikkelen van uitingen in de winkels
8. Onderzoek naar opt-out mogelijkheden

B.1. Onderzoek naar het maskeren van mac adressen

Maatregel Bluetrace:
Bluetrace stelt voor om onderzoek te doen naar mogelijkheden om het mac-adres te maskeren dan wel om dat om te zetten naar een uniek identificatie(kenmerk). Op deze wijze zou dan het mac-adres als middel om personen te identificeren weggenomen kunnen worden. Bluetrace stelt voor het proces van pseudonimisering onder te brengen bij een derde partij (outsourcing) zodat Bluetrace zelf (en zijn klanten) nog slechts gebruik te maakt van deze afgeleide gegevens. Het onderzoek zal voltooid zijn op [datum].

Reactie CBP:
Het CBP acht de voorgestelde maatregel te onbepaald om te kunnen inschatten voor welke van de geconstateerde overtredingen dit een concrete uitkomst biedt. Met het voltooien van dit onderzoek is er in elk geval nog geen concrete maatregel getroffen die in de praktijk leidt tot een aanpassing van de werkwijze van Bluetrace.

Het CBP zal in het rapport als bevinding opnemen dat Bluetrace voorstelt om onderzoek te doen naar pseudonimiseringsmaatregelen. In de beoordeling zal het CBP ingaan op de voorgestelde pseudonimisering. Het CBP wijst in dit verband op de opinie van de Artikel 29-werkgroep over anonimiseringstechnieken. Pseudonimisering is geen vorm van anonimisering. Pseudonimisering vermindert de relateerbaarheid van gegevens aan de identiteit van betrokkenen, en/of vereist daarvoor een extra tussenstap. Daardoor kan het een nuttige beveiligingsmaatregel zijn, omdat in geval van verlies of diefstal minder snel een verband met de individuele betrokkene kan worden gelegd door een derde die zich toegang verschaft tot de gepseudonimiseerde data. Het toepassen van pseudonimisering door de verantwoordelijke leidt echter niet tot de conclusie dat er geen sprake meer is van persoonsgegevens. Voor de verantwoordelijke zelf is immers te achterhalen hoe de pseudonieme gegevens zich verhouden tot c.q. zijn afgeleid uit de oorspronkelijke gegevens. Voor zover Bluetrace gegevens zou willen pseudonimiseren (in plaats van verwijderen of onomkeer anonimiseren) dient Bluetrace er ook dan rekening mee te houden dat er nog sprake kan zijn van gegevens die een persoon (in)direct kunnen identificeren. Daarom is er ook ten aanzien van pseudonieme gegevens informatievoorziening aan de betrokkene, een beleid inzake bewaartermijnen, en een grondslag voor de verwerking van gepseudonimiseerde gegevens noodzakelijk.

De zienswijze heeft op dit punt niet geleid tot aanpassingen van conclusies van het CBP in dit onderzoek.

B.2. Ontwikkelen Privacybeleid

Maatregel Bluetrace:
Bluetrace stelt voor om een privacybeleid op te stellen en informatie over het privacybeleid op zijn website te plaatsen. Bluetrace is daarnaast voornemens om haar klanten op de hoogte te stellen van het privacybeleid en hen aan te sporen dit te delen en te communiceren aan hun eigen klanten. Deze maatregel kan volgens het plan van aanpak voltooid zijn op [datum].

Reactie CBP:
Het CBP heeft in het rapport voorlopige bevindingen geconstateerd dat Bluetrace niet of nauwelijks zorgt voor informatieverstrekking aan het publiek over wifi-tracking. Het ontwikkelen van een privacybeleid door Bluetrace, waarin wordt ingegaan op de verwerking van persoonsgegevens bij wifi-tracking, is een noodzakelijke stap in de richting van het beeindigen van de overtredingen van de Wbp. Een privacybeleid kan bijdragen aan informatievoorziening aan de betrokkene, zoals bedoeld in artikel 34 van de Wbp, mits dit de betrokkene redelijkerwijs en tijdig bereikt.

