



AUTORITEIT
PERSOONSgegevens

Autoriteit Persoonsgegevens

Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
Gemeente Enschede
College van burgemeester en wethouders
Postbus 20
7500 AA ENSCHEDE

Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Besluit tot het opleggen van een bestuurlijke boete

Geacht college van burgemeester en wethouders van de gemeente Enschede,

De Autoriteit Persoonsgegevens (AP) heeft besloten aan het college van burgemeester en wethouders van de gemeente Enschede (het college B&W Enschede) een **bestuurlijke boete** van **€ 600.000** op te leggen. Het college B&W Enschede heeft zonder grondslag persoonsgegevens verwerkt van eigenaren/gebruikers van mobiele apparaten waarop de wifi stond ingeschakeld in de binnenstad van Enschede. Daarmee heeft het college B&W Enschede artikel 5, eerste lid onder a, jo. artikel 6, eerste lid van de Algemene Verordening Gegevensbescherming (AVG) overtreden.

Hierna wordt het besluit nader toegelicht. Hoofdstuk 1 betreft een inleiding en hoofdstuk 2 beschrijft het wettelijk kader. In hoofdstuk 3 beoordeelt de AP of er sprake is van persoonsgegevens, de verwerkingsverantwoordelijkheid en de overtreding. In hoofdstuk 4 wordt de (hoogte van de) bestuurlijke boete uitgewerkt en hoofdstuk 5 bevat het dictum en de rechtsmiddelenclausule.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

1. Inleiding

1.1 Betrokken overheidsinstantie

Dit besluit heeft betrekking op het college van burgemeester en wethouders van de gemeente Enschede (hierna: het college B&W Enschede). Op 17 juli 2018 heeft de AP een klacht van een klager ontvangen met daarin het verzoek om een corrigerende maatregel op te leggen aan de gemeente Enschede. De klager legde uit dat er in de binnenstad van Enschede sensoren hangen die gegevens van langslopende personen opvangen die de wifi op hun telefoon hebben ingeschakeld. Het opvangen en verwerken van deze gegevens gebeurt volgens de klager zonder grondslag in de zin van artikel 6, eerste lid, van de Algemene verordening gegevensbescherming (hierna: AVG). De AP is daarop een onderzoek gestart naar de naleving van de AVG door het college B&W Enschede. Gedurende het onderzoek ontving de AP twee soortgelijke klachten.

1.2 Procesverloop

Tijdens het onderzoek heeft de AP informatie opgevraagd bij het college B&W Enschede en bij Retail Management Center B.V. (hierna: Bureau RMC), de organisatie die in opdracht van het college B&W Enschede de wifimetingen in de binnenstad van Enschede verzorgt. Ook heeft de AP informatie opgevraagd bij [VERTROUWELIJK] (hierna: [VERTROUWELIJK]), de organisatie die Bureau RMC op haar beurt weer inhuurt voor het beheer van de sensoren en voor het verwerken van alle gegevens die met de sensoren worden verzameld. Daarnaast hebben toezichthouders van de AP op 29 mei 2019 onderzoek ter plaatse gedaan bij een aantal winkeliers in de binnenstad van Enschede waar een sensor hing. Diezelfde dag hebben andere toezichthouders van de AP op het kantoor van Bureau RMC in Amsterdam een verklaring afgenomen van de directeur van Bureau RMC en twee medewerkers van [VERTROUWELIJK] en ter plaatse documenten gekopieerd en gegevens gevorderd.

Bij brief van 8 mei 2020 heeft de AP aan het college B&W Enschede een voornemen tot handhaving verzonden. Daartoe tevens bij deze brief door de AP in de gelegenheid gesteld, heeft het college B&W Enschede op 14 juli 2020 schriftelijk een zienswijze gegeven over dit voornemen en het daaraan ten grondslag gelegde rapport. De AP heeft vervolgens op 14 januari 2021 nog nadere informatie gevraagd over deze zienswijze.

2. Wettelijk kader

2.1 Reikwijdte AVG

Ingevolge artikel 2, eerste lid, van de AVG is deze verordening van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Ingevolge artikel 4 van de AVG wordt voor de toepassing van deze verordening verstaan onder:



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

1. “Persoonsgegevens”: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”); [...].
2. “Verwerking”: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés [...].
7. “Verwerkingsverantwoordelijke”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen; [...].

2.2 Rechtmatigheid van de verwerking

Artikel 5, eerste lid, aanhef en onder a van de AVG bepaalt onder andere dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig is.

Artikel 6, eerste lid, van de AVG geeft vervolgens een limitatieve opsomming van de grondslagen voor een rechtmatige gegevensverwerking. Dit artikel stelt dat een verwerking alleen rechtmatig is indien en voor zover aan ten minste een van de zes genoemde grondslagen is voldaan. De voor het college B&W Enschede eventueel in aanmerking komende grondslagen zijn:¹

- c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

3. Beoordeling

3.1 Verwerking van persoonsgegevens

3.1.1 Inleiding

Het college B&W Enschede heeft wifimetingen laten uitvoeren met als doel het meten van de effecten van investeringen van de gemeente Enschede in de binnenstad met het oog op een verantwoord omgaan met publieke gelden. De AP zal eerst beoordelen of de gegevens die voor deze wifimetingen worden verwerkt persoonsgegevens zijn in de zin van artikel 4, onderdeel 1, van de AVG.

¹ In onderhavige situatie is er geen toestemming gevraagd aan de betrokkenen (grond a), de wifimetingen zijn niet noodzakelijk ter uitvoering van een overeenkomst met de betrokkene (grond b) en ze zijn ook niet noodzakelijk om bepaalde vitale belangen te beschermen (grond d).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

3.1.2 Feiten

Gezien het omvangrijke onderzoek in deze zaak, verwijst de AP voor de feiten naar het eerste hoofdstuk van bijlage 1 bij dit besluit. Hieronder volgt allereerst een korte samenvatting van de feiten waarna de AP tot een oordeel komt.

Het college B&W Enschede heeft het besluit genomen om per 6 september 2017 te starten met 24/7 metingen via sensoren in de binnenstad van Enschede. Het college B&W Enschede heeft deze opdracht gegund aan City Traffic B.V., thans Bureau RMC. Bureau RMC heeft vervolgens [VERTROUWELIJK] ingehuurd voor de installatie en het onderhoud van de sensoren in de binnenstad van Enschede en voor het verzamelen en valideren van de gegevens die met de sensoren worden verzameld.²

De AP heeft in het onderzoek geconstateerd dat er in ieder geval sinds 25 mei 2018 elf sensoren hangen bij verschillende winkeliers in de binnenstad van Enschede. Elke sensor heeft een bereik tot 20 à 30 meter. De sensoren hebben vanaf deze datum van alle binnen het bereik komende mobiele apparaten waarop de wifi stond ingeschakeld het MAC-adres, signaalsterkte, datum en tijdstip opgevangen en tijdelijk opgeslagen in het werkgeheugen van de sensor. Deze opslag duurde zolang het apparaat zich binnen het bereik van de sensor bevond plus twee minuten. Ook constateert de AP dat de sensoren continue scannen. Verder heeft de AP vastgesteld dat er van elk gedetecteerd apparaat bij binnenkomst en twee minuten na vertrek uit het bereik van de sensor realtime de volgende gegevens zijn verzonden naar de server: status 1 dan wel 2, gepseudonimiseerd MAC-adres, signaalsterkte, datum en tijdstip, spoofed indicator en sensor-ID.

Op alle sensoren draait één en dezelfde pseudonimiseringsmethode en deze methode is sinds 25 mei 2018 niet gewijzigd. Het pseudonimiseren heeft tot gevolg dat één MAC-adres op elk van de sensoren leidt tot één en hetzelfde gepseudonimiseerd MAC-adres.

De gegevens die op één dag zijn gemeten door de sensoren in de binnenstad van Enschede worden dagelijks verzameld in een kortetermijntabel. Het tijdstip op de dag waarop het apparaat door de sensor is gescand wordt hierbij op de seconde nauwkeurig vastgelegd. In de periode tot aan 1 januari 2019 is het gepseudonimiseerde MAC-adres bij binnenkomst op de server niet afgeknipt, in de periode vanaf 1 januari 2019 wel. Het afknippen betreft het verwijderen van [VERTROUWELIJK]. De andere gegevens die zijn verzonden naar de server, namelijk sensor-ID, datum, tijdstip, signaalsterkte, status en spoofed indicator zijn onbewerkt overgenomen in de kortetermijntabel.

Elke nacht werden op de kortetermijntabel twee filters toegepast, namelijk een opt-out filter en een bewonersfilter. Deze filters hebben tot gevolg dat bepaalde records uit de kortetermijntabel niet terechtkomen in de langetermijntabel. De AP heeft geconstateerd dat de bewonersfilter niet alle bewoners eruit filtert en dat er op de website van de gemeente hierover foutieve informatie wordt gegeven.

Na toepassing van de filters op de kortetermijntabel, leidde twee opeenvolgende records van hetzelfde (afgeknipte) gepseudonimiseerde MAC-adres tot één record in de langetermijntabel. Van 25 mei 2018 tot aan 1 januari 2019 bevatte de langetermijntabel de volgende gegevens: gepseudonimiseerd MAC-adres,

² De AP zal in paragraaf 3.2 nader ingaan op de verhouding tussen deze partijen.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

datum, TijdIn, TijdUit, Retention, SignalStrengthIn, SignalStrenghtOut. Per 1 januari 2019 is overgegaan op het afknippen van het gepseudonimiseerd MAC-adres en werd het gepseudonimiseerd MAC-adres gegeven vervangen door het afgeknipte gepseudonimiseerde MAC-adres. Ook constateert de AP dat er in de langetermijntabel vanaf 25 mei 2018 gegevens stonden over een periode van tussen de zes en zeven maanden.

Het college B&W Enschede heeft schattingen ontvangen van verschillende variabelen over unieke bezoekers aan de binnenstad van Enschede. Ten behoeve hiervan worden de van toepassing zijnde gegevens in de langetermijntabel ontdekt op basis van het afgeknipte gepseudonimiseerde MAC-adres en vervolgens worden er bepaalde statistische berekeningen op toegepast.

Het college B&W Enschede heeft op 30 april 2020 aan Bureau RMC de opdracht gegevens om per 1 mei 2020 de sensoren uit te zetten. De sensoren leveren geen telgegevens meer vanaf 1 mei 2020.³

De AP heeft geconstateerd dat het college B&W Enschede vanaf in ieder geval 25 mei 2018 tot en met 30 april 2020⁴ gegevens van grofweg 1,8 miljoen unieke mobiele apparaten heeft laten verwerken en dat het aantal detecties beduidend hoger zal liggen.

De AP heeft vervolgens vastgesteld dat er uit de langetermijntabel van na 1 januari 2019 duidelijke leefpatronen te destilleren zijn. Gezien de regelmatigheid van de patronen kan redelijkerwijs worden geconcludeerd dat de bij het patroon horende registraties toebehoren aan één mobiel apparaat. De leefpatronen kunnen bijvoorbeeld iemands woon- of werkplek prijsgeven, maar ook gevoeligere gegevens zoals bezoeken aan medische instellingen.

De AP merkt verder op dat Bureau RMC in haar privacyprotocol, dat specifiek ziet op verwerkingen via de City Traffic-methode, heeft opgenomen dat zij en/of haar partners vanaf in ieder geval 25 mei 2018 persoonsgegevens verwerken in de zin van de AVG. Verder heeft Bureau RMC ook in haar privacyprotocol opgenomen dat de rapportages die opdrachtgevers van Bureau RMC ontvangen geen persoonsgegevens bevatten.

3.1.3 Beoordeling

Gedurende het verwerkingsproces (van detectie door een sensor tot opslag in de langetermijntabel) zijn er verschillende sets aan gegevens te onderscheiden. Deze sets zijn hieronder in de tabel weergegeven, waarbij onderscheid is gemaakt tussen de periode voorafgaand aan invoering van het afknippen van gepseudonimiseerde MAC-adressen (25 mei 2019 – 1 januari 2019) en de periode na de invoering van dit afknippen (1 januari 2019 – 30 april 2020).

³ Brief van 16 februari 2021 van het college B&W Enschede aan de AP, pagina 3 en bijlage 2.

⁴ In de periode 10 december 2018 tot en met 3 januari 2019 heeft het college B&W Enschede de wifimetingen gepauzeerd. Eerder verzamelde gegevens waren in deze periode wel opgeslagen in de langetermijntabel, dus er werden in deze periode wel gegevens door het college B&W Enschede verwerkt. Zie ook bijlage 1, paragraaf 1.3 en 2.5.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Fase in verwerkingsproces	25 mei 2018 - 1 januari 2019	1 januari 2019 – 30 april 2020
Tijdelijke opslag op elke sensor	MAC-adres; Signaalsterkte; Datum; Tijdstip	<i>Idem als voorafgaand aan 1 januari 2019</i>
Verzending naar en ontvangst op de server	Gepseudonimiseerd MAC-adres; Signaalsterkte; Datum; Tijdstip; Sensor-ID; Status; Spoofed indicator	<i>Idem als voorafgaand aan 1 januari 2019</i>
Korttermijntabel op de server	Gepseudonimiseerd MAC-adres; Signaalsterkte; Datum; Tijdstip; Sensor-ID; Status; Spoofed indicator	Afgeknipt gepseudonimiseerd MAC-adres; Signaalsterkte; Datum; Tijdstip; Sensor-ID; Status; Spoofed indicator
Langtermijntabel op de server	ID; Gepseudonimiseerd MAC-adres; SignaalsterkteIN; SignaalsterkteUIT; Datum; TijdstipIN; TijdstipUIT; Verblijfstijd; Sensor-ID; BWCcode	ID; Afgeknipt gepseudonimiseerd MAC-adres; SignaalsterkteIN; SignaalsterkteUIT; Datum; TijdstipIN; TijdstipUIT; Verblijfstijd; Sensor-ID; BWCcode

In bovenstaande tabel zijn de meest waardevolle attributen voor wat betreft het kunnen identificeren van de natuurlijke personen vet gedrukt. Het betreft aan de ene kant het MAC-adres, eerst gepseudonimiseerd en later afgeknipt, en aan de andere kant de combinatie van Datum, Tijdstip in seconden en Sensor-ID. Deze laatste combinatie geeft heel precies weer wanneer een mobiel apparaat waar was; dit is dus een *locatiegegevens*. De AP spreekt hierna in dit kader dan ook van 'locatiegegevens'.⁵

Tevens zijn in bovenstaande tabel twee arceringen aangebracht, namelijk lichtgrijs voor het (gepseudonimiseerde) MAC-adres en donkergrijs voor het afgeknipte gepseudonimiseerde MAC-adres. In het vervolg van deze paragraaf zal de AP aantonen dat alle in de tabel hierboven opgenomen sets gegevens kwalificeren als persoonsgegevens in de zin van artikel 4, onderdeel 1, van de AVG.

Lichtgrijze vlakken: Het MAC-adres c.q. gepseudonimiseerd MAC-adres in combinatie met de locatiegegevens kwalificeren in elke fase van het verwerkingsproces als persoonsgegevens in de zin van de AVG

Artikel 4, aanhef en onderdeel 1, van de AVG bepaalt dat gegevens kwalificeren als persoonsgegevens als het informatie is over 'een geïdentificeerde of identificeerbare natuurlijke persoon'. Van de eerste situatie,

⁵ Over locatiegegevens van mobiele apparaten hebben de Europese gegevensbeschermingstoezichthouders reeds in 2011 onderkend dat deze veel prijs kunnen geven over de eigenaren van die apparaten. Zie ook Pagina 7 en 8 van WP185 Advies 13/2011 over geolocatediensten op slimme mobiele apparaten: "De meeste mensen zijn geneigd om hun mobiele apparaten dicht bij zich te houden, zoals in een broek- of jaszak, in een tas of op het nachtkastje naast het bed. (...) Het gebeurt zelden dat iemand een dergelijk apparaat aan een ander uitleent. (...) Zo kan uit een patroon van inactiviteit in de nacht de slaappleaats worden afgeleid en uit een regelmatig reispatroon in de ochtend de locatie van de werkgever."



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

informatie over een 'geïdentificeerde persoon' is in onderhavige situatie geen sprake omdat de identiteit van de natuurlijke persoon niet direct volgt uit het MAC-adres dan wel het gepseudonimiseerde MAC-adres en de locatiegegevens.

Om persoonsgegevens te zijn moeten de gegevens dus informatie zijn over 'een identificeerbare natuurlijke persoon'. In dit geval zal de natuurlijke persoon direct of indirect te identificeren moeten zijn aan de hand van identificatoren of kenmerkende elementen. Mogelijke identificatoren in onderhavige situatie kunnen zijn: het MAC-adres, het gepseudonimiseerde MAC-adres en de locatiegegevens.

Een MAC-adres – mits niet gespoofed⁶ – is een uniek identificatienummer van een mobiel apparaat. Omdat mobiele apparaten zoals smartphones en tablets zeer persoonsgebonden zijn, kan de natuurlijke persoon in kwestie via zijn/haar mobiele apparaat worden gekoppeld aan het MAC-adres. Dit betekent dat een niet-gespoofed MAC-adres een identificator kan zijn van een natuurlijk persoon.

Het gepseudonimiseerde MAC-adres is zoals in de feiten toegelicht een omzetting van een MAC-adres naar een andere unieke karakterreeks. Dit heeft tot gevolg dat ook het gepseudonimiseerde MAC-adres – mits het onderliggend MAC-adres niet is gespoofed – een identificator van een natuurlijk persoon kan zijn.⁷

Voor de locatiegegevens geldt dat deze in artikel 4, onderdeel 1, van de AVG expliciet zijn genoemd als mogelijke identificator van een natuurlijk persoon aangezien locatiegegevens veel prijs kunnen geven over de eigenaar van het mobiele apparaat.

De vraag is nu of in elke fase van het verwerkingsproces aan de hand van de hiervoor genoemde identificatoren een natuurlijk persoon kan worden geïdentificeerd. Hierna beschrijft de AP per fase in het verwerkingsproces een voorbeeld van een manier waarmee het redelijkerwijs mogelijk was om de natuurlijke persoon waarover de gegevens gaan te identificeren.

Manier 1: Identificatie van personen aan de hand van de gegevens opgeslagen op de sensor

De AP heeft tijdens het onderzoek vastgesteld dat het MAC-adres en de locatiegegevens tijdelijk worden opgeslagen in het werkgeheugen van elke sensor en dat het gepseudonimiseerde MAC-adres en de locatiegegevens worden verzonden naar de server. [VERTROUWELIJK] is verantwoordelijk voor het beheer van alle sensoren in de binnenstad van Enschede en het verzamelen van de gegevens. Bij [VERTROUWELIJK] is dus de exacte locatie van de sensoren bekend en heeft men toegang tot het werkgeheugen en de software die draait op elke sensor.⁸ Tegelijk met een nieuwe detectie van een mobiel apparaat door een sensor is het bijvoorbeeld voor iemand van [VERTROUWELIJK] mogelijk om ter plaatse of via een camera waar te nemen welke persoon binnen het bereik van de sensor komt lopen. Vooral op

⁶ Spoofing is in dit verband een informele term voor "MAC Address Randomization", een techniek waarmee een deel van het MAC-adres soms willekeurig verandert met als doel de mogelijkheid een apparaat te volgen door tijd en ruimte te verminderen.

⁷ Zie hoofdstuk 4 van WP 216 Advies 5/2014 over anonimiseringstechnieken.

⁸ Bijvoorbeeld door direct op de sensor in te loggen of door aan hun softwarecode toe te voegen dat het werkgeheugen moet worden weggeschreven naar een andere locatie waar de medewerkers bij kunnen.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

stille momenten in de binnenstad leidt dit direct tot identificatie van de natuurlijke persoon. Ter controle kan de persoon worden gevraagd naar zijn/haar MAC-adres. Dezelfde manier van identificeren is mogelijk in geval van gepseudonimiseerde MAC-adressen en de bijbehorende locatiegegevens, omdat ook dan op het moment van detectie ter plaatse of via een camera de persoon in kwestie waargenomen kan worden.

Manier 2: identificatie van personen aan de hand van de gegevens in de kortetermijntabel (tot 1 januari 2019)

Deze manier beschrijft dat aan de hand van de gegevens in de kortetermijntabel het ook mogelijk is om de natuurlijke personen te identificeren. [VERTROUWELIJK] draagt zorg voor het verzamelen en valideren van de gegevens. De kortetermijntabel berust dus bij [VERTROUWELIJK]. Van mobiele apparaten die het bereik van een sensor ingaan worden er gegevens met daaraan gekoppeld 'status 1' opgenomen in de kortetermijntabel en als hetzelfde mobiele apparaat even later het bereik van de sensor weer verlaat, dan worden er gegevens met 'status 2' verzonden naar de kortetermijntabel. Indien echter een mobiel apparaat binnen het bereik van een bepaalde sensor blijft, bijvoorbeeld omdat die persoon daarbinnen woont of werkt, dan staat er in de kortetermijntabel dus alleen een status 1 record met daarbij het gepseudonimiseerde MAC-adres, Datum en Tijdstip. Als voor langere tijd een status 2 record uitblijft dan is het bij [VERTROUWELIJK] bekend dat de betreffende bewoner of winkelmedewerker zich nog steeds binnen het bereik van de sensor bevindt. Iemand van [VERTROUWELIJK] kan vervolgens ter plaatse vaststellen om welke persoon het gaat en de persoon identificeren.

Manier 3: identificatie van personen aan de hand van de gegevens in de langetermijntabel (tot 1 januari 2019)

Tot slot is het voor [VERTROUWELIJK] ook op basis van de historische gegevens opgenomen in de langetermijntabel mogelijk om natuurlijke personen te identificeren. De AP heeft vastgesteld dat er in de langetermijntabel van ná 1 januari 2019, dus na invoering van het afknippen, leef- en beweegpatroon te herkennen zijn.⁹ Dit zal ook het geval zijn in de langetermijntabel van vòòr 1 januari 2019, toen er nog unieke gepseudonimiseerde MAC-adressen in stonden, omdat toen ook steeds zes maanden aan gegevens werden bewaard. Aan de hand van een patroon is het voor [VERTROUWELIJK] mogelijk om te voorspellen wanneer de betreffende natuurlijke persoon zich ergens bevindt, bijvoorbeeld de persoon die elke nacht tussen 04:00 en 05:00 zich beweegt tussen sensoren in de binnenstad van Enschede. In de nacht lopen er nauwelijks andere mensen op straat en is derhalve voor [VERTROUWELIJK] mogelijk om ter plaatse of via een camera deze persoon te identificeren.

Bij bovenstaande drie voorbeelden van manieren van identificatie van natuurlijke personen door [VERTROUWELIJK] is rekening gehouden met overweging (26) van de AVG waarin staat dat rekening dient te worden gehouden met 'alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren'. De AP concludeert dat bovenstaande drie manieren van identificatie van natuurlijke personen gelet op de vereiste tijd, kosten en mankracht geen excessieve inspanning van [VERTROUWELIJK] vergen. Ook is voldaan aan de criteria uit het arrest Breyer/Duitsland¹⁰, want de manieren zijn niet bij wet verboden noch in praktijk ondoenlijk. Dat medewerkers van

⁹ Zie ook bijlage 1, paragraaf 1.2, pagina 46 en verder.

