Gemeente Amsterdam

Retouradres: Postbus 94652, 1090 GR Amsterdam

**Gemeente Amsterdam**
**Commissie Persoonsgegevens**

Aan: Directeur Verkeer& Openbare Ruimte, mevrouw E. J. Schieven
Aan: Manager IV Ruimte& Economie, de heer [redacted]
C.c. Stedelijk directeur Ruimte & Economie, de heer L. Loeven
C.c. CIO, de heer J. Flippo
C.c. Privacy Officer Ruimte & Economie, mevrouw [redacted], programmamanager Crowd Management, de heer 5.1, 2, e [redacted], projectleider CMSA, de heer [redacted]

| | |
|---|---|
| Datum | 22-02-2018 |
| Ons kenmerk | |
| Behandeld door | Mw. 5.1, 2, e [redacted] |
| Doorkiesnummer | |
| Faxnummer | nvt |
| E-mail | 5.1, 2, e [redacted]amsterdam.nl |
| Bijlage | 1 |
| Onderwerp | Wifi- tracking |

Geachte mevrouw Schieven, de heer 5.1, 2, e [redacted],

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 25 januari 2018 waren namens de gemeente Amsterdam aanwezig: de heer 5.1, 2, e [redacted] (Programmamanager Crowd Management V&OR), de heer 5.1, 2, e [redacted] (Projectleider CMSA V&OR), mevrouw 5.1, 2, e [redacted] (TU Delft), mevrouw 5.1, 2, e [redacted] (TU Delft), de heer 5.1, 2, e [redacted] (TU Delft), mevrouw 5.1, 2, e [redacted] (team verkeerstaktiek,V&OR), de heer 5.1, 2, e [redacted] (V&OR) en mevrouw 5.1, 2, e [redacted] (project CMSA).

Bij het agendapunt "Wifi- tracking" is het volgende besproken.

U heeft de CPA geïnformeerd over het project Crowd Monitoring Systeem Amsterdam (CMSA) en de hierbij te nemen privacybeschermende maatregelen.

Het project is bedoeld om kwantitatief inzicht te krijgen in voetgangersbewegingen in drukke voetgangersgebieden, historisch en realtime. Er wordt gewerkt met infraroodtelcamerasensoren en wifisensoren die informatie geven over het aantal waargenomen personen per tijdseenheid. Het is de bedoeling om tot een meetlat te komen waarmee wordt vastgesteld of een plek te druk wordt en of er daardoor maatregelen moeten worden genomen om de voetgangersstromen in andere banen te leiden.

De CPA heeft reeds eerder in haar vergadering d.d. 28 september 2017 gesproken over Wifi-tracking. Daar werd gewezen op de brief van de Autoriteit Persoonsgegevens (AP) d.d. 15 juni 2016 inzake Wifi- tracking. De AP stelde dat een belangrijke waarborg omtrent Wifi-tracking, het onmiddellijk en onomkeerbaar anonimiseren van gegevens is, zodra deze door sensoren of andere meetinstrumenten worden vastgesteld. In het CPA advies werd verder vastgesteld dat de techniek verder is ontwikkeld. Er wordt direct een onmiddellijke en onomkeerbare versleuteling op de sensor toegepast, waarbij een deel van de code van het MAC- adres wordt afgekapt en weggegooid. Door deze ruistoevoeging zou het originele MAC- adres niet meer zijn te achterhalen. Het afgekapte MAC- adres wordt vervolgens elke 24 uur nogmaals gehashed. Daardoor is een reispatroon na 24 uur niet meer te koppelen aan een nieuw patroon.

Er is veel discussie over de vraag of een MAC- adres gezien moet worden als een persoonsgegeven. CMSA heeft professor 5.1, 2, e gevraagd om advies te geven over deze discussie. Professor 5.1, 2, e meent dat sinds het arrest van het Hof van Justitie in de Breyer-zaak een MAC- adres niet als een persoonsgegevens aangemerkt kan worden. In dit arrest heeft het Hof de vraag beantwoord of een dynamisch IP- adres een persoonsgegeven is, als de website die over dat IP- adres beschikt niet bekend is met de identiteit van de internetgebruiker die daarvan gebruik maakt. Het Hof ging in dit arrest voorbij aan het single- out criterium en meent dat er sprake is van een persoonsgegeven als de website de wettige middelen heeft om extra gegevens te achterhalen bij een derde partij die nodig zijn om een internetgebruiker te identificeren.[1] In de context van CMSA kan een MAC- adres alleen als persoonsgegeven worden gekwalificeerd als de gemeente de juridische mogelijkheden heeft om de extra gegevens te achterhalen waarmee kan worden achterhaald wat de identiteit is van de gebruiker van het desbetreffende randapparaat.