De zienswijze heeft op dit punt geleid tot een aanvulling van de feitelijke bevindingen. Het CBP zal in het rapport opnemen dat Bluetrace naar aanleiding van het onderzoek heeft voorgesteld om een privacybeleid te ontwikkelen. Ook zal het CBP vermelden dat Bluetrace van plan is om zijn (mede-verantwoordelijke) klanten te vragen om het privacybeleid te delen.

Deze voorgestelde maatregel leidt tot een aanvulling in de beoordeling in het rapport definitieve bevindingen. De conclusies van het CBP blijven echter ongewijzigd, omdat er [op het moment van schrijven] feitelijk nog geen informatieverstrekking aan de betrokkene die in en rond winkels wordt onderworpen aan wifi-tracking (voorzien) is, zoals bedoeld in artikel 34 van de Wbp. Artikel 34 schrijft voor dat de verantwoordelijke de betrokkene voor aanvang van de gegevensverwerking moet informeren over zijn identiteit en over het doel en de omvang van de gegevensverwerking waar de betrokkene mee te maken krijgt als gevolg van wifi-tracking in en rondom winkels.
Informatieverstrekking door Bluetrace – of door of vanwege de klanten van Bluetrace – aan de betrokkene is een randvoorwaarde voor het gebruik van wifi-tracking in de praktijk binnen de kaders van de Wbp. Dat wil zeggen dat Bluetrace een dienst levert die niet toegestaan is zonder adequate informatievoorziening, in lijn met artikel 34. Met de voltooiing van de voorgenomen maatregel is er op korte termijn geen zicht op concrete verbeteringen die deze randvoorwaarde waarborgen, terwijl wifi-tracking op dit moment wel actief toegepast wordt in en rondom Nederlandse winkels door Bluetrace. Het CBP betwijfelt, onder meer, of de informatie uit het privacybeleid de betrokkene tijdig bereikt. Aangezien de betrokkene niet rechtstreeks een product afneemt van de website van Bluetrace, zal deze naar verwachting niet tijdig geïnformeerd worden wanneer Bluetrace een privacybeleid op haar website vertoond. Daarmee is er, gelet op artikel 6 van de Wbp, nog steeds sprake van een onrechtmatige gegevensverwerking.

In het op te stellen privacybeleid moet de verantwoordelijke voldoende begrijpelijke informatie verstrekken voor de betrokkenen, in casu winkelbezoekers, omwonenden en voorbijgangers op de openbare weg, over de doeleinden van de verwerking(en) en de verschillende aspecten van de gegevensverwerking die voor hen van belang zijn. Betrokkenen moeten uit de informatie zonder moeite kunnen opmaken wat er wel en niet met hun gegevens gebeurt. Bluetrace dient betrokkenen tevens nader te informeren over de (soorten) persoonsgegevens, die zij via de smartphone verzamelt en verwerkt en dit relateren aan verschillende verwerkingsdoeleinden.
De plicht tot nadere informatieverstrekking volgt uit artikel 34, derde lid, van de Wbp, gelet op de aard van de gegevens die Bluetrace verwerkt, de omstandigheden waaronder zij worden verkregen en tenslotte het gebruik dat er van wordt gemaakt.

Ten aanzien van de aard van de gegevens onderstreept het CBP dat Bluetrace persoonsgegevens verwerkt van gevoelige aard, namelijk de locatie van de betrokkenen. Omdat Bluetrace de plaats waar wifi-tracking actief is onvoldoende afbakent of toelicht, kan een gemiddelde consument in een winkel(straat) de aard en omvang van de gegevensverwerking niet bepalen.

Ten aanzien van de omstandigheden waaronder de gegevens worden verkregen, is van belang dat Bluetrace de persoonsgegevens op indirecte wijze verkrijgt van betrokkenen (de meetgegevens uit de smartphones). Bovendien worden bij wifi-tracking buiten winkels gegevens verzameld van personen die zich op de openbare weg of in een aangrenzend pand bevinden. Tot slot vinden bepaalde (verdere) verwerkingen uitsluitend plaats in de systemen van Bluetrace, en onttrekken zich daarmee in hun geheel aan het zicht van de betrokkenen.