¹⁰ HvJ EU, 19 oktober 2016, ECLI:EU:C:2016:779, r.o. 46.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

[VERTROUWELIJK] deze middelen in de praktijk niet inzetten om personen in de binnenstad van Enschede te identificeren doet niet af aan het feit dat ze dit redelijkerwijs zouden kunnen. Naast identificatie door [VERTROUWELIJK] stelt de AP vast dat de identificatie ook door medewerkers van Bureau RMC gedaan kan worden. De AP heeft namelijk vastgesteld dat Bureau RMC op basis van de service level agreement met [VERTROUWELIJK] toegang heeft tot alle gegevens die [VERTROUWELIJK] verzameld. Daarnaast constateert de AP dat zelfs het college B&W Enschede de identificatie kan doen, omdat zij op basis van de bewerkersovereenkomst met Bureau RMC ook toegang heeft tot alle gegevens. Eventueel zou identificatie van de natuurlijke personen ook kunnen plaatsvinden door de persoonsgegevens verzameld met de sensoren te koppelen aan de data die wordt verzameld via de verschillende smart-city-projecten in Enschede.¹¹

Ten aanzien van het gebruik van MAC-adressen en locatiegegevens wordt opgemerkt dat de voorganger van de AP in 2015 in een onderzoek naar een bedrijf dat wifitracking verzorgde heeft geoordeeld¹² dat het registreren van MAC-adressen en locatiegegevens via sensoren kwalificeert als het verwerken van persoonsgegevens omdat identificatie van de natuurlijke personen mogelijk was op de hiervoor beschreven Manier 1.¹³ Daarnaast hebben de gezamenlijke Europese gegevensbeschermingstoezichthouders in hun opinie over apps op 'smart devices' gesteld dat locatiegegevens en unieke identificatoren van mobiele apparaten persoonsgegevens zijn.¹⁴ In hun opinie over de voorgestelde e-Privacy Verordening is door hen gesteld: *In this context, it should be noted that these MAC addresses are personal data, even after security measures such as hashing have been undertaken.*¹⁵

De AP concludeert op basis van het voorgaande dat de combinatie van MAC-adres en locatiegegevens en de combinatie gepseudonimiseerd MAC-adres en locatiegegevens op de sensor vanaf 25 mei 2018 tot en met 30 april 2020 en in de korte- en langetermijntabel tot aan 1 januari 2019 kwalificeren als persoonsgegevens in de zin van de AVG.

¹¹ www.smartenschede.nl

¹² In het rapport is getoetst aan de definitie van persoonsgegeven in artikel 1 onder a van de Wet bescherming persoonsgegevens: 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. De huidige definitie van persoonsgegevens in de AVG is gelijklopend.

¹³ Paragraaf 5.1 van het rapport definitieve bevindingen 'Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace' (z2014-00944) van 13 oktober 2015. Vindbaar op www.autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-wifi-tracking-rond-winkels-strijd-met-de-wet. De AP heeft destijds ook de VNG per brief geïnformeerd over haar standpunten inzake wifitracking: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_ap_vng_wifi-tracking.pdf.

¹⁴ WP202 Opinion 02/2013 on apps on smart devices, pagina 8. Beschikbaar via de website van de AP: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/int/wp202_en_opinion_on_mobile_apps.pdf

¹⁵ WP247 Opinion 01/2017 on Proposed Regulation for the ePrivacy Regulation, pagina 11. Zie ook WP223 Opinion 8/2014: *Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed. For instance, wearable things kept in close proximity of data subjects result in the availability of a range of other identifiers, such as the MAC addresses of other devices which could be useful to generate a fingerprint allowing data subject location tracking. The collection of multiple MAC addresses of multiple sensor devices will help create unique fingerprints and more stable identifiers which IoT stakeholders will be able to attribute to specific individuals. These fingerprints and identifiers could be used for a range of purposes, including location analytics or the analysis of movement patterns of crowds and individuals. Such a trend must be combined with the fact that such data can later be combined with other data issued from other systems (e.g. CCTV or internet logs). In such circumstances, some sensor data are particularly vulnerable to re-identification attacks.*



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Uit het privacy protocol van Bureau RMC en de infographic waarmee Bureau RMC een toelichting geeft op de City Traffic-methode concludeert de AP dat ook Bureau RMC van mening is dat zij en/of haar partners persoonsgegevens verwerkten tot aan het moment van afknippen van het gepseudonimiseerde MAC-adres.

Donkergrijze vlakken: Het afknippen van het gepseudonimiseerde MAC-adres sluit niet alle drie de risico's op herleidbaarheid, koppelbaarheid en deduceerbaarheid uit waardoor het nog steeds persoonsgegevens zijn in de zin van de AVG

Bureau RMC stelt dat de korte- en de langetermijntabel na de invoering van het 'anonimiseren op de server' geen persoonsgegevens in de zin van de AVG meer bevatten. De infographic over de City Traffic-methode¹⁶ formuleert dit als volgt: *"De geanonimiseerde code is nu niet meer herleidbaar, koppelbaar en identificeerbaar naar een uniek apparaat. Daarmee bevat onze data geen persoonsgegevens."*

De AP concludeert hierna dat de gekozen anonimiseringsmethode van het (alleen) afknippen van een klein gedeelte van het gepseudonimiseerde MAC-adres onvoldoende de risico's op herleidbaarheid, koppelbaarheid en deduceerbaarheid uitsluit en dat de gegevens kwalificeren als persoonsgegevens. De AP licht dit hierna toe.

Koppelbaarheid

Het risico op koppelbaarheid is aanwezig als de mogelijkheid bestaat om ten minste twee records over dezelfde betrokkene of groep betrokkenen met elkaar in verband te brengen (in dezelfde database of in twee verschillende databases).

De AP constateert dat het koppelen van records over dezelfde betrokkene of groep betrokkenen daadwerkelijk plaatsvindt. Er worden namelijk twee opeenvolgende records met hetzelfde afgeknipte gepseudonimiseerde MAC-adres in de kortetermijntabel gekoppeld en opgenomen in de langetermijntabel. Daarnaast worden de gegevens in de langetermijntabel ontdebeld op basis van het afgeknipte gepseudonimiseerde MAC-adres om als basis te dienen voor de cijfers voor het college B&W Enschede over unieke bezoekers aan de binnenstad van Enschede. De AP wijst hier ook op de verklaring van de medewerkers van [VERTROUWELIJK]¹⁷ dat het detailverlies door het afknippen van een deel van de symbolen van het gehashte Mac-adres beperkt is waardoor koppeling nog steeds mogelijk is.

Uit het voorgaande volgt dat de gekozen anonimiseringstechniek niet het risico op koppelbaarheid uitsluit. Omdat is vereist dat alle drie de risico's worden uitgesloten, kan reeds nu de conclusie worden getrokken dat de anonimiseringstechniek faalt en dat re-identificatie van natuurlijk personen mogelijk is. Voor de volledigheid behandelt de AP ook de twee andere risico's.

¹⁶ Zie bijlage 1, paragraaf 1.2, figuur 2.

¹⁷ Zie bijlage 1, paragraaf 1.2, pagina 44.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Herleidbaarheid

Het risico op herleidbaarheid is aanwezig als de mogelijkheid bestaat om een persoon in een dataset te individualiseren door bepaalde records uit te lichten.

De AP heeft kunnen aantonen dat er uit de langetermijntabel duidelijke leefpatronen af te leiden zijn. Deze patronen zijn gekoppeld aan één afgeknipt gepseudonimiseerd MAC-adres, wat betekent dat het mogelijk is dat de patronen de locatiegegevens van meerdere mobiele telefoons bevatten. Echter, gezien de regelmatigheid van de patronen kan redelijkerwijs worden geconcludeerd dat alle registraties die behoren tot het patroon afkomstig zijn van één enkel mobiel apparaat, en daarmee dus één natuurlijk persoon. Hierdoor is een persoon te individualiseren. De AP concludeert daarom dat ook het risico op herleidbaarheid niet uitgesloten is.

Deduceerbaarheid

Een risico op deduceerbaarheid is aanwezig als de mogelijkheid bestaat om de waarde van een persoonskenmerk met grote waarschijnlijkheid af te leiden uit de waarden van een reeks andere attributen. Uit de drie visualisaties van de langetermijntabel¹⁸ kan met grote waarschijnlijkheid een waarde van een persoonskenmerk worden afgeleid, bijvoorbeeld de slaappleaats of de locatie van de werkgever. De AP concludeert daarom dat het afknippen van het gepseudonimiseerde MAC-adres ook het risico op deduceerbaarheid niet uitsluit.

De AP concludeert op basis van het voorgaande dat de vanaf 1 januari 2019 gehanteerde korte- en langetermijntabel onvoldoende bestand zijn tegen re-identificatie.

Daarnaast concludeert de AP dat de combinatie van de afgeknipte gepseudonimiseerde MAC-adressen en de gedetailleerde locatiegegevens in deze tabellen kwalificeren als persoonsgegevens in de zin van artikel 4 onderdeel 1 van de AVG, omdat de eerder beschreven manieren 2 en 3 van identificatie ook opgaan in geval van afgeknipte gepseudonimiseerde MAC-adressen. Manier 2 werkt omdat het ook dan in de kortetermijntabel zichtbaar is als er alleen een status 1 record is, en dus dat de persoon die hoort bij het afgeknipte gepseudonimiseerde MAC-adres zich nog steeds binnen het bereik van de sensor bevindt. Iemand van [VERTROUWELIJK] kan vervolgens ter plaatse vaststellen om welke persoon het gaat en de persoon identificeren. Voor manier 3 geldt dat de AP deze al had gebaseerd op de langetermijntabel met afgeknipte gepseudonimiseerde MAC-adressen.

3.1.4 Zienswijze college B&W Enschede en reactie AP

Het hoofdpunt van het college B&W Enschede is dat het college slechts anonieme, geaggregeerde data van Bureau RMC ontvangt. Hierna volgt een samenvatting van de zienswijze van het college B&W Enschede met daarop de reactie van de AP.

Werking en opslag sensoren

Naar het college van B&W Enschede van Bureau RMC/[VERTROUWELIJK] begrijpt, heeft een sensor een bereik van in potentie tot wel 70 meter rondom het meetpunt. De sensor vangt de wifi-signalen die een

¹⁸ Zie bijlage 1, paragraaf 1.2, pagina 46 en verder.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

device uitstoot binnen het sensorgebied op. De sensor ontvangt een ‘pakketje’ gegevens waaronder het MAC-adres van het device en de wifi-sterkte. Volgens het college van B&W worden er geen (overige) tot de persoon herleidbare gegevens geregistreerd. Er worden ook geen longitude, latitude of adresgegevens ontvangen door de sensor.

De statusmeldingen die naar de server worden gestuurd gaan vergezeld van het gehashte MAC-adres. Deze hashing¹⁹ vindt direct bij doorzending plaats. De AP geeft in haar onderzoek aan, dat er ongepseudonimiseerde (dus originele) MAC-adressen worden opgeslagen op het werkgeheugen van de sensor. Volgens het college van B&W Enschede klopt dat, maar dat is slechts zeer tijdelijk (enkele milliseconden); zonder die tijdelijke opslag in het werkgeheugen van de sensor zou er immers geen hashing plaats kunnen vinden. Hiermee kan echter volgens het college van B&W Enschede geen identificatie plaatsvinden. Men kan zich immers geen toegang tot de sensor verschaffen, zodanig dat men een MAC-adres zou kunnen achterhalen. Er worden geen MAC-adressen permanent bewaard en er zijn bijvoorbeeld ook geen lijsten of databases met MAC-adressen voorhanden. Bureau RMC/[VERTROUWELIJK] kan zich geen toegang verschaffen tot de MAC-adressen op de sensoren.

De AP volgt de zienswijze van het college van B&W niet. Dat de sensors in potentie een bereik hebben tot 70 meter doet niet af aan het feit dat in dit geval de sensoren bij installatie zijn “geijkt” en afgesteld op de overkant van de weg.²⁰ De sensoren hebben aldus geen bereik van 70 meter rondom het meetpunt, maar een bereik tot aan de overkant van de straat. Voorts merkt de AP op dat er voor de bepaling van de locatie geen GPS gegevens nodig zijn. De locatie van de sensor is immers bij [VERTROUWELIJK] bekend en het sensor-ID wordt meegestuurd naar de server. Dat deze gegevens in een andere databank staan betekent niet dat [VERTROUWELIJK] daar geen toegang tot heeft.

Het college van B&W Enschede benoemt voorts dat er geen toegang mogelijk is tot de MAC-adressen op de sensor. De AP wil als reactie hierop graag het volgende benadrukken. Op de sensor zijn twee modules actief. De eerste [VERTROUWELIJK] is de ontvangstmodule en houdt MAC-adressen bij zoals ze worden ontvangen. In het werkgeheugen van deze module zitten dus alle MAC-adressen die óók binnen de afgelopen twee minuten zijn ontvangen door de sensor. De tweede module [VERTROUWELIJK] ontvangt status-1 en status-2 berichten van de eerste module. Het eerste bericht betekent “er is een nieuwe telefoon waargenomen” en het tweede betekent “de telefoon is langer dan twee minuten niet meer gezien”. De twee modules communiceren middels een zogenaamde [VERTROUWELIJK]²¹ en daarover worden ongehashte MAC-adressen verstuurd. Het hashen vindt pas plaats in de tweede module, vlak voordat de gegevens naar de server worden verstuurd. [VERTROUWELIJK]²². [VERTROUWELIJK].²³ [VERTROUWELIJK].

¹⁹ Hashen is het omzetten van een reeks getallen en/of letters naar een andere unieke reeks door middel van een algoritme.

²⁰ Verslag van verklaring van Bureau RMC en [VERTROUWELIJK] afgelegd op 29 mei 2019, pagina 2 (documentnummer 49).

²¹ [VERTROUWELIJK]

²² [VERTROUWELIJK]

²³ [VERTROUWELIJK]



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Identificatie natuurlijke personen

Voorts stelt het college van B&W Enschede zich op het standpunt dat de MAC-adressen die de sensor opvangt, al dan niet in combinatie met een locatiegegeven, niet direct dan wel indirect tot identificatie van een individuele natuurlijke persoon kan leiden. Het college van B&W Enschede betwist de constatering van de AP dat een MAC-adres, bijvoorbeeld in combinatie met een locatiegegeven, in sommige situaties een natuurlijke persoon zou kunnen identificeren, niet. Het college van B&W Enschede wil echter benadrukken dat pas van directe of indirecte identificeerbaarheid sprake zou kunnen zijn, indien er sprake is van (koppeling met) bijkomende gegevens.

De AP neemt in haar rapportage in de ogen van het college van B&W Enschede te snel aan dat er sprake is van herleidbaarheid. Uit de publicatie van WP29 blijkt volgens het college van B&W Enschede uitdrukkelijk dat het enkele MAC-adres niet als persoonsgegeven wordt beschouwd. Een MAC-adres is volgens WP29 pas een persoonsgegeven als er sprake is van een combinatie met andere gegevens. In casu is er echter geen sprake van combinatie van de MAC-adressen met andere gegevens. Het enige andere gegeven dat in dit verband mogelijk een rol zou kunnen spelen is een (grof) locatiegegeven. Dit locatiegegeven is in casu echter te onnauwkeurig om in samenhang met een MAC-adres een individu te kunnen identificeren.

Het college B&W Enschede stelt zich daarnaast op het standpunt dat er niet is voldaan aan de criteria uit het arrest Breyer / Duitsland om te kunnen spreken van persoonsgegevens. De MAC-adressen worden namelijk niet bewaard, maar direct op de sensor gehasht waarna het originele MAC-adres wordt verwijderd. Men kan dan ook niet bij de originele MAC-adressen komen. Toekomstige identificatie is alleen om die reden al onmogelijk.

De data die worden verzonden vanaf de sensor hebben volgens het college B&W Enschede geen directe locatiegegevens bij zich. Het Sensor-ID is niet meer of minder dan een aanduiding van de sensor, het zegt nog niet waar de sensor zich exact bevindt. Bovendien komt het Sensor-ID pas voor het eerst in beeld bij het versturen van de gehashte MAC-adressen van de sensor naar de server. Door de gescheiden opslag kan koppeling van het Sensor-ID met het MAC-adres pas later in het telproces plaatsvinden. Vanaf dat moment is het MAC-adres echter niet meer voorhanden. Het MAC-adres wordt bij het versturen daarvan naar de server immers gehasht, en vervolgens getruncate. Identificatie, ook aan de hand van een zogenaamd locatiegegeven, kan derhalve niet plaatsvinden volgens het college B&W Enschede.

De AP volgt de zienswijze van het college van B&W Enschede niet. Het college B&W Enschede legt ten onrechte de nadruk op het feit dat de MAC-adressen worden getransformeerd en niet zelfstandig voor enige tijd worden bewaard. Zij gaat hierbij echter voorbij aan de gegevens die door de AP worden gezien als persoonsgegevens.

De combinatie (pseudonieme identicator + datumtijd + locatie) is een persoonsgegeven. Hier is dat de combinatie afgeknipte gehashte MAC-adres, datum plus tijd in seconden en het ID van de sensor. De eventuele mogelijkheid om van een *gehashte en getruncate MAC-adressen* terug te gaan naar het originele MAC-adres is daarom irrelevant. Het gaat er hier de AP om dat de pseudonieme identicator in de tijd te weinig is veranderd.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

De mogelijkheid tot herleiding (en uiteindelijk identificatie) is een gevolg van ontwerpbeslissingen in het platform. Het voor lange duur opslaan van de onveranderde identificatoren maakt het mogelijk om individuen te kunnen volgen. Zij zijn op dat moment alleen nog weergegeven als nummer. Maar dit is hetzelfde nummer gedurende zes maanden. Men kan in dit geval niet spreken van robuuste anonimiseringstechnieken. Daarvan was tijdens het onderzoek van de AP in ieder geval geen sprake.

Doordat dezelfde identificator keer op keer langs komt, is het tracken van personen dus mogelijk. Daarmee wordt tijd en locatie een factor. En zoals hiervoor door de AP reeds is vermeld, is daarbij de exacte locatie van de sensoren bij [VERTROUWELIJK] bekend waarbij het bereik van de sensoren is afgesteld tot aan de overkant van de straat en niet 70 meter. Bewegingspatronen zijn in hoge mate individueel. Het college B&W Enschede onderschat de gevoelige aard van locatiegegevens die steeds een half jaar bewaard werden.

Leefpatronen

De AP concludeert dat uit de gehashte en getruncate gegevens ook leefpatronen gedestilleerd kunnen worden die op zichzelf te herleiden zijn tot een individu. De gemeente Enschede is echter van mening dat herleidbaarheid naar een individu op basis van een leefpatroon in casu niet mogelijk is.

In de ogen van het college B&W Enschede kan het uitgaan van de aanname dat een bepaald patroon zich ook in de toekomst zal voordoen nooit de basis van een reële, indirecte, identificatie zijn. Profilering is immers alleen mogelijk als er van een pseudoniem meerdere tellingen worden verzameld. Naar de gemeente begreep worden in casu de meeste tellingen gedaan op basis van eenmalige tellingen. Zulks geldt voor om en nabij 70% van de tellingen.

Daarnaast kan er in de leefpatronen die de AP meent te kunnen abstraheren, theoretisch overlap plaatsvinden van meerdere devices, vanwege de truncating van de gehashte waarden. Het is niet op voorhand uit te sluiten dat twee of meer gehashte, en vervolgens getruncate, gegevens dezelfde waarde krijgen. Voorts geldt dat niet alleen individuen devices met een MAC-adres bij zich hebben, maar dat zich ook diverse overige devices zoals pinapparaten, smart tv's en printers in het gebied kunnen bevinden.

Deze enige mogelijke wijze van identificatie die de AP schetst, is identificatie door een medewerker van Bureau RMC/ [VERTROUWELIJK] ter plaatse dan wel via camerabeelden op afstand. Deze enige identificatiemogelijkheid is volgens het college B&W Enschede onwerkbaar of sterker nog: onmogelijk. De ongepastheid van een verzoek, namelijk aan een persoon vragen welk MAC-adres hij/zij heeft, is niet meer dan een theoretische. Bovendien geldt dat Bureau RMC/[VERTROUWELIJK] helemaal geen MAC-adres tot haar beschikking heeft om dat MAC-adres te verifiëren. Het MAC-adres wordt immers volgens het college B&W Enschede direct gehasht en later geanonimiseerd. Het MAC-adres wordt bovendien niet vastgelegd in een lijst of bijvoorbeeld een database, waardoor identificatie en controle achteraf niet plaats kan vinden.

Realtime identificatie, toch echt noodzakelijk om een natuurlijk persoon te kunnen identificeren en ook het enige voorbeeld van identificatie dat de AP in haar onderzoeksrapport geeft, kan volgens het college B&W Enschede niet plaatsvinden vanwege de vertraging die zich in de telssystematiek voordoet en omdat



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

het zoekgebied te groot is. De AP moet zich er voorts rekenschap van geven dat er zich op drukke momenten honderden, zo niet duizenden mensen in het sensorgebied kunnen bevinden.

Overigens heeft de gemeente Enschede, anders dan de AP meent, helemaal geen mogelijkheid om kennis te nemen van eventueel tot individuen herleidbare gegevens bij Bureau RMC/[VERTROUWELIJK]. De enkele contractuele mogelijkheid is volgens het college B&W Enschede onvoldoende om aan te nemen dat de gemeente daadwerkelijk toegang tot bedoelde gegevens had en heeft.

De AP volgt de zienswijze van het college van B&W Enschede grotendeels niet. Zoals hiervoor vermeld acht de AP de toegepaste anonimiseringstechnieken onvoldoende, waardoor het dus wel mogelijk was om bij het gedurende lange tijd opslaan van de onveranderde identificatoren individuen te kunnen volgen. De AP gaat wel mee in het feit dat in 70% van de gevallen de tellingen gedaan worden op basis van eenmalige tellingen. Dat doet echter niet af aan het feit dat het college B&W Enschede van tienduizenden burgers wel meerdere tellingen verwerkt en dat de eenmalige bezoekers te identificeren waren aan de hand van de gegevens op de sensoren. En hoewel er natuurlijk ook enkele devices zoals printers in de stad bevinden, lijkt het de AP onvoorstelbaar dat deze zichtbaar zijn op meerdere locaties omdat deze zich door de stad bewegen. Het bewonersfilter doet juist een poging dit soort apparaten eruit te filteren.

De AP blijft verder bij haar standpunt dat identificatie van natuurlijk personen mogelijk is op de drie manieren beschreven in paragraaf 3.1.3. De AP heeft daarbij rekening gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.²⁴ De combinatie (pseudonieme identificator + datumtijd + locatie) maakt het mogelijk om iemand te kunnen identificeren. Niet voor niets beschouwt artikel 4, onderdeel 1, van de AVG locatiegegevens als een identificator.²⁵ Nadat iemand is geïdentificeerd kan men ter controle diegene vragen naar zijn MAC-adres. De AP heeft deze controlevraag als voorbeeld genoemd. Er zijn echter veel manieren om de identiteit van personen te controleren.

Indien Bureau RMC/[VERTROUWELIJK] alle bedoelde technische maatregelen goed hadden uitgevoerd dan was er geen sprake van tracking. De stap om daadwerkelijk te identificeren vergt daardoor onder andere niet disproportioneel veel inspanning volgens de AP. En in sommige gevallen – de nachtelijke wandelaar bijvoorbeeld – vergt identificatie slechts een zeer beperkte inspanning. Uit de verzamelde data zijn leefpatronen te herleiden, waardoor je iemands woon- of werkplek kan achterhalen. De AP verwijst verder naar pagina 12 van dit besluit voor de uitleg waarom realtime identificatie wel degelijk mogelijk was.

Tot slot is niet vereist dat alle informatie aan de hand waarvan de betrokkene kan worden geïdentificeerd, bij een en dezelfde persoon berust.²⁶ Hierbij is van belang dat het college B&W Enschede rechtmatig toegang heeft tot alle middelen die kunnen worden gebruikt om een natuurlijk persoon direct of indirect te

²⁴ Overweging 26 AVG.

²⁵ Zie voor een verdere verdieping ook <https://www.nature.com/articles/srep01376>

²⁶ HvJ EU, 19 oktober 2016, ECLI:EU:C:2016:779, r.o. 43.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

identificeren. Dat het college B&W Enschede contractueel heeft afgesproken om gegevens te kunnen opvragen bij Bureau RMC en [VERTROUWELIJK], geeft het college bij uitstek een rechtmatige toegang tot de persoonsgegevens. Dat het college B&W Enschede daar geen gebruik van (wil) maken is juridisch irrelevant.