De CPA vroeg zich tijdens de vergadering af of alleen de MAC- adressen uitgelezen kunnen worden en of de resultaten niet worden vervuild door andere Wifizenders. CMSA meende dat de sensoren alleen MAC- adressen kunnen opvangen. Stilstaande MAC- adressen worden direct uitgefilterd, zodat alleen de bewegende MAC- adressen worden geteld. Vervolgens wordt het MAC- adres direct geanonimiseerd in de sensor. Een deel van het

[1] HvJEU 19 oktober 2016, C- 582/14, ECLI:EU:C:2016:779, rov. 49. (Breyer)

MAC- adres wordt afgeknipt en de rest wordt onomkeerbaar ge- encrypt, waardoor het niet meer herleidbaar is naar een persoon.

Het apparaat krijgt elke dag een andere code. Hierdoor is het gecodeerde adres niet te volgen na 24 uur. De sleutel is maar maximaal 24 uur hetzelfde, waardoor het risico wordt ondervangen dat men door combinatie met andere gegevens kan ontwaren en herleiden naar een persoon.

De CPA vroeg zich tijdens de vergadering af of het technisch mogelijk is om het aantal sensoren op te sporen. CMSA meent dat dit mogelijk is. Er wordt immers met de politie gesproken over het opzoeken van alle wifisensoren in de stad. Men denkt ook aan manieren om de wifisensoren aan het publiek kenbaar te maken.

*Advies*
De CPA concludeert dat de aangeleverde documenten en de presentatie hebben geleid tot een verheldering van een aantal vragen van de CPA.

Uit het advies van professor 5.1, 2, e komt naar voren dat er verschillen van inzicht bestaan omtrent de juistheid van diens opvatting. Meningen zijn verdeeld over de vraag of er toch moet worden uitgegaan van het feit dat een MAC- adres een persoonsgegeven is. Ondanks de kanttekeningen geeft het advies van professor 5.1, 2, e ook een aantal goede nuanceringen.

De CPA dankt de CMSA en de TU Delft voor de heldere presentatie. Na afloop van de vergadering krijgt de CPA een rondleiding door de Kalverstraat om de plaatsing van de infraroodcamera's en wifisensoren waar te nemen.

Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

Hoogachtend,
5.1, 2, e
5.1, 2, e

De heer mr. dr. U van de Pol
Voorzitter Commissie Persoonsgegevens Amsterdam

**Commissie Persoonsgegevens Amsterdam**
**Uittreksel van het concept-verslag van de openbare vergadering op donderdag 25 januari 2018**

## 7. Wifitracking

Het project Crowd Monitoring System Amsterdam (hMSA) is bedoeld om kwantitatief inzicht te krijgen in voetgangersbewegingen in drukke voetgangersbewegingen, historisch en realtime. Daarbij wordt gewerkt met wifisensoren en infrarood tel/lcamerasensoren die informatie geven over het aantal waargenomen personen per tijdseenheid. De beelden worden niet bewaard. De wifisensoren volgen het MAC-adres van mobiele telefoons en dat zou een privacy probleem kunnen opleveren. Op enkele plaatsen staan ook verificatiecamera's om de testresultaten te controleren. Na validatie worden die beelden verwijderd. Door de resultaten van de sensoren en de camera's met elkaar te vergelijken kan men een correctiefactor berekenen voor het aantal opgevangen wifisignalen, omdat immers niet elke voetganger een actief mobiel wifiapparaat bij zich heeft. De bedoeling is te komen tot een meetlat waarmee men kan vaststellen dat het ergens te druk wordt en dat maatregelen moeten worden genomen om de voetgangersstromen in andere banen te leiden. Op termijn wil men ook toe naar uitwisseling met ProRail en bijvoorbeeld Schiphol (waar tweeduizend sensoren actief zijn) om te kunnen anticiperen op drukke momenten. Daarover staan gesprekken op stapel.

De CPA vraagt of men nog meer dan alleen het MAC-adres kan uitlezen en of de resultaten niet vervuild worden door andere wifizenders in de omgeving, bijvoorbeeld van printers en telefoons in huizen en winkels.

Het antwoord is dat deze sensoren uitsluitend MAC-adressen kunnen opvangen. Alleen bewegende MAC-adressen worden meegeteld, stilstaande worden er meteen uitgefilterd om die genoemde vervuiling te voorkomen. Het MAC-adres wordt onmiddellijk in de sensor geanonimiseerd. Er wordt een deel van afgeknipt en de rest wordt onomkeerbaar ge-encrypt zodat het niet meer herleidbaar is naar een telefoon of persoon.

De CPA merkt op dat men het aldus gecodeerde adres wel kan blijven volgen gedurende enkele dagen en dat vervolgens met andere middelen wel de identiteit van de persoon met het betreffende apparaat kan worden vastgesteld. Dan is er dus wel degelijk sprake van een persoonsgegeven.