B.3. Onderzoek naar de consequenties van het anonimiseren van mac-adressen

Maatregel Bluetrace:
Bluetrace kondigt aan dat het bedrijf gaat onderzoeken wat de consequenties zijn van het anonimiseren van mac-adressen binnen een bepaalde tijd na de eerste vastlegging (bijvoorbeeld 24 uur). Dit onderzoek kan, conform het plan van aanpak, worden voltooid op [datum].

Reactie CBP:
Het volledig en onomkeerbaar anonimiseren van mac-adressen zou ertoe kunnen leiden dat er geen sprake meer is van de verwerking van persoonsgegevens, omdat de gegevens dan niet meer herleidbaar zijn tot een identificeerbare persoon. Ten aanzien van anonimisering wijst het CBP op het advies over anonimiseringstechnieken en het advies over geolocatiefuncties op mobiele apparaten van de Artikel 29-werkgroep. In deze adviezen is aangegeven dat het binnen 24 uur anonimiseren van mac-adressen een maatregel is die een belangrijke waarborg biedt voor de belangen van de betrokkene op bescherming van de persoonlijke levenssfeer.

Het CBP spreekt geen oordeel uit over het feit dat Bluetrace aangeeft dat er enige tijd gemoeid is met het ontwikkelen van een aangepaste werkwijze op dit punt, aangezien de methode van wifi-tracking grotendeels is gebaseerd op het verzamelen van mac-adressen. Het CBP acht de voorgestelde maatregel echter te onbepaald om te kunnen inschatten of het voorgestelde onderzoek van Bluetrace binnen een redelijke termijn zal leiden tot een (technische) wijziging van de huidige werkwijze. Met het louter voltooien van dit onderzoek is er in elk geval nog geen concrete maatregel getroffen die aanleiding is voor een andere beoordeling van de vraag of er sprake is van de verwerking van persoonsgegevens.

De zienswijze heeft op dit punt geleid tot een aanvulling van de feitelijke bevindingen. Het CBP zal in het rapport opnemen dat Bluetrace naar aanleiding van het onderzoek van het CBP heeft voorgesteld om onderzoek te doen naar de consequenties van het anonimiseren van mac-adressen binnen een bepaalde tijd.
Deze voorgestelde maatregel leidt echter niet tot een aanpassing van de onderzoeksconclusies, omdat er [op het moment van schrijven] feitelijk nog geen

verandering komt in de wijze waarop Bluetrace gegevens verwerkt in het kader van wifi-tracking. Er is dus onverminderd sprake van de verwerking van persoonsgegevens en toepasselijkheid van de Wbp op deze verwerking.

B.4. Onderzoek naar gevolgen van het beperken van wifi-tracking tot binnen de winkel

Zienswijze Bluetrace:
Bluetrace stelt voor om onderzoek te doen naar de consequenties (voor de eigen bedrijfsvoering, lopende contractuele verplichtingen en het zakelijke bedrijfsmodel van Bluetrace) van het beperken van wifi-tracking tot binnen de winkels. Dit onderzoek kan, conform het plan van aanpak, voltooid zijn binnen [periode].

Reactie CBP:
In het rapport voorlopige bevindingen stelt het CBP vast dat het beperken van de reikwijdte van wifi-tracking in tijd en ruimte essentiele maatregelen zijn die ervoor kunnen zorgen dat recht wordt gedaan aan de beginselen van proportionaliteit en subsidiariteit. Dat wil zeggen, dat met het beperken van het gebied waarbinnen aan wifi-tracking wordt gedaan voorkomen wordt dat er meer gegevens worden verzameld dan strikt noodzakelijk is voor het doel van de verwerking. Aangezien het CBP – onder andere – heeft vastgesteld dat Bluetrace geen grondslag heeft voor wifi-tracking buiten winkels, en dat voor een geslaagd beroep op artikel 8 onder f van de Wbp voor wifi-tracking buiten winkels bijzonder zware eisen gelden, zou het beperken van tracking tot binnen winkels ervoor kunnen zorgen dat een van de overtredingen van artikel 8 van de Wbp wordt beëindigd.