3.2 Verwerkingsverantwoordelijke

3.2.1 Inleiding

In het kader van de vraag of het college B&W Enschede de persoonsgegevens in lijn verwerkt met artikel 5, eerste lid, aanhef en onder a jo. artikel 6, eerste lid, van de AVG is ook van belang om te bepalen wie aan te merken is als verwerkingsverantwoordelijke als bedoeld in artikel 4, onderdeel 7, van de AVG. Daarbij is bepalend wie het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

3.2.2 Feiten

Gezien het omvangrijke onderzoek in deze zaak, verwijst de AP voor de feiten naar het tweede hoofdstuk van bijlage 1 bij dit besluit. Hieronder volgt een korte samenvatting van de feiten, waarna de AP tot een oordeel komt.

Het college B&W Enschede heeft besloten om per 6 september 2017 te starten met 24/7 metingen via sensoren in de binnenstad van Enschede. De opdracht hiervoor is gegund aan City Traffic B.V., thans bureau RMC. Daarnaast heeft de gemeente Enschede op haar website zowel een persbericht als een aantal Q&A's over de wifimetingen geplaatst.

De wifimetingen zijn uitgevoerd met als doel het meten van de effecten van gemeentelijke investeringen in de binnenstad van Enschede met het oog op een verantwoord omgaan met publieke gelden. Daarnaast wijst de gemeente erop dat de metingen inzicht kunnen verschaffen in onderwerpen die van belang zijn voor de invulling van haar publieke taak, zoals de effecten van wegwerkzaamheden, het houden van koopzondagen en marktdagen, binnenstadpromotie, de aantrekkelijkheid van evenementen, de acquisitie van winkels en horeca en het bepalen of en wanneer ingegrepen moet worden in het kader van orde en veiligheid.

Op 26 september 2017 hebben het college B&W Enschede en de voorganger van Bureau RMC een bewerkersovereenkomst gesloten in het kader van de wifimetingen in de binnenstad van Enschede. In deze overeenkomst is bepaald dat het college B&W Enschede verwerkingsverantwoordelijke is voor de verwerking van persoonsgegevens. Verder is bepaald dat de bewerker, Bureau RMC, de gegevens verwerkt ten behoeven van het college B&W Enschede. Bureau RMC verwerkt de gegevens slechts in opdracht van het college B&W Enschede en zal tevens alle redelijke instructies dienaangaande opvolgen. Ten alle tijden worden op verzoek van het college B&W Enschede alle van de gemeente Enschede afkomstige gegevens met betrekking tot de bewerkersovereenkomst aan het college B&W Enschede ter hand gesteld. Bureau RMC mag de werkzaamheden slechts uitbesteden aan derden na voorafgaande schriftelijke toestemming van het college B&W Enschede. En partijen gaan ermee akkoord dat Bureau RMC de data laat verwerken door [VERTROUWELIJK], waarmee Bureau RMC een level service agreement heeft gesloten.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Het college B&W Enschede heeft een sturende rol gehad in het aantal en de locaties van de sensoren die gebruikt worden voor de wifimetingen. Daarnaast heeft het college B&W Enschede naar aanleiding van de publicatie van de AP op 30 november 2018 over wifitracking aan Bureau RMC de opdracht gegeven de wifimetingen in de binnenstad van Enschede tijdelijk te pauzeren. Per 1 januari 2019 heeft Bureau RMC op verzoek van het college B&W Enschede het zogenaamde “anonimiseren op de server” ingevoerd, waarbij de laatste drie karakters van de gepseudonimiseerde MAC-adressen worden afgeknipt. Het college B&W Enschede heeft tot slot op 30 april 2020 aan Bureau RMC de opdracht gegevens om per 1 mei 2020 de sensoren uit te zetten.

3.2.3 Beoordeling

Artikel 4, aanhef en onderdeel 7, van de AVG definieert een verwerkingsverantwoordelijke als een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In dit geval is dat de verwerking van het MAC-adres van het mobiele apparaat, het tijdstip (in seconden) en de datum van de detectie door de sensor en het sensor-ID. Daarbij is niet vereist dat dat de verwerkingsverantwoordelijke de persoonsgegevens onder zich heeft.²⁷

De AP is van oordeel dat het college B&W Enschede verwerkingsverantwoordelijke is voor de verwerking van persoonsgegevens door middel van de wifitellingen in de binnenstad van Enschede, omdat zij degene is die zowel het doel als deels de middelen voor de verwerking heeft vastgesteld. Zij motiveert dit als volgt.

Degene die het doel van de verwerking van de persoonsgegevens vaststelt, is degene die bepaalt *waarom* de verwerking plaatsvindt. Zoals in paragraaf 3.2.2 besproken is het college B&W Enschede degene geweest die besloten heeft om wifimetingen uit te voeren. Daarnaast worden de gegevens verwerkt voor een door het college B&W Enschede bepaald doeleinde, namelijk het meten van de effecten van gemeentelijke investeringen in de binnenstad van Enschede. De andere doeleinden die het college B&W Enschede in haar zienswijze aanhaalt voor de wifimetingen (bijvoorbeeld het meten van de effecten van wegwerkzaamheden, binnenstadpromotie en koopzondag) zijn ook door het college bepaald en zijn bovendien gebaseerd op de Gemeentewet.²⁸ Verder heeft het college B&W Enschede op 30 november 2018 Bureau RMC de verwerking tijdelijk laten pauzeren en op 1 mei 2020 de sensoren laten uitzetten. Het college B&W Enschede is ook degene geweest die met haar collegebesluit bepaald heeft dat er persoonsgegevens verwerkt worden, en degene die dus kan besluiten om daarmee te stoppen. Daarmee heeft het college B&W Enschede zeggenschap over het wel of niet verwerken van de persoonsgegevens. De AP concludeert dat het college B&W Enschede de doeleinden voor de verwerking van persoonsgegevens heeft bepaald.

²⁷ HvJ EU, 5 juni 2018, ECLI:EU:C:2018:388 (Wirtschaftsakademie) en HvJ EU, 29 juli 2019, ECLI:EU:C:2019:269 (Fashion ID).

²⁸ Het college B&W Enschede betoogt in haar zienswijze dat de metingen ook inzicht verschaffen in effecten van wegwerkzaamheden, het houden van koopzondagen en marktdagen, binnenstadpromotie, de aantrekkelijkheid van evenementen, de acquisitie van winkels en horeca en het bepalen of en wanneer ingegrepen moet worden in het kader van orde en veiligheid.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Degene die beslist *hoe* de verwerking plaatsvindt moet worden beschouwd als degene die de middelen vaststelt. Zoals in paragraaf 3.2.2 besproken heeft het college B&W Enschede besloten om voor de verwerking van persoonsgegevens gebruik te maken van een dienstverlener, namelijk Bureau RMC. De technische uitwerking van de verwerking van de persoonsgegevens is gedelegeerd aan Bureau RMC, waarbij het college B&W Enschede op grond van de bewerkersovereenkomst wel de mogelijkheid had om instructies te geven. Het college B&W Enschede heeft ook invloed uitgeoefend op de middelen voor de verwerking door mede te bepalen hoeveel sensoren geplaatst zouden worden en waar deze geplaatst zouden worden. De AP concludeert dat het college B&W Enschede door te bepalen door wie de verwerking uitgevoerd zou worden en tevens de wijze waarop de verwerking plaatsvindt, bijvoorbeeld door het aantal sensoren en de locaties daarvan te bepalen, deels bepaald heeft *hoe* de verwerking van persoonsgegevens plaatsvond.

Op basis van het bovenstaande concludeert de AP dat het college B&W Enschede zowel het doel als deels de middelen voor de verwerkingen heeft vastgesteld en daarmee kwalificeert als verwerkingsverantwoordelijke in de zin van artikel 4, aanhef en onderdeel 7, van de AVG voor de verwerking van persoonsgegevens via sensoren in de binnenstad van Enschede.

3.2.4 Zienswijze college B&W Enschede en reactie AP

Het college B&W betoogt in haar zienswijze dat zij géén verwerkingsverantwoordelijke in de zin van de AVG is. Zij maakt daarbij onderscheid tussen haar verantwoordelijkheid als opdrachtgever, die ze niet betwist, en het begrip verwerkingsverantwoordelijke als omschreven in de AVG. Hoewel het college B&W Enschede zichzelf als verwerkingsverantwoordelijke aanwijst in de bewerkersovereenkomst zijn er volgens haar feitelijke omstandigheden die erop duiden dat zij geen, dan wel slechts gezamenlijk verwerkingsverantwoordelijke is. Zo worden de werking van de wifitellingentechniek, de wijze waarop de gegevens worden verzameld, welke gegevens er precies worden verzameld voor de gewenste output, de keuze voor hashing en truncating, de opslag en de (al dan niet in overleg) bewaartermijn bepaald door Bureau RMC. Ook heeft het college B&W Enschede geen toegang tot de gegevens en geen zeggenschap over het feit dat Bureau RMC gegevens aan derden verstrekt of zelfs verkoopt. Ook voert het college B&W Enschede aan dat zij niet de kaders en/of voorwaarden voorschrijft waarbinnen de gegevens worden verwerkt. Verder geeft Bureau RMC in artikel 1.1 van haar Privacy Protocol CityTraffic aan dat zij zelf verwerkingsverantwoordelijke is.

De AP heeft kennis genomen van het betoog van het college B&W Enschede, maar volgt dit niet. Hieronder zal eerst worden toegelicht waarom de AP van oordeel is dat het college B&W Enschede wel de verwerkingsverantwoordelijke is. Vervolgens zal de AP bespreken waarom er geen sprake is van gezamenlijke verwerkingsverantwoordelijkheid.

Verwerkingsverantwoordelijkheid

De feitelijke omstandigheden waar het college naar verwijst zien allemaal op de middelen voor de verwerking. Het gaat er daarbij immers om *hoe* de verwerking plaatsvindt. Hoewel Bureau RMC invloed heeft op de wijze van verwerking, is het College B&W Enschede degene die ervoor gekozen heeft om van de door Bureau RMC aangeboden diensten gebruik te maken, degene die bepaald heeft hoeveel sensoren er



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

geplaats zouden worden en waar deze geplaatst zouden worden. Hiermee heeft de gemeente (ook) bepaald welke middelen er worden gebruikt voor de verwerking.

Dat de gemeente geen toegang zou hebben tot de gegevens die Bureau RMC verwerkt betekent volgens de AP niet dat zij geen verwerkingsverantwoordelijke in de zin van de AVG kan zijn. Het Hof van Justitie van de Europese Unie (HvJ EU) heeft bepaald dat het niet vereist dat alle informatie aan de hand waarvan de betrokkene kan worden geïdentificeerd, bij een en dezelfde persoon berust.²⁹

Het college B&W Enschede wijst er verder op dat Bureau RMC kan bepalen de gegevens aan een derde partij te verkopen. De AP maakt hierbij een onderscheid tussen verschillende verwerkingen. Allereerst is er de verwerking van persoonsgegevens door Bureau RMC voor het doeleinde van het college B&W Enschede, namelijk het meten van de effecten van gemeentelijke investering in de binnenstad. Dit is de verwerking waar het onderzoek op ziet en waar de AP het college voor als verwerkingsverantwoordelijke kwalificeert. Deze verantwoordelijkheid is beperkt tot de verwerkingen waarvoor het college B&W Enschede het doel en deels de middelen vaststelt. Daarnaast is er de mogelijke verwerking waarbij Bureau RMC andere partijen toegang kan geven tot de informatie die zij ook gebruikt voor het aanleveren van de gegevens aan het college B&W Enschede. Bureau RMC heeft deze mogelijk omdat in de bewerkersovereenkomst bepaald is dat Bureau RMC recht heeft op een afslagbestand (ontdaan van persoonsgegevens), een kopie van de data die gebruikt kan worden voor eenieder die een aanvraag doet over bijvoorbeeld drukte op een bepaalde plek in de binnenstad van Enschede. In die tweede situatie is er sprake van een verwerking die buiten de doeleinden van het college B&W Enschede valt, en daarmee ook buiten haar verantwoordelijkheid als verwerkingsverantwoordelijke. Dat het college B&W Enschede voor deze andere, tweede verwerking geen verwerkingsverantwoordelijke is doet niet af aan de conclusie dat het college B&W Enschede nog steeds degene is die voor de eerste verwerking het doel en deels de middelen bepaald en daarom daarvoor kwalificeert als verwerkingsverantwoordelijke.

Het college B&W Enschede voert verder aan dat zij niet de kaders en/of voorwaarden voorschrijft waarbinnen de gegevens worden verwerkt. De AP volgt dit betoog niet. In de bewerkersovereenkomst is bepaald Bureau RMC alle redelijke instructies van de het college B&W Enschede zal opvolgen. Bureau RMC heeft dit reeds gedaan door twee maal op verzoek van het college B&W de verwerking te staken. De AP concludeert hieruit dat het college, indien gewenst, wel de kaders en/of voorwaarden waarbinnen de gegevens worden verwerkt kan bepalen. Dat de gemeente niet altijd gebruik heeft gemaakt van deze mogelijkheid, of dat niet van plan is, doet niet af aan het bestaan daarvan.

Tot slot voert het college aan dat in het Privacy Protocol van CityTraffic is bepaald dat Bureau RMC verwerkingsverantwoordelijke is. De AP volgt ook dit betoog niet. Allereerst staat in paragraaf 1.1 van het Privacy Protocol dat CityTraffic de verantwoordelijke is, voor zover zij (alleen of gezamenlijk met anderen) de doeleinden en de middelen van de verwerking van MAC-adressen bepaalt. Dat betekent volgens de AP niet dat Bureau RMC in elk geval de verwerkingsverantwoordelijke is. Voorts hebben Bureau RMC en het college B&W Enschede in de tussen hen gesloten bewerkersovereenkomst vastgelegd dat juist het college B&W Enschede de verwerkingsverantwoordelijke is. Nu de bewerkersovereenkomst de tussen partijen

²⁹ HvJ EU, 19 oktober 2016, ECLI:EU:C:2016:779, r.o. 43.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

gesloten overeenkomst is, in tegenstelling tot het privacy protocol van Bureau RMC, moet aansluiting gezocht worden bij deze bewerkersovereenkomst. Daarnaast is het college B&W Enschede degene die feitelijk de doeleinden en deels de middelen voor de verwerking bepaalt. In een dergelijke situatie, waarbij de feitelijke situatie afwijkt van een “papieren” werkelijkheid, zoals het privacy protocol, is de feitelijke situatie leidend.

Gezamenlijke verwerkingsverantwoordelijkheid

Het college van B&W betoogt dat, indien de AP van oordeel is dat het college verwerkingsverantwoordelijke is, dat er dan slechts sprake is van gezamenlijke verwerkingsverantwoordelijkheid. De AP volgt dit betoog niet en motiveert dat als volgt.

Artikel 26 van de AVG bepaalt dat wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zij gezamenlijk verwerkingsverantwoordelijken zijn. In artikel 4, aanhef en onderdeel 7, van de AVG, is ook bepaald dat de verwerkingsverantwoordelijke degene is die, alleen of samen met anderen, het doel en de middelen van de verwerking bepaalt. In beide artikelen is bepaald dat de (gezamenlijke) verwerkingsverantwoordelijke het doel *en* de middelen voor de verwerking bepaalt. Uit de door het college B&W Enschede aangehaalde feitelijke omstandigheden blijkt dat Bureau RMC een mate van invloed heeft op de middelen voor de verwerking. Echter, niet is gebleken dat Bureau RMC de doeleinden bepaalt voor de verwerking van persoonsgegevens voor het college B&W Enschede. Nu Bureau RMC de doeleinden voor de verwerking niet bepaald kan zij daarvoor geen verwerkingsverantwoordelijke zijn. Hierdoor kan er ook geen sprake zijn van gezamenlijke verwerkingsverantwoordelijkheid. Dat Bureau RMC deels invloed heeft op het bepalen van de middelen voor de verwerking maakt dit niet anders, omdat de (gezamenlijk) verwerkingsverantwoordelijke doel *en* middelen van de verwerking moet bepalen.

3.3 Rechtmatigheid van de verwerking

3.3.1 Inleiding

In paragraaf 3.2 heeft de AP geconstateerd dat het college B&W Enschede de verwerkingsverantwoordelijke is voor de verwerkingen in het kader van de wifimetingen. De AP zal in het navolgende beoordelen of het college B&W Enschede voor deze verwerking een succesvol beroep kan doen op één van de grondslagen uit artikel 6 van de AVG.

3.3.2 Beoordeling en reactie op zienswijze

Artikel 5, eerste lid, aanhef en onder a, van de AVG bepaalt onder andere dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig is. Er wordt gehandeld in overeenstemming met dit beginsel van rechtmatigheid, indien er een deugdelijke rechtsgrondslag voor de verwerking aanwezig is.

Artikel 6, eerste lid, van de AVG geeft vervolgens een limitatieve opsomming van de grondslagen voor een rechtmatige gegevensverwerking. Dit artikel stelt dat een verwerking alleen rechtmatig is indien en voor zover aan ten minste een van de zes genoemde grondslagen is voldaan. De voor het college B&W Enschede



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

eventueel in aanmerking komende grondslagen zijn:³⁰ c) noodzakelijk om te voldoen aan een wettelijke verplichting; e) noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag; f) gerechtvaardigd belang.

3.3.2.1 Wettelijke taak of taak van algemeen belang

Artikel 6, derde lid, van de AVG bepaalt dat de verwerkingen van persoonsgegevens die plaatsvinden op de rechtsgronden c) en e) moeten zijn vastgesteld bij Unierecht of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is. Het doel van de verwerking moet in het Unierecht of lidstatelijk recht zijn vastgesteld, of is voor wat betreft rechtsgrond e) noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend.

Overweging 45 van de AVG luidt: *“Deze verordening schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is. Er kan worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen op grond van een wettelijke verplichting die op de verwerkingsverantwoordelijke rust, of voor verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang dan wel voor een taak in het kader van de uitoefening van het openbaar gezag. (...)”*

Overweging 41 van de AVG stelt wel dat de wetgeving op basis waarvan de verwerkingen plaatsvinden voldoende duidelijk, nauwkeurig en voorspelbaar moet zijn: *“Deze rechtsgrond of wetgevingsmaatregel moet evenwel duidelijk en nauwkeurig zijn, en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is, zoals vereist door de rechtspraak van het Hof van Justitie van de Europese Unie („Hof van Justitie”) en het Europees Hof voor de Rechten van de Mens.”*

De grondslagen c) en e) vereisen alle twee dat de verwerking noodzakelijk is. Dit noodzakelijkheidsvereiste betekent dat moet worden voldaan aan de beginselen van proportionaliteit en subsidiariteit. Het proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de bij de verwerking van de persoonsgegevens betrokken personen niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Op grond van het subsidiariteitsbeginsel mag het doel waarvoor de persoonsgegevens worden verstrekt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokken persoon, minder nadelige wijze kunnen worden verwezenlijkt.

Het college B&W Enschede stelt in haar zienswijze dat de verwerkingen in het kader van wifitellingen kunnen worden gebaseerd op artikel 6, lid 1 sub e, van de AVG. De AP miskent volgens het college dat de gemeente Enschede een zeer brede taak heeft. Uit de Gemeentewet volgt dat de gemeente het ‘dagelijks bestuur’ van de gemeente moet voeren. Deze taak is volgens het college niet zomaar ruim geformuleerd, maar juist met een doordachte reden. In de ogen van de gemeente blijken haar verantwoordelijkheden, en in het verlengde daarvan de noodzaak tot het uitvoeren van de wifitellingen om aan die verschillende verantwoordelijkheden te voldoen, uit diverse (formele en materiële) wet- en regelgeving en documenten.

³⁰ In onderhavige situatie is er geen toestemming gevraagd aan de betrokkenen (grond a), de wifitellingen zijn niet noodzakelijk ter uitvoering van een overeenkomst met de betrokkene (grond b) en ze zijn ook niet noodzakelijk om bepaalde vitale belangen te beschermen (grond d).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Het college B&W Enschede verwijst hiervoor naar artikel 160 lid 1 sub a en h, artikel 212 lid 1, artikel 213 lid 1, artikel 172 lid 1 van de Gemeentewet. En naar de retailagenda van de landelijke overheid, Visie bruisende binnenstad en de mobiliteitsvisie, de APV van Enschede, het toetsingskader evenementenvergunningen, de nadere regels voor terrassen, de gemeentebegroting en de subsidieverordening.

Met passantentellingen kan volgens het college B&W Enschede inzicht worden verkregen in diverse aspecten die voor gemeenten van belang zijn om haar beleid op diverse vlakken te kunnen baseren en derhalve om invulling te geven aan de 'publieke taak' die zij als gemeente jegens haar inwoners heeft. Deze informatie is volgens het college pas echt waardevol als het "continue" informatie is, dat wil zeggen niet uitsluitend informatie die is gebaseerd op incidentele gebeurtenissen. In de ogen van de gemeente is de gekozen wijze van tellen juist privacy-vriendelijker dan bijvoorbeeld handmatige tellingen. Handmatige tellingen kent veel nadelen: dubbeltellingen kunnen niet worden voorkomen, en dus geven handmatige tellingen geen betrouwbaar beeld. Bovendien is dit zeer arbeidsintensief en dus kostbaar. In het laatste geval ziet de teller immers per definitie welke persoon zich waar bevindt. Andere alternatieven voor tellingen dan via wifi zijn eigenlijk niet voorhanden. Er bestaan wel infraroodtellingen, maar ook deze methode haalt geen dubbeltellingen uit de tellingen.

De AP heeft aan het college B&W Enschede gevraagd of het voor de gemeentelijke taken noodzakelijk is om bezoekersstromen of het aantal bezoekers per (meet)punt te weten. Het college B&W Enschede heeft hierover het volgende verklaard. Bij de start van de passantentellingen leefde het college B&W Enschede nog in de veronderstelling – op basis van informatie die het college op dat moment verkreeg van Bureau RMC – dat Bureau RMC anonieme informatie over bezoekersstromen zou verstrekken. De term "bezoekersstromen" stond ook vermeld in het collegebesluit om over te stappen op de bezoekerstellingen via wifi. Dit verklaart volgens het college B&W Enschede waarom er in de zienswijze van het college soms over bezoekersstromen wordt gesproken. Na de start van de bezoekerstellingen en de eerste resultaten van de teldata (rond begin 2018), bleek echter dat het college geen stromen kon zien, maar wel drukte per sensorpunt. Het college B&W Enschede heeft dus verklaard alleen het aantal passanten op een bepaald punt en moment nodig te hebben.³¹

De AP volgt de zienswijze van het college van B&W Enschede niet en komt tot de volgende beoordeling. De AP constateert allereerst dat er op het college B&W Enschede geen wettelijke verplichting rust, vastgelegd in Unierecht of nationaal recht, om de wifimetingen in de binnenstad te laten verrichten. Ook vindt de verwerking van persoonsgegevens geen basis in een ruimer geformuleerde zorgplicht of wettelijke verplichting. De AP stelt daarom ten eerste vast dat het college B&W Enschede geen geslaagd beroep kan doen op de grondslag in artikel 6, eerste lid onder c, van de AVG.

De AP onderzoekt hierna of de wifimetingen verwerkingen zouden kunnen zijn die noodzakelijk zijn voor een taak van algemeen belang. De AP heeft reeds geconcludeerd dat de wifimetingen verwerkingen zijn in het kader van de gemeentelijke overheidstaken. Overheidstaken zijn taken van algemeen belang. Zo is het college B&W Enschede op grond van artikel 160 Gemeentewet bevoegd om 'het dagelijks bestuur van de

³¹ Brief van 16 februari 2021 van het college B&W Enschede aan de AP, pagina 2.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

gemeente te voeren'. Dit betreft een taak van algemeen belang, waar bijvoorbeeld het op orde houden van de financiën van de gemeente, ruimtelijke ordening en stedelijke ontwikkeling onder kunnen worden geschaard.