Het antwoord is dat dit zou kunnen kloppen, ware het niet dat men net als op Schiphol elke 24 uur de versleuteling wijzigt. Het apparaat krijgt dus de volgende dag een andere code. De sleutel is nog maar maximaal 24 uur hetzelfde en daardoor wordt het risico ondervangen dat men door combinatie met andere gegevens van bijvoorbeeld camera's patronen van hetzelfde apparaat kan ontwaren en herleiden naar een persoon. Dat wordt gezien als een belangrijke verbetering van de privacy waarborgen. Dat is tevens het antwoord op een openstaande vraag van de CPA uit de vorige bespreking. Ook kan men nu melden dat er inderdaad direct geanonimiseerd wordt en dat de opslag van gegevens grotendeels plaatsvindt bij de gemeente met incidenteel een zijsprong naar een partner in Denemarken. De VS wordt nadrukkelijk uitgesloten van opslag vanwege de daar geldende voorwaarden.

De samenwerking met de TU Delft levert via hun onderzoek veel nieuwe inzichten op waar de stad zijn voordeel mee kan doen.

De CPA vraagt of al deze gegevens ook worden ingezet voor commerciële doeleinden. Men kan zich voorstellen dat winkeliers belangstelling hebben om hun aanbod op deze gegevens af te stemmen. De ervaring leert dat gegevens gaandeweg op verschillende manieren gebruikt worden.

V&OR hanteert als doelstelling dat men wil werken aan een prettige, bereikbare en veilige stad. Daarvoor worden deze gegevens verzameld en niet met de opzet winkeliers aan een hogere omzet te helpen. Als een winkelier wil meehelpen aan die doelstelling kan men die vraag afwegen omdat alles nu nog in een afgesloten eigen systeem is opgeslagen. Daardoor kan men nu nog eerst goed gaan nadenken over deze vraag. Op een gegeven moment zullen geaggregeerde gegevens echter wel naar buiten komen.

De CPA vraagt of niet meer gegevens verzameld worden dan strikt noodzakelijk is voor dit doel en hoeveel systemen op dit moment in Amsterdam in gebruik zijn.

Volgens V&OR heeft de gemeente er op dit moment circa vijftig in gebruik en heeft de NS er op stations ook een vergelijkbaar aantal hangen. Schiphol heeft een substantieel omvangrijker systeem, om o.a. reizigersprocessen inzichtelijk te krijgen en te optimaliseren. Daarnaast hangen er in de stad waarschijnlijk nog wel meer sensoren, maar die zijn niet van de gemeente. Het zou een goede zaak zijn als men tot goede afspraken zou kunnen komen met ondernemers over het delen van dit soort informatie ten behoeve van de leefbaarheid in de stad.

De CPA is benieuwd of het technisch mogelijk is sensoren op te sporen.

Dat schijnt wel mogelijk te zijn en er wordt met de politie ook gesproken over het in kaart brengen van alle wifisensoren in de stad. Ook wordt er gedacht over het zichtbaar maken voor het publiek van het dashboard zodat men kan zien dat het op bepaalde plekken wel erg druk wordt. Daar spelen ook afwegingen een rol rond de vraag welke gegevens men wel en niet openbaar moet maken met het oog op de veiligheid. Meer inzicht in wat de gemeente doet met wifitracking zou ook goed zijn voor de burger.

De voorzitter concludeert dat de aangeleverde documenten en deze presentatie een antwoord geven op een aantal punten. Het meegestuurde advies van professor 5.1, 2, e geeft naar zijn mening ook een aantal goede nuanceringen.

Binnen de CPA blijken verschillen van inzicht te bestaan over de juistheid van diens opvatting dat singling-out geen opgeld meer zou doen. Ook stelt men vraagtekens bij het advies om voor alle zekerheid er toch maar van uit te gaan dat het MAC-adres een persoonsgegeven is omdat veel gebruikers dat wel zo ervaren. Een ander vindt het juist goed dat het advies aanstipt dat een MAC-adres niet automatische een persoonsgegeven is. Een derde vindt dat het advies voorbijgaat aan de context waarin de detectie plaatsvindt en dat een redelijk toegerust persoon via die context bepaalde persoonsgegevens zou kunnen achterhalen.

De voorzitter vraagt of het dan wenselijk is de professor uit te nodigen voor een nadere discussie. Hij constateert dat dit niet het geval is en dat de commissie zich kan vinden in de lijn om los van alle juridische discussies aan te sluiten bij de wijze waarop het publiek en de toezichthouder dit ervaren tot er letterlijk ergens een uitspraak komt dat het niet zo is. Onder deze kanttekening neemt de CPA het conceptadvies voor kennisgeving aan.