Echter, het enkel voltooien van een onderzoek naar de gevolgen van het afbakenen van wifi-tracking tot alleen binnen de winkel voor Bluetrace als bedrijf is, zonder dat daaraan concrete acties zijn gekoppeld die in de praktijk leiden tot een aanpassing van de werkwijze van Bluetrace, niet voldoende om de geconstateerde overtredingen te beeindigen.

De zienswijze heeft op dit punt geleid tot een aanvulling van het rapport voorlopige bevindingen. Het CBP zal in het rapport opnemen dat Bluetrace voornemens is om naar aanleiding van het onderzoek van het CBP in kaart te brengen wat de gevolgen van het beperken van wifi-tracking tot binnen de winkel zijn voor het bedrijf. De zienswijze heeft niet geleid tot aanpassing van de beoordeling van de werkwijze van Bluetrace en de conclusies in het rapport.

B.5. Onderzoek naar gevolgen van het beperken van metingen tot winkelopeningstijden

Maatregel Bluetrace:
Bluetrace stelt voor om onderzoek te doen naar de consequenties (voor de eigen bedrijfsvoering, lopende contractuele verplichtingen en het zakelijke bedrijfsmodel van Bluetrace) van het beperken van wifi-tracking in tijd, bijvoorbeeld tot binnen de winkelopeningstijden. Dit onderzoek kan, conform het plan van aanpak, voltooid zijn binnen [periode]. Bluetrace geeft in het plan van aanpak geen concrete inschatting van de maatregelen die eventueel kunnen worden ontwikkeld naar aanleiding van dit onderzoek en de opleverdatum van het onderzoek.

Reactie CBP:
In het rapport voorlopige bevindingen stelt het CBP vast dat het beperken van de reikwijdte van wifi-tracking in tijd en ruimte essentiele maatregelen zijn die ervoor kunnen zorgen dat recht wordt gedaan aan de beginselen van proportionaliteit en subsidiariteit. Dat wil zeggen, dat met het beperken van wifi-tracking tot bijvoorbeeld winkel-openingstijden voorkomen wordt dat er meer gegevens worden verzameld dan strikt noodzakelijk is voor het doel van de verwerking. Daarmee kan ook de impact van wifi-tracking op de persoonlijke levenssfeer van anderen sterk verminderd worden. Aangezien het CBP – onder andere – heeft vastgesteld dat Bluetrace geen grondslag heeft voor wifi-tracking in en buiten winkels, omdat niet is voldaan aan het noodzakelijkheidsvereiste, zou het beperken van tracking tot gezette tijden ervoor kunnen zorgen dat er een stap wordt gezet richting de beëindiging van de overtredingen van artikel 8 van de Wbp. Immers, het beperken van de tijden waarop wordt gemeten kan worden gezien als een extra waarborg voor bepaalde groepen personen die bijzonder vaak langs de winkel lopen, bijvoorbeeld omdat zijn een omwonende zijn. De beperking van de meettijden zou bovendien leiden tot het verminderen van de hoeveelheid gegevens die wordt verwerkt, waarmee meer recht gedaan wordt aan het beginsel van subsidiariteit.

Echter, het enkel voltooien van een onderzoek naar de gevolgen die het afbakenen van wifi-tracking tot beperkte tijden zou hebben voor Bluetrace als bedrijf en diens verplichtingen jegens anderen is, zonder dat daaraan concrete acties zijn gekoppeld die in de praktijk leiden tot een aanpassing van de werkwijze van Bluetrace, niet voldoende om de geconstateerde overtredingen te beeindigen. Bovendien is in het rapport van voorlopige bevindingen aangegeven dat er meer waarborgen voor de belangen van de betrokkene vereist zijn voor een geslaagd beroep op artikel 8 sub f van de Wbp.

De zienswijze heeft op dit punt geleid tot een aanvulling van het rapport voorlopige bevindingen. Het CBP zal in het rapport opnemen dat Bluetrace voornemens is om naar aanleiding van het rapport voorlopige bevindingen van het CBP onderzoek te doen naar de gevolgen van het beperken van wifi-tracking tot gezette tijden, bijvoorbeeld de winkelopeningstijden. De zienswijze heeft niet geleid tot aanpassing van de beoordeling van de werkwijze van Bluetrace en de conclusies in het rapport.