De AP constateert dat overweging 45 van de AVG stelt dat niet voor elke afzonderlijke verwerking specifieke wetgeving nodig is. In onderhavig geval betekent dit dat de verscheidene verwerkingen die zijn vastgesteld gebaseerd kunnen worden op één wettelijke bepaling. Overweging 41 van de AVG vereist echter wel een zekere mate van concreetheid van de wetgeving. Deze overweging stelt namelijk dat de wetgeving, in dit geval de taak van algemeen belang, duidelijk, nauwkeurig en voorspelbaar moet zijn.³² Deze voorzienbaarheidseis brengt onder meer mee dat de (wettelijke) gevolgen van bepaalde handelingen in een bepaalde mate voorzienbaar moeten zijn voor de burger.

Uit de eis dat een inmenging in de uitoefening van het recht op respect voor het privéleven als bedoeld in artikel 8 van het EVRM moet zijn voorzien bij wet («in accordance with the law») vloeit voort dat die inmenging moet berusten op een naar behoren bekendgemaakt wettelijk voorschrift waaruit de burger met voldoende precisie kan opmaken welke op zijn privéleven betrekking hebbende gegevens met het oog op de vervulling van een bepaalde overheidsstaak kunnen worden verzameld en vastgelegd, en onder welke voorwaarden die gegevens met dat doel kunnen worden bewerkt, bewaard en gebruikt. Vereist is dus een voldoende precieze wettelijke grondslag. Dat betekent dat bijvoorbeeld de algemene taakstelling van een overheidsdienst niet in alle gevallen kan dienen als rechtsgrond voor gegevensverwerking.³³ Het betekent ook dat een verplichting voor een overheidsinstantie tot gegevensverstrekking terwijl die overheidsinstantie een wettelijk geregelde geheimhoudingsplicht heeft, uitdrukkelijk en duidelijk in een wettelijk voorschrift moet zijn neergelegd, en dat het niet toelaatbaar is dat een dergelijke verplichting uitsluitend wordt afgeleid uit de totstandkomingsgeschiedenis van of de samenhang tussen wettelijke bepalingen of wordt verondersteld omwille van de effectiviteit van een wettelijke regeling.³⁴

De AP komt tot het oordeel dat de wettelijke taak 'het dagelijks bestuur van de gemeente voeren' niet aan bovenstaande eisen voldoet, omdat deze taak te ruim is geformuleerd, niet concreet is en daarmee niet voldoende voorspelbaar is.³⁵ Een burger kan onvoldoende uit artikel 160 Gemeentewet opmaken welke op zijn privéleven betrekking hebbende gegevens met het oog op de vervulling van deze overheidsstaak kunnen worden verzameld en vastgelegd, en onder welke voorwaarden die gegevens met dat doel kunnen worden bewerkt, bewaard en gebruikt. De AP is er daarbij van bewust dat de wetgever artikel 160 Gemeentewet doelbewust ruim heeft geformuleerd. Alleen dit heeft tot gevolg dat deze ruim geformuleerde taakomschrijving (omwille van de effectiviteit van een wettelijke regeling) niet zonder meer kan dienen als rechtsgrond voor deze gegevensverwerking.

³² Zie in dit kader ook ECLI:NL:RBROT:2020:2257.

³³ Zie ook HR 24 februari 2017, ECLI:NL:HR:2017:288 (Belastingdienst ANPR zaak)

³⁴ ABRvS 3 februari 2016, ECLI:NL:RVS:2016:253

³⁵ De wetgever heeft expliciet gekozen voor het ruim geformuleerde begrip 'dagelijks bestuur' en niet voor meer uitgewerkte taken omdat 'zo een opsomming bijna per definitie gedoemd [is] niet sluitend te zijn'. *Kamerstukken II 2000/01, 27 751, nr. 3, p. 61.*



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Het college B&W Enschede verwijst verder in haar zienswijze naar verschillende artikelen in de Gemeentewet, de APV en meerdere documenten. De AP merkt op dat alleen artikel 160 Gemeentewet de bevoegdheid van het college B&W Enschede regelt. De andere artikelen zien op bevoegdheden van andere organen van de gemeente. Het college van B&W is door de AP aangewezen als verwerkingsverantwoordelijke, waardoor de andere wetsartikelen om die reden niet van toepassing kunnen zijn als lidstatelijk recht waarin de taak van algemeen belang *aan de verwerkingsverantwoordelijke opgedragen* is geregeld.

De AP heeft voorts de gehele APV van Enschede doorgenomen, maar de AP kwam hier geen artikelen tegen waar een burger uit kan afleiden dat de genoemde persoonsgegevens in paragraaf 3.1 kunnen worden verwerkt voor overheidstaken en onder welke voorwaarden die gegevens met dat doel kunnen worden bewerkt, bewaard en gebruikt. De overige aangehaalde documenten door het college B&W Enschede kunnen tot slot ook geen grondslag zijn voor de verwerking van persoonsgegevens omdat dit geen wettelijke voorschriften zijn.

De AP stelt daarom vast dat het college B&W Enschede in dit geval geen geslaagd beroep kan doen op de grondslag in artikel 6, eerste lid onder e, van de AVG. Hiermee wil de AP niet zeggen dat een gemeente nooit een wettelijke grondslag kan hebben voor het tellen van bezoekers. Het wettelijk voorschrift dient echter voor deze situatie concreter geformuleerd en daarmee voldoende voorspelbaar te zijn.

Ten overvloede, de AP blijft ook bij haar standpunt dat in onderhavige situatie ook niet is voldaan aan het noodzakelijkheidsvereiste omdat niet is voldaan aan de beginselen van proportionaliteit en subsidiariteit. De inbreuk op de privacy van honderdduizenden burgers wiens MAC-adressen en locatiegegevens via de sensoren zijn opgevangen en verwerkt is onevenredig in verhouding tot het met de verwerking te dienen doel, namelijk het toetsen van de effectiviteit van investeringen in de binnenstad van Enschede. In deze beoordeling neemt de AP in aanmerking dat het recht op bescherming van de persoonlijke levenssfeer van burgers in de openbare ruimte zwaar weegt, gelet op de redelijke verwachting van het publiek om als voorbijganger niet ongemerkt gevolgd te kunnen worden en het feit dat gegevens systematisch en voor langere tijd vastgelegd werden. Met name voor bewoners en frequente bezoekers van de gemeente Enschede is de voorliggende verwerking van persoonsgegevens een extra grote inbreuk op de bescherming van de persoonlijke levenssfeer. Dat het college B&W Enschede niet tot doel had om persoonsgegevens te verwerken doet niet af aan het feit dat er persoonsgegevens onder de verantwoordelijkheid van het college werden verwerkt. Dit doet afbreuk aan het gevoel van de burger om zich in het openbaar onbespied te wanen en om vertrouwen te hebben in de overheid.

Daarnaast is ook niet voldaan aan het subsidiariteitsbeginsel omdat de nagestreefde doelen van het college B&W Enschede op een andere, minder vergaande wijze, kunnen worden gediend. Zelfs op manieren waarbij geen persoonsgegevens worden verwerkt. Het college B&W Enschede heeft, of het nu bedoeld of onbedoeld was, onder diens verantwoordelijkheid persoonsgegevens laten verwerken waarmee het mogelijk was om burgers te volgen. Het college B&W Enschede heeft echter verklaard dat het geen bezoekersstromen nodig heeft maar alleen de drukte per sensorpunt. Hierdoor was de verwerking van persoonsgegevens onder de verantwoordelijkheid van het college B&W Enschede tussen 25 mei 2018 tot



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

en met 30 april 2020 niet noodzakelijke en daarnaast ook bovenmatig. Naast het feit dat er in de gehanteerde database onvoldoende technische maatregelen zijn genomen, werden de persoonsgegevens ook onnodig (nog los van de ruwe data) steeds een half jaar bewaard.

Er zijn voldoende methodes om de drukte op een bepaalde plek te meten waarbij de bescherming van persoonsgegevens beter is gewaarborgd. Men kan bijvoorbeeld inzicht krijgen in drukte door marktonderzoeken. Maar ook personen tellen via een automatische bezoekersteller die een infraroodstraal uitzendt is bij uitstek een effectieve techniek. Deze techniek is ook betaalbaar en geeft de mogelijkheid om de continue informatie te verschaffen die het college B&W Enschede nodig heeft. Dubbeltellingen kan men met statistisch berekeningen eruit filteren. Vrijwel iedere ingezette methodiek of techniek kent meetfouten en vergt kalibratie, vaak ook op het niveau van individuele sensoren. Hiermee kan men de eventuele meetfouten in de tellingen corrigeren. Daarnaast is een kleine meetfout, voor zover deze na kalibratie nog zou bestaan, gezien het feit dat men uiteindelijk getallen totaliseert en groepeerd, niet onoverkomelijk.

3.3.2.2. Gerechtvaardigd belang

Het eerste lid van artikel 6 van de AVG bepaalt dat grondslag f) gerechtvaardigd belang niet geldt voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken. Overweging (47) van de AVG geeft hierop de volgende toelichting: “(...) *Aangezien het aan de wetgever staat om de rechtsgrond voor persoonsgegevensverwerking door overheidsinstanties te creëren, mag die rechtsgrond niet van toepassing zijn op de verwerking door overheidsinstanties in het kader van de uitvoering van hun taken.*”

Overheidsinstanties zullen in de uitoefening van hun taak geen gebruik kunnen maken van de grondslag ‘gerechtvaardigd belang’, maar zullen gebruik moeten maken van andere grondslagen. Dit geldt niet voor zover de overheidsinstantie ‘typisch bedrijfsmatige handelingen’ verricht waarbij persoonsgegevens worden verwerkt, zoals bijvoorbeeld de verwerking van persoonsgegevens die noodzakelijk is voor de beveiliging van overheidsgebouwen. Voor handelingen die buiten de uitoefening van de taak vallen, mag er wel een grondslag worden aangenomen in het gerechtvaardigd belang van de organisatie. De overheid onderscheidt zich hierin niet wezenlijk van een private partij.

Artikel 6, eerste lid, van de AVG bepaald dus dat grondslag f) niet geldt voor ‘verwerkingen door overheidsinstanties in het kader van de uitoefening van hun taken’. Dit geldt niet voor zover de overheidsinstantie ‘typisch bedrijfsmatige handelingen’ verricht. De AP heeft hiervoor al vastgesteld dat het doel van de wifimetingen het toetsen van de effectiviteit van gemeentelijke investeringen in de binnenstad van Enschede is, dit met het oog op het verantwoord omgaan met publieke gelden. De AP concludeert hieruit dat de wifimetingen verwerkingen zijn in het kader van de gemeentelijke overheidsstaken. De AP stelt daarom vast dat het college B&W Enschede geen beroep kan doen op de grondslag gerechtvaardigd belang in de zin van artikel 6, eerste lid onder f, van de AVG. Het is aan de wetgever om voor dit soort gevallen de rechtsgrond voor persoonsgegevensverwerking door overheidsinstanties te creëren.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Het college B&W Enschede is in haar zienswijze echter van mening dat het verzamelen van informatie over bezoekersaantallen en bezoekersstromen in het kader van wifitellingen een gerechtvaardigd belang is voor het college B&W Enschede, de ondernemers, investeerders, bezoekers en inwoners. De AP heeft volgens het college B&W Enschede in de Bluetrace-zaak erkend dat er sprake kan zijn van een gerechtvaardigd belang voor het verzamelen van dergelijke informatie.³⁶

Voorts stelt het college B&W Enschede dat met de verwerkingen in het kader van wifitellingen wél is voldaan aan het noodzakelijkheidsvereiste. De wifitellingen zijn namelijk noodzakelijk om de hiervoor beschreven belangen die worden nagestreefd te verwerkelijken. Het is niet mogelijk om deze informatie op een minder ingrijpende wijze te verzamelen. Met wifitellingen kunnen er volgens het college B&W Enschede veel duurzamere, efficiëntere en betrouwbaardere resultaten worden verzameld. Daar komt volgens het college B&W Enschede bij dat Bureau RMC allerlei maatregelen heeft getroffen die met zich meebrengen dat aan het vereiste van proportionaliteit en subsidiariteit wordt voldaan. Zoals eerder in deze zienswijze beschreven is het college B&W Enschede hierbij steeds afgegaan op de deskundigheid van Bureau RMC als professioneel opdrachtnemer. Verder informeert de gemeente Enschede iedereen, die de binnenstad van Enschede betreft, actief middels waarschuwingborden over de wifitellingen. De betrokkenen worden eveneens via de website van de gemeente Enschede hierover geïnformeerd.

Tot slot stel het college B&W Enschede dat Bureau RMC omstreeks 2016 reeds heeft gecorrespondeerd met de AP over haar werkwijze in het kader van wifitellingen. In dat kader heeft Bureau RMC de door de AP verstrekte aanwijzingen opgevolgd. Bureau RMC kon in dat verband – mede doordat de AP nadien niets meer van zich heeft laten horen – ervan uitgaan dat haar werkwijze in overeenstemming is met de privacywet- en regelgeving en bovendien is goedgevonden door de AP.

De AP volgt de zienswijze van het college van B&W Enschede niet en blijft bij haar standpunt dat het college B&W Enschede geen succesvol beroep kan doen op de grondslag gerechtvaardigd belang. Het college B&W Enschede heeft immers zelf uitgebreid uitgelegd dat de verwerkingen in het kader van wifitellingen noodzakelijk zijn voor de gemeentelijke overheidstaken en niet voor ‘*typisch bedrijfsmatige handelingen*’. Het feit dat het college B&W Enschede hierboven zelf naar haar wettelijke taken heeft verwezen onderstreept deze beoordeling des te meer. De AP komt hierdoor niet toe aan een belangenafweging onder artikel 6, eerste lid onder f, van de AVG. En voor wat betreft de Bluetrace-zaak, het gaat het in die zaak om een bedrijf en niet een overheidsinstantie waardoor de vergelijking door het college B&W Enschede niet opgaat.

De AP merkt tot slot op dat zij wel degelijk het onderzoek naar Bureau RMC heeft afgesloten met een formele brief. In deze brief heeft de AP nadrukkelijk vermeld dat de AP geen oordeel geeft over de gegevensverwerking waar het onderzoek betrekking op had. De stelling van het college B&W Enschede dat Bureau RMC er hierdoor vanuit kon gaan dat haar werkwijze in overeenstemming is met de privacywet- en regelgeving en bovendien is goedgevonden door de AP acht de AP dus onjuist.

³⁶ CBP, *Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace*, z2014-00944, 13 oktober 2015, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapport_db_bluetrace.pdf, p. 40.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

4. Boete

4.1 Inleiding

Het college B&W Enschede heeft van 25 mei 2018 tot en met 30 april 2020 in strijd gehandeld met artikel 5, eerste lid, onder a, jo. artikel 6, eerste lid, van de AVG door persoonsgegevens van eigenaren/gebruikers van mobiele apparaten waarop de wifi staat ingeschakeld in de binnenstad van Enschede onrechtmatig te verwerken.

De AP maakt voor de vastgestelde overtreding gebruik van haar bevoegdheid om aan het college B&W Enschede een boete op te leggen. De AP hanteert hiervoor de Boetebeleidsregels 2019.³⁷ Hierna zal de AP eerst kort de boetesystematiek uiteenzetten, gevolgd door de motivering van de boete (hoogte) in het onderhavige geval.

4.2 Boetebeleidsregels Autoriteit Persoonsgegevens 2019

Op grond van artikel 58, tweede lid, aanhef en onder i en artikel 83, vijfde lid, van de AVG, gelezen in samenhang met artikel 14, derde lid, jo. 18 van de UAVG, is de AP bevoegd aan het college B&W Enschede in geval van een overtreding van artikel 5 en 6 van de AVG een bestuurlijke boete op te leggen tot € 20.000.000. De boete voor de onderhavige overtreding van artikel 5, eerste lid, onder a van de AVG is afhankelijk gesteld van de onderliggende bepaling, zijnde artikel 6, eerste lid, van de AVG. Hiervoor geldt een categorie III boete, met een boetebandbreedte tussen € 300.000 en € 750.000 en een basisboete van € 525.000. [...].³⁸

Ingevolge artikel 7 houdt de AP onverminderd de artikelen 3:4 en 5:46 van de Algemene wet bestuursrecht (Awb) rekening met de factoren die zijn ontleend aan artikel 83, tweede lid, van de AVG en in de Beleidsregels genoemd onder a tot en met k.

4.3 Boetehoogte

4.3.1. Beoordeling omstandigheden

Bij de vraag of een bestuurlijke boete wordt opgelegd en over de hoogte daarvan houdt de AP rekening met verschillende factoren. De AP betreft bij deze beoordeling onder meer de aard, de omvang alsmede het aantal getroffen betrokkenen.

Rechtmatigheid is een van de basisbeginselen van de gegevensbescherming. Een verwerking van persoonsgegevens is rechtmatig als deze plaatsvindt op basis van een grondslag. Bij een inmenging op het privéleven van de burger zoals in het onderhavige geval, is in het bijzonder belangrijk dat een

³⁷ Stcrt. 2019, 14586, 14 maart 2019.

³⁸ Artikel 2, onder 2.2 en 2.3 van de Boetebeleidsregels jo. bijlage 2 van de Boetebeleidsregels 2019.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

overheidsinstantie haar handelen kan baseren op een voldoende toegankelijk, nauwkeurig en voorzienbaar wettelijk voorschrift. Met het verzamelen van persoonsgegevens zonder daarvoor een grondslag te hebben, heeft het college B&W Enschede het rechtmatigheidsbeginsel geschonden. Dit raakt de kern van het recht op de eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens. Het doet afbreuk aan het gevoel van de burger om zich in het openbaar onbespied te wanen en aan het vertrouwen in de overheid.

Het college B&W Enschede heeft van 25 mei 2018 tot en met 30 april 2020 zonder grondslag persoonsgegevens verwerkt van honderdduizenden burgers. Deze overtreding vond daarmee op structurele wijze plaats en duurde voor een lange periode voort. Uit de verzamelde data die onder verantwoordelijkheid van het college B&W Enschede werd verwerkt, kan men een gedetailleerd beeld opmaken van het gedrag van (individuele) burgers. De leefpatronen kunnen bijvoorbeeld iemands woon- of werkplek prijsgeven, maar ook gevoeligere gegevens zoals bezoeken aan medische instellingen of locaties die gegevens over iemands seksleven kunnen opleveren.³⁹ Het enkele feit dat dit mogelijk is kan ertoe leiden dat burgers zich niet langer onbespied wanen door de overheid. Gelet hierop was er volgens de AP sprake van een ernstige situatie.

Naast het feit dat het college B&W Enschede niet op basis van een voorzienbaar wettelijk voorschrift persoonsgegevens verwerkte, acht de AP het ook kwalijk dat het college B&W Enschede de persoonsgegevens bovenmatig en langer heeft verwerkt dan noodzakelijk was voor de beoogde doeleinden. Als een verwerkingsverantwoordelijke locatiegegevens verwerkt of laat verwerken dan dient men de grootst mogelijke zorgvuldigheid in acht te nemen om te voorkomen dat deze gegevens (indirect) identificeerbaar worden.

Gezien de bovenstaande omstandigheden ziet de AP aanleiding om aan het college B&W Enschede een boete op te leggen en het basisbedrag van de boete op grond van artikel 7, aanhef en onder a, van de Boetebeleidsregels 2019 te verhogen met € 75.000 tot € 600.000.

Zienswijze college B&W Enschede en reactie AP

Het college B&W Enschede stelt in haar zienswijze dat er nimmer bijzondere en strafrechtelijke persoonsgegevens zijn verwerkt. Gezien de zeer beperkte aard en ernst van de vermeende inbreuk op de AVG, meent het college B&W Enschede dan ook dat er sprake is van een boeteverlagende omstandigheid. Daar komt volgens het college bij dat de betrokkenen geen schade hebben geleden. Verder is de gemeente Enschede nog nooit eerder door de AP op haar vingers getikt vanwege een schending van de privacywet- en regelgeving en heeft de gemeente Enschede steeds haar volledige medewerking verleend aan het onderzoek van de AP. Het college B&W Enschede beschouwt deze omstandigheden dan ook als boeteverlagende factoren.

De AP volgt de zienswijze van het college van B&W Enschede niet en motiveert dit als volgt. Zoals hierboven vermeld kunnen er uit de verzamelde data gevoelige gegevens worden afgeleid. Een overheidsinstantie die persoonsgegevens verwerkt zonder daar een wettelijke grondslag voor te hebben is

³⁹ Zie ook WP202 Opinion 02/2013 on apps on smart devices.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

zeker wel schadelijk voor burgers. Het college B&W Enschede heeft daarnaast niet onderbouwd waarom de betrokkenen geen schade hebben geleden. Ondanks dat de AP niet eerder dezelfde inbreuk heeft vastgesteld bij het college B&W Enschede en er volgens het college B&W Enschede geen sprake is van schade, ziet de AP door de ernst van de overtreding en de verwijtbaarheid van het college B&W Enschede geen aanleiding om af te zien van het opleggen van een bestuurlijke boete of om het boetebedrag te verlagen. De AP is tot slot van oordeel dat de medewerking van het college B&W Enschede niet verder is gegaan dan haar wettelijke plicht om te voldoen aan artikel 31 van de AVG. Het college B&W Enschede heeft daarmee niet op bijzondere wijze samengewerkt met de AP.

4.3.2 Verwijtbaarheid en nalatige aard van de inbreuk

Ingevolge artikel 5:46, tweede lid, van de Awb houdt de AP bij de oplegging van een bestuurlijke boete rekening met de mate waarin deze aan de overtreder kan worden verweten.

Op grond van artikel 6, eerste lid, van de AVG is een verwerking van persoonsgegevens pas rechtmatig als deze plaatsvindt op basis van een grondslag. Dit is een voortzetting van wat ook al gold onder Richtlijn 95/46/EG en de Wet bescherming persoonsgegevens. Als uitgangspunt geldt dat het college B&W Enschede een eigen verantwoordelijkheid heeft om zich reeds vanaf inwerkingtreding van de AVG aan de daarin gestelde regels te houden. Dat de verwerkingen van gegevens in het kader van wifitellingen plaatsvonden bij Bureau RMC en [VERTROUWELIJK] doet daar niet aan af. Het college B&W Enschede heeft met het bepalen van de verwerkingsdoelstellingen de wettelijke taak om de verantwoordelijkheid te dragen voor de gegevensverwerking omtrent de wifitellingen. Het college B&W Enschede heeft nagelaten om zorgvuldig onderzoek te doen naar de verzamelde data of daar juridisch advies over in te winnen. Ook het feit dat Bureau RMC in de offerte had vermeld dat zij data omzetten en valideren naar bezoekersstromen en loopstromen van het winkelende publiek, had het college B&W Enschede alert moeten maken dat er ook bezoekersstromen uit de verzamelde gegevens weergegeven konden worden. In plaats daarvan ging het college B&W Enschede ervan uit dat een derde partij, met een commercieel belang, de verantwoordelijkheid op zich nam. De AP acht dit verwijtbaar.

Het college B&W Enschede heeft aangevoerd dat zij steeds gestuurd hebben op het waarborgen van privacy met betrekking tot de door Bureau RMC uitgevoerde wifitellingen. Dat is volgens het college aan te merken als een boeteverlagende omstandigheid, aangezien zij niet opzettelijk of bewust op onrechtmatige wijze persoonsgegevens verwerkt. Verder vindt het college B&W Enschede dat zij niet nalatig zijn geweest, gezien de getroffen maatregelen tot doel hadden om louter anonieme gegevens te verwerken die niet herleidbaar zijn tot individuen.

De AP ziet, mede onder verwijzing naar paragraaf 3.1.3, op basis hiervan geen aanleiding af te zien van het opleggen van een bestuurlijke boete of het boetebedrag te verlagen. De AP is van oordeel dat bovengenoemde aangevoerde omstandigheden het college B&W Enschede niet disculpeert. Van een overheidsinstantie mag, mede gelet op de grote omvang van de gegevensverwerking, worden verwacht dat zij zich terdege van de voor haar geldende normen vergewist en deze naleeft. Zeker in een samenleving waarbij het steeds moeilijker is om data te anonimiseren. Het college B&W Enschede had meer onderzoek moeten doen naar de gegevens die onder haar verantwoordelijkheid werden verwerkt. Of Bureau RMC de



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

afspraken met het college B&W Enschede al dan niet is nagekomen, is een civiele kwestie tussen Bureau RMC en het college. De AP merkt voorts op dat de overtreden bepaling van artikel 6, eerste lid, van de AVG geen opzet vereist als bestanddeel. Nu het hier gaat om een overtreding, is voor het opleggen van een bestuurlijke boete conform vaste rechtspraak niet vereist dat wordt aangetoond dat sprake is van opzet.⁴⁰ De AP mag verwijtbaarheid veronderstellen als het daderschap vaststaat.⁴¹

4.3.3 Evenredigheid en financiële omstandigheden

Tot slot beoordeelt de AP op grond van artikelen 3:4 en 5:46 van de Awb (evenredigheidsbeginsel) of de toepassing van haar beleid voor het bepalen van de hoogte van de boete gezien de omstandigheden van het concrete geval, niet tot een onevenredige uitkomst leidt. Toepassing van het evenredigheidsbeginsel kan onder andere spelen bij de draagkracht van de verwerkingsverantwoordelijke.

Het college B&W Enschede heeft de AP verzocht rekening te houden met de financiële omstandigheden van de gemeente, zonder daarmee uitdrukkelijk te stellen dat er sprake is van een beperkte financiële draagkracht. Het is volgens het college B&W Enschede algemeen bekend dat bij vrijwel alle gemeenten in Nederland, door onder andere Corona, de financiën onder druk staan.⁴²

Naar wat de AP begrijpt, wil het college B&W Enschede niet uitdrukkelijk stellen dat er sprake is van een beperkte financiële draagkracht maar dat de AP wel rekening moet houden met de financiële omstandigheden van de gemeente. Ongeacht dit tegenstrijdige signaal, heeft de AP de openbare financiële cijfers van de gemeente Enschede geraadpleegd. De AP stelt op basis van de (door de gemeente Enschede zelf gepubliceerde) cijfers vast, dat de gemeente Enschede eind 2020 algemene reserves had van bijna 60 miljoen euro en vorderingen van 40 miljoen euro.⁴³ Gezien deze algemene reserves en liquiditeit, acht de AP het onwaarschijnlijk dat de onderhavige boete continuïteitsproblemen bij de gemeente Enschede zal opleveren.

Concluderend ziet de AP geen aanleiding om af te zien van het opleggen van een bestuurlijke boete of om het boetebedrag te verlagen. De AP acht het boetebedrag van € 600.000 evenredig en er zijn geen andere feiten en omstandigheden die nopen tot matiging van het voornoemde bedrag.

4.4 Conclusie

De AP stelt het totale boetebedrag vast op € 600.000.

⁴⁰ vgl. College van Beroep voor het bedrijfsleven 29 oktober 2014, ECLI:NL:CBB:2014:395, rov. 3.5.4, 2 september 2015, ECLI:NL:CBB:2015:312, rov. 3.7 en 7 maart 2016, ECLI:NL:CBB:2016:54, rov. 8.3; Afdeling Bestuursrechtspraak van de Raad van State 29 augustus 2018, ECLI:NL:RVS:2018:2879, rov. 3.2 en 5 december 2018, ECLI:NL:RVS:2018:3969, rov. 5.1.

⁴¹ *Kamerstukken II* 2003/04, 29 702, nr. 3, p. 134.

⁴² Brief van 16 februari 2021 van het college B&W Enschede aan de AP, pagina 3.

⁴³ Gemeentebegroting 2021-2024, paragraaf 5.3. Zie: <https://documenten.enschede.nl/gb2021>.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

5. Dictum

De AP legt aan het college van burgemeester en wethouders van de gemeente Enschede, wegens overtreding van artikel 5, eerste lid, onder a, jo. artikel 6, eerste lid, van de AVG een bestuurlijke boete op ten bedrage van **€ 600.000** (zegge zeshonderdduizend euro).⁴⁴

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

drs. C.E. Mur
Bestuurslid

Rechtsmiddelenclausule

Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens. Het indienen van een bezwaarschrift schort de werking van dit besluit op. Voor het indienen van digitaal bezwaar, zie www.autoriteitpersoonsgegevens.nl, onder het kopje Bezwaar maken tegen een besluit, onderaan de pagina onder de kop Contact met de Autoriteit Persoonsgegevens. Het adres voor het indienen op papier is: Autoriteit Persoonsgegevens, postbus 93374, 2509 AJ Den Haag.

Vermeld op de envelop 'Awb-bezwaar' en zet in de titel van uw brief 'bezwaarschrift'.

Schrijf in uw bezwaarschrift ten minste:

- uw naam en adres;
- de datum van uw bezwaarschrift;
- het in deze brief genoemde kenmerk (zaaknummer); of een kopie van dit besluit bijvoegen;
- de reden(en) waarom u het niet eens bent met dit besluit;
- uw handtekening.

⁴⁴ De AP zal voornoemde vordering uit handen geven aan het Centraal Justitieel Incassobureau (CJIB).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Bijlage 1



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

1. Feiten omtrent het begrip persoonsgegevens

1.1 De sensoren opgehangen in de binnenstad van Enschede

Als op een mobiel apparaat de wifi staat ingeschakeld, dan zendt het apparaat met regelmatige tussenpozen het signaal uit dat het op zoek is naar een netwerk om mee te verbinden. De sensoren die zijn opgehangen in de binnenstad van Enschede vangen deze signalen op. Een medewerker van [VERTROUWELIJK] heeft verklaard dat er in Enschede consumentenrouters als sensoren worden gebruikt.⁴⁵

Het college B&W Enschede heeft verklaard dat de wifimetingen worden uitgevoerd met behulp van elf sensoren. Deze elf sensoren hingen er op 25 mei 2018 en dit aantal is sindsdien niet gewijzigd.⁴⁶ Bureau RMC heeft dit bevestigd.⁴⁷ Tot slot volgt het ook uit de met de sensoren verzamelde gegevens die de AP heeft ontvangen in het kader van het onderzoek⁴⁸ en uit de informatie op de website www.binnenstadsmonitorenschede.nl waar gebruikt wordt gemaakt van de met de sensoren verzamelde gegevens.

Uit de door Bureau RMC verstrekte informatie volgt dat de sensoren zijn opgehangen bij elf verschillende winkeliers die zijn gevestigd in de binnenstad van Enschede.⁴⁹ Toezichthouders van de AP hebben op 29 mei 2019 een aantal van deze winkeliers bezocht en hebben daar onderstaande kastjes met daarin de routers aangetroffen.⁵⁰



Figuur 1: Twee sensoren aangetroffen bij twee verschillende winkeliers

⁴⁵ Pagina 2 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁴⁶ Antwoorden op de 'Vragen over de sensoren', brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).

⁴⁷ Pagina 1 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁴⁸ Citytraffic_aantal_telpunt 4 Excelsheets en Citytraffic_weekoverzicht 4 Excelsheets, bijlage 14 en 15 bij brief van 24 mei 2019 van college B&W Enschede aan de AP (dossierstuk 26). Export Enschede sep-dec long term table.zip, ontvangen van [VERTROUWELIJK] op 12 december 2019 (dossierstuk 69) en Export Enschede jun - aug 2019 long term table.zip, ontvangen van [VERTROUWELIJK] op 16 december 2019 (dossierstuk 72).

⁴⁹ Excellijst locatie sensoren, bijlage bij e-mail van 23 mei 2019 van Bureau RMC aan de AP (dossierstuk 25).

⁵⁰ Verklaringen van Ambtshandelingen onderzoek ter plaatse bij acht winkeliers in de binnenstad van Enschede volgens Bureau RMC een sensor zo hangen (dossierstukken 30-38).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

De directeur van Bureau RMC heeft verklaard dat het bereik van elke sensor in principe de overkant van de straat is.⁵¹ Op de website www.citytraffic.nl wordt door Bureau RMC gesteld dat dit bereik 20 à 30 meter is.⁵²

De AP constateert op basis van het voorgaande dat er in ieder geval sinds 25 mei 2018 elf sensoren hangen bij verschillende winkeliers in de binnenstad van Enschede. Elke sensor heeft een bereik van 20 à 30 meter.

1.2 De verwerking van gegevens middels de City Traffic-methode

Bureau RMC noemt de methode om via sensoren gegevens van mobiele apparaten waarop de wifi staat ingeschakeld te verzamelen en te verwerken tot rapportages de 'City Traffic-methode'. Deze City Traffic-methode wordt toegepast in de binnenstad van Enschede. Op de website van Bureau RMC staat een infographic die deze methode (per 1 januari 2019) visualiseert.⁵³ In deze paragraaf behandelt de AP de verschillende fasen van verzamelen en verwerken van gegevens door middel van de City Traffic-methode.



Figuur 2: Infographic City Traffic-methode na 1 januari 2019

⁵¹ Pagina 2 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁵² www.citytraffic.nl/hoe-we-tellen.

⁵³ Schermafbeeldingen van webpagina's op www.rmc.nl vastgelegd op 26 april 2019 (dossierstuk 10).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

De verzameling van gegevens door de sensoren en verzending ervan naar de server

De eerste fase betreft het opvangen door de sensoren van bepaalde gegevens van mobiele apparaten waarop de wifi is ingeschakeld. Elke sensor heeft een bepaald bereik en in deze paragraaf wordt aangetoond dat zowel bij binnenkomst in het bereik als bij vertrek uit het bereik er gegevens van het mobiele apparaat worden verzameld en vervolgens deels gepseudonimiseerd worden verstuurd naar de centrale server.

Tijdens het onderzoek ter plaatse op 29 mei 2019 heeft een medewerker van [VERTROUWELIJK] verklaard dat op elke sensor in de binnenstad van Enschede dezelfde software draait en dat daarom elke sensor dezelfde werking heeft.⁵⁴ De medewerker heeft verder verklaard dat de werking van de sensoren niet is gewijzigd sinds 25 mei 2018.⁵⁵

Op de vraag van de AP welke gegevens van mobiele apparaten er door de sensoren worden opgevangen, heeft een medewerker van [VERTROUWELIJK] het volgende geantwoord: *“Het MAC-adres, de locatie-ID van de sensor, de datum en het tijdstip van ontvangst van het wifisignaal op de sensor en de signaalsterkte. Ook wordt er op de sensor bijgehouden wanneer je door de sensor voor het eerst gezien wordt en wanneer je voor het laatst gezien bent.”*⁵⁶

Het hiervoor genoemde MAC-adres van een apparaat is een door de fabriek ingebouwd wereldwijd uniek nummer.⁵⁷ Het is een reeks van 12 hexadecimale karakters (0-9, A-F) in de vorm 00:0C:6E:D2:11:E6. Zoals eerder aangegeven zendt een apparaat waarop de wifi aan staat met regelmatige tussenpozen het signaal uit dat het op zoek is naar een netwerk om mee te verbinden. Via dit signaal wordt het MAC-adres van het apparaat opgevangen door een sensor.

Later in de verklaring is door een medewerker van [VERTROUWELIJK] aangegeven dat op de sensoren ook wordt bepaald of een opgevangen MAC-adres een zogenaamd ‘gespoofed MAC-adres’ is: *“Het betreft het uitzenden van een fake MAC-adres, om het te kunnen volgen van telefoons tegen te gaan (e.g. door Apple). Spoofed adressen nemen we niet mee in onze tellingen (...)”*⁵⁸

Uit de door [VERTROUWELIJK] aan de AP verstrekte softwarecode die draait op de sensoren blijkt dat het volgende op de sensor gebeurt zodra een apparaat met wifi ingeschakeld *binnen* het bereik van de sensor komt:⁵⁹

1. Het MAC-adres en de signaalsterkte van het apparaat worden opgevangen.
2. De datum en het exacte tijdstip van ontvangst worden bepaald.

⁵⁴ Pagina 2 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁵⁵ Pagina 2 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁵⁶ Pagina 1 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁵⁷ Pagina 6 van WP185 Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten.

⁵⁸ Pagina 10 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁵⁹ [VERTROUWELIJK] en Verklaring van Ambtshandelingen analyse broncode van 18 februari 2020 (dossierstuk 78).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

3. Het MAC-adres, de signaalsterkte, datum en tijdstip worden opgeslagen in het werkgeheugen van de sensor (voor zolang het apparaat binnen het bereik van de sensor is).⁶⁰
4. Er wordt bepaald of het MAC-adres een 'spoofed MAC-adres' is of niet.⁶¹
5. Het MAC-adres wordt gepseudonimiseerd (zie volgende paragraaf o).
6. De volgende gegevens worden verzonden naar de server: Gepseudonimiseerd MAC-adres, signaalsterkte, datum, tijdstip, spoofed indicator en sensor-ID⁶², met hieraan gekoppeld 'status 1' om aan te geven dat de betreffende gegevens gaan over het moment dat het mobiele apparaat binnen het bereik kwam.⁶³

Over het moment waarop het MAC-adres wordt gepseudonimiseerd heeft de directeur van Bureau RMC verklaard: *"Het wordt op de sensor meteen vervangen, dus op de sensor wordt het MAC-adres meteen gehasht."*⁶⁴ Ook op de website www.citytraffic.nl staat dat het MAC-adres meteen wordt gepseudonimiseerd.⁶⁵ De AP constateert echter dat dit niet wordt bevestigd door de softwarecode van de sensoren. Daaruit blijkt namelijk, zoals toegelicht in het vorige randnummer, dat er ongepseudonimiseerde MAC-adressen worden opgeslagen in het werkgeheugen van de sensoren.

Een medewerker van [VERTROUWELIJK] heeft het volgende verklaard over wat er gebeurt zolang een apparaat waarop de wifi is ingeschakeld binnen het bereik van een sensor is: *"Het MAC-adres wordt de hele tijd opgevangen, de sensor checkt of het MAC-adres al eerder is gezien, zo ja, dan verhoogt hij de laatst geziene tijd en dit proces herhaalt zich tot dat het MAC-adres twee minuten niet gezien is."*⁶⁶ De softwarecode en een eigen analyse van deze softwarecode door een toezichthouder van de AP bevestigt deze werking.⁶⁷

Een medewerker van [VERTROUWELIJK] heeft het volgende verklaard over wanneer de gegevens worden doorgezonden aan een server: *"Het status 1 bericht wordt direct doorgestuurd naar de server, het status 2 bericht als het MAC-adres twee minuten uit het zicht is. Het wordt live doorgestuurd, niet bijvoorbeeld elke minuut. Dus van elke passant worden er twee keer gegevens doorgestuurd."*⁶⁸ De softwarecode en een eigen analyse van deze softwarecode door een toezichthouder van de AP bevestigt deze werking.⁶⁹ Het verzamelen van zowel het tijdstip waarop het MAC-adres voor het eerst binnen bereik komt (status 1) als het laatst geziene tijdstip (status 2) wordt gebruikt om de verblijftijd van het MAC-adres binnen het bereik van de sensor te bepalen, zie hiervoor bijlage 1, pagina 42 en verder (lange termijn tabel).

⁶⁰ Dit is bevestigd door de medewerkers van [VERTROUWELIJK], pagina 3 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁶¹ De indicator is 1 als er sprake is van een spoofed MAC-adres en 0 als het het MAC-adres niet spoofed is.

⁶² Dit is uniek nummer gekoppeld aan elke sensor.

⁶³ Naast 'status 1' wordt ook een 'status 2' gehanteerd, dit verwijst naar het moment dat het bereik van de sensor is verlaten.

⁶⁴ Pagina 3 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55). Bureau RMC en de medewerkers van [VERTROUWELIJK] hanteren in hun verklaringen soms het begrip 'hashen' om het pseudonimiseren aan te duiden.

⁶⁵ Schermafbeeldingen van webpagina's www.citytraffic.nl vastgelegd op 31 juli 2019 (dossierstuk 54).

⁶⁶ Pagina 3 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁶⁷ [VERTROUWELIJK] en Verklaring van Ambtshandelingen analyse broncode van 18 februari 2020 (dossierstuk 78).

⁶⁸ Pagina 2 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁶⁹ [VERTROUWELIJK] en Verklaring van Ambtshandelingen analyse broncode van 18 februari 2020 (dossierstuk 78).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Uit de softwarecode blijkt dat zodra een gedetecteerd mobiel apparaat *buiten* het bereik van de sensor is dat de volgende gegevens worden verzonden naar de server: Status '2', gepseudonimiseerd MAC-adres, laatste binnen het bereik gemeten signaalsterkte, laatste binnen het bereik bepaalde datum en tijdstip (dit betreft het tijdstip minus de twee minuten), spoofed indicator en sensor-ID.⁷⁰

Op de vraag hoe lang de MAC-adressen in het werkgeheugen van elke sensor blijven staan heeft een medewerker van [VERTROUWELIJK] geantwoord: *“De gegevens worden verstuurd naar de server zodra is geconstateerd dat het apparaat 2 minuten niet meer in bereik van de sensor is. Dan verdwijnen de gegevens van de sensor. Dus hoe lang de gegevens worden bewaard is afhankelijk van hoe lang iemand in het gebied/bereik van de sensor is plus 2 minuten.”*⁷¹ De softwarecode en een eigen analyse van deze softwarecode door een toezichthouder van de AP bevestigt deze werking.⁷²

De AP constateert op basis van het voorgaande dat in ieder geval vanaf 25 mei 2018 tot heden elke sensor in de binnenstad van Enschede dezelfde werking had. De sensoren hebben gedurende deze periode van alle binnen het bereik komende mobiele apparaten waarop de wifi stond ingeschakeld het MAC-adres, signaalsterkte, datum en tijdstip opgevangen en tijdelijk opgeslagen in het werkgeheugen van de sensor. Deze opslag duurde zolang het apparaat zich binnen het bereik van de sensor bevond plus twee minuten. Ook constateert de AP dat de sensoren continue scannen. Tot slot stelt de AP vast dat er van elk gedetecteerd apparaat bij binnenkomst en twee minuten na vertrek uit het bereik van de sensor realtime de volgende gegevens zijn verzonden naar de server: status 1 dan wel 2, gepseudonimiseerd MAC-adres, signaalsterkte, datum en tijdstip, spoofed indicator en sensor-ID.

Het pseudonimiseren van het MAC-adres op de sensoren

Een medewerker van [VERTROUWELIJK] heeft verklaard dat op elke sensor in Enschede dezelfde pseudonimiseringsmethode wordt toegepast en dat deze methode sinds 25 mei 2018 niet is gewijzigd.⁷³ Op de vraag van de AP welke methode wordt gehanteerd heeft een medewerker van [VERTROUWELIJK] geantwoord: “[VERTROUWELIJK]”⁷⁴ Dit blijkt ook uit de softwarecode⁷⁵ en een door [VERTROUWELIJK] opgesteld document over de pseudonimiseringsmethode.⁷⁶

Tijdens het onderzoek ter plaatse op 29 mei 2019 heeft een medewerker van [VERTROUWELIJK] verklaard: *“Één MAC-adres levert praktisch één gehasht nummer op, er is minimale kans op collision namelijk dat twee MAC-adressen dezelfde*

⁷⁰ [VERTROUWELIJK] en Verklaring van Ambtshandelingen analyse broncode van 18 februari 2020 (dossierstuk 78).

⁷¹ Pagina 2 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁷² [VERTROUWELIJK] en Verklaring van Ambtshandelingen analyse broncode van 18 februari 2020 (dossierstuk 78).

⁷³ Pagina 2 en 4 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55). De medewerker van [VERTROUWELIJK] hebben tevens verklaard dat dezelfde methode op al hun sensoren in Nederland draait.

⁷⁴ Pagina 4 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁷⁵ [VERTROUWELIJK] en Verklaring van Ambtshandelingen analyse broncode van 18 februari 2020 (dossierstuk 78).

⁷⁶ MAC hashing analysis opgesteld door [VERTROUWELIJK] (geen datum), ontvangen van [VERTROUWELIJK] op 3 juni 2019 (dossierstuk 43).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

*gehashte waarde opleveren.*⁷⁷ Uit het document over de pseudonimiseringsmethode blijkt dat [VERTROUWELIJK] juist voor deze methode heeft gekozen omdat er slechts een verwaarloosbare kans is op gelijke resultaten.⁷⁸

De AP constateert op basis van het voorgaande dat er één en dezelfde pseudonimiseringsmethode draait op alle sensoren in de binnenstad van Enschede en dat deze methode sinds 25 mei 2018 niet is gewijzigd. Daarnaast stelt de AP vast dat het pseudonimiseren tot gevolg heeft dat één MAC-adres op elk van de sensoren leidt tot één en hetzelfde gepseudonimiseerd MAC-adres.

De kortetermijntabel op de server

Hiervoor heeft de AP vastgesteld dat in ieder geval vanaf 25 mei 2018 in de binnenstad van Enschede van elk mobiele apparaat waarop de wifi stond ingeschakeld en die door het bereik van een sensor is gegaan er twee keer gegevens van het mobiele apparaat, namelijk bij binnenkomst in het bereik en twee minuten na vertrek uit het bereik, realtime zijn verstuurd naar de server. Daarnaast heeft de AP geconcludeerd dat per 1 januari 2019 alle op de server binnenkomende gepseudonimiseerde MAC-adressen worden afgeknipt. Hierover heeft een medewerker van [VERTROUWELIJK] verklaard: *“Als het gehashte⁷⁹ MAC-adres binnenkomt wordt het afgeknipt in het geheugen (real time) en die wordt daarna weggeschreven in een ruwe tabel, (...)”*⁸⁰

Ook heeft een medewerker van [VERTROUWELIJK] verklaard: *“We gebruiken op de server twee tabellen. Een korte termijn tabel die de data van vandaag bevat en een lange termijn tabel die de data van 6 maanden bevat.”*⁸¹ De AP zal eerst de kortetermijntabel behandelen.

Over wat er per 1 januari 2019 wordt afgeknipt van het gepseudonimiseerde MAC-adres heeft een medewerker van [VERTROUWELIJK] verklaard: *“[VERTROUWELIJK], de dubbele punt achterwege latend.”*⁸² En: *“Enkel het gehashte MAC-adres wordt afgeknipt en de rest van de gegevens daar verandert niets aan.”*⁸³ De softwarecode bevestigt het voorgaande, met de aanvulling dat ook de dubbele punten uit het afgeknipte gepseudonimiseerde MAC-adres worden verwijderd.⁸⁴ Het resultaat na afknippen is een reeks van [VERTROUWELIJK] bestaande uit 0-9 of a-z zonder dubbele punten (zie de kolom MACNUMBER in Figuur 3).

⁷⁷ Pagina 5 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁷⁸ Pagina 3 laatste alinea en pagina 4 derde alinea MAC hashing analysis opgesteld door [VERTROUWELIJK] (geen datum), ontvangen van [VERTROUWELIJK] op 3 juni 2019 (dossierstuk 43).

⁷⁹ [VERTROUWELIJK] gebruikt hier de term ‘gehasht’ als alternatief voor ‘gepseudonimiseerd’.