B.6. Aanpassen van contracten met klanten

Maatregel Bluetrace:
Bluetrace stelt voor om in overleg met zijn klanten nadere (contractuele) afspraken te maken over bewaartermijnen en eigendom van gegevens. Bluetrace geeft tevens aan dat deze afspraken zullen leiden tot technische aanpassingen. Deze maatregel zou voltooid kunnen zijn op [datum].

Reactie CBP:
De zienswijze heeft op dit punt geleid tot een aanvulling van het rapport voorlopige bevindingen. Het CBP zal in het rapport opnemen dat Bluetrace voornemens is om naar aanleiding van het onderzoek van het CBP bewaartermijnen vast te stellen en overeen te komen met klanten. De zienswijze heeft niet geleid tot aanpassing van de conclusies in het rapport.

Het CBP heeft in het onderzoek vastgesteld dat Bluetrace (nog) geen bewaartermijn heeft ingesteld voor de gegevens die zij via wifi-tracking verzamelt. Daarnaast is met deze maatregel niet gemotiveerd wat dan de noodzaak is van de in te voeren bewaartermijnen en voor welke gegevens die geldt. Dit is de kern van de overtreding van artikel 10 van de Wbp (noodzaak bewaartermijnen). De voorgestelde maatregel is niet concreet genoeg om op kortere termijn een concreet uitzicht te bieden op het beëindigen van de geconstateerde overtreding.

Bluetrace beschikt over alle gegevens sinds de lancering van de wifi-tracking dienstverlening. Het CBP heeft in het rapport opgenomen dat Bluetrace aan een plan werkt om bewaartermijnen te gaan bepalen van de gegevens die zij verkrijgt via wifi-tracking. Maar zolang dat beleid niet concreet is bepaald en doorgevoerd, voldoet de gegevensverwerking niet aan artikel 10 van de Wbp. Dit gelet op de belangen van betrokkenen, en op de gevoelige aard van de locatiegegevens van mobiele apparatuur.

Het is aan Bluetrace zelf om de periode te bepalen die noodzakelijk is om zijn diensten te leveren. Bluetrace wordt als verantwoordelijke partij geacht om beleid te bepalen op het gebied van bewaren, beveiligen en eigendom van gegevens, op grond van de afweging tussen het belang van zijn klanten, het belang van het winkelend publiek dat in en rondom winkels te maken krijgt met wifi-tracking en op grond van de plicht om persoonsgegevens te verwijderen nadat ze niet langer noodzakelijk zijn voor de verwerkelijking van de doeleinden waarvoor ze zijn verzameld.

Voor het overige acht het CBP de voorgestelde maatregel 6 te onbepaald om te kunnen inschatten voor welke van de geconstateerde overtredingen dit een concrete uitkomst biedt.

B.7. Onderzoek doen naar (en) het ontwikkelen van uitingen in de winkel

Maatregel Bluetrace:
Bluetrace stelt voor om onderzoek te doen naar uitingen over wifi-tracking in winkels die kunnen worden ontwikkeld. Bluetrace zal in overleg met klanten bepalen welke uitingen in winkels gedaan moeten worden over wifi-tracking. De afspraken daarover zullen worden vastgelegd in overeenkomsten. Bluetrace verwacht dat deze maatregel kan worden voltooid per [datum].

Reactie CBP:
In het licht van de informatieplicht van artikel 34 van de Wbp is het ontwikkelen van informatiemateriaal, stickers et cetera voor in de winkel een nuttige maatregel. Meer informatievoorziening in en rondom de winkel die de betrokkene daadwerkelijk bereikt en voorziet van eenvoudig te begrijpen informatie over het doel en de omvang van de gegevensverwerking draagt bij aan het beëindigen van de geconstateerde overtreding van artikel 34 van de Wbp. Het CBP acht het van groot belang dat Bluetrace voorstelt om dit in samenwerking met haar (mede-verantwoordelijke) klanten te doen.

Het CBP wijst er in dit verband op dat informatie op stickers op de winkelruit, folders, posters et cetera voldoende specifiek en begrijpelijk moet zijn met betrekking tot de

(soorten) gegevens die met wifi-tracking verwerkt worden, waar en met welke reden dat gebeurt en welke organisatie(s) daarvoor verantwoordelijk zijn.