⁸⁰ Pagina 6 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁸¹ Pagina 7 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁸² Pagina 6 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁸³ Pagina 6 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁸⁴ [VERTROUWELIJK] en Verklaring van Ambtshandelingen analyse broncode van 18 februari 2020 (dossierstuk 78).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Tijdens het onderzoek ter plaatse heeft een medewerker van [VERTROUWELIJK] de toezichthouders van de AP inzage gegeven in de kortetermijntabel.⁸⁵ Tevens hebben deze medewerker op een later tijdstip een gedeelte van de kortetermijntabel met de op 29 mei 2019 in Enschede verzamelde gegevens aangeleverd aan de AP.⁸⁶ Een schermafbeelding van de eerste paar records van deze kortetermijntabel gefilterd op de sensor [VERTROUWELIJK] betreft:

	A	B	C	D	E	F	G	H
1	HOSTNAME	MACNUMBER	DATUM	TIJD	SIGNAL	STATUS	SPOOF	
15			29-5-2019	00:00:07	-75	2	0	
33			29-5-2019	00:00:42	-65	1	1	
79			29-5-2019	00:01:45	-67	2	1	
97			29-5-2019	00:02:02	-85	1	0	
103			29-5-2019	00:02:18	-72	1	0	
153			29-5-2019	00:03:51	-71	1	1	
214			29-5-2019	00:06:51	-48	1	0	
225			29-5-2019	00:06:55	-85	1	0	
231			29-5-2019	00:06:59	-92	2	0	
232			29-5-2019	00:07:00	-88	1	0	
233			29-5-2019	00:07:01	-70	1	1	
234			29-5-2019	00:07:01	-66	2	1	
241			29-5-2019	00:07:05	-73	1	0	
254			29-5-2019	00:07:11	-86	2	0	
302			29-5-2019	00:07:51	-83	1	0	
303			29-5-2019	00:07:51	-83	2	0	
341			29-5-2019	00:08:46	-75	2	0	
384			29-5-2019	00:09:28	-75	1	0	
440			29-5-2019	00:10:18	-87	1	0	
467			29-5-2019	00:11:18	-92	1	0	
496			29-5-2019	00:11:53	-83	1	0	
565			29-5-2019	00:13:26	-75	2	0	
566			29-5-2019	00:13:26	-80	2	0	
570			29-5-2019	00:13:30	-89	2	0	
641			29-5-2019	00:15:08	-91	2	0	

Figuur 3: Schermafbeelding eerste gedeelte kortetermijntabel over 29 mei 2019 voor een sensor

Een medewerker van [VERTROUWELIJK] heeft de volgende toelichting gegeven op de kolommen:

- 'HOSTNAME' is de unieke identificatie van de sensor, de locatie-ID van een sensor.
- 'MACNUMBER' is het gepseudonimiseerde en afgeknipte MAC-adres.
- 'DATUM' is de dag-week-jaar.
- 'TIJD' is het tijdstip op die dag wanneer het apparaat gescand is. (...).
- 'SIGNAL' is de signaalsterkte waarmee het apparaat is waargenomen.
- 'STATUS' 1 is het moment waarop hij voor het eerst is waargenomen en status 2 is het moment waarop hij buiten het bereik van de sensor is.
- 'SPOOFED' is 1 als het een gespoofd mac-adres betref (en 0 als niet). (...).⁸⁷

⁸⁵ Verklaring van Ambtshandelingen onderzoek ter plaatse Bureau RMC en [VERTROUWELIJK] op 29 mei 2019 (dossierstuk 39).

⁸⁶ Export Enschede 29-5-2019.zip, ontvangen van [VERTROUWELIJK] op 3 juni 2019 (dossierstuk 42). De eerste detectie (record in de tabel) was op tijdstip 00:00:00 en de laatste op tijdstip 20:20:37.

⁸⁷ Pagina 9 en 10 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

De AP merkt op dat DATUM op dagniveau en de TIJD op de seconde nauwkeurig wordt vastgelegd. De HOSTNAME is de unieke sensor-ID, elk van de elf sensoren in de binnenstad van Enschede heeft een unieke [VERTROUWELIJK]-code.⁸⁸

In de schermafbeelding hierboven zijn in blauw en in rood twee opvolgende status 1 en status 2 records van hetzelfde afgeknipte gepseudonimiseerde MAC-adres omkaderd ([VERTROUWELIJK]). Later toont de AP aan dat elk van deze twee records wordt samengevoegd tot één record in de langetermijntabel.

De AP constateert op basis van het voorgaande dat in ieder geval sinds 25 mei 2018 de gegevens die op één dag zijn gemeten door de sensoren in de binnenstad van Enschede dagelijks zijn verzameld in de kortetermijntabel.⁸⁹ Het tijdstip op de dag waarop het apparaat door de sensor is gescand wordt hierbij op de seconde nauwkeurig vastgelegd. In de periode tot aan 1 januari 2019 is het gepseudonimiseerde MAC-adres bij binnenkomst op de server niet afgeknipt, in de periode vanaf 1 januari 2019 wel. Het afknippen betreft het verwijderen van de laatste drie karakters van het gepseudonimiseerde MAC-adres (zonder dubbele punt). De andere gegevens die zijn verzonden naar de server, namelijk sensor-ID, datum, tijdstip, signaalsterkte, status en spoofed indicator zijn onbewerkt overgenomen in de kortetermijntabel.

De toepassing van filters

Tijdens het onderzoek ter plaatse bij Bureau RMC op 29 mei 2019 is door een medewerker van [VERTROUWELIJK] verklaard dat op de kortetermijntabel, behandeld in de vorige paragraaf, elke nacht bepaalde filters worden toegepast waarna de overgebleven records aan de langetermijntabel worden toegevoegd.⁹⁰ Deze medewerker van [VERTROUWELIJK] heeft hierover in een document toegelicht: *“De code voor de filters (...) draaien in de ochtend om 00:15:00 in tijdzone Europe/Amsterdam op de detecties van de vorige dag. We gebruiken twee soorten filters wanneer de data wordt verwerkt van de RAWRESULTS_HTTP_WIFI tabel naar tabellen waar de data voor een langere termijn staat. Dit zijn het opt-out filter en het bewonersfilter.”*⁹¹

De toelichting van [VERTROUWELIJK] op het opt-out filter betreft: *“Het opt-out filter verwijdert detecties uit de (...) tabel wanneer de detecties een hashed en afgeknipt mac adres bevatten die ook in de opt-out lijst staat.”*⁹²

Over deze opt-out lijst geeft het college B&W Enschede sinds de start van de wifimetingen op de website van de gemeente de volgende toelichting: *“Iedereen heeft de mogelijkheid om zijn MAC-adressen van mobiele apparaten op de website van City Traffic aan te melden voor een opt-out register. Hierna worden deze MAC-adressen niet langer geteld en meegenomen in onze onderzoeken. Het opt-out register vindt u op <http://citytraffic.nl/site/page/opt->*

⁸⁸ Tijdens het onderzoek ter plaatse bij Bureau RMC op 29 mei 2019 is aan de AP een lijst met de sensor-ID's en de bijbehorende straat in de binnenstad van Enschede overlegd.

⁸⁹ Met uitzondering van de periode van 10 december 2018 tot en met 3 januari 2019, omdat toen de sensoren waren uitgeschakeld, zie bijlage 1, paragraaf 2.5.

⁹⁰ Pagina 7 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁹¹ Pagina 3 van broncode, afknippen en filters.pdf, ontvangen van [VERTROUWELIJK] op 20 juni 2019 (dossierstuk 46).

⁹² Pagina 3 van broncode, afknippen en filters.pdf, ontvangen van [VERTROUWELIJK] op 20 juni 2019 (dossierstuk 46).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

out.⁹³ Op de genoemde webpagina op www.citytraffic.nl staat een invulveld waarmee iemand het MAC-adres van zijn/haar mobiele apparaat op de opt-out lijst kan laten plaatsen.

De AP merkt op dat omdat de opt-out filter pas wordt toegepast op de kortetermijntabel het niet zo is dat MAC-adressen die zijn opgegeven niet meer worden opgevangen door de sensoren.

De toelichting van [VERTROUWELIJK] op het bewonersfilter betreft: *“Het bewonersfilter verwijdert de detecties uit de (...) tabel voor een mac adres wanneer het mac adres bij dezelfde scanner op een dag zowel tussen 05:00 en 07:00 gezien is als tussen 22:00 en 23:59:59.”*⁹⁴

Uit de softwarecode blijkt dat de bewonersfilter als volgt werkt:⁹⁵ alle records van een afgeknipt gepseudonimiseerde MAC-adres in de kortetermijntabel worden verwijderd als dat afgeknipte gepseudonimiseerde MAC-adres zowel tussen 5 en 7 uur als tussen 22 en 24 uur in of buiten het bereik van eenzelfde sensor komt. Er moet namelijk sprake zijn van *een detectie in beide tijdsperiodes*. Deze werking heeft tot gevolg dat als bijvoorbeeld een persoon met een mobiel apparaat waarop de wifi staat ingeschakeld woont binnen het bereik van een sensor en de gehele dag thuis is, de records van zijn/haar mobiele apparaat *niet* eruit worden gefilterd. Hetzelfde geldt bijvoorbeeld voor bewoners die alleen tussen 5 en 7 of tussen 22 en 24 uur het huis verlaten c.q. thuiskomen.

Ten aanzien van de bewonersfilter merkt de AP op dat deze elke nacht op de dagelijks verzamelde gegevens wordt toegepast, wat betekent dat elke dag opnieuw wordt bepaald of iemand kwalificeert als bewoner of niet.⁹⁶ Uit Figuur 7 op pagina 48 volgt dat de kwalificatie dagelijks kan verschillen.

Het college B&W Enschede heeft sinds de start van de wifimetingen in september 2017 op de website van de gemeente de volgende Q&A staan voor bewoners van de binnenstad van Enschede:⁹⁷

“Ik woon in de binnenstad, wat wordt er met mijn gegevens gedaan?”

City Traffic telt het aantal passanten in de winkelstraat. De sensoren hebben daarom een automatisch filter om bewoners niet mee te nemen in de tellingen. City Traffic weet dat signalen van bewoners voornamelijk voor en na winkelopeningstijden gemeten worden. Daarom gaat City Traffic er van uit dat wanneer eenzelfde signaal twee keer per dag gezien wordt, één keer in de ochtend en één keer in de avond, dit een signaal is van een bewoner. Deze signalen worden vanaf dat moment iedere dag er automatisch uitgefilterd. Als u in de buurt van een telpunt woont, wordt u dus niet meegenomen in de tellingen.”

De AP merkt op dat deze tekst meerdere onjuistheden bevat. Ten eerste staat er dat de sensoren de filter toepassen, terwijl dit pas op de server wordt gedaan. Ten tweede wordt gesuggereerd dat eenmalig wordt bepaald of iemand in de buurt van een sensor woont om daarna automatisch iedere dag eruit te worden uitgefilterd, terwijl in werkelijkheid de filter elke nacht opnieuw bepaald of iemand een bewoner is of niet.

⁹³ www.enschede.nl/sites/default/files/QandAokt2017.pdf, laatst door de AP bezocht op 6 januari 2020.

⁹⁴ Pagina 3 van broncode, afknippen en filters.pdf, ontvangen van [VERTROUWELIJK] op 20 juni 2019 (dossierstuk 46).

⁹⁵ ConvertWifi.php, ontvangen van [VERTROUWELIJK] op 20 juni 2019 (dossierstuk 46). Verklaring van Ambtshandelingen analyse broncode van 18 februari 2020 (dossierstuk 78).

⁹⁶ Verklaring van Ambtshandelingen analyse broncode van 18 februari 2020 (dossierstuk 78).

⁹⁷ Q&A's, bijlage 5 en 6 bij de brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Tot slot is ook de stelling dat bewoners niet worden meegenomen in de tellingen niet in alle gevallen juist, zoals hierboven volgt uit de analyse van de bewonersfilter.

De AP constateert op basis van het voorgaande dat er elke nacht op de kortetermijntabel twee filters worden toegepast, namelijk een opt-out filter en een bewonersfilter. Deze filters hebben tot gevolg dat bepaalde records uit de kortetermijntabel niet terechtkomen in de langetermijntabel. Daarnaast constateert de AP dat de bewonersfilter niet alle bewoners eruit filtert en dat er op de website van de gemeente hierover foutieve informatie wordt gegeven.

De langetermijntabel op de server

Omdat het afknippen van het gepseudonimiseerde MAC-adres per 1 januari 2019 is ingevoerd bevatte de langetermijntabel tot aan 1 januari 2019 gepseudonimiseerde MAC-adressen en na 1 januari 2019 alleen afgeknipte gepseudonimiseerde MAC-adressen. Een medewerker van [VERTROUWELIJK] heeft verklaard: *“De gehashte mac adressen die rond die periode in de database stonden hebben we met terugwerkende kracht afgeknipt.”*⁹⁸

Op verzoek van de AP heeft [VERTROUWELIJK] op 6 september 2019 de langetermijntabel met de gegevens over Enschede over alleen 29 mei 2019 aangeleverd.⁹⁹ Een schermafbeelding van de eerste paar records van deze langetermijntabel, gefilterd op de twee afgeknipte gepseudonimiseerde MAC-adressen die in de kortetermijntabel in Figuur 3 zijn omkaderd, betreft:

	A	B	C	D	E	F	G	H	I	J	K
1	ID		MAC	Datum	TijdIn	TijdUit	Retention	BWCode	SignalStrengthIn	SignalStrengthOut	LocationId
2	1980590288			29-5-2019	00:06:55	00:06:59	4 W		-85	-92	0
3	1980579807			29-5-2019	14:28:49	14:28:50	1 W		-83	0	0
4	1980553174			29-5-2019	14:29:34	14:30:04	30 W		-78	-87	0
5	1980590289			29-5-2019	00:11:18	00:15:08	230 W		-92	-91	0
6	1980590290			29-5-2019	00:23:31	00:25:43	132 W		-91	-91	0
7	1980590291			29-5-2019	00:28:33	00:31:26	173 W		-92	-91	0
8	1980590292			29-5-2019	00:41:51	00:41:51	0 W		-91	-91	0
9	1980590293			29-5-2019	00:50:59	00:56:03	304 W		-91	-91	0
10	1980590294			29-5-2019	01:00:37	01:03:37	180 W		-92	-91	0
11	1980590295			29-5-2019	01:07:07	01:17:53	646 W		-91	-92	0
12	1980590296			29-5-2019	01:22:56	01:27:49	293 W		-91	-92	0
13	1980590297			29-5-2019	01:33:49	01:36:17	148 W		-92	-91	0
14	1980590298			29-5-2019	01:40:23	01:47:15	412 W		-90	-92	0
15	1980590299			29-5-2019	01:50:44	01:55:25	281 W		-92	-91	0

Figuur 4: Schermafbeelding gedeelte langetermijntabel

Uit een vergelijking tussen de blauw en rood omkaderde records in de kortetermijntabel en de langetermijntabel (Figuur 3 en Figuur 4) blijkt dat twee opvolgende records (met status 1 en 2) van hetzelfde afgeknipte gepseudonimiseerde MAC-adres in de kortetermijntabel leidt tot één record in de langetermijntabel. De tijdIn (status 1) en TijdUit (status 2) worden achter elkaar gezet en de Retention in

⁹⁸ Pagina 3 van broncode, afknippen en filters.pdf, ontvangen van [VERTROUWELIJK] op 20 juni 2019 (dossierstuk 46) en pagina 6 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

⁹⁹ Export Enschede 29-5-2019 long term table.zip, ontvangen van [VERTROUWELIJK] op 6 september 2019 (dossierstuk 60).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

seconden (de tijd ertussen) wordt berekend. Ook blijkt uit de vergelijking van beide tabellen dat gespoofde MAC-adressen in de kortetermijntabel niet worden opgenomen in de langetermijntabel.¹⁰⁰

[VERTROUWELIJK] heeft in een document de volgende toelichting gegeven op de kolommen in de langetermijntabel:¹⁰¹

ID = id van record

Mac = afgeknipte hash waarde van een mac adres

Datum = Datum van waarneming

TijdIn = starttijd waarneming

TijdUit = eindtijd waarneming

Retention = TijdUit – TijdIn

*BWCode = type detectie (B = bluetooth, W = wifi),
tegenwoordig hebben we enkel nog W detecties*

*SignalStrengthIn = signaalsterkte starttijd
waarneming*

*SignalStrengthOut = signaalsterkte eindtijd
waarneming*

LocationId = altijd 0, niet meer in gebruik

De AP merkt op dat in bovenstaande lijst door [VERTROUWELIJK] de kolom “[VERTROUWELIJK]” per abuis niet is opgenomen, deze kolom betreft de eerdergenoemde sensor-ID. Daarnaast constateert de AP dat de TijdIn en TijdUIT in seconden zijn waardoor de Retention (de verblijfstijd) ook in seconden is.

Over de bewaartermijn van de gegevens in de langetermijntabel heeft Bureau RMC verklaard: “Bij de gemeente Enschede was het vanaf de start van de tellingen een bewaartermijn van een halfjaar, dit is sindsdien niet gewijzigd.”¹⁰² Later is door de directeur van Bureau RMC toegelicht dat op de eerste van de maand de gegevens van de maand van zes maanden geleden worden verwijderd.¹⁰³

De AP constateert op basis van het voorgaande dat, na toepassing van de filters op de kortetermijntabel, twee opeenvolgende records van hetzelfde (afgeknipte) gepseudonimiseerde MAC-adres leidde tot één record in de langetermijntabel. Van 25 mei 2018 tot aan 1 januari 2019 bevatte de langetermijntabel de volgende gegevens: gepseudonimiseerd MAC-adres, datum, TijdIn, TijdUit, Retention, SignalStrengthIn, SignalStrengthOut. Per 1 januari 2019 is overgegaan op het afknippen van het gepseudonimiseerd MAC-adres en werd het gepseudonimiseerd MAC-adres gegeven vervangen door het afgeknipte gepseudonimiseerde MAC-adres. Ook constateert de AP dat er in de langetermijntabel vanaf 25 mei 2018 gegevens stonden over een periode van tussen de zes en zeven maanden.

De bewerkingen op de ruwe data en de cijfers die het college B&W Enschede van Bureau RMC ontvangt

De gegevens in de langetermijntabel vormen de basis voor de cijfers die het college B&W Enschede van Bureau RMC ontvangt. Uit de volgende verklaringen van de directeur van Bureau RMC volgt dat de gegevens in de langetermijntabel eerst worden ontdebeld en dat er daarna statistische bewerkingen op worden toegepast.

¹⁰⁰ Zie ook bijlage 1, paragraaf 1.2, pagina 35 waarin de verklaring van medewerkers [VERTROUWELIJK] is opgenomen dat spoofed MAC-adressen niet worden meegenomen in de tellingen.

¹⁰¹ Kolommen.doc, ontvangen van [VERTROUWELIJK] op 6 september 2019 (dossierstuk 60).

¹⁰² Pagina 7 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

¹⁰³ E-mails van 20 december 2019 en 15 januari 2020 van Bureau RMC aan de AP (dossierstukken 76 en 77).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Een medewerker van [VERTROUWELIJK] heeft tijdens het onderzoek ter plaatse op 29 mei 2019 verklaard: *“Ja, binnen een zone ontdebelen we.”* De directeur van Bureau RMC vulde hierbij aan: *“We willen dit ontdebelen omdat we op zoek zijn naar unieke bezoekers aan de binnenstad. De klant is op zoek naar portemonnees en niet naar passanten. Iemand die 10x geteld is, is niet 10x een koper, maar is 1x een koper die 10x gezien is. De klanten willen het aantal unieke bezoekers binnen een zone weten. (...). Dus als je met zijn tweeën de binnenstad van Enschede inloopt en er is verder niemand, dan kom je in het geaggregeerde halfuurs-beeld alleen terug bij de eerste sensor waar je bent gezien. Voor het meten geldt dit niet, als je door de binnenstad van Enschede loopt dat wordt je bij elke sensor gezien en dit komt terecht in de ruwe data.”*¹⁰⁴

Een medewerker van [VERTROUWELIJK] heeft daarna verklaard: *“Om te ontdebelen hebben we het gepseudonimiseerde MAC-adres nodig. We tellen unieke aantallen, dus als een MAC-adres wordt opgevangen door de sensor en dat MAC-adres komt een uur later daar terug dan zien we dat het dezelfde telefoon is, omdat het dezelfde hash is. De pseudonimiseringsmethode is op alle sensoren hetzelfde en we anonimiseren op de server door het afknippen dus we kunnen over de set van sensoren zien of hetzelfde MAC-adres waar geweest is (niet enkel op de sensor). We hebben wel detailverlies omdat we afknippen op de server, maar met een bepaalde zekerheid kunnen we wel zeggen dat dezelfde telefoon bij sensor A en later bij sensor B is geweest.”*

Over de statistische bewerkingen die daarna worden toegepast op de ontdebeld data heeft de directeur van Bureau RMC verklaard: *“Er is eenmalig bij de installatie van elke sensoren ‘gehand-ijkt’. Dan wordt de conversie bepaald van het aantal signalen naar het aantal passanten, want niet iedereen heeft ook zijn wifi aan staan. Dit doen we eenmalig en verder doen we marktonderzoek naar de eventuele toename of afname van wifigebruik.”*¹⁰⁵

En: *“Bij het hand-ijking wordt vastgesteld hoeveel procent van de voorbijgangers bijvoorbeeld een fietser is. Dit percentage wordt later van de verzamelde data afgetrokken zodat we alleen de passanten overhouden. Dit is een kansberekening. Dit maakt onze tellingen iets minder betrouwbaar want hoeveel fietsers en auto’s er langskomen op het tijdstip van ijken passen we toe als een gemiddelde voor de hele dag. Dit vertellen we ook heel nadrukkelijk aan klanten.”*¹⁰⁶

Het college B&W Enschede heeft op verzoek van de AP enkele rapportages die zij van Bureau RMC heeft ontvangen aan de AP overlegd.¹⁰⁷ Daaruit volgt dat het college B&W Enschede ten eerste schattingen in cijfers en grafieken ontvangt van verschillende variabelen over de unieke bezoekers aan de binnenstad van Enschede. Hierna is een schermafbeelding getoond met de cijfers over de week van 1 april 2019 tot 7 april 2019.¹⁰⁸ De namen van de elf sensoren staan hier ook in opgenomen.

¹⁰⁴ Pagina 9 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

¹⁰⁵ Pagina 8 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

¹⁰⁶ Pagina 8 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

¹⁰⁷ Uitdraai rapport week 37 2018 uit City Traffic Tool, bijlage 2 bij de brief van 20 september 2018 van het college B&W Enschede aan de AP (dossierstuk 3). Citytraffic_aantal_telpunt 4 Excelsheets en Citytraffic_weekoverzicht 4 Excelsheets, bijlage 14 en 15 bij de brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).

¹⁰⁸ enschede_Whole_export_2019w14.xls in Citytraffic_weekoverzicht 4 Excelsheets, bijlage 15 bij de brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

	A	B	C	D	E	F	G	H	I	J	K	L
1	locatie	enschede										
2	zone	Whole										
3	Periode	01-04-2019 to 07-04-2019										
4												
5	Unieke bezoekers	Uniek %	nieuwe bezoekers	verblijfsijd	bzk. frequentie							
6	293.159	77,3%	31,6%	1h33m51s	1,3							
7												
8	bezoekers tegen				bezoekfrequentie			drukte verdeling			distributie verblijfsijd	
9	datum	Unieke bezoekers	verblijfsijd		aantal bezoeken	percentage					verblijfsijd klasse	percentage
10	maandag	34.528	1h35m		1	83%					0-30 min.	30%
11	dinsdag	38.305	1h33m		2	11%					30-60 min.	18%
12	woensdag	36.393	1h34m		3	4%					1-2 uur	22%
13	donderdag	41.711	1h32m		4	2%					2-3 uur	12%
14	vrijdag	41.257	1h35m		>4	1%					> 3 uur	17%
15	zaterdag	57.580	1h33m									
16	zondag	43.385	1h35m									
17												
18												
19												
20												
21												
22												

Figuur 5: Weekrapportage van Bureau RMC aan college B&W Enschede week 1 tot en met 7 april 2019

Ten tweede ontvangt het college B&W Enschede schattingen van het aantal unieke bezoekers per uur per sensor.¹⁰⁹

De AP constateert op basis van het voorgaande dat het college B&W Enschede schattingen ontvangt van verschillende variabelen over unieke bezoekers aan de binnenstad van Enschede. Ten behoeve hiervan worden de van toepassing zijnde gegevens in de langetermijntabel ontdekt op basis van het afgeknipte gepseudonimiseerde MAC-adres en vervolgens worden er bepaalde statistische berekeningen op toegepast.

Privacyprotocol City Traffic-methode van Bureau RMC

Specifiek over de verwerkingen van persoonsgegevens in het kader van de City Traffic-methode heeft Bureau RMC een privacyprotocol opgesteld. Gedurende de periode van 25 mei 2018 tot en met 21 april 2020 hebben er op de website van Bureau RMC opeenvolgend twee versies van dit privacyprotocol bestaan, in beide versies waren de volgende passages opgenomen:¹¹⁰

“1.1 Om onze dienstverlening mogelijk te maken, verwerken wij diverse passantengegevens. De passantengegevens omvatten gegevens van passanten die direct of indirect herleidbaar zijn tot een individuele passant. De passantengegevens zijn daarom aan te merken als persoonsgegevens in de zin van de Algemene verordening gegevensbescherming (AVG). (...).”

3.1 (...) De analysesresultaten worden uitsluitend op geaggregeerde basis gerapporteerd aan onze opdrachtgevers. Dit betekent dat de gegevens in deze rapportages niet meer terug te herleiden zijn tot het versleutelde nummer (van het MAC-adres van het apparaat) van een passant, en evenmin tot de gegevens van een apparaat, dat een passant bij zich draagt. Wij verstrekken dus geen persoonsgegevens aan onze opdrachtgevers.”

¹⁰⁹ Antwoord op 'Vragen over de informatie die de gemeente Enschede van bureau RMC ontvangt' en Citytraffic_aantal_telpunt 4 Excelsheets, bijlage 14 bij brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).

¹¹⁰ Privacy protocol passantentellingen Bureau RMC laatste update 10 april 2018 (dossierstuk 8) en Privacy protocol passantentellingen Bureau RMC laatste update 22 januari 2019 (dossierstuk 11).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

In de eerste passage verklaart Bureau RMC dat zij in het kader van de City Traffic-methode persoonsgegevens in de zin van de AVG verwerkt. Het privacyprotocol benoemt niet tot welk moment in de fase van het verwerkingsproces dit het geval is. Uit de tekst bij stap 4 ‘Anonimiseren’ in de infographic over de City Traffic-methode (zie Figuur 2) leidt de AP af dat Bureau RMC van mening is dat zij persoonsgegevens verwerkt tot aan het moment van anonimiseren. De tekst luidt namelijk: *“Op de server wordt de gepseudonimiseerde data afgeknipt, zodat deze op geen enkele wijze te herleiden valt naar een uniek apparaat of individu. De data die we hebben is daardoor anoniem.”*

De AP concludeert op basis van het voorgaande dat Bureau RMC in haar privacyprotocol, dat specifiek ziet op verwerkingen via de City Traffic-methode, heeft opgenomen dat zij en/of haar partners vanaf in ieder geval 25 mei 2018 persoonsgegevens verwerken in de zin van de AVG. De AP concludeert ook dat Bureau RMC in haar privacyprotocol heeft opgenomen dat de rapportages die opdrachtgevers van Bureau RMC ontvangen geen persoonsgegevens bevatten.

Leefpatronen te herleiden uit de langetermijntabel

Zoals in bijlage 1 paragraaf 2.5 door de AP wordt vastgesteld, is door Bureau RMC per 1 januari 2019 het ‘anonimiseren op de server’ ingevoerd. Dit betekent dat van elk gepseudonimiseerd MAC-adres bij ontvangst op de server de laatste drie karakters (zonder dubbele punt) worden verwijderd.

De AP merkt op dat, in tegenstelling tot over het pseudonimiseren van het MAC-adres, de AP van [VERTROUWELIJK] of Bureau RMC geen document heeft ontvangen met een uitgebreide toelichting op het afknippen en waarom er gekozen is voor deze manier van anonimiseren.¹¹¹ In het algemeen geldt dat het afknippen van een attribuut een anonimiseringstechniek is waarmee een attribuut wordt gegeneraliseerd. Zo kunnen bijvoorbeeld tijdstippen in minuten worden gegeneraliseerd tot een tijdsinterval (uur, dag, maand).

Het afknippen heeft tot gevolg dat niet één maar meerdere gepseudonimiseerde MAC-adressen leiden tot één en hetzelfde afgeknipte gepseudonimiseerde MAC-adres.¹¹² Het afknippen ziet op wereldwijd uitgegeven MAC-adressen; MAC-adressen worden niet per land of locatie uitgegeven.

Om te toetsen of het afknippen op *lokaal niveau*, namelijk in de binnenstad van Enschede, heeft geleid tot voldoende mobiele apparaten met hetzelfde afgeknipte gepseudonimiseerde MAC-adres om de gegevens anoniem te maken, heeft een toezichthouder van de AP de langetermijntabel met gegevens van een aantal veel voorkomende afgeknipte gepseudonimiseerde MAC-adressen over de weken 23 tot en met 34 van 2019 geanalyseerd.¹¹³ Als er lokaal voldoende apparaten met hetzelfde afgeknipte gepseudonimiseerde MAC-adres in de binnenstad zouden bewegen dan zouden er geen leefpatronen zichtbaar moeten zijn in de gegevens. Dit omdat het dan leefpatronen van meerdere apparaten (en dus personen) betreft.

¹¹¹ Het document over de pseudonimiseringsmethode betreft het document MAC hashing analysis opgesteld door [VERTROUWELIJK], ontvangen van [VERTROUWELIJK] op 3 juni 2019 (dossierstuk 43).

¹¹² Zie pagina 19 van WP 216 Advies 5/2014 over anonimiseringstechnieken.

¹¹³ Export Enschede sep-dec long term table.zip en Export Enschede jun - aug 2019 long term table.zip, aangeleverd door [VERTROUWELIJK] op 12 en 16 december 2019 (dossierstukken 69 en 72).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

De AP heeft na eigen onderzoek geconstateerd dat er uit de gegevens van bepaalde afgeknipte gepseudonimiseerde MAC-adres wel duidelijke leefpatronen van individuen zijn af te leiden. Dit volgt uit de hieronder opgenomen Figuur 6, Figuur 7, Figuur 8 en Figuur 9 met daarin visualisaties van de gegevens van vier afgeknipt gepseudonimiseerde MAC-adressen.¹¹⁴ In elke visualisatie staan horizontaal de dagen van de week en verticaal het weeknummer in 2019. Ieder grijs vlakje representeert een hele dag, van 0:00 's nachts tot 23:59:59. De uren 8:00 en 18:00 zijn gemarkeerd. Een gekleurd streepje of vlak houdt in dat het afgeknipte gepseudonimiseerde MAC-adres in kwestie van het beginmoment tot het eindmoment binnen bereik was van de betreffende sensor.

De eerste visualisatie hieronder toont een consistente aanwezigheid binnen het bereik van de sensor [VERTROUWELIJK] (rood), namelijk elke maandagmiddag, woensdag en zaterdag van ongeveer 10:00 tot 18:00 en donderdag van ongeveer 10:00 tot 21:00. Het patroon vertoont sterke overeenkomsten met de winkeltijden die gelden in de binnenstad van Enschede, waarbij het donderdag koopavond is.¹¹⁵ Ook volgt uit het patroon dat het afgeknipte gepseudonimiseerde MAC-adres elke laatste zondag van de maand voor een paar uur binnen de rode sensor was. Gezien dit patroon acht de AP het niet ondenkbaar dat het toebehoort aan een medewerker of bedrijfsleider van een van de winkels in de Langestraat in Enschede, waar de sensor [VERTROUWELIJK] hangt.¹¹⁶



Figuur 6: Eerste visualisatie van afgeknipt gepseudonimiseerd MAC-adres

¹¹⁴ Verklaring van Ambtshandelingen analyse langetermijntabel van 18 februari 2020 (dossierstuk 79).

¹¹⁵ <https://www.enschede.nl/vrijetijd/openingstijden-winkels-en-koopzondagen>

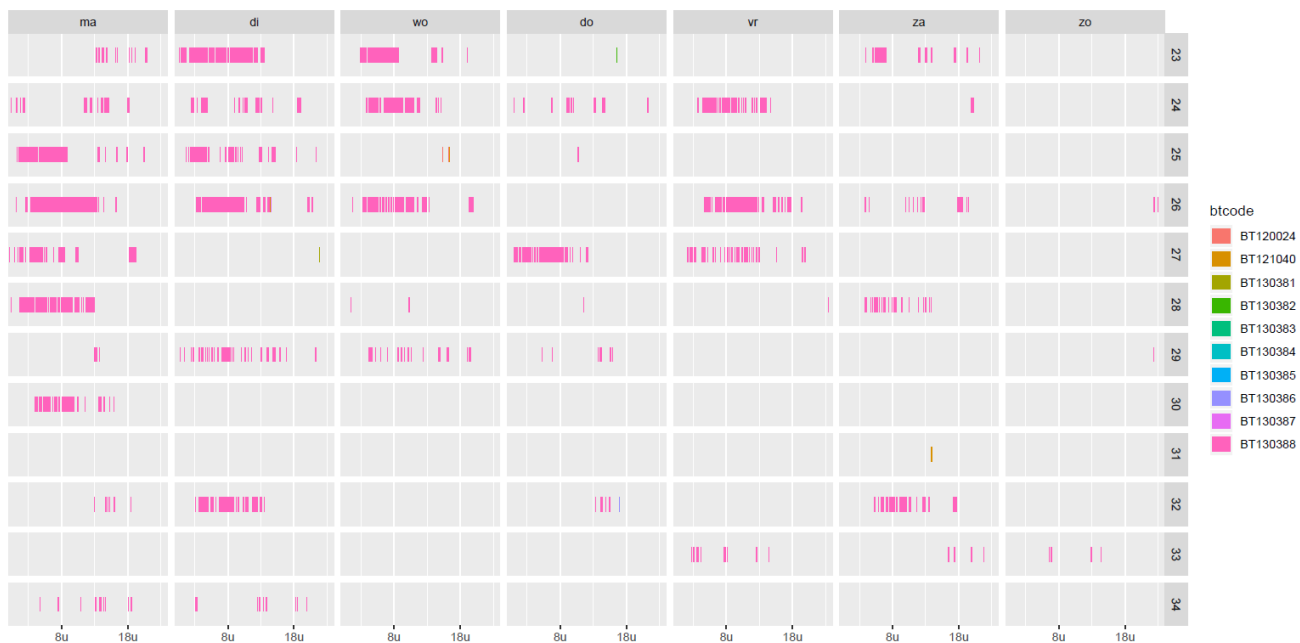
¹¹⁶ Excellijst locatie sensoren, bijlage bij e-mail van 23 mei 2019 van Bureau RMC aan de AP (dossierstuk 25).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Net als bij bovenstaande visualisatie is er ook bij onderstaande visualisatie meerdere uren op één dag aanwezig binnen het bereik van één sensor (roze). Hier valt op dat er op één dag ofwel geen enkele registratie te zien is (geen streepjes) ofwel registraties over de dag verspreid. Dit is het gevolg van het op pagina 40 en 41 beschreven feit dat de bewonersfilter dagelijks wordt toegepast en dus elke dag een andere uitkomst kan hebben (wel of geen bewoner). Daarnaast is te zien in bijvoorbeeld de dinsdag in week 23 dat als er wel registraties zijn tussen 5 en 7 uur maar niet tussen 22 en 24 uur, dat dan het bewonersfilter niet geactiveerd wordt (er staan immers streepjes in deze dag). De AP acht het niet ondenkbaar, gezien de nachtelijke registraties, dat bovenstaand patroon toebehoort aan een bewoner.



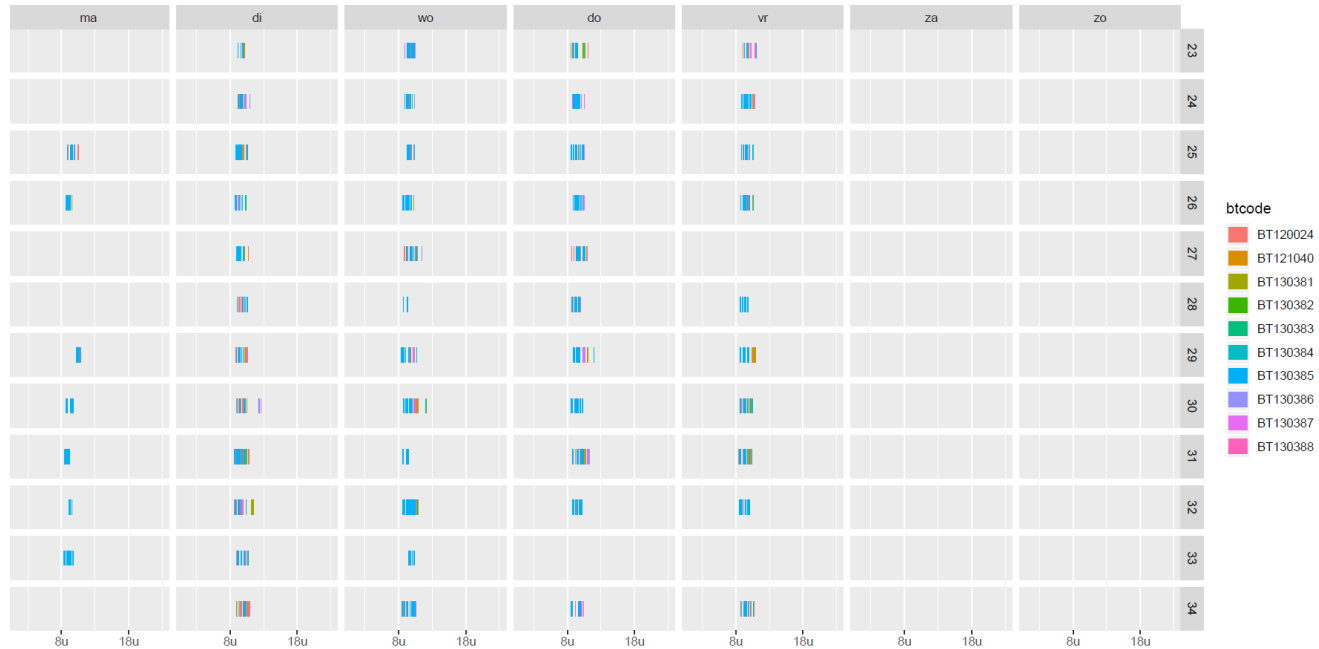
Figuur 7: Tweede visualisatie van afgeknipt gepseudonimiseerd MAC-adres

De derde visualisatie hieronder toont een afgeknipt gepseudonimiseerd MAC-adres dat op dinsdag tot en met vrijdag elke dag tussen ongeveer 8:00 tot 11:00 gesignaleerd wordt door veel van de sensoren in de binnenstad van Enschede. Het toont een regelmatig beweegpatroon over meerdere sensoren heen. Het patroon zou bijvoorbeeld kunnen zijn van een pakketbezorger.



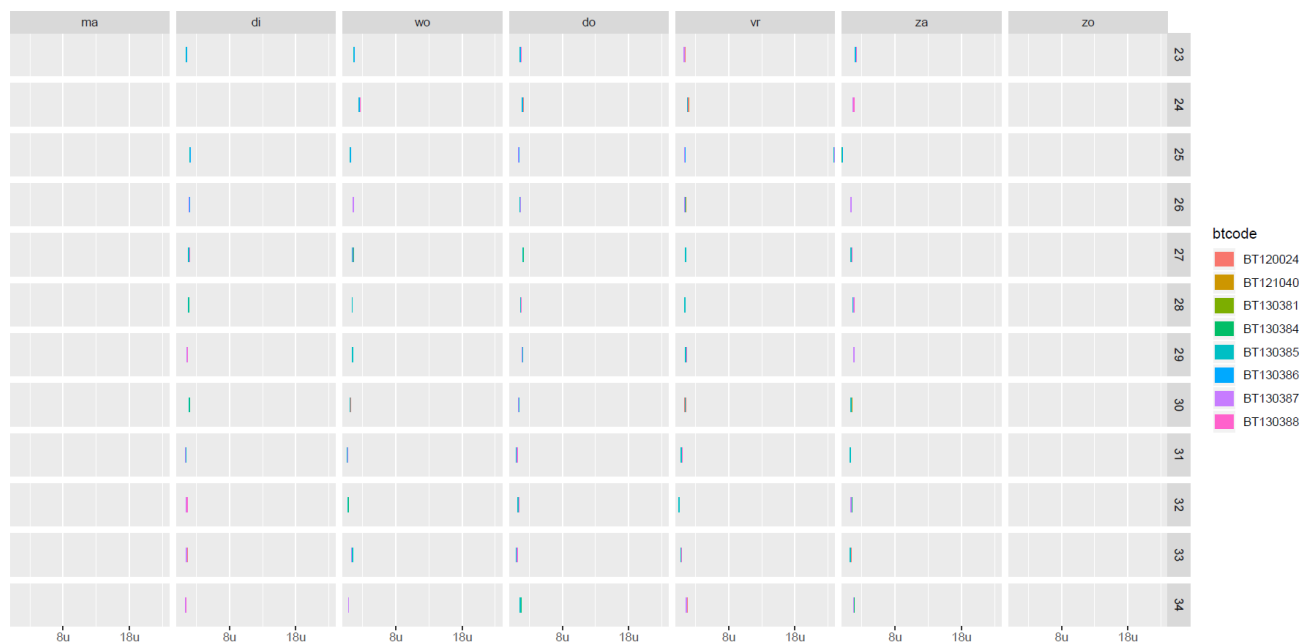
Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]



Figuur 8: Derde visualisatie van afgeknipt gepseudoniseerd MAC-adres

De vierde visualisatie hieronder toont een afgeknipt gepseudoniseerd MAC-adres dat op dinsdag tot en met zaterdag tussen 04:00 en 05:00 's nachts door een aantal van de sensoren in de binnenstad van Enschede is opgevangen. Wellicht betreft dit een persoon die graag 's nachts een wandeling maakt.



Figuur 9: Vierde visualisatie van afgeknipt gepseudoniseerd MAC-adres



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

De AP constateert op basis van het voorgaande dat er uit de langetermijntabel van na 1 januari 2019 duidelijke leefpatronen te destilleren zijn. Gezien de regelmatigheid van de patronen kan redelijkerwijs worden geconcludeerd dat de bij het patroon horende registraties toebehoren aan één mobiel apparaat.¹¹⁷

1.3 Duur verwerking en aantal betrokkenen

De AP heeft hierboven vastgesteld dat in ieder geval sinds 25 mei 2018 er in de binnenstad van Enschede gegevens van mobiele apparaten waarop de wifi staat ingeschakeld worden verzameld en verwerkt. De AP heeft vastgesteld dat de sensoren in de periode vanaf 10 december 2018 tot en met 3 januari 2019 uit hebben gestaan, dus in deze periode zijn er geen nieuwe gegevens verzameld.¹¹⁸ Echter, eerder verzamelde gegevens hebben in deze periode wel opgeslagen gestaan in de langetermijntabel, dus er werden in deze periode wel gegevens verwerkt.

Tot het eind van het verrichtte onderzoek (21 april 2020) had de AP meerdere aanwijzingen dat de wifimetingen nog steeds uitgevoerd worden. Zo vermeldde de website van de gemeente Enschede nog steeds dat er wifimetingen in de binnenstad werden verricht¹¹⁹ en rapporteerde ook de website www.binnenstadsmonitorenschede.nl nog steeds wekelijks over het aantal unieke bezoekers in de binnenstad van Enschede.¹²⁰ Daarnaast geldt dat de AP noch van het college B&W Enschede noch van Bureau RMC tijdens het onderzoek een bericht heeft ontvangen dat de wifimetingen zijn gestopt. Tijdens de handhavingprocedure van de AP heeft het college B&W Enschede in haar zienswijze vermeld dat het college gestaakt is met de wifitellingen. Het college B&W Enschede heeft op 30 april 2020 aan Bureau RMC de opdracht gegeven om per 1 mei 2020 de sensoren uit te zetten. De sensoren leveren geen telgegevens meer vanaf 1 mei 2020.¹²¹ De AP stelt daarom vast dat de duur van de verwerkingen de periode van 25 mei 2018 tot en met 30 april 2020 is.

Het precieze aantal betrokkenen van wie in periode van 25 mei 2018 tot april 2020 via zijn of haar mobiele apparaat gegevens zijn verwerkt kan niet worden bepaald, omdat door [VERTROUWELIJK] en Bureau RMC de gegevens niet langer worden bewaard dan tussen de zes en zeven maanden. Aan de hand van de door [VERTROUWELIJK] aan de AP verstrekte langetermijntabel met gegevens over de periode van 1 juni 2019 tot en met 6 december 2019 kan wel een schatting worden gemaakt van het aantal mobiele apparaten van betrokkenen waarvan er in de periode vanaf 25 mei 2018 tot 4 april 2020 gegevens zijn verwerkt.¹²²

In onderstaande grafiek is het aantal *unieke* afgeknipte gepseudonimiseerde MAC-adressen in de 27 weken in de periode van 1 juni 2019 tot en met 6 december 2019 uitgezet. Elk afgeknipte gepseudonimiseerd MAC-adres komt derhalve in de grafiek éénmaal voor, namelijk in de week waarin deze voor het eerst is gedetecteerd door een sensor in de binnenstad van Enschede.

¹¹⁷ Registraties die buiten dit patroon vallen kunnen wel afkomstig zijn van andere mobiele apparaten.

¹¹⁸ Zie ook bijlage 1, paragraaf 2.5.

¹¹⁹ <https://www.enschede.nl/bestuur/privacy/wifi-tellingen-binnenstad> (laatst bezocht op 26 februari 2020).

¹²⁰ <https://www.binnenstadsmonitorenschede.nl/bezoekers-weekcijfers> (laatst bezocht op 26 februari 2020).

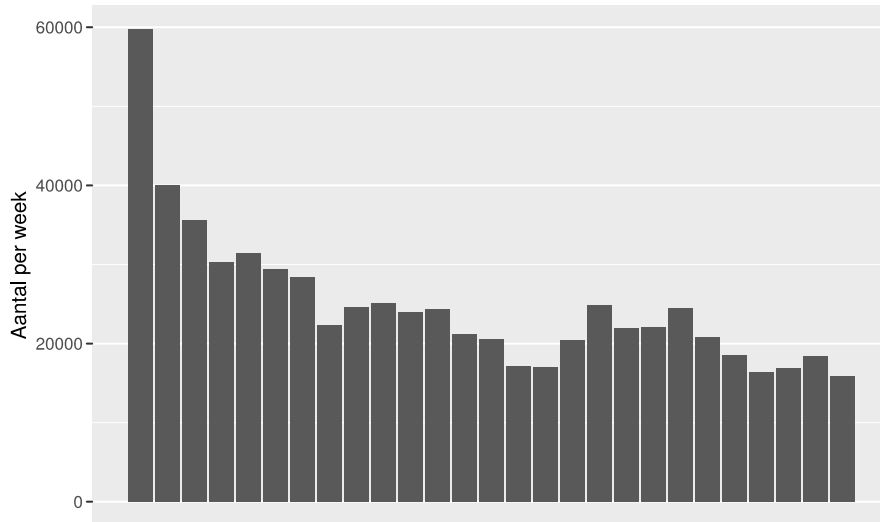
¹²¹ Brief van 16 februari 2021 van het college B&W Enschede aan de AP, pagina 3 en bijlage 2.

¹²² Het unieke aantal afgeknipte gepseudonimiseerde MAC-adressen wordt hiervoor gehanteerd als schatter voor het aantal unieke mobiele apparaten.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]



Figuur 10: wekelijks aantal detecties van 1 juni tot en met 6 december 2019

De grafiek laat zien dat er in eerste weken veel nieuwe gedetecteerde mobiele apparaten zijn. In de weken erna vlakt het aantal nieuwe detecties af. In de laatste week ging het om ongeveer 16.000 mobiele apparaten. In totaal stonden er in deze periode van 27 weken gegevens van 671.701 unieke mobiele apparaten in de langetermijntabel.