De zienswijze heeft op dit punt geleid tot een aanvulling in de bevindingen van het onderzoek. Het CBP zal in het rapport van definitieve bevindingen opnemen dat Bluetrace naar aanleiding van het onderzoek werkt aan een eigen onderzoek naar de ontwikkeling en verbetering van informatie over wifi-tracking in winkels. Het CBP zal ook toevoegen dat na voltooing van dit onderzoek nadere afspraken gemaakt worden met de klanten van Bluetrace over het doen van communicatie-uitingen in de winkels over wifi-tracking.
De zienswijze heeft niet geleid tot aanpassing van de constatering dat er zeer weinig informatie wordt verstrekt aan betrokkenen die zich bevinden in een gebied waar Bluetrace wifi-tracking uit heeft gerold en laat de conclusies in het rapport onverlet.

Zoals eerder in deze bijlage is opgemerkt, is het enkel voltooien van een onderzoek, zonder dat daaraan concrete acties zijn gekoppeld die in de praktijk leiden tot een aanpassing van de werkwijze van Bluetrace niet voldoende om de geconstateerde overtredingen te beeindigen.
Daarnaast bevat het plan van aanpak geen concrete voorstellen van uitingen, zodat het CBP niet kan beoordelen in hoeverre er daadwerkelijk communicatie-uitingen zullen worden gedaan, in winkels, in welke vorm of omvang dat voorzien is en met welke inhoud.

B.8. Onderzoek naar de vraag of opt-out mogelijkheden kunnen worden aangeboden

Maatregel Bluetrace:
Bluetrace stelt voor om technisch te onderzoeken in hoeverre opt-out mogelijkheden kunnen worden ingezet. Dit onderzoek kan binnen [vertrouwelijk] worden voltooid, volgens het plan van aanpak.

Reactie CBP:
In het kader van de beoordeling of de door Bluetrace in de praktijk toegepaste werkwijze van wifi-tracking voldoet aan artikel 8 van de Wbp heeft het CBP een belangenafweging gemaakt tussen enerzijds het (gerechtvaardigde) belang van Bluetrace om wifi-tracking aan te bieden en , anderzijds, het belang van de betrokkene op eerbiediging van de persoonlijke levenssfeer.
Deze belangenafweging kan slechts leiden tot de conclusie dat de verwerking geoorloofd is wanneer Bluetrace voldoende waarborgen treft ter bescherming van de belangen van de betrokkene.
Het is daarmee niet zo dat wanneer er opt out mogelijkheden zouden zijn, dat daarmee is voldaan aan artikel 8 van de Wbp. Het aanbieden van opt out mogelijkheid kan worden gezien als een extra waarborg, die, in combinatie met andere waarborgen, kan leiden tot de slotsom dat de verantwoordelijke voldoende rekening met de belangen van de betrokkenen heeft gehouden.

Het aanbieden van opt-out mogelijkheden voor het publiek, waarmee een betrokkene zich kan onttrekken aan de gegevensverwerking indien hij dat wenst draagt bij aan het herstellen van de balans die nodig is voor het beëindigen van de geconstateerde overtreding van artikel 8 van de Wbp, maar is daarvoor niet voldoende.

De zienswijze heeft op dit punt geleid tot een aanvulling in de bevindingen van het onderzoek. Het CBP zal in het rapport van definitieve bevindingen opnemen dat Bluetrace naar aanleiding van het onderzoek werkt aan een eigen onderzoek naar de ontwikkeling van opt-out mogelijkheden voor de betrokkene.

De zienswijze heeft niet geleid tot aanpassing van de constatering dat mogelijkheden voor de betrokkene om zich te onttrekken aan de verwerking ontbreken en laat de conclusies ten aanzien van artikel 8 Wbp in het rapport onverlet.

Zoals eerder in deze bijlage toegelicht, is het enkel voltooien van een onderzoek, zonder dat daaraan concrete acties zijn gekoppeld die in de praktijk leiden tot een aanpassing van de werkwijze van Bluetrace niet voldoende om de geconstateerde overtredingen te beeindigen.