Als voorgaande cijfers over de periode 1 juni - 6 december 2019 worden toegepast op de periode van 25 mei 2018 tot 4 april 2020, dan leidt dit tot een schatting van grofweg 1,8 miljoen unieke mobiele apparaten waarvan sinds 25 mei 2018 gegevens zijn verwerkt via de sensoren in Enschede. Hierbij is aangenomen dat de eerste 27 weken na 25 mei 2018 hetzelfde verlopen als bovenstaande grafiek. Ook is aangenomen dat na de 27 weken tot aan 4 april 2020 het aantal nieuwe detecties wekelijks 16.000 is.¹²³ Dit aantal houdt overigens geen rekening met het feit dat voor bewoners en personen die werken in de binnenstad van Enschede en die wifi hebben ingeschakeld op hun mobiele apparaat geldt dat zij niet éénmaal maar (veel) vaker door de sensoren zijn gedetecteerd.

De AP constateert op basis van het voorgaande dat het college B&W Enschede vanaf in ieder geval 25 mei 2018 tot heden gegevens van grofweg 1,8 miljoen unieke mobiele apparaten heeft laten verwerken en dat het aantal detecties beduidend hoger zal liggen.

¹²³ Vanaf 25 mei 2018 tot 4 april 2020 betreft 31 weken in 2018, 52 weken in 2019 en 14 weken in 2020. De berekening is dus als volgt: 671.701 (voor de eerste 27 weken vanaf 25 mei 2018) + ((31-27)+52+14) x 16.000 = 1.791.701.



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

2. Feiten omtrent het begrip verwerkingsverantwoordelijke

2.1 Besluit starten wifimetingen

Het besluit om via sensoren gegevens over bezoekers van de binnenstad van Enschede te verzamelen (hierna ook: het uitvoeren van wifimetingen) is genomen door het college B&W Enschede. Dit volgt uit het collegebesluit waarvan de eerste pagina hierna is weergegeven.¹²⁴

Gemeente  Enschede 8.B

Agendaformulier B&W-vergadering 5 september 2017

Portefuillehouder	[REDACTED] (Agendaletter B)		
	0 0		
Onderwerp	start 24/7 passantentellingen met sensoren in de binnenstad		
Openbaar	Openbaar: ja		
Programma	Economie & Werk	Corsanummer:	1700087130
Opsteller	[REDACTED]	Casenummer	BV17000445
	(053) 481 52 98		
Urgentie			
Raadsbesluit nodig	Nee		
Raad informeren	Ja, via brief		

Mee geadviseerd door	[REDACTED] (functionaris voor de gegevensbescherming)
Parafen	1. Controller (optioneel)
	2. Directeur
	3. Gemeentesecretaris
	4. Portefuillehouder
Advies gemeentesecretaris	

.....

Conceptbesluit
Voorstel portefeuillehouder om:

- per 6 september te starten met 24/7 passantentellingen via sensoren in de binnenstad.
- De raad hierover per brief te informeren.

Kernboodschap
De binnenstad is één van de toplocaties van onze stad. We willen graag weten hoe deze locatie zich ontwikkelt: hoeveel passanten lopen er door de straten, hoeveel bezoekers heeft de binnenstad, hoe lang blijven mensen in de binnenstad en waar lopen ze langs? Om hier een beter beeld bij te krijgen stappen wij vanaf 6 september over van 1-jaarlijkse handmatige tellingen naar 24/7 tellingen via sensoren. Bij deze tellingen wordt de privacy goed in acht genomen en kan geen link worden gelegd naar persoonlijke gegevens. Het gebruik van wifidata voor 24/7 monitoring van de binnenstad is een initiatief vanuit de Smart City agenda.

B&W besluit dd. [REDACTED]	(In te vullen na de vergadering door gemeentesecretaris)
	VERGADERING BURG. EN WETH. [REDACTED]
	05 SEP, 2017 [REDACTED]

Figuur 11: Eerste pagina collegebesluit, d.d. 5 september 2017, start wifimetingen.

¹²⁴ Collegebesluit van 5 september 2017, bijlage bij e-mail van 23 september 2019 van het college B&W Enschede aan de AP (dossierstuk 62).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

Uit deze pagina volgt dat het college B&W Enschede op 5 september 2017 heeft ingestemd met het voorstel van de wethouder om per 6 september 2017 over te stappen van 1-jaarlijkse handmatige tellingen naar 24/7 wifimetingen.

Na het collegebesluit van 5 september 2017 heeft het college B&W Enschede de gemeenteraad van Enschede per brief geïnformeerd.¹²⁵ Daarnaast is er op de website van de gemeente zowel een persbericht als een aantal Q&A's over de wifimetingen geplaatst.¹²⁶ In deze communicatie is aangegeven dat City Traffic B.V. de wifimetingen zou gaan uitvoeren.

City Traffic B.V. was destijds een vennootschap in eigendom van Bureau RMC en [VERTROUWELIJK]. Op 24 mei 2018 is deze vennootschap opgeheven.¹²⁷ Sindsdien voert Bureau RMC in opdracht van het college B&W Enschede de wifimetingen uit, waarbij Bureau RMC bepaalde diensten afneemt van [VERTROUWELIJK]. Bureau RMC hanteert de term 'City Traffic' nu voor haar dienst om via wifimetingen unieke bezoekers in o.a. steden te tellen.¹²⁸

Over het offertetraject dat voorafging aan het collegebesluit heeft de directeur van Bureau RMC het volgende verklaard: *"City Traffic bestaat vanaf 2010 en heeft zich gepositioneerd om als alternatief voor Locatus passantentellingen te doen. Locatus was de partij die handtellingen deed één keer per jaar. Ik heb toen CityTraffic opgericht om meer dynamische data te genereren. Zowel Locatus als CityTraffic is gevraagd door de Gemeente Enschede om een voorstel te doen om daar wifitellingen te doen. (...) De aanleiding voor het verzoek van de gemeente was het feit dat er via een bepaalde subsidie gratis wifinetwork wilde uitrollen met NDIX¹²⁹ en toen is aan bureau RMC gevraagd of wij op dat netwerk konden aansluiten om passanten te tellen. Onderdeel van de competitie was ook dat we een correlatie moesten laten zien tussen de tellingen van NDIX. Later is besloten om geen gebruik te maken van de tellingen van NDIX."*¹³⁰ De door Bureau RMC uitgebrachte offerte bevestigt dat het college B&W Enschede had verzocht om aansluiting met het netwerk van NDIX.¹³¹

Op vragen van de AP over de invloed van de gemeente op de locatie van de sensoren heeft de directeur van Bureau RMC geantwoord: *"De locaties van de sensoren voor het NDIX netwerk waren al bepaald. De gemeente Enschede gaf vervolgens aan welke gebieden/straten ze mistte en dus waar sensoren geplaatst moesten worden. De*

¹²⁵ Brief van 5 september 2017 van het college B&W Enschede aan de gemeenteraad, bijlage 3 bij de brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).

¹²⁶ Persbericht van 6 sept 2017 over meten drukte met sensoren en Q&A nadere informatie 24/7 tellingen in de binnenstad, bijlage 4 en 5 bij de brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).

¹²⁷ Uittreksel Kamer van Koophandel City Traffic B.V. van 9 augustus 2019 (dossierstuk 81).

¹²⁸ Pagina 10 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55). Zie ook www.citytraffic.nl (dossierstuk 54).

¹²⁹ NDIX B.V. is een organisatie gevestigd in Enschede dat werkt aan het beheren en verder uitbouwen van een digitale marktplaats en het beschikbaar stellen van maximale bandbreedte aan bedrijven om innovatie te stimuleren. Zie www.ndix.net.

¹³⁰ Pagina 10 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

¹³¹ Pagina 2 van offerte Monitoring Bezoekersstromen Binnenstad Enschede van Bureau RMC, bijlage 1 bij brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

*gemeente heeft dus de locaties van de sensoren bepaald. (...) de gemeente had de regierol in de opdrachtverstrekking. Voor wat betreft het aantal sensoren had ik er liever veel meer gehad.*¹³²

De AP constateert op basis van het voorgaande dat het college B&W Enschede het initiatief en het uiteindelijke besluit heeft genomen om per 6 september 2017 te starten met 24/7 metingen via sensoren in de binnenstad van Enschede. Het college B&W Enschede heeft daarvoor twee bedrijven een offerte laten uitbrengen. De opdracht is gegund aan City Traffic B.V., thans Bureau RMC. Tot slot constateert de AP dat het college B&W Enschede een sturende rol had in het aantal en de locaties van de sensoren.

2.2 Doel van de wifimetingen voor het college B&W Enschede

In het collegebesluit van 5 september 2017 heeft het college B&W Enschede het doel van de wifimetingen in de binnenstad als volgt geformuleerd: *“We willen graag weten hoe deze locatie zich ontwikkelt: hoeveel passanten lopen er door de straten, hoeveel bezoekers heeft de binnenstad, hoe lang blijven mensen in de binnenstad en waar lopen ze langs? Om hier een beter beeld bij te krijgen stappen wij vanaf 6 september over van 1-jaarlijkse handmatige tellingen naar 24/7 tellingen via sensoren.”*¹³³

In de Q&A op de website van de gemeente Enschede staat sinds december 2017 het volgende over het doel van de wifimetingen: *“De gemeente Enschede investeert veel in de binnenstad en wil de effecten hiervan kunnen meten. Dit doen we via de passantentellingen via sensoren die ons dagelijks inzicht geven in het aantal bezoekers en de bezoekersstromen in de binnenstad. Hiermee krijgen we een beeld van de aantrekkingskracht van onze binnenstad, van de invloed van ruimtelijke veranderingen in de binnenstad en van effecten van bijvoorbeeld evenementen, promotiecampagnes en winkeltijden. De tellingen via sensoren zijn ook interessant voor ondernemers die gevestigd zijn of die zich willen vestigen in de binnenstad en voor investeerders.”*¹³⁴

Na de start van de wifimetingen heeft de klager een klacht ingediend bij het college B&W Enschede.¹³⁵ In reactie op de klacht schrijft het college B&W Enschede in een brief aan de klager:

*“- Er is sprake van een duidelijk doel (wij investeren veel in de binnenstad en willen de effecten daarvan meten);
- De grondslag voor de tellingen is “gerechtvaardigd belang” (verantwoord omgaan met publieke gelden);”*¹³⁶

De AP constateert op basis van het voorgaande dat de wifimetingen worden uitgevoerd met als doel het meten van de effecten van investeringen van de gemeente Enschede in de binnenstad met het oog op een verantwoord omgaan met publieke gelden. Het college B&W Enschede acht de wifimetingen rechtmatig omdat zij volgens haar plaatsvinden op basis van de grondslag ‘gerechtvaardigd belang’.

¹³² Pagina 11 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 en e-mail van 19 augustus 2019 van Bureau RMC aan de AP (dossierstukken 49 en 55).

¹³³ Zie Figuur 1 in dit rapport.

¹³⁴ Q&A aangepast december 2017, bijlage 6 bij de brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26). Een tekst met gelijke strekking stond er vanaf het collegebesluit van 5 september 2017 op de website van de gemeente.

¹³⁵ Brief van 10 november 2017 van klager aan gemeente Enschede, bijlage bij brief van 16 juli 2018 van klager aan de AP (dossierstuk 1).

¹³⁶ Brief van 21 december 2017 van het college B&W Enschede aan de klager, bijlage bij brief van 16 juli 2018 van de klager aan de AP (dossierstuk 1).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

2.3 Bewerkersovereenkomst tussen college B&W Enschede en Bureau RMC

Op 26 september 2017 hebben het college B&W Enschede en de voorganger van Bureau RMC specifiek voor wat betreft de verwerkingen van persoonsgegevens in het kader van de wifimetingen in de binnenstad van Enschede een bewerkersovereenkomst als bedoeld in artikel 14 van de toen geldende Wet bescherming persoonsgegevens (hierna: Wbp) gesloten.¹³⁷

De aanhef benoemt de twee partijen tussen wie de overeenkomst is gesloten: *“De Gemeente Enschede, verder te noemen de verantwoordelijke, ten deze rechtsgeldig vertegenwoordigd door: [VERTROUWELIJK] en City Traffic, gevestigd te Amsterdam, verder te noemen de bewerker, ten deze rechtsgeldig vertegenwoordigd door [VERTROUWELIJK], verklaren te zijn overeengekomen (...)”*

Het eerste, derde en vijfde lid van artikel 4 van de bewerkersovereenkomst bepaalt het volgende over de rechten en plichten van de twee partijen:

- “1. Het College van Burgemeester en Wethouders van de Gemeente Enschede is verantwoordelijke in de zin van de Wbp.*
- 3. De bewerker verwerkt gegevens ten behoeve van de verantwoordelijke in overeenstemming met diens instructies.*
- 5. De bewerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van persoonsgegevens. De bewerker verwerkt persoonsgegevens slechts in opdracht van de Afdeling Strategie en Beleid en zal alle redelijke instructies dienaangaande opvolgen, behoudens afwijkende wettelijke verplichtingen.*
- 6. De bewerker zal te allen tijde op eerste verzoek van de verantwoordelijke onmiddellijk alle van de Gemeente Enschede afkomstige persoonsgegevens met betrekking tot deze bewerkersovereenkomst aan verantwoordelijke ter hand stellen.”*

Artikel 7, over inschakeling van derden, bepaalt:

- “1. De bewerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande schriftelijke toestemming van de verantwoordelijke.*
- 2. Wij gaan akkoord dat de bewerker de data laten verwerken door [VERTROUWELIJK]. Bewerker heeft met deze partij een bewerkingsovereenkomst gesloten.*
(...)”

De AP constateert op basis van het voorgaande dat het college B&W Enschede zichzelf als verwerkingsverantwoordelijke beschouwt in de zin van de Wbp (thans de AVG) voor het uitvoeren van wifimetingen. Daarnaast constateert de AP dat City Traffic B.V., thans Bureau RMC, persoonsgegevens verwerkt in opdracht van het college B&W Enschede, diens instructies moet opvolgen en op verzoek van het college B&W Enschede de persoonsgegevens moet overleggen. Tot slot volgt uit het voorgaande dat het college B&W Enschede ermee heeft ingestemd dat Bureau RMC [VERTROUWELIJK] heeft ingehuurd voor het verwerken van de persoonsgegevens.

¹³⁷ Bewerkersovereenkomst monitor bezoekersstromen binnenstad Enschede d.d. 26 september 2017, bijlage 2 bij brief van 29 oktober 2018 van het college B&W Enschede aan de AP (dossierstuk 6).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

2.4 De diensten die [VERTROUWELIJK] aan Bureau RMC levert

Bureau RMC huurt voor de installatie en het onderhoud van de sensoren in de binnenstad van Enschede [VERTROUWELIJK] in. Dit blijkt uit de volgende verklaringen van de directeur van Bureau RMC:

“RMC koopt een abonnement in bij [VERTROUWELIJK] voor de sensoren en daar zit alles in: de hardware, software, firmware, installatie, service, onderhoud etc. Dit is geregeld in een service level agreement tussen RMC en [VERTROUWELIJK]. Het fysieke beheer van de sensoren ligt bij [VERTROUWELIJK]. Vervolgens neemt de gemeente Enschede voor deze sensoren een abonnement af bij RMC.”¹³⁸

En, op de vraag wie bij installatie de sensor iijkt: *“De installateur van de sensor, dus iemand van [VERTROUWELIJK].”¹³⁹*

Het hiervoor genoemde service level agreement is door de directeur van Bureau RMC aan de AP overlegd. Het service level agreement van 31 oktober 2016 bevestigt dat [VERTROUWELIJK] de installatie en onderhoud van de sensoren uitvoert voor Bureau RMC.¹⁴⁰

Uit het service level agreement blijkt ook dat Bureau RMC [VERTROUWELIJK] inhuurt voor het verzamelen van gegevens met de sensoren en het valideren van die gegevens.¹⁴¹ Dit wordt bevestigd door het feit dat gedurende het onderzoek de medewerkers van [VERTROUWELIJK] over het algemeen de detailvragen van de AP over het verzamelen en verwerken van de gegevens hebben beantwoord¹⁴² en de benodigde documentatie hebben overlegd. Ook volgt uit de overlegde factuur dat [VERTROUWELIJK] betaalt voor de gehuurde serverruimte bij Amazon AWS.¹⁴³

Over de met de sensoren verzamelde gegevens is in artikel 7 van het service level agreement de volgende afspraak opgenomen tussen [VERTROUWELIJK] (de ‘opdrachtnemer’) en Bureau RMC (de ‘afnemer’): *“Opdrachtnemer is op een geen enkele manier gerechtigd om data van afnemer op enige manier te verwerken in een doel anders dan primair voor afnemer van toepassing. (...) Afnemer kan op elk moment de data opeisen alsmede de opdrachtnemer verplichten om data te verwijderen.”*

De AP constateert op basis van het voorgaande dat Bureau RMC [VERTROUWELIJK] inhuurt voor de installatie en het onderhoud van de sensoren in de binnenstad van Enschede en voor het verzamelen en valideren van de gegevens die met de sensoren worden verzameld. Ook stelt de AP vast dat Bureau RMC op grond van het service level agreement op elk moment de gegevens die [VERTROUWELIJK] verzamelt en verwerkt kan opeisen.

¹³⁸ Pagina 1 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

¹³⁹ Pagina 8 van verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

¹⁴⁰ Artikel 1 van de Service Level Agreement [VERTROUWELIJK]-Bureau RMC, bijlage 1 deel 4 bij het Verslag van Ambtshandelingen onderzoek ter plaatse bij Bureau RMC op 29 mei 2019 (dossierstuk 39).

¹⁴¹ De inleiding van de Service Level Agreement [VERTROUWELIJK]-Bureau RMC (dossierstuk 39).

¹⁴² Verslag van verklaring van Bureau RMC en medewerkers [VERTROUWELIJK] afgelegd op 29 mei 2019 (dossierstukken 49 en 55).

¹⁴³ Factuur Aws June 2019, ontvangen van [VERTROUWELIJK] op 29 juli 2019 (dossierstuk 50).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

2.5 Besluit pauzeren wifimetingen en overgaan op 'anonimiseren op de server'

Op 30 november 2018 heeft de AP een nieuwsbericht naar buiten gebracht waarin staat dat op grond van de AVG bedrijven alleen bij hoge uitzondering mensen mogen volgen met wifitracking.¹⁴⁴ Naar aanleiding hiervan heeft [VERTROUWELIJK] binnen de gemeente Enschede, een e-mail gestuurd aan de directeur van Bureau RMC met de volgende vragen:¹⁴⁵

"Hai Huib, ik belde nav het onderstaande bericht. Vragen aan jou:

- Hoe interpreteer jij deze uitspraak?*
- Vallen de metingen van CT (red: City Traffic) hieronder?*
- Zo ja is anonimiseren dan misschien nog een optie?*
- (...)"*

Naar aanleiding van het nieuwsbericht van de AP heeft het college B&W Enschede contact gezocht met Bureau RMC en haar de opdracht gegeven om de wifimetingen te pauzeren. Dit volgt uit de door het college B&W Enschede aan de gemeenteraad verstuurd brief van 6 december 2018:

*"(...) de Autoriteit Persoonsgegevens (AP) [heeft] een artikel gepubliceerd over wifitracking. (...) In het kader van zorgvuldigheid hebben wij ervoor gekozen om City Traffic de opdracht te geven de wifitellingen vooralsnog te pauzeren. In de tussentijd zijn wij in gesprek met City Traffic om in het licht van de publicatie dit op te lossen."*¹⁴⁶

Op 14 december 2018 heeft [VERTROUWELIJK] de volgende e-mail aan de directeur van Bureau RMC gestuurd: *"Wij zijn bezig met een brief aan de raad dat de tellingen weer opgepakt kunnen worden vanaf 1 januari 2019 omdat vanaf dat moment geanonimiseerd wordt geteld. (...) Kun jij ons per mail bevestigen dat jullie ook daadwerkelijk per 1 januari 2019 geanonimiseerd tellen?"*¹⁴⁷

De directeur van Bureau RMC antwoordde op 16 december 2018: *"(...) Wij kunnen hierbij bevestigen dat we vanaf 1 januari 2019 naast het pseudonimiseren op de sensor, zullen anonimiseren op de server. (...)"*

Als bewijs voor de feitelijke invoering van dit 'anonimiseren op de server' is door [VERTROUWELIJK] een schermafbeelding van de wijziging in de softwarecode van de server overlegd aan toezichthouders van de AP.¹⁴⁸ Hieruit volgt dat eind december 2018 het 'anonimiseren op de server' is geïmplementeerd, althans dat [VERTROUWELIJK] van het gepseudonimiseerde MAC-adres (zonder de dubbele punten) worden afgeknipt. Bijlage 1, pagina 38 tot en met 40 beschrijft het afknippen in meer detail.

Op 18 december 2018 is de gemeenteraad door het college B&W Enschede per brief op de hoogte gesteld van het feit dat de wifimetingen zouden worden hervat.¹⁴⁹ In deze brief staat:

¹⁴⁴ www.autoriteitpersoonsgegevens.nl/nl/nieuws/bedrijven-mogen-mensen-alleen-bij-hoge-uitzondering-met-wifitracking-volgen.

¹⁴⁵ E-mail van 3 december 2018 van [VERTROUWELIJK] aan [VERTROUWELIJK] van Bureau RMC, bijlage 7 bij de brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).

¹⁴⁶ Brief van 6 december 2018 aan Raad Enschede pauzeren wifitellingen, bijlage 8 bij de brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).

¹⁴⁷ E-mail van 16 december 2018 van RMC bevestiging anonimiseren, bijlage 10 bij de brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).

¹⁴⁸ Pagina 3 van broncode, afknippen en filters.pdf, bijlage 2 van documenten ontvangen van [VERTROUWELIJK] op 20 juni 2019 (dossierstuk 46).

¹⁴⁹ Brief van 18 december 2018 aan Raad herstart wifitellingen, bijlage 11 bij de brief van 24 mei 2019 van het college B&W Enschede aan de AP (dossierstuk 26).



Datum
11 maart 2021

Ons kenmerk
[VERTROUWELIJK]

“City Traffic werkte tot voor kort met pseudonimisering van data op de sensor (MAC adres die worden versleuteld op de sensor). Dit wordt door de AP gezien als een persoonsgegeven en moet daarmee voldoen aan de Algemene Verordening Gegevensbescherming (AVG). (...) Met geanonimiseerde data is er geen sprake van persoonsgegevens. In dat geval is de Algemene Verordening Gegevensbescherming niet van toepassing. Dit wordt bevestigd in de publicatie van de AP van 30 november j.l. bij de nadere uitleg van de normen. (...) Wij kunnen u melden dat City Traffic ons heeft bevestigd dat zij vanaf 1 januari 2019 overgaan op geanonimiseerd tellen. Op deze manier blijven wij de privacy van bezoekers van onze binnenstad waarborgen. Vanaf 1 januari 2019 worden de sensoren weer geactiveerd en zullen wij weer maandelijks kunnen rapporteren over de tellingen.”

Uit de informatie van het college B&W Enschede volgt dat Bureau RMC over de periode van 10 december 2018 tot en met 3 januari 2019 geen cijfers heeft gerapporteerd aan het college B&W Enschede.¹⁵⁰

De AP constateert op basis van het voorgaande dat het college B&W Enschede naar aanleiding van de publicatie van de AP van 30 november 2018 Bureau RMC de opdracht heeft gegeven de wifimetingen in de binnenstad van Enschede te pauzeren en dat over de periode van 10 december 2018 tot en met 3 januari 2019 er door Bureau RMC geen cijfers aan het college B&W Enschede zijn gerapporteerd. De AP concludeert op basis hiervan dat de sensoren in de binnenstad van Enschede in de genoemde periode uit hebben gestaan. Tevens constateert de AP dat Bureau RMC (op verzoek van het college B&W Enschede) per 1 januari 2019 het zogenaamde ‘anonimiseren op de server’ heeft ingevoerd, waarbij de laatste drie karakters van de gepseudonimiseerde MAC-adressen worden afgeknipt.

¹⁵⁰ aandeelperingang.xls in folder 20190212, bijlage 14 bij brief van 24 mei 2019 van college B&W Enschede aan de AP (dossierstuk 26).